# Air-Gap Covert Channels

by

Brent Carrara

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
In partial fulfillment of the requirements
For the Doctorate in Philosophy degree in
Electrical and Computer Engineering

School of Electrical Engineering and Computer Science
Faculty of Engineering
University of Ottawa

**Abstract**

A fresh perspective on covert channels is presented in this work. A new class, *air-gap covert channels*, is defined as *an unintentional communication channel established between systems that are physically and electronically isolated from one another.* A specific class of *air-gap covert channel* is studied in depth, *out-of-band covert channels* (OOB-CCs), which are defined *as policy-breaking communication channels established between isolated, physically unmodified systems.* It is shown that OOB-CCs can be categorized by the physical channel that they communicate over: acoustic, light, seismic, magnetic, thermal, and radio-frequency, and the hardware that is required at the transmitter and receiver to make covert communication possible. In general, OOB-CCs are not as high-bandwidth as conventional radio-frequency channels; however, they are capable of leaking sensitive information that requires low data rates to communicate (e.g., text, recorded audio, cryptographic key material). The ability for malware to communicate information using a specific type of OOB-CC, the covert-acoustic channel, is also analyzed. It is empirically demonstrated that using physically unmodified, commodity systems (e.g., laptops, desktops, and mobile devices), covert-acoustic channels can be used to communicate at data rates of hundreds of bits per second, without being detected by humans in the environment, and data rates of thousands of bits per second when nobody is around to hear the communication. Defence mechanisms to counter covert-acoustic channels are also proposed and evaluated, and, as a result, best practices for the designers of secure systems and secure facilities are presented. Additionally, the *covertness* of OOB-CCs, i.e., the amount of data that can be leaked before the channel is detected, is also determined for classical communication channels as well as for covert-acoustic channels.

**Acknowledgements**

I would like to extend my deepest thanks to my supervisor, Dr. Carlisle Adams, for his support and guidance over the last four years. He always made himself available to answer my questions and guided me successfully to a number of publications. Based on our discussions and team meetings, I was able to get essential feedback on rough ideas that I had for the direction of this work. Under Dr. Adams' guidance, I have now successfully completed two graduate degrees — I will forever be indebted to you.

This work would not have been possible without the gracious support of my employer. In particular, the early support of George, François, and Cathy. George made every attempt to provide me with an opportunity to focus on my research. He also proved an invaluable sounding board to present ideas to and debate the possible direction of my work. I would not have been able to finish this degree without George's support. Thank you.

Most importantly, I would like to thank my wife, Julie, for her support. My journey in pursuit of this degree has been challenging, and I have been accompanied by an extremely supportive and caring life partner. While working on this degree we welcomed two sons, Henry and Ryan, into this world. Our boys were a continuous source of motivation for me — we are so proud of you and cannot wait to see what you become!

*Dedicated to my sons,*

Henry Thomas and Ryan Edward,

*and my wife,*

Julie Elizabeth.

# Table of Contents

**List of Tables** **ix**

**List of Figures** **xi**

**Nomenclature** **xv**

**1 Introduction** **1**

1.1 Model and Thesis Statement . . . . . 3

1.2 Outline of this Dissertation . . . . . 5

1.3 Previous Publications . . . . . 7

**2 A Brief Review of Information Theory and Digital Communications** **9**

2.1 Mathematical Notation . . . . . 9

2.2 Probability Theory . . . . . 10

2.3 Random Variables . . . . . 10

2.3.1 Relevant Random Variables . . . . . 13

2.4 Information Theory . . . . . 15

2.4.1 Communication Theory . . . . . 17

2.5 Digital Modulation . . . . . 19

2.5.1 Energy- and Power-Type Signals . . . . . 20

2.5.2 Fourier Transform . . . . . 20

2.5.3 Multi-carrier Modulation . . . . . 21

2.5.4 Reception of Signals . . . . . 22

2.5.5 Spread-Spectrum Communication . . . . . 23

**3 State of the Art in Covert Channels** **27**
3.1 Access Control . . . 27
3.2 Covert Channels . . . 29
3.2.1 What is a Covert Channel? . . . 29
3.2.2 Applications for Covert Channels . . . 31
3.2.3 History and Classification of Covert Channels . . . 32
3.3 Covert Channel Analysis and Design . . . 34
3.3.1 Covert Channel Analysis . . . 35
3.3.2 Covert Channel Design . . . 36
3.3.3 Undetectable Covert Channels . . . 37
3.4 Covert Channel Taxonomy . . . 41
3.4.1 Background on Covert Channel Taxonomies . . . 41
3.4.2 Proposed Covert Channel Taxonomy . . . 42
3.5 Measuring Covert Channels . . . 46
3.5.1 When do Covert Channels Pose a Risk? . . . 47
3.5.2 Steganographic Capacity . . . 49

**4 Problem Statement** **52**
4.1 Terminology and Model . . . 53
4.2 Scope . . . 55

**5 Out-of-Band Covert Channels** **58**
5.1 Survey of Out-of-Band Covert Channels . . . 59
5.1.1 Out-of-Band Covert-Acoustic Channels . . . 59
5.1.2 Out-of-Band Covert-Light Channels . . . 63
5.1.3 Out-of-Band Covert-Seismic Channels . . . 65
5.1.4 Out-of-Band Covert-Magnetic Channels . . . 68
5.1.5 Out-of-band Covert-Thermal Channels . . . 69
5.1.6 Out-of-band Covert-RF Channels . . . 70
5.1.7 Survey Summary . . . 73
5.2 Out-of-Band Covert Channel Taxonomy . . . 78

**6 Measuring and Characterizing Out-of-Band Covert Channels 82**
6.1 Measuring the Steganographic Capacity of Memoryless Channels . . . . . 84
6.1.1 Information-Theoretic Capacity for Memoryless Channels . . . . . 84
6.1.2 Capacity for Memoryless Channels Corrupted by AWGN . . . . . 89
6.2 Measuring the Steganographic Capacity of Band-Limited Channels . . . . 93
6.2.1 Information-Theoretic Capacity for Band-Limited Channels . . . . 93
6.2.2 Estimating the KL Divergence . . . . . 94
6.3 Steganographic Capacity with a Random Transmitter . . . . . 100

**7 The Achievable Data Rate of Covert-Acoustic Channels 109**
7.1 Acoustic Channel . . . . . 110
7.1.1 Lab Environment and System Requirements . . . . . 111
7.1.2 Measured Channel Characteristics . . . . . 113
7.2 Modulation and Demodulation Schemes . . . . . 118
7.2.1 Analysis of the Data Rates for OFDM and FHSS . . . . . 120
7.2.2 Algorithms and Synchronization . . . . . 124
7.3 Lab Experiments and Results . . . . . 125
7.3.1 Effective Data Transfer Rate . . . . . 131
7.4 Covert-Acoustic Channel Attacks . . . . . 134
7.4.1 Real-World Experiments and Results . . . . . 135

**8 The Covertness of Covert-Acoustic Channels 141**
8.1 Detection of Undetectable Covert-Acoustic Channels . . . . . 142
8.1.1 Detection of Covert-Acoustic FSK and OFDM Signals . . . . . 143
8.2 Detection of Secure Undetectable Covert-Acoustic Channels . . . . . 146
8.3 Disruption of Secure Undetectable Covert-Acoustic Channels . . . . . 153
8.4 Defence Mechanisms . . . . . 156
8.4.1 Prevention . . . . . 156
8.4.2 Detection . . . . . 156
8.4.3 Disruption . . . . . 157

**9 Conclusion 158**
9.1 Contributions . . . . . 161
9.2 Future Work . . . . . 164

**APPENDICES** **166**

**A Maximum Percentage Error for Approximating $\chi^2_\eta$** **167**

**B Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$** **169**

**C Algorithm for Calculating Maximum Percentage Error** **178**

C.1 Algorithm to Calculate $\chi^2_\eta$ Error . . . . . 178

C.2 Algorithm to Calculate $\chi^2_{\eta,\lambda}$ Error . . . . . 179

**D Detailed Results for Chapter 7** **180**

**References** **216**

# List of Tables


3.1 Recommendations for Handling and Measuring Covert Channels by System Type . . . . . 51

5.1 Out-of-Band Covert Channel Summary (Table 1 of 3) . . . . . 74
5.2 Out-of-Band Covert Channel Summary (Table 2 of 3) . . . . . 75
5.3 Out-of-Band Covert Channel Summary (Table 3 of 3) . . . . . 76
5.4 Average Size of Popular Document Types . . . . . 77

7.1 The Systems Used in This Study . . . . . 111
7.2 Distance Between Audio1 and the Other Systems in the Lab Environment 113
7.3 Data Rates for FHSS and OFDM ($\frac{\text{bits}}{\text{second}}$) . . . . . 124
7.4 OFDM Results for All Transmitters and All Receivers . . . . . 132
7.5 Distance Between Audio8 and the Other Systems in Both Environments . 135
7.6 Configuration Parameters for the Experiments . . . . . 136
7.7 Average Time to Leak Popular Document Types . . . . . 138

8.1 Jamming Results with the Covert Analyst at Full Power . . . . . 155
8.2 Jamming Results with the Covert Analyst at Half Power . . . . . 155

A.1 Maximum Percentage Error for Approximating $\chi^2_\eta$ . . . . . 168

B.1 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 1 of 8) . . . . . 170
B.2 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 2 of 8) . . . . . 171
B.3 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 3 of 8) . . . . . 172
B.4 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 4 of 8) . . . . . 173
B.5 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 5 of 8) . . . . . 174
B.6 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 6 of 8) . . . . . 175
B.7 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 7 of 8) . . . . . 176

B.8 Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 8 of 8) . . . . . 177

D.1 OFDM Results for All Receivers, by Transmitter (Table 1) . . . . . 212
D.2 OFDM Results for All Receivers, by Transmitter (Table 2) . . . . . 213
D.3 OFDM Results for All Transmitters, by Receiver (Table 1) . . . . . 214
D.4 OFDM Results for All Transmitters, by Receiver (Table 2) . . . . . 215

# List of Figures


1.1 Basic Covert Channel Model . . . . . 4

2.1 Relationship Between Entropy and Mutual Information . . . . . 17
2.2 Communication System . . . . . 17
2.3 Gaussian Channel . . . . . 18
2.4 Bandwidth of Baseband and Passband Signals . . . . . 21
2.5 Power Spectral Density of a BPSK Modulated Carrier . . . . . 24
2.6 Power Spectral Density of a DSSS Modulated Signal . . . . . 25
2.7 Frequency Hoping Spread Spectrum . . . . . 25

3.1 Types of Air-Gap Covert Channels . . . . . 33
3.2 Classes of Covert Channels . . . . . 34
3.3 Communication Channels from the Perspective of a Reference Monitor . . 39
3.4 General Covert Channel Model . . . . . 46

4.1 Basic Covert Channel Model with Terminology . . . . . 53
4.2 The *Prisoners Problem* in the Context of an Air-Gapped System . . . . . 54

5.1 Out-of-Band Covert Channel Taxonomy (Part 1) . . . . . 79
5.2 Out-of-Band Covert Channel Taxonomy (Part 2) . . . . . 80

6.1 Basic Passive Adversary Covert Channel Model . . . . . 83
6.2 Number of Channel Uses, $n$, Before Wendy Detects Alice with Probability $> 1 - \epsilon$ . . . . . 86
6.3 The Steganographic Capacity for Memoryless Channels in AWGN . . . . . 92
6.4 Energy Detector Block Diagram . . . . . 94
6.5 Observation Interval Before Wendy Detects Alice's Band-Limited Communications with Probability $> 0.500$ . . . . . 99

6.6 Observation Interval, $T_{min}$ . . . . . 99
6.7 Steganographic Capacity for Band-Limited Systems . . . . . 100
6.8 Alice Pseudorandomly Transmitting . . . . . 101
6.9 Energy Detector Receiver Operating Characteristics . . . . . 102
6.10 Trade-off Between an Energy Detector's $\alpha$ and $p$ . . . . . 104
6.11 Number of Channel Uses, $n$, Before Wendy Detects Alice's Covert-Acoustic Communication Using an Energy Detector . . . . . 105
6.12 Trade-off Between the Per-Observation Time, $T$, and Wendy's SNR, $SNR_W$ 106
6.13 The Steganographic Capacity of Covert-Acoustic Channels . . . . . 107
6.14 Wendy's Sum of Errors Versus Her Distance from Alice . . . . . 108

7.1 The Lab Environment . . . . . 112
7.2 Visualizing Multipath in the Acoustic Channel . . . . . 115
7.3 Normalized Multipath Intensity Profile in the Audible Spectrum . . . . . 115
7.4 Normalized Multipath Intensity Profile in the Near-Ultrasonic Spectrum . 116
7.5 Frequency Response of Commodity Microphones and Speakers . . . . . 117
7.6 Spectrogram of a Received FHSS Signal . . . . . 119
7.7 Spectrogram of a Received OFDM Signal . . . . . 119
7.8 Synchronization Probability versus Number of Preamble Symbols . . . . . 126
7.9 Synchronization Probability and Bit Error Rate versus Transmitted Samples per Symbol . . . . . 127
7.10 Synchronization Probability and Bit Error Rate versus Guard Interval . . . 128
7.11 Synchronization Probability and Bit Error Rate versus Frequency . . . . . 129
7.12 Synchronization Probability and Bit Error Rate versus Offset Angle . . . . 130
7.13 Synchronization Probability and Bit Error Rate versus the Transmitter's Volume . . . . . 130
7.14 BER by OFDM Sub-Channel . . . . . 133
7.15 Distribution of Errors when using FSK . . . . . 134
7.16 Ultrasonic Data Rates in the Real-World Environments . . . . . 137
7.17 Ultrasonic BER in the Real-World Environments . . . . . 137
7.18 BER using Ultrasonic Signals over Increased Distances . . . . . 139

8.1 PDF of the Background Noise Energy Captured in the Lab Environment . 145
8.2 Energy Detector Distributions . . . . . 147

8.3 Energy Detector Distributions with Random Delays . . . . . 148
8.4 Energy Detector Distributions for FHSS . . . . . 151

D.1 Probability of Synchronization versus Number of Preamble Bytes for Each Device as Transmitter . . . . . 181
D.2 Probability of Synchronization versus Number of Preamble Bytes for Each Device as Receiver (Part 1) . . . . . 182
D.3 Probability of Synchronization versus Number of Preamble Bytes for Each Device as Receiver (Part 2) . . . . . 183
D.4 Bit Error Rate versus Transmitted Samples per Symbol for Each Device as Transmitter . . . . . 184
D.5 Probability of Synchronization versus Transmitted Samples per Symbol for Each Device as Transmitter . . . . . 185
D.6 Bit Error Rate versus Transmitted Samples per Symbol for Each Device as Receiver (Part 1) . . . . . 186
D.7 Bit Error Rate versus Transmitted Samples per Symbol for Each Device as Receiver (Part 2) . . . . . 187
D.8 Probability of Synchronization versus Transmitted Samples per Symbol for Each Device as Receiver (Part 1) . . . . . 188
D.9 Probability of Synchronization versus Transmitted Samples per Symbol for Each Device as Receiver (Part 2) . . . . . 189
D.10 Bit Error Rate versus Guard Interval for Each Device as Transmitter . . . 190
D.11 Probability of Synchronization versus Guard Interval for Each Device as Transmitter . . . . . 191
D.12 Bit Error Rate versus Guard Interval for Each Device as Receiver (Part 1) 192
D.13 Bit Error Rate versus Guard Interval for Each Device as Receiver (Part 2) 193
D.14 Probability of Synchronization versus Guard Interval for Each Device as Receiver (Part 1) . . . . . 194
D.15 Probability of Synchronization versus Guard Interval for Each Device as Receiver (Part 2) . . . . . 195
D.16 Bit Error Rate versus Volume for Each Device as Transmitter . . . . . 196
D.17 Probability of Synchronization versus Volume for Each Device as Transmitter 197
D.18 Bit Error Rate versus Volume for Each Device as Receiver (Part 1) . . . . 198
D.19 Bit Error Rate versus Volume for Each Device as Receiver (Part 2) . . . . 199
D.20 Probability of Synchronization versus Volume for Each Device as Receiver (Part 1) . . . . . 200

D.21 Probability of Synchronization versus Volume for Each Device as Receiver (Part 2) . . . 201
D.22 Bit Error Rate versus Carrier Frequencies for Each Device as Transmitter . 202
D.23 Probability of Synchronization versus Carrier Frequencies Each Device as Transmitter . . . 203
D.24 Bit Error Rate versus Carrier Frequencies for Each Device as Receiver (Part 1) . . . 204
D.25 Bit Error Rate versus Carrier Frequencies for Each Device as Receiver (Part 2) . . . 205
D.26 Probability of Synchronization versus Carrier Frequencies for Each Device as Receiver (Part 1) . . . 206
D.27 Probability of Synchronization versus Carrier Frequencies for Each Device as Receiver (Part 2) . . . 207
D.28 Bit Error Rate versus Receiver Offset Angle for Each Device as Transmitter 208
D.29 Probability of Synchronization versus Receiver Offset Angle for Each Device as Transmitter . . . 209
D.30 Bit Error Rate versus Receiver Offset Angle for Each Device as Receiver . 210
D.31 Probability of Synchronization versus Receiver Offset Angle for Each Device as Receiver . . . 211

# Nomenclature

## Abbreviations

| | |
|---|---|
| ALS | Ambient light sensor |
| AM | Amplitude modulation |
| API | Application program interface |
| APT | Advanced persistent threat |
| ARQ | Automatic repeat request |
| AWGN | Additive white Gaussian noise |
| BER | Bit error rate |
| BSC | Binary symmetric channel |
| CC | Common Criteria |
| CRT | Cathode ray tube |
| CTCPEC | Canadian Trusted Computer Product Evaluation Criteria |
| DAC | Discretionary access control |
| dB | Decibel |
| DoD | Department of Defence |
| DPA | Differential power analysis |
| DTMF | Dual-tone multi-frequency |
| FEC | Forward error correcting |
| HVAC | Heating, ventilation, and cooling |
| ICI | Inter-channel interference |
| ICS | Industrial control systems |
| IOI | Item of interest |
| IR | Infrared |
| ISI | Inter-symbol interference |
| ITSEC | Information Technology Security Evaluation Criteria |
| LCD | Liquid crystal display |
| LED | Light emitting diode |
| LPD | Low probability of detection |
| MAC | Mandatory access control |
| malware | Malicious software |
| MLS | Multilevel security |

| | |
|---|---|
| NFC | Near-field communication |
| NSA | National Security Agency |
| OFDM | Orthogonal frequency-division multiplexing |
| OOB-CC | Out-of-band covert channel |
| OOK | On-off keying |
| OSI | Open Systems Information |
| RF | Radio frequency |
| RFID | Radio-frequency identification |
| SAS | Short authenticated strings |
| SCADA | Supervisory control and data acquisition |
| SNR | Signal-to-noise ratio |
| SPA | Simple power analysis |
| SSL | Secure sockets layer |
| TCSEC | Trusted Computer System Evaluation Criteria |
| TEMPEST | Transient ElectroMagnetic Pulse Emanation STandard |
| URL | Uniform resource locator |

# Chapter 1

# Introduction

In February, 2015, the security community learned of a sophisticated, unprecedented malicious software (malware) tool named Fanny operating in the wild [109]. Fanny was exceptional because it had the ability to gather information from computer systems on networks that were not connected to the Internet. In order to accomplish this feat, the malicious software used a novel communication channel to execute custom commands (ingress path) as well as collect their output (egress path). This communication link was established by reading from and writing to hidden storage volumes created within the raw file allocation table (FAT) structure of removable media that Fanny had infected. Fanny's communication channel not only provided its operators with the ability to gather information from Internet-disconnected systems, but it also allowed its operators to perform reconnaissance on networks, services, and devices that were never intended to be connected to the Internet.

Fanny was also notable because it used multiple exploits[1] to automatically propagate to vulnerable systems, which it shared with the Stuxnet malware [108, 109]. Stuxnet was an advanced persistent threat (APT), also discovered in the wild, that was presumed to be designed to force industrial control systems (ICS) to operate outside of their designed parameters in order to destroy them [61]. Stuxnet and Fanny employed a similar infection vector to gain access to isolated systems as well, as did Gauss, another APT in the Stuxnet family [26, 107]. In a similar fashion to Fanny, the Gauss malware infected removable media such that when they were plugged into vulnerable machines the malware would automatically execute and steal information from the systems. Gauss used the infected removable media as a communication channel to egress stolen data as well.

Fanny, Stuxnet, and Gauss all provide real-world examples of malware designed to defeat the security of Internet-disconnected, isolated systems or *air-gapped systems*. Formally, an *air-gapped system* is a computer or network that is physically and electronically separated from computers and networks that are connected to the Internet [194]. The term *air-gap* relates to the literal physical gap between the separated systems and its name predates wireless technology. Air-gapped systems are used in environments where

[1] An exploit is software code designed to leverage a vulnerability or vulnerabilities in other software applications in order to automatically execute a program on a system or gain higher privileged access to a system [226].

security is of paramount concern, including government (e.g., intelligence [151, 194] and military [140, 194]) as well as non-government organizations (e.g., SCADA [28], ICS [28] and financial systems [140]). There is also anecdotal evidence that air-gapped systems have been used in nuclear power facilities [199] as well as in the aviation industry [252]. Moreover, their security is based on the *security by isolation* principle, which calls for networks with different security requirements to operate completely isolated from one another, each within their own *security domain* [69]. This level of protection is designed to safeguard air-gapped systems from unauthorized access by malicious parties [194] and the technique is sometimes referred to as *compartmentalization* [151].

Despite the rigorous level of protection that air-gapped systems provide, there are still a number of ways that malware could be installed on these systems, including:

1. **Insider threat:** A malicious insider with physical access to the air-gapped system could install malware onto it using removable media (e.g. USB, DVD, CD) [181].

2. **Trojan horse:** Any of the software installed on the system could be a Trojan horse. A Trojan horse is a software application that offers a useful function, while simultaneously performing hidden malicious actions. A Trojan horse could be installed on the air-gapped system at either system installation time or when software is added to the system (e.g., during a new offline software installation or an offline software upgrade) [226].

3. **Malicious payload:** Any file copied to the air-gapped system could contain a virus or worm [220].

4. **Supply chain:** An attacker with physical access to the air-gapped system prior to the victim taking possession of it could install malware onto the machine [60].

Since air-gapped systems are completely isolated from one another, malware that is installed on an air-gapped system cannot rely on an underlying communication network to receive further tasking or transmit stolen information, and, therefore, the malware and its operators are required to establish a communication channel that does not rely on the existence of such a network. Moreover, given that malware is a software component, it is also required to establish a covert communication link without any physical modifications to the systems that it is installed on.

In this thesis, malware communication between systems separated by an air-gap is studied and two important questions are answered: *can covert communication channels, capable of bridging the air gap, be designed and built without physical access to the target systems?* And, relatedly, from a defence perspective, *can mechanisms, i.e., tools and best practices, be put in place to eliminate or reduce the threat that these covert communication channels pose?* These questions are directly related to the threat that malware poses to information systems whose security is of paramount concern and, as such, this work looks to appropriately quantify and assess the risk that malware capable of bridging the air-gap poses to these *secure systems*.

While studying the performance of communication channels that are capable of bridging the air-gap could be perceived as aiding malware developers, there are a number of other applications where improving their performance through engineering analysis is justified. Channels established using unmodified systems whose communication is difficult to detect could be used for communication between entities that are not willing to or allowed to use traditional network links. This is a common problem in applications supporting the expression of free speech in oppressive environments and during times of protest when traditional communication links are taken down, in whistle blower scenarios where sensitive information needs to be exfiltrated, and, in general, when the fact that communication is taking place needs to be kept hidden from detection by a third-party (e.g., governments, criminals, etc.). Communication channels that have these properties have been discussed as a possible solution to hide the use of strong encryption [250] and in 2015, governments in North America and Europe [8] as well as India [52] are considering proposals to weaken encryption standards or mandate back doors in cryptographic algorithms. Therefore, the protection of communications from prying eyes is appropriate motivation for studying the performance of covert channels.

## 1.1 Model and Thesis Statement

All security studies begin by defining their analyzed security model as well as the actors that play a role in the model [14]. In subsequent chapters of this thesis a more detailed security model is used; however, as motivation for this work, a basic security model is first introduced. To this end, Simmons' *prisoners' problem* [209], the model generally used to motivate studies in information hiding, is presented: two individuals, incarcerated in a prison, wish to communicate with one another in order to develop an escape plan. The warden of the prison permits his trustees, the guards, to pass messages between the prisoners in the hopes that he can deceive one of them into accepting a message modified or fraudulently created by the warden as genuine; however, since the warden suspects the prisoners will develop an escape plan, he will only allow messages to be passed between them if he can read the messages and they appear to be innocuous. The prisoners, on the other hand, are willing to communicate under these conditions so that they can in fact develop a plan. The problem for the prisoners is, therefore, to communicate in full view of the warden yet deceive him and communicate an escape plan in secrecy. Furthermore, the prisoners, fully expecting the warden to try and deceive them, will only accept messages if they are able to authenticate the origin of the messages.

The model that is studied in this work is an extension of this problem: the warden has become increasingly suspicious of the prisoners and has placed them both in solitary confinement. The two prisoners still wish to formulate an escape plan; however, neither the warden nor any agent of the prison will pass messages between them. As a result, the prisoners must find a new method of communication. Furthermore, they must sufficiently hide their communication so as to not arouse the suspicion of the guards, since the warden has also decided that if any evidence of communication is found one of the prisoners will be transferred to a different facility. This problem has been termed the *solitary confinement*

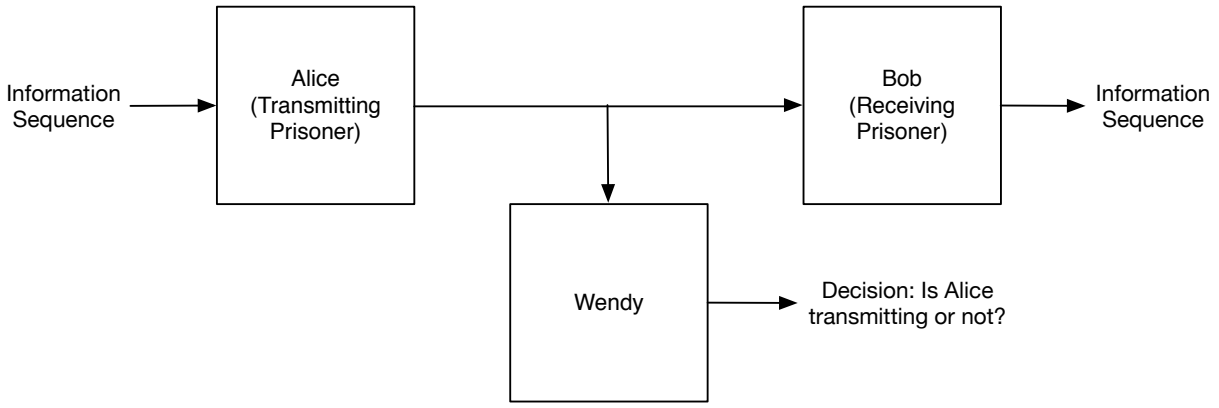



Figure 1.1: The basic covert channel model studied in this thesis. The transmitting prisoner, *Alice*, modulates an information sequence onto a shared communication channel, which the receiving prisoner, *Bob*, demodulates to obtain the information that Alice transmitted. The warden, Wendy, also has access to the communication channel, listens, and makes a determination as to whether or not Alice and Bob are communicating.

*problem*, which can be viewed from two different perspectives: the perspective of the prisoners, who wish to communicate covertly in order to establish an escape plan, and the perspective of the guards, who wish to thwart the efforts of the prisoners and find concrete evidence proving that the prisoners are communicating. The problem, in detail, for the prisoners is therefore to:

1. find a channel to communicate over such that:

   (a) the transmitting prisoner, Alice, can modulate data symbols by effecting changes in the channel, and

   (b) the receiving prisoner, Bob, can observe changes in the channel and demodulate the changes into data symbols;

2. agree upon a modulation and demodulation scheme; and,

3. secure the channel so that the guards cannot detect that communication is taking place.

The solitary confinement problem, from the perspective of the guards and the warden, conversely, is to detect and eliminate or constrain communication between the prisoners. A diagram showing the basic security model can be seen in **Figure 1.1**.

In the context of this dissertation, the communicating prisoners, Alice and Bob, represent malware that is attempting to bridge the air-gap between isolated systems. Given the abstract *solitary confinement problem* and the basic security model shown in **Figure 1.1**, the remainder of this work looks to prove the following hypotheses:

1. covert channels can be established between systems separated by an air-gap without physically accessing the transmitting and receiving systems;
2. the established covert channels can be engineered to leak sensitive information (e.g., captured keystrokes, cryptographic key material, documents, etc.);
3. the established covert channels can be engineered to improve their level of *covertness*; and,
4. conversely, technical solutions and best practices can be developed to detect, eliminate, or reduce the capacity of these covert channels.

In order to prove these hypotheses, the ability for covert channels to leak sensitive information is measured by the rate at which information can be communicated over the channel and the *covertness* of covert channels is measured by the amount of information, in bits, that can be communicated over the channel before the warden's probability of detecting the channel reaches a given threshold. This dissertation shows that while covert channels capable of leaking sensitive information can be built without physical modification to the target systems, the guards can detect the constructed channels under certain circumstances, and there is a trade off for the prisoners between achieving a higher rate of communication and a more covert communication channel.

## 1.2 Outline of this Dissertation

This thesis is written for an audience that possesses a basic understanding of probability theory, information theory, and digital communications. In **Chapter 2**, a brief overview of these areas is presented.

In **Chapter 3**, the state of the art in covert channels is presented and their origin is traced back to the study of access control. Covert channels are categorized into single-host, network, and a novel class, *air-gap covert channels*. *Air-gap covert channels*, are *covert communication channels that are designed to allow illicit communication between isolated systems.* The history of the design and analysis of covert channels is also discussed and it is shown that covert channel designers can pull from the information hiding literature to increase the *covertness* of covert channels. Recommendations on how to secure covert channels are also provided. Additionally, covert channels are classified as those that require *invasive covert exploits* and those that require *semi-* or *non-invasive covert exploits*, i.e., those that require hardware modification and those that require software modification or no modification at all, to be realized.

The history of secure systems is also discussed in **Chapter 3** and the traits of *fixed-* and *continuous-source* systems are presented, i.e., a system whose security is compromised if its design allows a covert channel to communicate a small, fixed amount of information or communicate information at a sufficiently high, continuous rate, respectively. The analysis of these different classes of systems shows that the relevant security criterion for *continuous-source* systems is an acceptable communication rate, but that the most appropriate security

criterion for *fixed-source* systems is Moskowitz and Myong's *small message criterion* [171]. Consequently, the traditional method that has been used to measure covert channels, which is based on Shannon capacity [206], is examined and it is argued that a new measure, *steganographic capacity* [112], is more appropriate when assessing the risk posed by covert channels in *fixed-source* systems.

In **Chapter 4**, a specific class of *air-gap covert channel*, *out-of-band covert channels* (OOB-CCs), is formally introduced and the scope of this dissertation is discussed. An *out-of-band covert channel* is defined as *a covert channel that uses* semi- *and* non-invasive *covert exploits to enable communication between isolated systems.* The work in **Chapter 5** then demonstrates that given the wide support set of sensors that are now embedded in commodity hardware, there are a number of viable alternatives to creating OOB-CCs. Furthermore, the survey shows that while these covert channels are not as high-bandwidth as conventional radio-frequency channels, they are, in general, capable of transferring information that requires a low data transfer rate (e.g., text, keystrokes, cryptographic key material, etc.). Additionally, the analysis in **Chapter 5** shows that state of the art OOB-CC solutions rely on an oblivious passive adversary in order to remain covert and, as a result, an enhanced security model is introduced to properly assess the *covertness* of covert channels.

In **Chapter 6**, a measure, *steganographic capacity*, that is capable of evaluating the *covertness* of OOB-CCs is presented and is used to evaluate OOB-CCs in the context of the enhanced security model introduced in **Chapter 5**. *Steganographic capacity*, in the context of this study, is *the amount of data that can be transferred through an OOB-CC before a passive warden's probability of detecting the channel reaches a given threshold.* Traditional communication systems use capacity and bit error rate (BER) to measure a channel; while important parameters, they do not capture the *covertness* of the channel, however. By using *steganographic capacity* the *covertness* of OOB-CCs can be analyzed when a passive warden employs technical solutions to detect the channel.

In **Chapter 7**, the achievable data rate of a specific class of OOB-CC, covert-acoustic OOB-CCs, is studied. Covert-acoustic channels are OOB-CCs that use speakers and microphones to transmit and receive information over the acoustic channel. In **Chapter 7**, the audio channel is characterized and it is shown that orthogonal frequency-division multiplexing (OFDM) is a much more appropriate modulation scheme to use in order to achieve a higher data rate as compared to modulation schemes that have been used in previous studies [89, 90]. This increased performance also demonstrates that commodity audio hardware can, in general, be used to communicate data using ultrasonic audio signals while people are present in the environment as well as using audible audio signals when people are absent from the environment, in an attack termed the *overnight attack*.

In **Chapter 8**, the *covertness* of covert-acoustic OOB-CCs is studied and an optimal detection device, an energy detector, is employed by Wendy to detect Alice and Bob's communications. It is shown that the covert channels established in **Chapter 7** can be detected before Alice and Bob can communicate any information covertly provided that Wendy observes their communication at a sufficient signal-to-noise ratio (SNR). Countermeasures that Alice and Bob could employ to counter Wendy's detection efforts are also studied:

spread spectrum techniques, lowering the transmission power, and communicating symbols at randomly selected time intervals as opposed to transmitting symbols continuously are all examined and their effect on the *covertness* of the channel is measured. Additionally, the effect of Wendy employing active jamming techniques on the BER observed by Bob is also studied. To the best of the author's knowledge the analysis in this chapter represents the most comprehensive study of the detection and disruption of covert-acoustic channels to date. Lastly, best practices for secure system developers and the designers of secure facilities are also presented.

In **Chapter 9**, a summary of this dissertation is presented and the contributions that are derived from this work as well as the future direction of this research are covered.

## 1.3 Previous Publications

This thesis is an amalgamation of my previous publications on covert channels.

All of the work presented in **Chapter 3** was accepted by the Association for Computing Machinery (ACM) for publication in the proceedings for the Workshop on Information Hiding and Multimedia Security, 2016 and was written by me alone under the supervision of Dr. Carlisle Adams:

- B. Carrara and C. Adams. A Survey and Taxonomy Aimed at the Detection and Measurement of Covert Channels. *ACM Workshop on Information Hiding and Multimedia Security*. ACM, 2016 (to appear).

The work presented in **Chapter 5** was accepted by the ACM for publication in the Computing Surveys journal and was written entirely by me alone under the supervision of Dr. Carlisle Adams:

- B. Carrara and C. Adams. Out-of-Band Covert Channels - A Survey. *ACM Computing Surveys*. ACM, 2016 (to appear).

The work presented in **Chapter 6** combines two published works. All the material in **Chapter 6**, except for the closed-form approximation of the steganographic capacity of band-limited channels, was published by the ACM in the conference proceedings for the Workshop on Information Hiding and Multimedia Security, 2015. A variation of the section on the closed-form approximation of the steganographic capacity of continuous band-limited channels in **Chapter 6** was published in the proceedings of the IEEE Conference on Electrical and Computer Engineering, 2016. Both works were written by me alone under the supervision of Dr. Carlisle Adams:

- B. Carrara and C. Adams. On Characterizing and Measuring Out-of-Band Covert Channels. *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security*. ACM, 2015.

- B. Carrara and C. Adams. Estimating the Steganographic Capacity of Band-Limited Channels. *IEEE Conference on Electrical and Computer Engineering*. IEEE, 2016.

The work presented in **Chapter 7** was published by Springer in the conference proceedings for the Symposium on Foundations & Practice of Security, 2014. This work was entirely written by me alone under the supervision of Dr. Carlisle Adams:

- B. Carrara and C. Adams. On Acoustic Covert Channels Between Air-Gapped Systems. *Foundations and Practice of Security*. Springer, 2014.

Lastly, the work presented in **Chapter 7** and **Chapter 8** will be combined and submitted to a journal.

# Chapter 2

# A Brief Review of Information Theory and Digital Communications

In this section, a brief review of probability theory, information theory, and digital communications is presented. Unless otherwise stated, the material presented in this section is candidly taken from the following sources:

- T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley & Sons, 2012 [46].
- J. G. Proakis and M. Salehi. *Fundamentals of Communication Systems*. Pearson Education, 2007 [188].
- R. L. Peterson, R. E. Ziemer, and D. E. Borth. *Introduction to Spread-Spectrum Communications*. Prentice Hall, 1995 [184].

## 2.1 Mathematical Notation

In this dissertation, uppercase letters, $X$, are used to denote random variables and lowercase letters, $x$, $x \in X$, are used to denote a realization of a random variable. The notation $X \sim P_X$ indicates that $X$ is distributed according to the probability distribution $P_X$ and sequences of random variables are denoted with the notation $X^n = X_1, X_2, \ldots, X_n$. If each $X$ is independent and identically distributed (i.i.d.), the shorthand notation $P_{X^n} = P_X^n$ is used. Furthermore, the notation $\mathcal{N}(\mu, \sigma^2)$ is used as shorthand for the Normal distribution with mean $\mu$ and variance $\sigma^2$. The notation $P(X = x)$ is used to denote the probability of event $x \in X$ occurring.

$f(n) = \Theta(g(n))$ is Big-Theta notation, which can be read as there exists $c_1, c_2 \in \mathbb{R}$ and $k \in \mathbb{Z}^+$ such that $0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n)$ for all $n \geq k$, $n \in \mathbb{Z}^+$. Similarly, $f(n) = O(g(n))$ is Big-O notation, which can be read as there exists $c \in \mathbb{R}$ and $k \in \mathbb{Z}^+$ such that $|f(n)| \leq c|g(n)|$ for all $n \geq k$, $n \in \mathbb{Z}^+$ and $f(n) = o(g(n))$ is little-o notation,

which can be read as for all $c \in \mathbb{R}$ there exists a $k \in \mathbb{Z}^+$ such that $|f(n)| \leq c|g(n)|$ for all $n \geq k$, $n \in \mathbb{Z}^+$, i.e., $g(n)$ grows much faster than $f(n)$.

The notation $f(x_1, x_2, \ldots; a_1, a_2, \ldots)$ is also used to denote a function, $f$, that is parameterized by $a_1, a_2, \ldots$ and has input values $x_1, x_2, \ldots$. The notation $\mathbb{Z}^+$ denotes the set of positive integers. Lastly, the log function is taken to the base 2 unless otherwise indicated. In the event that the log function has a different base, i.e., $a$, the notation $\log_a$ will be used.

## 2.2 Probability Theory

Probability theory mathematically describes the outcome of random experiments by using a probabilistic model, which consist of a *sample space*, *events*, and a *probability measure*. A *sample space* is the collection of all possible outcome events of the random experiment, denoted by $\Omega$, and can be either *discrete*, if the number of elements in $\Omega$ is finite or countably infinite, or the sample space can be *non-discrete*. An *event*, $E$, is a collection of outcomes from the *sample space* and a *probability measure*, $P$, is a function that assigns values to all events in the *sample space*. Most importantly, a *probability measure* has the following properties:

1. $0 \leq P(E) \leq 1, \forall\ \mathrm{E} \subseteq \Omega$
2. $P(\Omega) = 1$
3. For disjoint events, $E_1$, $E_2$, ..., $P(\cup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} P(E_i)$

Furthermore, given two events, $E_1$, and $E_2$, with probabilities $P(E_1)$ and $P(E_2)$, respectively, if an observer knows that event $E_2$ has occurred, then the probability that event $E_1$ will occur is no longer necessarily simply $P(E_1)$, but instead could be dependant on $P(E_2)$. This mathematical relationship is referred to as *conditional probability* and is defined as:

$$P(E_1|E_2) = \begin{cases} \frac{P(E_1 \cap E_2)}{P(E_2)}, & P(E_2) \neq 0 \\ 0, & \text{otherwise} \end{cases},$$

where $\cap$ denotes set *intersection*. In the event that $P(E_1|E_2) = P(E_1)$, then knowledge of $E_2$ occurring does not affect the probability of $E_1$ occurring, and the two events are said to be *independent*. In that case $P(E_1 \cap E_2) = P(E_1)P(E_2)$.

## 2.3 Random Variables

A random variable simply maps all events from the sample space, $\Omega$, to the set of real numbers, $\mathbb{R}$. Importantly, a random variable is said to be *discrete* if its range of values is

finite or countably infinite, and *continuous* if its range of values is a continuum. The two important functions that describe a random variable are its *cumulative distribution function* (CDF) and *probability mass function* (PMF) or *probability density function* (PDF), for *discrete* and *continuous* random variables, respectively.

The CDF of a random variable, $X$, is defined as

$$\begin{aligned} F_X(x) &= P\{w \in \Omega : X(w) \leq x\} \\ &= P(X \leq x), \end{aligned}$$

and has the following properties:

1. $0 \leq F_X(x) \leq 1$,
2. $F_X(x)$ is non-decreasing,
3. $\lim_{x \to -\infty} F_X(x) = 0$ and $\lim_{x \to +\infty} F_X(x) = 1$,
4. $F_X(x)$ is right-continuous, i.e., $\lim_{\epsilon \to 0^+} F_X(x + \epsilon) = F_X(x)$,
5. $P(a < X \leq b) = F_X(b) - F_X(a)$,

where the notation $F_X(a^-)$ has been used to denote the *one-sided left limit*, i.e., $\lim_{x \to a^-} f(x)$. Moreover, the CDF of a continuous random variable is a continuous function and the CDF of a discrete random variable is a *step function*.

The PDF of a *continuous* random variable is defined as the derivative of its CDF and is denoted by $f_X(x) = \frac{d}{dx} F_X(x)$. The PDF of a random variable also has the following properties:

1. $f_X(x) \geq 0$,
2. $\int_{-\infty}^{\infty} f_X(x) dx = 1$,
3. $\int_a^b f_X(x) = P(a < X \leq b)$,
4. In general, $P(X \in A) = \int_A f_X(x) dx$,
5. $F_X(x) = \int_{-\infty}^{x} f_X(u) du$.

For *discrete* random variables, the PMF is defined as $p(x) = P(X = x)$, and it follows that $p(x) \geq 0$ as well as $\sum_{x \in X} p(x) = 1$.

Two important functions that describe the behaviour of a random variable are its mean, or expectation:

$$\begin{aligned}\mathcal{E}(X) &= \int_X x f_X(x) dx \\ &= \mu_X,\end{aligned}$$

and variance:

$$\begin{aligned}\sigma_X^2 &= \mathcal{E}\left[(X - \mathcal{E}(X))^2\right] \\ &= \mathcal{E}(X^2) - (\mathcal{E}(X))^2 \\ &= \text{VAR}(X),\end{aligned}$$

where, in general, the $n$th moment of a random variable is defined as

$$\mathcal{E}(X^n) = \int_X x^n f_X(x) dx.$$

Note that the *standard deviation*, $\sigma_X$, is, therefore, simply the positive square root of the variance, $\sigma_X^2$, and that the $n$th moment of a *discrete* random variable is $\mathcal{E}(X^n) = \sum_i x_i^n P(X = x_i)$. Important properties of the expectation of a random variable include:

- For any constant $c$,
  1. $\mathcal{E}(cX) = c\mathcal{E}(X)$,
  2. $\mathcal{E}(c) = c$,
  3. $\mathcal{E}(X + c) = \mathcal{E}(X) + c$,
- $\mathcal{E}(Y) = \mathcal{E}(g(X)) = \int_{-\infty}^{\infty} g(x) f_X(x) dx$, for any function $Y = g(X)$.

Important properties of the variance of a random variable include, for any constant $c$:

1. $\text{VAR}(cX) = c^2 \text{VAR}(X)$,
2. $\text{VAR}(c) = 0$,
3. $\text{VAR}(X + c) = \text{VAR}(X)$.

Lastly, if $X$ and $Y$ are two random variables defined on the same sample space, $\Omega$, then their *joint CDF* is defined as

$$\begin{aligned}F_{XY}(x, y) &= P\left\{w \in \Omega : X(w) \leq x, Y(w) \leq y\right\} \\ &= P(X \leq x, Y \leq y),\end{aligned}$$

and their *joint PDF* is, therefore,

$$f_{XY}(x, y) = \frac{\partial^2}{\partial_x \partial_y} F_{XY}(x, y).$$

### 2.3.1 Relevant Random Variables

Throughout this dissertation, the following *discrete* random variables are used: Bernoulli and geometric, as well as the following *continuous* random variables: Normal (or Gaussian), chi-squared, and non-central chi-squared.

#### Bernoulli Random Variables

Bernoulli random variables are discrete random variables that take on the values 1 or 0 with probability $p$ and $1-p$, respectively, and are generally used to model experiments that result in a success/fail outcome or, as is the case in this dissertation, experiments that result in the detection of communication or not. The PMF of a Bernoulli random variable is

$$P(X=k) = \begin{cases} p, & k=1 \\ 1-p, & k=0, \end{cases}$$

and the CDF is

$$F_X(k) = \begin{cases} 0, & k<0 \\ 1-p & 0 \leq k < 1 \\ 1 & k \geq 1. \end{cases}$$

#### Geometric Random Variables

A geometric random variable captures the number, $X$, of independent Bernoulli trials that are required before one success is observed. The support set for the random variable is the positive integers, $\mathbb{Z}^+$, and, again, the probability of success (i.e., a 1) is $p$ and the probability of a failure (i.e., a 0) is $1-p$. The PMF of the geometric random variable, which describes the probability that the first success occurs on the $k$th trial, is

$$P(X=k) = (1-p)^{k-1}p,$$

and the CDF is

$$F_X(k) = 1-(1-p)^k.$$

### Normal Random Variables

The Gaussian, or normal random variable, is a continuous random variable whose PDF and CDF are parameterized by the random variable's mean, $\mu \in \mathbb{R}$, and variance, $\sigma^2 > 0$. The PDF of a normal random variable is

$$f_X(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}},$$

and the shorthand $\mathcal{N}(\mu, \sigma^2)$ is used throughout this dissertation to denote a normal distribution with mean, $\mu$, and variance, $\sigma^2$. Moreover, the random variable $\mathcal{N}(0, 1)$ is referred to as the *standard normal*.

An important property that is used in the analysis of this dissertation is that for two constants, $a$, $b$, and two Gaussian random variables, $X \sim \mathcal{N}(0, \sigma_X^2)$, $Y \sim \mathcal{N}(0, \sigma_Y^2)$, the random variable $Z = aX + bY$ is also Gaussian and is distributed according to $\mathcal{N}(0, a^2\sigma_X^2 + b^2\sigma_Y^2)$.

### Chi-Squared Random Variables

A chi-squared random variable with $\eta \in \mathbb{Z}^+$ degrees of freedom is the sum of the squares of $\eta$ independent standard normal random variables, i.e.,

$$Y = \sum_{i=i}^{\eta} X_i^2,$$

where $X_i \sim \mathcal{N}(0, 1)$, and is denoted by $\mathcal{X}_\eta^2$ in this work. The PDF of a chi-squared random variable is

$$f_X(x; \eta) = \frac{1}{2^{\frac{\eta}{2}}\Gamma\left(\frac{\eta}{2}\right)} x^{\frac{\eta}{2}-1} e^{-\frac{x}{2}},$$

where $\Gamma\left(\frac{\eta}{2}\right)$ is the gamma function and is defined as

$$\Gamma(n) = (n-1)!. \tag{2.1}$$

### Non-Central Chi-Squared Random Variables

A non-central chi-squared random variable is the sum of squares of $\eta$ independent normal random variables with means $\mu_i$ and unit variances, i.e.,

$$Y = \sum_{i=1}^{\eta} X_i^2,$$

where $X_i \sim \mathcal{N}(\mu_i, 1)$. In this dissertation, a non-central chi-squared random variable is denoted by $\mathcal{X}^2_{\eta,\lambda}$, and the non-centrality parameter, $\lambda$, is defined as

$$\lambda = \sum_{i=1}^{k} \mu_i^2.$$

The PDF of a non-central chi-squared distribution is

$$f_x(x; \eta, \lambda) = \frac{1}{2} e^{-\frac{x+\lambda}{2}} \left(\frac{x}{\lambda}\right)^{\frac{\eta}{2}-\frac{1}{2}} I_{\frac{\eta}{2}-1}\left(\sqrt{\lambda x}\right),$$

where

$$I_\nu(y) = \left(\frac{y}{2}\right)^\nu \sum_{j=0}^{\infty} \frac{\left(\frac{y^2}{4}\right)^j}{j!\Gamma(\nu + j + 1)}$$

is the modified Bessel function of the first kind and $\Gamma(n)$ is defined in **Equation 2.1**.

## 2.4 Information Theory

*Entropy* is the measure of uncertainty in a random variable, i.e., a measure of the "surprise" of a random variable. If $X$ is a discrete random variable on the sample space $\Omega$ with PMF $p(x) = P(X = x)$, $\forall x \in \Omega$, then the entropy of $X$ is defined as

$$H(X) = -\sum_{x \in \Omega} p(x) \log p(x)$$

where the log is taken to base 2 and, therefore, *entropy* is measured in bits.

Some important properties of the *entropy* of a random variable are

1. $H(X) \geq 0$,
2. $H(X) = \mathcal{E}\left(\log\left(\frac{1}{p(X)}\right)\right)$, since $\mathcal{E}(g(X)) = \sum_{x \in \Omega} g(x)p(x)$.

Moreover, for two random variables, $X$, $Y$, defined on sample spaces $\Omega_1$ and $\Omega_2$, respectively,

1. $H(X, Y) = -\mathcal{E}(\log p(X, Y))$,
2. $H(Y|X) = -\mathcal{E}(\log p(Y|X))$,

where $p(X, Y)$ is the joint PMF of $X$ and $Y$. Lastly, the *Chain Rule* for *entropy* is

$$H(X, Y) = H(X) + H(Y|X),$$

which extends to collections of random variables, $X_1, X_2, \ldots, X_n$, that are distributed according to $p(x_1, x_2, \ldots, x_n)$ as follows

$$H(X_1, X_2, \ldots, X_n) = \sum_{i=1}^{n} H(X_i|X_{i-1}, \ldots, X_1).$$

It is also important to point out that in the case where all the random variables, $X_i$, are independent, $H(X_1, X_2, \ldots, X_n) = \sum H(X_i)$.

The *distance* between any two distributions is captured by the *relative entropy* or the *Kullback-Leibler divergence* (KL divergence) and is denoted by

$$\begin{aligned} D(p\|q) &= \sum_{x\in\Omega} p(x) \log\left(\frac{p(x)}{q(x)}\right) \\ &= \mathcal{E}\left(\log\left(\frac{p(x)}{q(x)}\right)\right), \end{aligned}$$

where $p$ and $q$ are two PMFs defined on the sample space $\Omega$ and the KL divergence is only defined if $q(x) = 0$ then $p(x) = 0$. Some important properties of *relative entropy* include

1. $D(p\|q) \geq 0$, with equality if and only if $p = q$,
2. $D(p\|q)$ is not necessarily equal to $D(q\|p)$.

The *mutual information*, $I(X;Y)$, between two random variables, $X$ and $Y$, defined on sample spaces $\Omega_1$ and $\Omega_2$, respectively, is the *relative entropy* of their joint distribution and their product distribution:

$$\begin{aligned} I(X;Y) &= \sum_{x\in\Omega_1}\sum_{y\in\Omega_2} p(x,y) \log\left(\frac{p(x,y)}{p(x)p(y)}\right) \\ &= D(p(x,y)\|p(x)p(y)) \\ &= \mathcal{E}\left(\log\left(\frac{p(X,Y)}{p(X)p(Y)}\right)\right). \end{aligned}$$

*Mutual information* can also be written in terms of *entropy* as

$$I(X;Y) = H(X) - H(X|Y),$$

and, therefore, can be interpreted as the reduction in the entropy of a random variable $X$ after observing $Y$. Other representations of *mutual information* in terms of *entropy* include

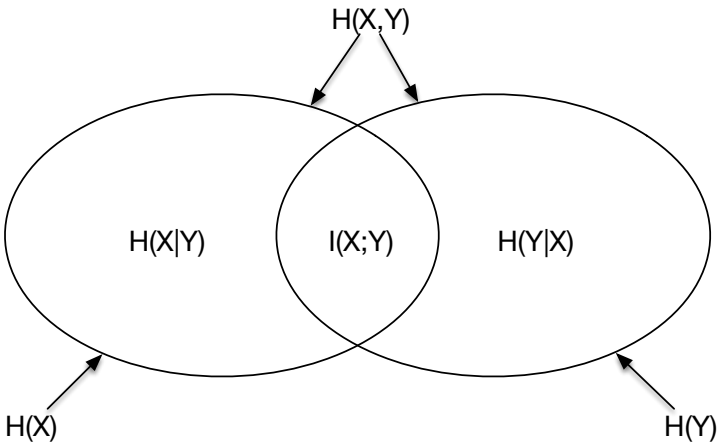



Figure 2.1: Relationship Between Entropy and Mutual Information (this diagram was recreated from [46])

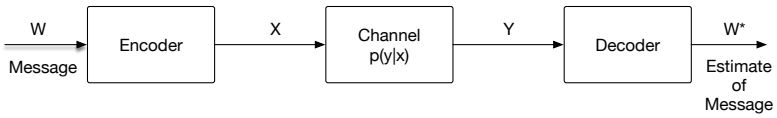



Figure 2.2: Communication System (this diagram was recreated from [46])

$$I(X;Y) = H(X) - H(Y|X)$$

$$I(X;Y) = H(Y) - H(X|Y)$$

$$I(X;Y) = H(X) + H(Y) - H(X,Y)$$

$$I(X;Y) = I(Y;X)$$

$$I(X;X) = H(X)$$

See **Figure 2.1** for a pictorial view of these equations.

### 2.4.1 Communication Theory

A *communication channel* is a system that consists of an input alphabet, $\mathcal{X}$, an output alphabet, $\mathcal{Y}$, and a probability measure, $p(y|x)$ (see **Figure 2.2**). The probability measure, $p(y|x)$, represents the probability that the channel output, $y$, will be produced given that $x$ was the input. A *channel* is said to be *memoryless* if the output of the channel is only dependant on the current input at the time $y$ was received.

The *channel capacity* of a channel is defined as

$$C = \sup_{p(x)} I(X;Y) \ \frac{\text{bits}}{\text{channel use}}, \tag{2.2}$$

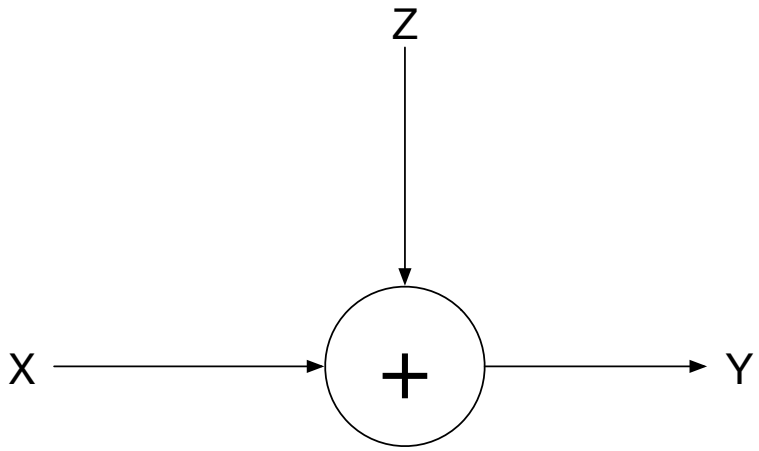



Figure 2.3: Gaussian Channel (this diagram was recreated from [46])

where the supremum is taken over the set of all possible input distributions, $p(x)$. **Equation 2.2** is the famous result first presented by Claude Shannon and is referred to in this dissertation as "Shannon capacity" [206].

An important channel that is used in this work is the *Gaussian channel* (see **Figure 2.3**). The output of the *Gaussian channel* is the sum of the input symbol, $X$, plus noise, $Z$, where the noise is modelled by a Gaussian random variable with variance $N$, hence $Z \sim \mathcal{N}(0, N)$, and $Z$ is assumed to be independent of $X$. Therefore,

$$Y = X + Z.$$

In this system model, $X$ is said to be corrupted by additive white Gaussian noise (AWGN).

If the noise variance is zero then it follows that $Y = X$ and, therefore, the capacity of the channel is $H(X)$. Conversely, if the noise variance, $N$, is non-zero, but there is no constraint on the input alphabet $X$, then an arbitrary infinite number of subsets of inputs can be chosen that are sufficiently far apart, such that they are distinguishable after they are corrupted by noise without error. A noisy channel with unconstrained input, therefore, has infinite capacity.

A common limitation that is placed on communication systems, and the one that is used in the analysis of this dissertation, is a limit on the power of the input alphabet, which is captured by the following equation:

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P$$
$$\mathcal{E}\left(X^2\right) \leq P.$$

The *channel capacity* of the Gaussian channel with *power constraint*, $P$, is then,

$$
\begin{aligned}
C &= \sup_{\{f_X(x):\mathcal{E}(X^2)\leq P\}} I(X;Y) \\
&= \sup_{\{f_X(x):\mathcal{E}(X^2)\leq P\}} \frac{1}{2}\log\left(1+\frac{P}{N}\right),
\end{aligned}
$$

where it is assumed the input alphabet, $X$, is corrupted by an additive white Gaussian noise signal distributed according to $\mathcal{N}(0, N)$.

## 2.5 Digital Modulation

Information can be transmitted digitally through modulating signal wave forms. The basic modulation techniques include: amplitude modulation, phase modulation, and frequency modulation. In the case of amplitude modulation a *baseband* signal waveform, $s_m(t)$, $m = 1, 2, \ldots, M$, is multiplied by a sinusoidal carrier, $\cos(2\pi f_c t)$, to create the *passband* signal

$$
u(t) = s_m(t)\cos(2\pi f_c t),
$$

where $f_c$ is the *carrier frequency* and $\{t : t \geq 0, t \in \mathbb{R}\}$ represents time (the power spectrum of a baseband signal and passband signal are shown in **Figure 2.4a** and **Figure 2.4b**, respectively). Phase-modulated signals modify the phase of the carrier function to transmit information and the basic construction of phase-modulated wave forms can be expressed as

$$
u(t) = \cos\left(2\pi f_c t + \frac{2\pi m}{M}\right),
$$

where $m = 0, 1, 2, \ldots, M-1$, $0 \leq t \leq T$, and $T$ is the duration of each modulated symbol. Lastly, frequency-modulated signals modify the frequency of the signal being transmitted and can be expressed as

$$
u(t) = \cos\left(2\pi f_c t + 2\pi m\Delta f t\right),
$$

where $m = 0, 1, 2, \ldots, M-1$, $\Delta f$ is the frequency separation between successive frequencies, i.e., $\Delta f = f_m - f_{m-1}$, where $f_m = f_c + m\Delta f$, and $0 \leq t \leq T$. These aforementioned signalling schemes are referred to as amplitude shift keying (ASK), phase shift keying (PSK) and frequency shift keying (FSK), respectively. Furthermore, in the case that $M = 2$ the signalling scheme is also referred to as a binary signalling scheme, whereas when $M > 2$, the signalling scheme is referred to as $M$-ary.

### 2.5.1 Energy- and Power-Type Signals

A signal $u(t)$ is an *energy-type* signal if and only if $\xi_u$ is finite, where

$$\begin{aligned}\xi_u &= \int_{-\infty}^{\infty} |u(t)|^2 dt \\ &= \lim_{T\to\infty} \int_{-\frac{T}{2}}^{\frac{T}{2}} |u(t)|^2 dt,\end{aligned}$$

and $\xi_u$ is termed the *energy* of the signal $u(t)$. Conversely, $u(t)$ is a *power-type* signal if

$$0 < P_u < \infty,$$

where

$$P_u = \lim_{T\to\infty} \frac{1}{T} \int_{-\frac{T}{2}}^{\frac{T}{2}} |u(t)|^2 dt,$$

and $P_u$ is termed the *power* of the signal $u(t)$.

For signals of the form $A\cos(2\pi ft + \theta)$ their *energy* is infinite and, therefore, periodic signals of this form are typically *power-type*. Moreover, the power content of a periodic signal can be expressed as

$$P_u = \frac{1}{T_0} \int_{-\frac{T_0}{2}}^{\frac{T_0}{2}} |u(t)|^2 dt,$$

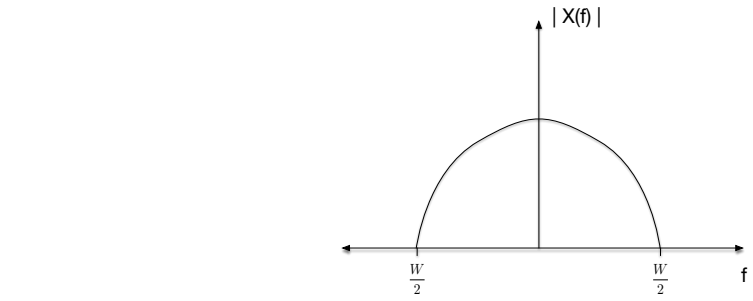
which states that the *power* content of a periodic signal is equal to the average power in one period, where $T_0$ is the duration of one period of $u(t)$.

### 2.5.2 Fourier Transform

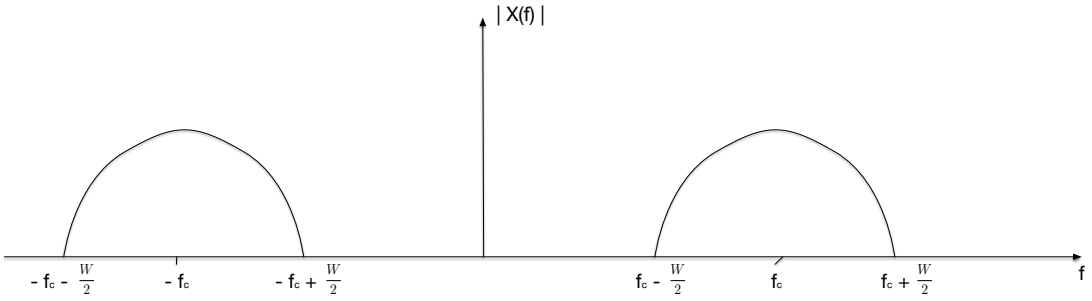
The *Fourier transform* of a signal, $x(t)$, decomposes the signal into its frequency components by transforming the signal $x(t)$ from a function in the time domain, i.e., dependant variable is $t$, to a function in the frequency domain, where the dependant variable is $f$. Formally, the *Fourier transform* of $x(t)$ is

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt.$$

and the original signal, $x(t)$, can be recovered from its *Fourier transform*, $X(f)$, by taking the *inverse Fourier transform*




(a)




(b)

Figure 2.4: Bandwidth of Baseband (a) and Passband (b) Signals

$$x(t) = \int_{-\infty}^{\infty} X(f) e^{j2\pi ft} df.$$

Given the definition of the *Fourier transform* the *bandwidth* of a signal, $x(t)$, can be expressed as $W$, where $W$ is the range of frequencies that contain the signal's spectral content. Or, in other words, frequencies outside of the range $W$ contain no spectral content. Formally, if $x(t)$ is a baseband signal, and $X(f)$ is the Fourier transform of $x(t)$, then the bandwidth of $x(t)$, $W$, is defined as $|X(f)| = 0, \forall |f| > |\frac{W}{2}|$. *Bandwidth* is shown pictorially in **Figure 2.4**.

### 2.5.3 Multi-carrier Modulation

A popular technique in digital modulation that is used to increase the data rate of the communication as well as combat the interfering effects of the communication channel is to transmit data through multiple channels simultaneously. Orthogonal frequency-division multiplexing (OFDM) is one such technique where the bandwidth being used for communication is split up into $K$ sub-channels and information is transmitted on each of the $K$ sub-channels. As an example, using ASK, the signal transmitted on the $k$th sub-channel, $0 \leq k \leq K-1$, would have the form

$$u_k(t) = s_{m_k}(t) \cos\left(2\pi f_k t\right),$$

where $m_k$ is the symbol being transmitted on the $k$th sub-channel. The complete transmitted signal on all $K$ sub-channels would, therefore, be

$$\begin{aligned} u(t) &= \sum_{k=1}^{K} u_k(t) \\ &= \sum_{k=1}^{K} s_{m_k}(t) \cos\left(2\pi f_k t\right). \end{aligned}$$

When employing multi-carrier modulation schemes, such as OFDM, proper care must be taken to ensure that the sub-channels are appropriately separated from one another to ensure that *inter-channel interference* (ICI) does not occur, i.e., one must prevent energy from one sub-channel leaking into adjacent sub-channel(s) and causing interference. In order to reduce ICI, sub-channel carriers must be separated by the bandwidth of the signals transmitted on each-sub-channel, $W$. OFDM is used heavily throughout this dissertation given the nature of the acoustic channel that is studied.

### 2.5.4 Reception of Signals

Once a signal, $u(t)$, is transmitted over a channel, it is subject to additive noise, $n(t)$, which was described in **Section 2.4.1**, as well as attenuation. The received waveform, $r(t)$ is, furthermore, a delayed version of the transmitted signal, which results in a phase offset at the receiver. Putting these three effects together, the received waveform, $r(t)$ has the form

$$\begin{aligned} r(t) &= \alpha u(t-\tau) + n(t) \\ &= \alpha A \cos\left(2\pi f_c\left(t-\tau\right)\right) + n(t) \\ &= \alpha A \cos\left(2\pi f_c t - 2\pi f_c \tau\right) + n(t) \\ &= \alpha A \cos\left(2\pi f_c t - \theta\right) + n(t), \end{aligned}$$

where $\tau$ is the time delay that results from the transmitted waveform travelling to the receiver, $\alpha$ is the attenuation factor, and $\theta$ is the phase offset of the received signal.

Practically speaking, the attenuation factor, $\alpha$, is a product of multiple factors, especially over the acoustic channel that is studied in this dissertation. The attenuation of acoustic signals through air, as an example, is dependant on the distance between the transmitter and receiver, the temperature of the air, the humidity of the air, and the frequency content of the signals being transmitted. As a general rule of thumb, however, the attenuation factor for acoustic signals can be approximated as being inversely proportional to the distance between the sender and receiver squared, i.e., $\alpha \propto \frac{1}{d^2}$, where $d$ is the distance between the transmitter and receiver.

Moreover, there are two general strategies that can be employed by the receiver when there is a phase-offset between the received signal and the transmitted signal, i.e., $\theta \neq 0$. *Phase-recovery* is the practice of estimating the phase, $\hat{\theta}$ such that $|\hat{\theta} - \theta| \to 0$. This mode of reception often requires the use of a *phase-locked loop*, which is an algorithm designed to iteratively reduce this distance. Demodulation techniques that rely on phase-recovery are referred to as *coherent* reception techniques. Conversely, *non-coherent* reception techniques do not attempt to recover the phase of the transmitted signal and, as a result, their design is often simpler than their *coherent* counterparts, but tend to be less accurate in terms of symbol recovery.

Lastly, combining this section and the previous section, if we assume that the transmitted signal $u(t)$ has an average power of $P$, is band-limited to a bandwidth $W$, and the additive noise is Gaussian with spectral density $\frac{N_0}{2}$ watts/Hz, then the capacity of the channel is

$$C = W \log \left(1 + \frac{\alpha^2 P}{N_0 W}\right),$$

where the capacity, $C$, is in bits per second, and the ratio $\frac{\alpha^2 P}{N_0}$ is referred to as the received signal-to-noise ratio (SNR) of the transmitted signal.

### 2.5.5 Spread-Spectrum Communication

Spread spectrum modulation is categorically implemented in three different ways: direct-sequence spread spectrum (DSSS), frequency hoping spread spectrum (FHSS), and hybrid (i.e., a combination of DSSS and FHSS).

In the case of DSSS, conceptually, a data-modulated signal is modulated a second time by a wideband spreading signal which spreads the original data-modulated signal's power out over a much larger bandwidth. The spreading signal is designed to facilitate demodulation by the true recipients, who have a copy of the spreading signal, while making demodulation difficult for eavesdroppers, who do not have a copy. The use of the spreading signal not only makes it difficult for unintended recipients to demodulate the data-modulated signal, but it also makes the signals resistant to jamming as well as difficult to detect in the presence of background noise. When DSSS communication is used, an eavesdropper, who is attempting to detect the communication, is forced to use wideband detection techniques in place of demodulation because the eavesdropper is unable to correlate the received signal with a copy of the spreading signal. A DSSS modulated signal takes the form

$$s(t) = c(t)u(t) \tag{2.3}$$

where $t \geq 0$, $t \in \mathbb{R}$, and $t$ represents time, $u(t)$ is the data-modulated signal, and $c(t)$ is the spreading signal. The spreading signal takes on values of $\pm 1$, which are generated pseudorandomly, and is often referred to as a *pseudo-noise* (PN) signal because it is a

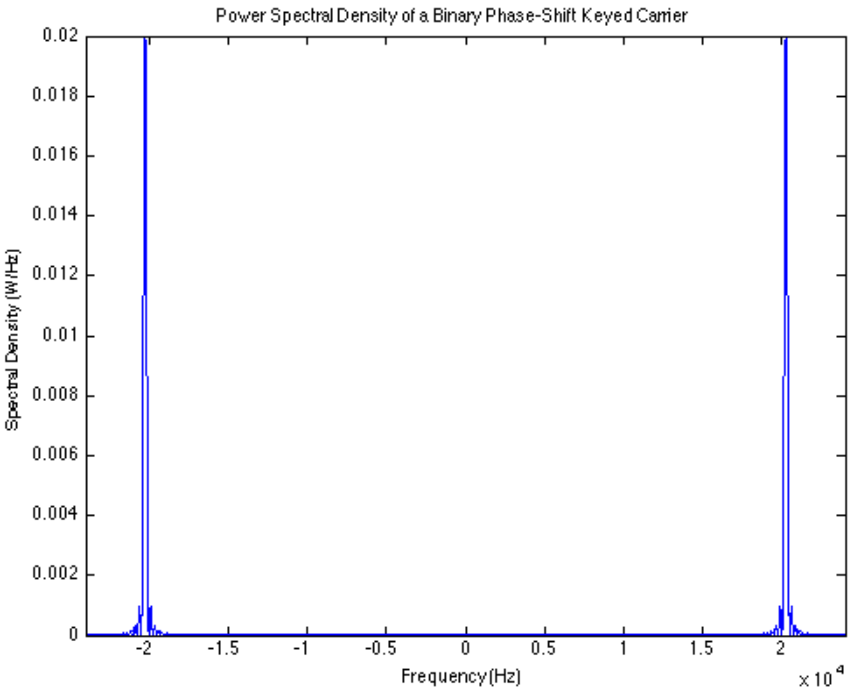



Figure 2.5: The power spectral density of a binary phase-shift keyed modulated carrier where the carrier frequency, $f_0 = 20.250$ kHz, the average power of the signal is 10 dB, and the symbol interval, $T$, is 4 ms.

synthesized noise-like random signal. In order to demodulate a received spread-spectrum signal,

$$r(t) = c(t-\tau)u(t-\tau) + n(t)$$

where $\tau$ is the transmission delay between sender and receiver, and $n(t)$ is the additive channel noise, the receiver correlates $r(t)$ with $c(t-\hat{\tau})$, where $\hat{\tau}$ is the receiver's estimate of $\tau$. If the receiver's estimate of $\tau$ is accurate then the receiver is left with

$$\begin{aligned} r(t) &= c(t-\tau)c(t-\hat{\tau})u(t-\tau) + c(t-\hat{\tau})n(t) \\ &= u(t-\tau) + c(t-\hat{\tau})n(t) \end{aligned}$$

because the spreading signal is designed such that $c(t)^2 = 1$. In **Figure 2.5** and **Figure 2.6**, the power spectral density (PSD) of a binary PSK modulated signal and a DSSS version of the same signal are shown, respectively, where the power spectral density of a signal is defined as

$$U(f) = \frac{1}{2}PT\{\text{sinc}^2[(f-f_c)T] + \text{sinc}^2[(f+f_c)T]\}, \tag{2.4}$$

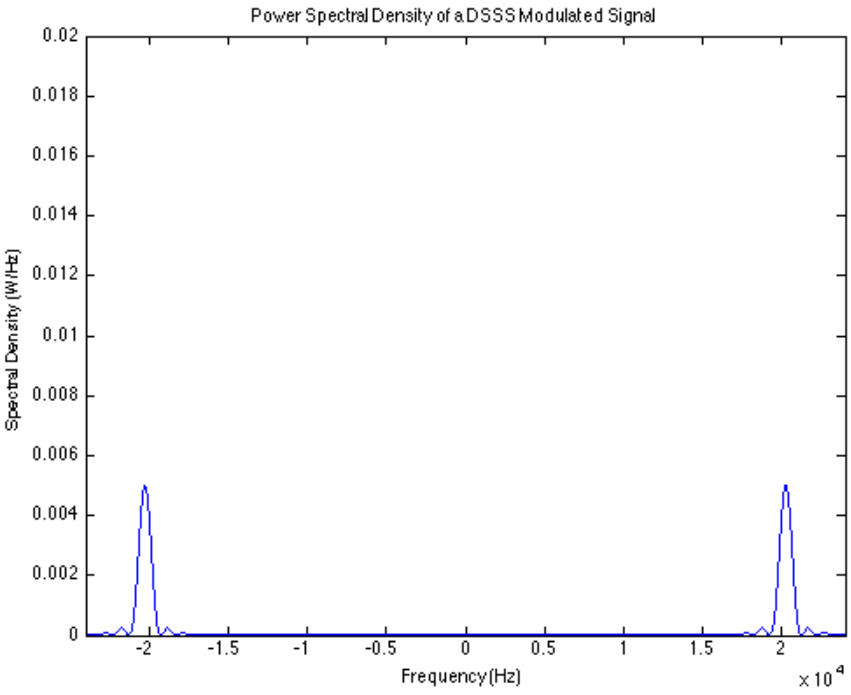



Figure 2.6: A direct-sequence spread spectrum version of the signal shown in **Figure 2.5**. With a chip rate of $T_c = 1$ ms.

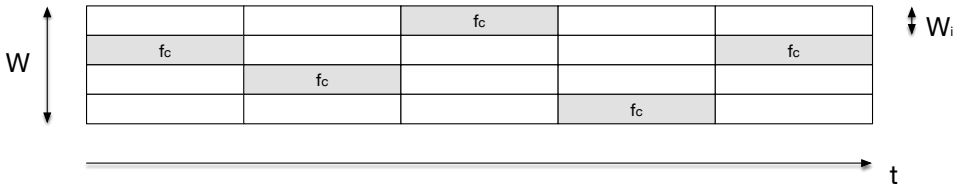



Figure 2.7: Frequency Hoping Spread Spectrum (this diagram was recreated from [184])

and it is assumed that the data-modulated signal, $u(t)$, is a binary phase-shift keyed signal, $P$ is the average power in $u(t)$, $f_c$ is the carrier frequency, and $T$ is the symbol interval. To generate **Figure 2.6**, $T$ is replaced with $T_C$, where $T_C$ is the spreading code symbol interval and is referred to as the code *chip*. It is clear from the figures that the DSSS version of the signal reduces the PSD by a factor of four while increasing the signal's bandwidth by the same factor. By increasing the signal's bandwidth, an eavesdropper is forced to detect the communications over a bandwidth potentially much larger than the original signal's bandwidth; thus, the eavesdropper's SNR is decreased because more noise is received while the data signals' power remains the same.

FHSS, on the other hand, modifies the carrier of the data-modulated signal periodically and divides the available bandwidth up into sub-channels of equal width. In the case of FHSS, the data-modulated signal is not modulated a second time, but instead the carrier of the signal is switched in time, i.e., the carrier frequency, $f_c$, becomes a function of $t$, $f_c(t)$.

The effect of using FHSS is shown in **Figure 2.7**. As a result of modulating using FHSS, an eavesdropper must try to detect communication by monitoring each of the sub-channels of bandwidth $W_i$ and combine the results in an optimal way, which could add complexity to the detector, or, alternatively, try to detect communication by monitoring the entire bandwidth, $W$, at all times, which will decrease the observed SNR from the eavesdropper's perspective.

In the next chapter, background information on covert channels is presented.

# Chapter 3

# State of the Art in Covert Channels

In this chapter, covert channels are contextualized and framed as a problem in access control (**Section 3.1**). In **Section 3.2** covert channels are defined, the various classes of covert channels are presented, and applications for covert channels are discussed. In **Section 3.3**, the analysis and design of covert channels is covered and recommendations for covert channel designers are presented. Additionally, in **Section 3.4** a taxonomy for covert channels is given and, lastly, in **Section 3.5** the classification of secure systems based on their security requirements is discussed.

## 3.1 Access Control

Access control is the "protection of system resources against unauthorized use" [208]. More specifically, access control is the process by which a request by a subject[1] to perform an operation[2] on an object[3] is governed. The study of access control is rooted in military applications and was first applied to multilevel security (MLS) systems [14]. In MLS systems, subjects and objects are given clearance and classification levels (e.g., confidential, secret, top secret), respectively. Access control decisions, i.e., whether to grant or deny an operation, are based on the subject's clearance, the object's classification and the access control policy of the system. Access control policies define the mode in which permissions are managed as well as the access rights for subjects.

There are two fundamental access control modes that are relevant to the study of covert channels: discretionary access control (DAC) and non-discretionary (i.e., mandatory) access control (MAC[4]). Systems implementing DAC allow the creator or owner of an object to set its access control permissions. DAC, therefore, allows subjects to discretionarily pass

[1] An active system entity that can initiate requests to perform an operation, e.g., process, domain [64].

[2] An activity performed by a subject, e.g., read, write, etc. [64]

[3] A system entity that operations can be performed on. A system object usually can store information, e.g., file, database, etc. [64].

[4] Note that the term *MAC* is used in other contexts to mean *message authentication code*, *media access control* (e.g., MAC address), and Macintosh computers sold by Apple. To be clear, none of these other meanings are are used in this dissertation

on permissions to other subjects in the system [130]. Conversely, in a system implementing MAC, all operations performed by subjects on objects are mediated by the system, i.e., the access control policy is set and enforced system-wide and subjects cannot set individual permissions on objects [130]. Harrison, Ruzzo, and Ullman showed that systems which allow subjects to grant permissions to other subjects cannot be guaranteed to remain in a safe state, i.e., in a state consistent with the system's security requirements, throughout their operation [92]. Given Harrison, Ruzzo, and Ullman's result, systems must implement MAC to ensure subjects do not create information flows which contravene the security of the system.

In 1972, Anderson introduced an abstract system component called the *reference monitor* to enforce access control decisions and defined three design principles it must adhere to [12]:

1. **Completeness:** the reference monitor must always be active and enforcing the system's access control policy.
2. **Isolation:** the reference monitor must be tamper-proof, i.e., unable to be modified such that the system's access control policy is not enforced.
3. **Verifiable:** the reference monitor must provably be shown to be implemented correctly.

Given these design principles there are two classes of attack against reference monitors that are relevant to this work. The first class covers attacks that circumvent the *isolation* principle and encompasses illegal information flows that are enabled by tampering with the system. The second class of attack covers illegal information flows that exploit objects that are either not protected by the reference monitor (e.g., passing information via the lock status of a file) or mechanisms that enable communication but are not overseen by the reference monitor (e.g., directly accessing the raw hard drive device to read or write files as opposed to using the operating system's file system application program interface (API)). This second class circumvents the *completeness* principle of the reference monitor.

Given this description, a reference monitor can be characterized as one of the following types:

- **Host-based reference monitor:** A reference monitor which mediates operating system (OS) resource access requests. A number of modern operating systems employ host-based reference monitors including Android, Secure Linux (SELinux), and Windows as well as hardware virtualization software.
- **Network reference monitor:** A reference monitor which mediates network resource access requests. A number of hardware and software systems can be used as network reference monitors including firewalls and intrusion detection systems.

- **Air-gap reference monitor:** A reference monitor which mediates air-gapped resource access requests. A number of hardware systems can be used to enforce the air-gap security policy (i.e., no communication), including electromagnetic (EM) and acoustic shielding.

In the next section, covert channels are defined and classified based on the type of reference monitor that they circumvent.

## 3.2 Covert Channels

*Information hiding* is the discipline within *communications security* that prevents an adversary from learning anything about the transfer of messages [185]. This is in contrast to the related discipline of *cryptography*, which looks at protecting the *confidentiality* and *integrity* of messages (as well as enforcing *non-repudiation* and *origin authentication* in certain applications) [162]. Information hiding has historically been broken down into the sub-disciplines of covert channels, anonymity, steganography, watermarking, and low probability of detection (LPD) radio systems [185]. In **Section 3.3**, the study of covert channels is related to other relevant sub-disciplines within information hiding and in this section covert channels are defined, their applications are discussed, and the classes of covert channels are presented.

### 3.2.1 What is a Covert Channel?

Covert channels are often conceptualized by first introducing a system that consists of two subjects, a HIGH security subject and a LOW security subject, as well as an access control policy: HIGH cannot write to LOW and LOW cannot read from HIGH. A covert channel is then usually introduced and implicitly defined as any information flow that allows information to be passed from HIGH to LOW. This extends to scenarios where HIGH and LOW could be executing on the same host, two separate hosts that are connected via a network, or two separate hosts that are not connected to one another at all. While this provides a general idea of what a covert channel is, attempting to define the term has led to some discussion amongst researchers over a number of years.

Lampson, in the first documented work on covert channels, originally defined a covert channel as a "communication channel that is not *intended* for information transfer at all." [128]. Similarly, Kemmerer stated that covert channels arise from "the use of an entity not normally viewed as a data object to transfer information" [110]. Both these definitions describe the channel as being counter to the original design of the channel/entity itself; however, as pointed out in the Trusted Computer System Evaluation Criteria's (TCSEC) "light pink book" on covert channels, these definitions do not appropriately place covert channels within communications security [77]. Moreover, Huskamp stated that covert channels "are a result of resource allocation policies and resource management implementation" [101] and Girling defined covert channels as a "transfer of information in a

way that would normally be contrary to a network's security policy" [76]. Both definitions place covert channels firmly within the realm of communications security by explicitly stating that a covert channel is an information flow that is contrary to the system's security policy (i.e., access control policy); however, both Huskamp and Girling's definitions are too narrowly focused on standalone systems and distributed systems, respectively, to be generally accepted.

Moskowitz and Miller defined a covert channel as "a communication channel established contrary to the design of a system" [172] and as part of developing the TCSEC, Gligor defined a covert channel as "a communication channel that allows a process to transfer information in a manner that violates the system's security policy" [77]. These definitions make it clear that a covert channel generally circumvents the security of the system regardless of the type of system and we conclude that, given that the reference monitor is the system component responsible for enforcing the system's security policy, the TCSEC's definition is equivalent to stating that a covert channel *is an information flow that circumvents the system's reference monitor,* the definition we use herein. Furthermore, we term a *true covert channel* as a channel that not only circumvents the system's reference monitor but is also *harmful*[5] to the system. Conversely, McHugh defines *benign covert channels* as channels that exhibit one of the following characteristics [159]:

1. HIGH and LOW are the same process,
2. under the system's security policy HIGH and LOW are permitted to communicate with one another, or
3. a covert channel exists between HIGH and LOW, but there is no practical way to communicate data through the channel.

The focus in this work is on *true covert channels*. Moreover, while an updated definition has been derived for the term *covert channel* it is not necessarily intuitive to apply this definition to the term given the vernacular sense of the word "covert." To bridge the provided definition with its vernacular meaning, the following explanation is given: since a covert channel evades a reference monitor, the channel is therefore hidden, in a sense, from the perspective of the reference monitor[6].

The model that is generally used to analyze covert channels consists of two communicating parties, usually referred to as Alice and Bob, and a security policy enforcer, i.e., a reference monitor, referred to as the warden, Wendy (see **Figure 1.1**). Furthermore, in the study of covert channels it is assumed that both Alice and Bob are jointly interested in successfully leaking information (e.g., malware in an air-gapped environment). This assumption is what separates the study of covert channels from the study of *side channels.* Side channels study the unintentional leakage of information, usually from cryptographic

[5]In **Section 3.5.1** we analyze when a covert channel is *harmful* to a system.

[6]Note that this is a very informal treatment of the term as covert channels can exist that are known to the system's designers but which cannot be removed because their removal would severely impact the performance or feature set of the system.

systems, where only the receiver is interested in successful transmission (see [254] for a survey on the subject). Broadly speaking, a covert channel is thus any intentionally created information flow that is outside of what is preventable and detectable by the security policy enforcer, Wendy, and therefore, in this work, covert channels are analyzed from the perspective of Wendy unless otherwise noted.

### 3.2.2 Applications for Covert Channels

There is clearly an adversarial relationship between the covert communicators, Alice and Bob, and the system's policy enforcer, Wendy. While Alice and Bob want to covertly communicate without detection, Wendy wants to either eliminate or greatly reduce the ability for Alice and Bob to do so. This relationship brings about a measures and countermeasures game between the two parties [213]. While this adversarial relationship is clear, the legitimacy of covert channels is not.

It is well documented that malware as well as alleged government implants[7] have used air-gap jumping covert channels to egress data from protected systems [4, 107, 109] and that malware has also used covert channels to attack ICS's [61]. Additionally, malware has been found to use network covert channels to leak data [50, 224] as well as coordinate distributed denial of service (DDOS) attacks [54]. Contrariwise, network covert channels have been developed to facilitate communication through restrictive firewalls by exploiting the redundancy and unused nature of various protocol fields in the network stack (e.g., ICMP [221], TCP [1, 197], HTTP [97], DNS [104])[8], which can be enabling technologies for citizens of countries that employ Internet censorship to restrict free speech [18, 44].

In addition to being used by malware as well as in freedom of speech applications, covert channels are also assumed to be applicable in general scenarios where the communicating entities are not able or willing to communicate through traditional means. This type of situation arises in various scenarios, e.g., when traditional communication links are taken down as is common in times of protest, or in whistle blower scenarios where the whistle blower is trying to avoid detection. Furthermore, Zander, et al., [250] provided a list of applications for network covert channels which includes using covert channels to transmit authentication information [51, 155, 156], to facilitate trace-back in denial of service attacks [103, 190], and to hide network management communication from network attackers [68]. It has also been demonstrated that covert channels can be used to deannonymize hidden services in the Tor network [175] as well as leak information from anonymous networks [170]. While these applications relate more to covert channels between networked or systems separated by an air-gap, covert channels on single hosts have also been observed in the wild [163] and recently a number of publications have demonstrated the use of covert channels to attack the Android OS [53, 93, 178]. In general, covert channels are more often found in the lab than the real world, however. One of the forefathers of covert channels,

[7] Implant is the United States National Security Agency's (NSA) term for malware [4].

[8] Note that this is a very short list of examples of covert channel tools that have been developed to circumvent firewalls. This list is meant to be representative rather than complete.

Jonathan Millen, surmises the reason for this is because "when information is stolen via covert channel, the original data is still in place, so the theft can go unnoticed" [174].

The list of parties interested in the detection and development of covert channels is demonstrably long. Governments are interested in covert channels to hide the presence of their communications as well as to defend against their use; criminals are interested in covert channels for the purposes of leaking sensitive information and controlling malware; citizens in oppressive regimes are interested in covert channels to avoid censorship; and, in general, the average citizen can be interested in covert channels to protect their private communications from being detected. This last point is topical since covert channels have been proposed as a means to hide the use of strong encryption [250] and in 2015 governments in North America and Europe [8] as well as India [52] are considering and discussing proposals to weaken encryption standards or mandate back doors in cryptographic algorithms. Therefore, protection of communications from prying eyes is a topic worth exploring (see **Section 3.3**). As is usually the case in computer and network security, there is a dual-use for covert channels. While covert channels can be used by free speech advocates and privacy-conscious users, these same channels can be exploited by elements to support nefarious activity. A responsible study of covert channels and associated techniques looks at both covert channel design as well as analysis. In this dissertation, both the design of covert channels and the analysis of covert channels is, therefore, covered.

### 3.2.3 History and Classification of Covert Channels

In analyzing the various methods that a program could use to leak sensitive information to a third party, Lampson introduced the *confinement problem*[9] and covert channels [128]. Lipner then applied MAC security models to the confinement problem and argued that when used in conjunction with other techniques (e.g., virtual resource allocation), the problem could be solved for known communication channels, but acknowledged that covert channels are difficult, if not impossible, to eliminate completely [143]. Multiple methods, however, have been developed to systematically identify covert channels on MAC systems: the shared-resource matrix methodology [110], covert flow trees [111], non-interference methods [78], and security kernels [165]. Recently, the shared-resource matrix methodology has been extended to covert channels between systems separated by an air-gap as well [91].

The United States Department of Defence (DoD) developed a process for certifying secure systems, which is documented in the TCSEC [130]. Their certification process focused on MAC systems and required covert channel analysis, which can be separated into four general, not necessarily non-overlapping, areas of research: modelling, searching, measuring, and mitigating [163]. Since the publication of the TCSEC, a number of papers have been written on the modelling [78, 110, 160, 165, 234], searching [85, 94, 111, 144, 161, 203, 236, 246], measuring [152, 164, 168, 171, 172, 207] and mitigating [79, 100, 105, 106, 158, 219] of covert channels. Furthermore, various covert channel techniques have been developed to circumvent the security of operating systems implementing MAC, including:

[9]The problem of constraining a program in order to prevent it from leaking sensitive information is referred to as the *confinement problem*.

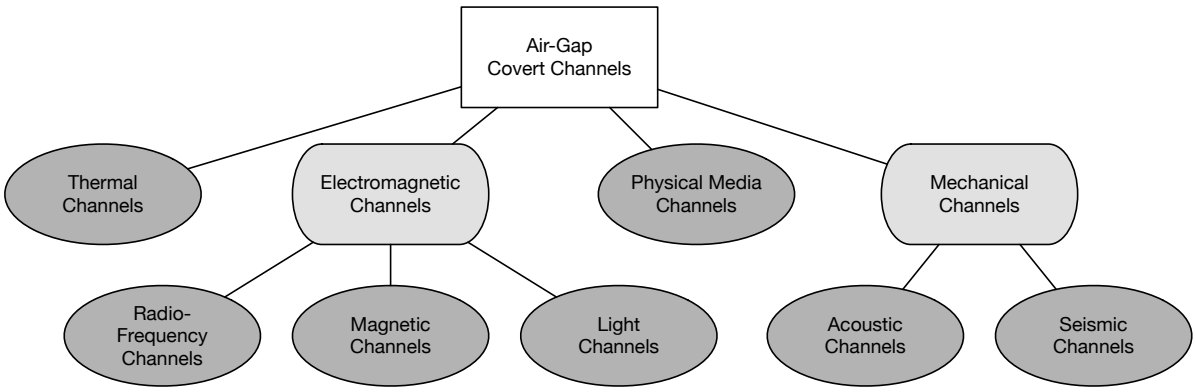



Figure 3.1: Types of Air-Gap Covert Channels

a file-lock covert channel on systems that share a file system [77], the disk-arm channel on KVM/370 systems [203], the bus-contention channel on multiprocessor systems [99] as well as virtualized environments [247], and the acoustic channel on Android [53, 178]. In general, these covert channel techniques were designed to circumvent a host-based reference monitor and have been classified as *host-based covert channels*.

In 1987, Girling presented the first work on covert channels in a networked environment [76]. Since Girling's seminal work, a large number of researchers have developed techniques which manipulate some property of network traffic in order to establish covert communication between networked hosts (see the surveys of Zander, et al. [250] and Wendzel, et al. [244]). Wendzel, et al., surveyed over 100 different network covert channel techniques and found that they could be grouped into general patterns not tied to specific network protocols [244]. The researchers separated techniques into patterns based on whether they modified the structure or timing of network traffic as well as whether they modified the payload or header fields of protocols. Zander, et al., similarly surveyed a large number of network protocol covert channel techniques and found that they could be grouped by the general technique they used to communicate (e.g., modifying unused space), as well as by the protocol they modified. Generally speaking, the research following Girling's initial work has uncovered various methods for misusing different fields within the protocols of the Open Systems Information (OSI) model to circumvent the security of a network reference monitor. The class of covert channels that do so are commonly referred to as *network covert channels.*

In the last decade, a growing body of research has been developed that examines various methods for leaking information from air-gapped systems. Government organizations have known about compromising electromagnetic emanations from electronic equipment since the 1980's and the NSA and DoD have studied this type of leakage under the program name TEMPEST (Transient ElectroMagnetic Pulse Emanation STandard) [95]. While the techniques covered by the TEMPEST program are classical side channels, the leaky nature of various system devices (e.g., video display units, cables, central processing units (CPUs), etc.) has been exploited to demonstrate effective covert channels [17, 82, 93, 125]. A number of other devices, not normally considered as transmitters, have also been exploited

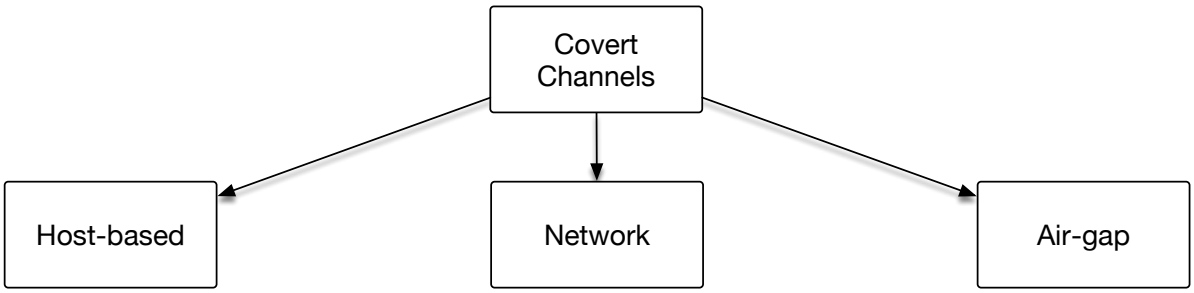



Figure 3.2: Classes of Covert Channels

to leak information from air-gapped systems including speakers and CPUs in acoustic channels [53, 83, 89, 90, 93, 134, 178, 178, 181, 232, 233], light emitting diodes (LEDs) and displays in light-based channels [19, 20, 93, 126, 178], CPUs in thermal channels [154, 175], and vibration devices in seismic channels [11, 53, 178, 223]. Furthermore, there is empirical evidence that physical media is also an effective air-gap covert channel [61, 107, 109]. In general, these channels provide communication between processes running in isolated environments and can be used to circumvent an air-gap reference monitor. While no classification for this category of covert channel has been proposed in the literature to date, covert channels that circumvent the security of an air-gap reference monitor could be labelled as *air-gap covert channels*. Moreover, covert channel techniques that bridge the air-gap can be grouped based on their defining physical characteristic: thermal channels, electromagnetic channels (e.g., radio-frequency (RF), magnetic, light), mechanical channels (e.g., acoustic, seismic), and physical media channels (see **Figure 3.1** for the hierarchy of air-gap covert channels). Air-gap covert channels are the primary focus of this dissertation and are explored in much more depth in **Chapter 5**.

Given that covert channels circumvent the security policy enforcement of a reference monitor, they can be classified into *host-based covert channels*, *network covert channels*, and *air-gap covert channels* (see **Figure 3.2** for an updated classification of covert channels that now includes *air-gap covert channels*). This grouping clearly identifies to secure system designers the class or classes of attacks that they have to protect against given the type of reference monitor that they are implementing and allows individual covert channel techniques to be compared and their novelty assessed, a topic explored in more detail in **Section 3.4**. In the next section, the analysis and design of covert channels is discussed and recommendations that covert channel designers should follow in order to create more secure covert channels are presented.

## 3.3 Covert Channel Analysis and Design

The practical application of covert channels can be broken down into *covert channel analysis* (CCA) and *covert channel design* (CCD). CCA and CCD are examined in this section before the taxonomy that is used in this thesis is presented in **Section 3.4**. The analysis of covert channels in secure systems follows.

### 3.3.1 Covert Channel Analysis

The TCSEC was initially conceived to encourage the adoption and availability of trusted computer systems [130]. The certification process achieved this by providing vendors with a metric, based on levels, that could be used to quantitatively evaluate the security of systems ("A" level systems were the most secure followed by "B", "C", and "D"). The TCSEC also provided guidance to system vendors on how to develop and document systems in order to obtain each level. The successor to the TCSEC was the Common Criteria (CC) whose goal was to unify disparate national secure system certification standards (the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) in Canada, the Information Technology Security Evaluation Criteria (ITSEC) in Europe and the TCSEC in the US) into one international standard [2]. The CC thus provided vendors with one security certification standard that they could obtain and have internationally recognized. In comparison, the CC and TCSEC were both based on assurance, but the CC was a much more general certification process than the TCSEC, achieved mainly by separating the certification levels from the individual security requirements for classes of products. Where the security requirements were tied to the certification level in the TCSEC, the CC set security requirements on a per product basis and the certification process verified that a product met its stated requirements.

Covert channel analysis was required by both the TCSEC and CC at their highest levels of assurance[10]. CCA is the process of systematically searching for and handling illegal information flows in a system [3] and has been broken down into three general stages [77]: (1) Identifying illegal information flows and determining their maximum bandwidth[11]. (2) Based on the covert channel's bandwidth, handling the channel in a manner that is consistent with the certification requirements of the product under evaluation. (3) Providing assurance evidence which demonstrates that the covert channel is handled appropriately, i.e., in a manner commensurate with the certification level being sought.

Once discovered, covert channels, typically, can either be eliminated, bandwidth limited, or audited [77]. Elimination generally requires the system's design to be updated so that the covert channel can no longer be exploited; bandwidth limitation generally calls for the introduction of noise or delays into the system's design in order to reduce the capacity of a covert channel; and auditing generally calls for instrumentation to be added to the system in order to determine when and if a covert channel is actively being exploited. Auditing is implemented primarily to deter the use of the covert channel.

In general, CCA requires solving two general search problems [29]:

1. **Identification:** identifying covert channels by statically analyzing the system's design, and
2. **Detection:** revealing the active exploitation of covert channels by dynamically analyzing events in the system in order to detect anomalies.

[10] In the CC, CCA is required at EAL5 (informal search) as well as EAL6 and EAL7 (formal search). In the TCSEC, CCA is required at B2 (informal search) and A1 (formal search) [3, 130]

[11] Bandwidth estimation and covert channel measurement is discussed in general in **Section 3.5**.

Identification is performed at system design time and often requires the use of formal methods as well as manual input from the system's designers (e.g., the identification of shared resources is commonly a manual task). Furthermore, once a covert channel is identified, elimination of the covert channel can have an impact on the system's performance [29, 105, 171]. Detection, similarly, is also a challenging task which occurs continuously while the system is running. Detection requires the system's designers to know where to look (i.e., the covert channel's mechanism for communication needs to be instrumented), when to look (i.e., the covert channel's mechanism needs to be audited with an appropriate time granularity in order to detect the use of the covert channel) and what to look for (i.e., the system needs to be able to correctly interpret its audit as proof that a covert channel is in use) in order to develop a detection mechanism that will effectively deter the active exploitation of a covert channel. Despite these inherent difficulties, a number of researchers have presented methods for detecting active covert channels [29, 30, 32, 74, 87, 182, 193, 214, 215, 217, 218] and the argument has been made that detection (versus identification and elimination) can be less impactful to system performance [29].

### 3.3.2 Covert Channel Design

CCD, by contrast, consists of the following stages: (1) identifying a *covert exploit*[12] that can be leveraged to create a covert channel and (2) establishing a method to communicate through the channel. In general, once an exploit is found the channel designer can adopt one of two general strategies for constructing the covert channel within a given system:

1. the designer can assume that the system is not designed to, nor will be updated to, detect the covert channel; or
2. the designer can assume that the system is instrumented to, or will be updated to, detect the covert channel.

Channels that implement the former strategy can be referred to as *detectable covert channels* and defined as true covert channels whose design does not take detection into account. Conversely, channels that implement the latter strategy can be referred to as *undetectable covert channels* and defined as true covert channels whose design does take detection into account. *Undetectable covert channels*, by definition, take a truly cautious approach to covert communication.

In the design of *detectable covert channels* the only thing that is "required is the ingenuity" of the designer [50] and once an exploitable information flow is found the problem for the covert channel designer reduces to a traditional communication problem, i.e., choosing appropriate modulation, channel and source coding schemes. Hidden communication systems that rely solely on novelty for security, however, have not stood the test of time [185]. The problem faced by the designer of an *undetectable covert channel* is common

[12] A *covert exploit* refers to a specific technique used to create a covert channel [215]. Given this definition, a covert channel is the result of applying a covert exploit.

in the study of information hiding and one that is modelled by Simmons' aforementioned "prisoners' problem" [209].

The topics of identifying and detecting covert channels have received much attention by the research community, however, the systematic design and development of covert channels that maximize their capacity while minimizing their detection is not a well explored topic. Smith and Knight explored the systematic design of network covert channels in the presence of a passive adversary and examined the trade-off between three design metrics: probability of detection, reliability (i.e., BER), and system efficiency, where system efficiency measured the effect of adding coding and undetectability to the covert channel [214, 215]. Furthermore, Moulin and O'Sullivan as well as Wang and Moulin have studied the systematic design of covert channels in the presence of an active adversary [173, 242]. By modelling covert channels as a game theory problem the researchers were able to provide capacity bounds based on distortion constraints at both the covert transmitter and active attacker. Their research, however, focused on disrupting communications and did not take the detection of covert signals into account.

### 3.3.3 Undetectable Covert Channels

In order to develop an effective *undetectable covert channel* some form of information hiding must be applied to the messages that are passed through the channel. While no formal definition for *undetectable communication* exists, the notion of *undetectability* does: "*undetectability* of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not" [186]. For the purposes of this discussion, an IOI is any message that is passed through the covert channel and the attacker is Wendy, the policy enforcer. In **Section 3.5** different possible methods for measuring *undetectability* are discussed, but for the purposes of this section the reader can interpret *undetectability* as a probability measure, i.e., the probability that the attacker detects messages being passed through the channel, or an entropy measure, i.e., a measure of the uncertainty that the attacker has with respect to the covert channel being used or not. Given Pfitzmann and Hansen's definition for undetectability, an *undetectable communication* system can be conceptualized as a communication system that, given an adversarial model, maximizes *undetectability*. The literature on information hiding covers a number of communication systems whose designs take undetectability into account including steganography, LPD radio systems, and imperceptible communication systems, which are techniques that hide information in a cover, in background noise, or outside the perceptible range of the attacker, respectively. Each of these techniques is reviewed herein.

Steganography is the discipline of embedding secret messages into a cover and literally means "covered writing" in Greek [185]. In the literature, the *embedded* message is the secret information and the *cover* is referred to as either *cover-text* [27, 212], *cover-image* [38] or *cover-audio* [102], depending on the type of cover that is used. The process of embedding a secret message is governed by the *stego-key* and successful execution of the process results in the creation of a *stego-object*. A steganographic system takes as input a message, a cover object, and a stego-key and the goal of the system is to render the

embedded message undetectable by an attacker. Steganographic systems accomplish this by placing the embedded message in locations of the cover that have high entropy, i.e., locations where there is a high degree of uncertainty as to their expected value. It is this uncertainty that prevents the attacker from easily determining whether an embedded message exists in the cover or not.

There are also two special cases of steganographic systems that could be relevant to covert channel design: subliminal channels [209], which hide information in cryptographic exchanges, and supraliminal channels [47], which hide information in the semantic meaning of messages. In 1984, Simmons was the first to introduce subliminal channels [209]. In his work, Simmons presented two examples that demonstrated that it is possible to generate several cipher texts using different parameters that decrypt to the same message, and that by this fact information can be communicated in secret not by modifying the message itself, but rather by the choice of the cipher parameters used to encrypt or sign messages. Subliminal channels can be found in cryptographic algorithms such as El-Gamal and the Digital Signature Algorithm [15, 210, 211]. In 1998, Craver argued that information could also be hidden in the semantic meaning of overt messages and defined supraliminal channels [47]. In his work, Craver summarized the properties of his new channel as follows: modifications to the hidden message should be detectable by the communicating parties, the secret message should not be hidden but instead should be placed in plain view, and the secret message must not draw any suspicion to the hidden channel. Supraliminal channels have been demonstrated in a videoconferencing application [48] as well as an audio application [136].

LPD radio communication systems have been the focus of military researchers for a number of years and much of this focus has been on time and frequency spread spectrum modulation schemes, i.e., direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) [184, 189], respectively. Where the goal of steganographic systems is to hide information in an authentic cover, the goal of LPD radio systems is to hide signals in background noise. Spread spectrum systems accomplish this by spreading a signal's energy out over a bandwidth that is much larger than the information bearing signal's bandwidth. The spreading is done by pseudorandomly manipulating the information bearing signal in the time or frequency domain (or both in hybrid spread spectrum systems), where the pseudorandom manipulation is keyed by a secret shared between the transmitter and receiver. By using spread spectrum modulation an attacker is forced to observe the larger bandwidth and thus is also forced to observe more background noise. Spread spectrum, therefore, lowers a signal's signal-to-noise ratio (SNR) as observed by an attacker and makes the hidden transmission much more difficult to detect.

Lastly, imperceptible communication systems hide signals not in a cover or background noise, but outside of the perceptible or observable range of an attacker. Imperceptible communication systems are subject to additional risk as compared to steganographic and LPD systems because if the attacker becomes aware of the technique being used by the communicators, the attacker could possibly update her detection mechanism and detect their communication. Imperceptible communication systems that rely on their communication method remaining unknown use "security through obscurity" as protection since the covert communicating parties are only safe while the attacker is not aware of their method

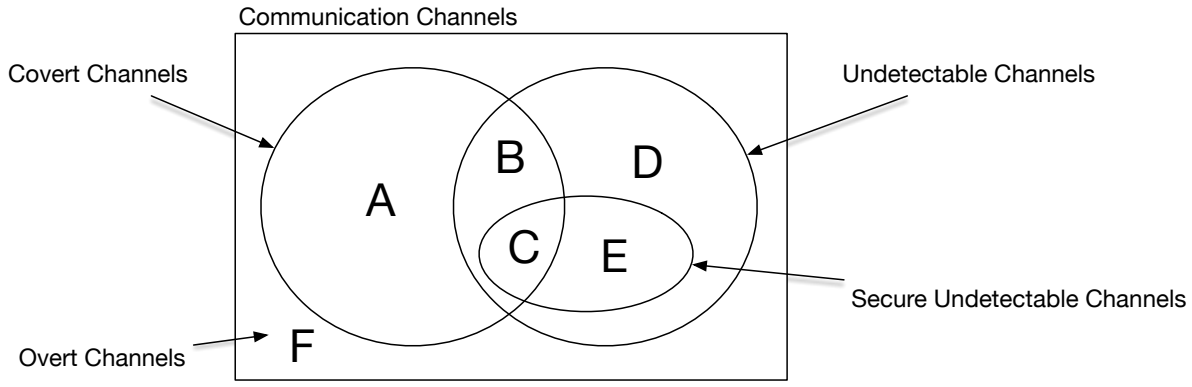



Figure 3.3: Communication Channels from the Perspective of a Reference Monitor

of communication.

Although undetectable communication systems are not cryptographic systems, designers of undetectable communication systems can learn from their design principles. In 1883, Kerckhoff stated that the security of cryptographic systems must rely on keeping the cryptographic key secret as opposed to keeping the cryptographic algorithm secret[13] [118]. This advice extends to undetectable communication systems by assuming the attacker has access to the algorithm used to hide messages, but does not have access to the key material that is used by the algorithm. This applies to steganography directly by assuming the embedding algorithm is known but the stego-key is kept hidden. Similarly, in LPD radio systems the spread spectrum algorithm would also be known to the attacker but not the secret used by the pseudorandom spreading function. Systems that follow Kerckhoff's principle, therefore, can be referred to as *secure undetectable communication systems.*

There is possibly some ambiguity as to the difference between steganography and covert channels. Wendzel, et al., argued that the difference between the two disciplines is that in steganography information is hidden in "carriers" that are interpreted by humans (e.g., text, audio, video), whereas in covert channels information is hidden in "carriers" interpreted by machines (e.g., file locks, network protocol headers, etc.) [244]. Moskowitz, et al., argued that there are two important differences between the two areas of research: (1) the study of covert channels does not take into consideration undetectability[14] and (2) covert channels are assumed to transmit forever whereas steganographic channels are assumed to transmit only for the lifetime of the cover medium [being] used [169]. Smith agreed with Wendzel, et al., in the sense that steganographic channels exist at protocol levels above the networking layer in the OSI model, and further characterized steganographic channels as (1) channels that require a secret key to be shared amongst communicating parties in order to facilitate undetectable communication and (2) channels that are of higher bandwidth than covert channels [213]. Fundamentally, the main distinction between the two disciplines is that covert channels are designed to circumvent a reference monitor and the security policy of a system whereas steganographic systems are designed to hide informa-

[13]This principle is commonly known as *Kerckhoff's principle.*

[14]Moskowitz, et al., complemented this statement with the statement "although perhaps it should."

tion in a specific cover medium and circumvent detection by an adversary.

This argument broadly extends to the difference between covert channels and undetectable communication systems in general. While an undetectable communication system *could* be used to circumvent a reference monitor it is not necessarily the intent of the communication system to do so, nor is it true that all undetectable communication systems are covert channels. To clarify this distinction a Venn diagram is presented in **Figure 3.3**, which should be interpreted from the perspective of a reference monitor enforcing a security policy. **Region A** communication systems are *detectable covert channels* that the reference monitor either does not know about or cannot remove from the system for practical reasons. **Region B** and **Region C** communication systems are *undetectable covert channels* and *secure undetectable covert channels*, respectively, that again, the reference monitor does not know about nor can remove. Furthermore, the union of **Region D** and **Region E** systems are channels that do not circumvent the security of the system but are undetectable (also known as *benign* covert channels) and lastly **Region F** systems are overt communication channels that neither circumvent the security of the system or are undetectable. Clearly, from a defence perspective the application of covert channel analysis would ideally remove the class of *Covert Channels* and from an offensive perspective covert channel designers would be wise to find a covert exploit that allows them to establish a *secure undetectable covert channel* (**Region C**).

The discussion in this section is summarized by providing the following recommendations to covert channel designers:

1. The following assumptions should be made:

   (a) the reference monitor employs auditing techniques to detect the use of the covert channel,

   (b) the reference monitor knows the technique being used to hide messages in order to avoid detection;

2. information hiding techniques should be applied in order to render the channel undetectable; and,

3. an applicable information hiding technique should be chosen whose undetectability is based on the strength of a shared secret.

While this is a truly pessimistic view for covert channel designers to take, it is the only way to guarantee some measurable degree of protection against detection. In **Chapter 7**, an air-gap, **Region B**, covert channel using acoustic signals is designed and in **Chapter 8** air-gap, **Region C**, covert channels are presented.

## 3.4 Covert Channel Taxonomy

In this section, the classification of covert channels first proposed in **Section 3.2** is complemented with a taxonomy that is used in this dissertation to characterize covert channels. While aspects of the taxonomy have been presented in other works before, this collection of covert channel traits is novel because it not only generalizes the characterization of covert channels in all classes but it also models the reference monitor, takes into account the strategy used to hide communications, and captures the type of exploit required to enable the channel. The characterization of covert channels is important because it allows for their systematic study and comparison, it allows for general defences to be developed, and it allows best practices to be established. The section begins with a discussion on existing taxonomies.

### 3.4.1 Background on Covert Channel Taxonomies

Covert channels are usually classified primarily as either *storage* or *timing* channels [29, 31, 130, 143, 171, 180, 243, 246, 250]. *Storage channels* "involve the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process" [130]. *Timing channels*, on the other hand, allow a transmitting process to "signal information to another by modulating its own use of system resources in such a way that this manipulation affects the real response time observed by the second process" [130]. While classification along these lines seems to be universal, it is also widely acknowledged that there can be very little semantic difference between the two, as was first pointed out by Wray [246]. Moreover, covert channels are usually also classified as *noisy* or *noiseless* channels. Probabilistically speaking, if the inputs to a given channel are elements of the random variable $X$ and the outputs are elements of the random variable $Y$, we get that $P(Y = X) = 1$ for a noiseless channel and $P(Y = X) \leq 1$ for a noisy channel, where the output is instead governed completely by the input variable $X$ and the conditional probability distribution, $P(Y|X)$, of the channel.

While classification along the lines of storage or timing and noisy or noiseless is common, researchers have proposed additional characteristics by which covert channels can be classified. Wang and Lee separated covert channels into value-based and transition-based covert channels in addition to classifying them as either spatial or temporal [243]. A receiver in a value-based covert channel extracts information based on the value it sees, whereas in a transition-based covert channel the receiver extracts information based on a change in the value that it observes; the latter being similar to differential encoding [189]. Additionally, spatial and temporal channels are channels where the receiver either observes symbols directly or the receiver observes an order of events, respectively, and are very similar, if not identical, to classical storage and timing channels. Wang and Lee used their taxonomy to show that a novel class of covert channel, value-based temporal covert channel, existed. Okhravi, et al., also separated covert channels based on value and transition in addition to classifying them based on the source of the shared resource being modulated: a network resource, an OS resource, or a hardware resource [180].

Cabuk, similarly, also separated covert channels along the lines of storage or timing as well as network or host-based in addition to whether the transmitter (i.e., Alice) was active or passive [29]. Cabuk described an active-source covert channel as one where the covert transmitter is actively transmitting data and a passive-source covert channel as one where there is no participating source. While an interesting distinction, Cabuk's description of a passive-source channel is more similar to a side-channel than a covert channel[15]. Zander also separated network covert channels based on the participation level of the transmitter and labelled sources as active, semi-passive, or passive [249]. Zander described an active source in the same way as Cabuk; however, Zander defined a semi-passive source and a passive source as one that manipulates other applications to transmit data or modifies existing traffic while simply acting as a middleman, respectively. Of relevance to the taxonomy proposed in this chapter is Zander's separation of covert channels based on the degree of predictability of the cover that the transmitter embeds information within. Zander organized channels based on whether the cover was predictable, variable, or random, where variable covers and random covers have limited randomness or are completely random, respectively. This can be generalized and covert channels can be categorized as those that use a cover to hide information, i.e., *steganographic covert channels*, or those that do not, i.e., *open covert channels*.

Conversely, Meadows and Moskowitz took a different approach to classifying covert channels and proposed separating them based on their context as opposed to the mechanism they used to establish the channel [160]. The researchers classified channels as either high-to-low service channels, low-to-high service channels, or shared service channels, where policy-breaking communication is via a service running at a higher level, lower level, or at an incomparable level, respectively. This novel approach is orthogonal to the traditional classification of covert channels and was designed to be interpreted in conjunction with the security policy of the system to help secure system developers determine which class of covert channel is most relevant to them. This classification by Meadows and Moskowitz highlights the importance of context when evaluating covert channels and is a topic that is revisited in **Section 3.5.1**. A grab bag of other categorizations for covert channels also exists: frequency-based [31], protocol-based [31], statistical [167], sorting [10], counting [80], and hybrid, which is any combination of covert channel techniques.

### 3.4.2 Proposed Covert Channel Taxonomy

To date, the covert channel taxonomies proposed in the literature have been specific to a class of covert channel and, for the most part, have been designed to model covert channels so that their channel capacity can be estimated. The latter is in no small part due to the covert channel analysis requirements of the TCSEC and CC; and, while calculating the capacity of a communication channel, in general, is important, the analysis in the next section, **Section 3.5**, demonstrates that depending on a secure system's requirements, covert channels should also be measured under the condition that a system's reference

[15]To explain passive-source channels, Cabuk simply provided an example of a password checking algorithm that leaks data to a password cracker through the checking algorithm's execution time.

monitor attempts to detect the covert channel as well. The updated taxonomy in this section addresses this by characterizing covert channels based on attacker model and by the methodology used to hide information transferred through the covert channel. Moreover, the taxonomy presented in this section is more general than previous taxonomies, which is important because covert channel techniques can sometimes be used to circumvent the security of multiple reference monitors.

### Channel Noise Model: Noisy or Noiseless

The reception of symbols via a covert channel can be either noisy or noiseless based on the class of covert channel and environmental factors, including: competing processes, background noise, imprecision of devices reading the symbols, system and network delays, network packet loss, network packet reordering, etc. Furthermore, the reception of symbols by both the receiver and the attacker are subject to the channel noise model and in order to effectively categorize and measure a covert channel its noise model must be known or estimated. Moreover, the noise model can play a role in dictating which information hiding techniques, if any, can be applied, as the ability to use LPD radio techniques to hide information in noise is limited if the channel is noiseless.

### Channel Cover Model: Steganographic or Open

A *steganographic covert channel* is a communication channel that is established by a transmitter modifying a cover source that has at least some variability to it, i.e., the cover source is not deterministic but probabilistic in the parameter being modulated to communicate information. Conversely, an *open covert channel* is a channel that either does not use a cover source to hide information within or one that modifies a completely deterministic cover source. The key distinguishing characteristic between these two classes of channels is that the cover source follows some random distribution for *steganographic covert channels* and some deterministic value for *open covert channels*. Information hiding techniques based on steganography are therefore inappropriate for open covert channels.

### Channel Attacker Model: Mediated or Shared

The attacker, i.e., the reference monitor, Wendy, can either have shared access to the symbols being transmitted via the covert channel or can mediate the channel, i.e., all messages pass through Wendy. In the shared model, symbols are not sent from the transmitter to the attacker before being passed to the receiver as they are in the mediated model[16]. Instead, symbols are transmitted and are directly accessible by both the attacker and receiver [17]. The latter model is somewhat related to Simmons' prisoner problem, but is better modelled by the *solitary confinement problem* illustrated in **Chapter 1**. A metaphor which

[16]Note that the mediated channel model is the model that is described by the *prisoners' problem.*

[17]The shared channel model limits how *active* the attacker can be, e.g., if the attacker and the receiver have simultaneous access to the symbols then the attacker can't delete messages, for example

illustrates the difference in model is a scenario where the prisoners attempt to communicate an escape plan by tapping out Morse code on a shared radiator[18]. In this scenario, Wendy (or her delegates, the guards) as well as the receiver, Bob, both have shared access to the communication channel.

### Modulation Type: Detectable, Undetectable or Secure Undetectable Covert Channel

As discussed in **Section 3.3**, the designer of a covert channel can either implement a *detectable covert channel* or an *undetectable covert channel*, where the latter strategy takes into account the auditing capabilities of the system's reference monitor while the former strategy provides no inherent defence against detection. Moreover, a covert channel designer can either implement an *undetectable covert channel* that is dependent on a secret being shared between the transmitter and receiver, i.e., a *secure undetectable covert channel*, or one that is not. Obviously, if a *secure undetectable covert channel* is implemented there is an additional requirement on the system that Alice and Bob must be able to pre-share a secret in some fashion.

### Modulation Medium: Storage, Timing or Hybrid

As previously mentioned, covert channels can be categorized as either storage, timing or hybrid, if their symbols take the same time to transmit, different times to transmit, or both, respectively [171]. While it has been argued that semantically there is no difference between the medium used by the covert channel [246], measuring the channel capacity of a covert channel is dependent on the medium used to communicate symbols [171]. Covert storage channels can have their capacity measured either in bits per channel usage or bits per time unit, whereas covert timing channels must have their capacity measured in bits per time unit.

### Modulation Mode: Full Duplex, Half Duplex or Simplex

An important consideration in the design of covert channels is the mode of communication. Covert channels can provide either bidirectional or unidirectional, i.e., simplex, communication. Furthermore, bidirectional communication can allow for information to either flow back and forth between Alice and Bob simultaneously in both directions or in one direction at a time, i.e., in full duplex or half duplex mode, respectively. The communication mode of the channel has implications on the throughput[19] of the channel as duplex mode communication allows the receiver to indicate that a retransmission is required whenever a corrupted message is received or a message is lost (e.g., Automatic Repeat Request (ARQ)

[18]This hypothetical channel was first presented as a valid covert channel in McHugh's "Covert Channel Analysis" [159].

[19]The rate at which messages can be communicated with arbitrarily low probability of error.

schemes can be implemented to allow the receiver to indicate to the sender when to retransmit messages that have not been received correctly); whereas, simplex communication channels do not and thus simplex channels require additional Forward Error Correcting (FEC) schemes to be applied to ensure error-free communication.

### Covert Exploit: Invasive, Semi-Invasive or Non-Invasive

An often overlooked property of covert channels is the covert exploit that is used to enable communication through the channel. While classification based on covert exploit does not necessarily help measure covert channels, discrimination based on covert exploit provides a better understanding of how the channel is enabled and thus how to protect against its use. Furthermore, by separating the covert exploit from the other channel and modulation properties it allows the channel's capacity to be studied independently from the exploit [213]. This is particularly advantageous because it allows collections of covert channels which share common channel and modulation properties to be evaluated without consideration for their individual exploits. Additionally, defences for covert channels can be split into those that reduce the likelihood of a covert exploit taking advantage of a system's vulnerability and those that reduce or eliminate the possibility of information being transferred through the covert channel itself. Covert exploits can be separated into the classes of invasive, i.e., covert exploits that require hardware modification, semi-invasive, i.e., covert exploits that require software modification to the system's reference monitor, or non-invasive, i.e., covert exploits that require no hardware modification or software modification to the system's reference monitor. This classification is similar to that used in the study of side channels [16].

### Reference Monitor: Host-based, Network or Air-Gap

Without belabouring the point, covert channels can also be classified based on the reference monitor or reference monitors that they circumvent. Interestingly, certain covert channel mechanisms have been shown to circumvent the security policy of multiple reference monitors, e.g., covert-acoustic communication has been demonstrated to be an effective covert channel that circumvents both host-based and air-gap reference monitors [53, 178], and, therefore, a covert channel could in fact be classified as being capable of defeating multiple reference monitors.

Piecing together the criteria used to classify covert channels, a diagram depicting the covert channel model is provided in **Figure 3.4**[20]. This model is motivated by both the information hiding model first proposed at the First International Workshop on Information Hiding [187] as well as the basic construction of digital communication systems [189]. Moreover, the model depicted in **Figure 3.4** is a more general model than was first presented in **Figure 1.1**. This model is meant to be as comprehensive as possible and as such optional system parameters are placed in parenthesis, e.g., shared secret and cover object,

[20]Note that the *modulation medium* and *covert exploit* are not shown in the diagram.

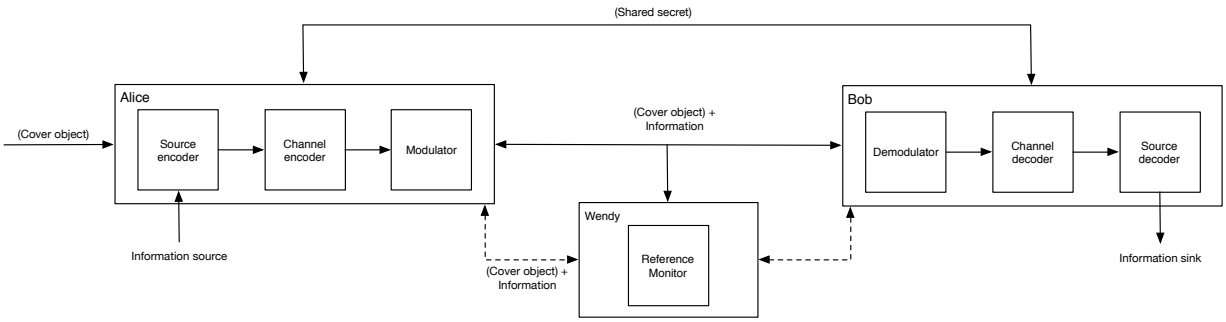



Figure 3.4: General Covert Channel Model

and the two proposed channel attacker models, i.e., shared and mediated, are depicted as a solid line and a dashed line between Alice, Bob and Wendy, respectively.

## 3.5 Measuring Covert Channels

In this section the history of measuring covert channels is presented, secure systems are classified based on their security requirements, and a new measure to assess the risk of covert channels is proposed for a specific class of secure system.

The TCSEC first published guidelines on measuring covert channels in the "light pink book" [77]. In the guideline, the authors mandated that covert channels be measured by either informal bandwidth estimation methods or formal information-theoretic measurements. In addition to providing guidelines on measuring covert channels, the TCSEC also outlined how certain factors impacting bandwidth should be handled. Given the volatility introduced by the indeterminate actions of processes or machines on a network, the TCSEC guideline instructed certification applicants to assume that there were no other active participants in the system other than the covertly communicating parties, i.e., they were instructed to assume that there was no noise in the system. The TCSEC also instructed applicants to estimate bandwidth by assuming an equal distribution of symbols and no channel coding. Furthermore, the TCSEC prescribed that the bandwidth calculation should not account for the synchronization time between transmitter and receiver; however, the timing of system primitives (i.e., API calls) used by the covert transmitter and receiver with the fastest execution times should be used in all timing calculations. Lastly, for covert channels that could be exploited in parallel, the TCSEC prescribed that their bandwidths be summed. In summary, all of these assumptions were made to maximize the bandwidth of the covert channel and generate a worst-case measure of the covert channel from the perspective of the secure system developers. Many of these assumptions continue to be made in modern studies where the bandwidth of covert channels is calculated.

The accurate measurement of covert channels allows proportional countermeasures to be employed by the developers of secure systems. Informal bandwidth estimation was first outlined in the work of Tsai and Gligor, where the authors estimated a channel's bandwidth, $B$, using the basic equation $B = \frac{b}{T_R + T_S + 2 * T_{CS}}$, where the units of $B$ are $\frac{\text{bits}}{\text{second}}$,

$b$ is the number of bits transmitted per use of the channel, $T_R$, $T_S$, and $T_{CS}$ are estimates for the time it takes to read the channel, write to the channel, and for the transmitter and receiver to perform a context switch[21], respectively. Millen, on the other hand, presented a more precise measurement methodology to calculate the bandwidth of covert channels using information theory [164]. Millen's methodology called for the channel to first be represented by a finite state transition diagram and the bandwidth of the system to be calculated by determining the number of possible messages, $N(t)$, that could be sent through the covert channel in a period of time, $t$. The bandwidth of the system was then taken to be

$$C = \lim_{t \to \infty} \frac{\log N(t)}{t}$$

and reduced to solving a system of equations in order to find an expression for $N(t)$.

While the TCSEC proposed using Tsai and Gligor's as well as Millen's methodologies for estimating the bandwidth of covert channels, it was Moskowitz and Myong who first provided a counterargument [171] as to why bandwidth was not the correct measure and proposed instead to use Shannon's channel capacity [206]. Moskowitz and Myong argued that since Shannon's channel capacity provided a maximum rate at which information could be sent through a channel it was the more appropriate measure for analyzing the threat posed by covert channels. The researchers provided the channel capacity calculation for continuous, band-limited systems as proof that bandwidth alone is not an accurate measure for a covert channel's maximum data rate:

$$C = W \log \left( 1 + \frac{P}{N_0 W} \right), \tag{3.1}$$

where $W$ is the channel's bandwidth (i.e., the Fourier transform, $X(f)$, of the transmission signal, $x(t)$, is zero for $|f| > |\frac{W}{2}|$), $P$ is the transmitter's average signal power, and $N_0$ is the power spectral density of the noise. To their point, **Equation 3.1** shows that capacity is in fact a function of bandwidth. Furthermore, the bandwidth estimation methodologies of Tsai and Gligor as well as Millen did not take noise into account, which can greatly reduce the capacity of the channel and thus their measures potentially over-inflate the risk posed by the measured channel. Properly accounting for noise as well as coding is important because underestimating or overestimating the threat posed by a covert channel can lead to unnecessarily reducing the system's performance or allowing high-capacity channels to persist in the system, respectively.

### 3.5.1 When do Covert Channels Pose a Risk?

The TCSEC quantitatively classified covert channels into three classes based on their bandwidth: high-bandwidth covert channels were classified as channels whose bandwidth

[21] This formula was initially presented to measure the bandwidth of host-based covert channels in Tsai and Gligor's work [235]. The time required for context switch might not be relevant to all covert channels. Similarly, reading and writing to the channel can be parallelized in many covert channel deployments.

was above 100 bits per second (bps), low-bandwidth covert channels were classified as channels whose bandwidth was between 1 bps and 100 bps and acceptable covert channels were classified as channels whose bandwidth was below 1 bps [130]. Moreover, the criteria required that all high-bandwidth covert channels be removed from the system and that all low-bandwidth channels be audited if they could not be removed [130]. The seemingly arbitrary threshold for high-bandwidth covert channels was based on the communication rate of remote terminals at the time the TCSEC was authored as the creators of the TCSEC felt that "it does not seem appropriate to call a computer system *secure* if information can be compromised at a rate equal to the normal output rate of some commonly used device" [130]. While the TCSEC's classification was relevant at the time, the output rate of modern devices is on the order of gigabits per second.

The CC took a more pragmatic approach to defining the threat of covert channels and left the definition of *secure* up to each product's[22] security requirements [3]. Instead of prescribing appropriate methods for handling covert channels based on their bandwidth, the CC certification process was designed to merely confirm and selectively validate (at EAL5 and above) the covert channel analysis of products. McHugh also supported a more pragmatic approach to defining criteria for handling covert channels [159]. McHugh stated explicitly that for a covert channel to be harmful to a system the covert communicators must be forbidden from communicating and they must be able to exploit a flaw in the system in order to communicate a "useful quantity of information" [159]. Neither the CC nor McHugh explicitly set criteria for handling covert channels based on their bandwidth because "it is important to consider the quantity of information that must be compromised to cause a serious breach of security" [159]. This context-dependent position was also shared by Meadows and Moskowitz [160].

In order to assess the security risk posed by a covert channel, secure systems can be generalized into two classes: *continuous-source systems* and *fixed-source systems*. Continuous-source systems are systems whose security is compromised if information is leaked above a defined rate. Systems in this category can be conceptualized as systems that produce sensitive information at such a relatively high rate that a "slow" leak via covert channel will not compromise the security of the system, i.e., by the time enough information is leaked via covert channel it is irrelevant. A large number of systems that fall into this category include systems that make private information available publicly periodically (e.g., declassifying information after a certain period of time, corporations filing for patents, etc.). The designers of continuous-source secure systems are thus interested in proving that their design does not contain covert channels that are capable of leaking information above a predetermined rate. As a result, Shannon's channel capacity is a relevant measure for covert channels when the security of this class of system is being analyzed. Conversely, fixed-source systems are systems whose security is compromised if a fixed amount of information is leaked from their system. Systems in this category can be characterized as systems that rely on a small and fixed amount of information (e.g., encryption keys, private signing key, etc.) being kept secret in order to remain secure. The designers of this type of secure system are interested in ensuring that a predetermined amount of information

[22]In CC parlance, products are *Targets of Evaluation* (TOE)

cannot be communicated via a covert channel in a given period of time and not necessarily in the long term average information rate of the covert channel (i.e., channel capacity).

For fixed-source systems, the *Small Message Criterion* (SMC) [171], as opposed to a predefined rate, is a more appropriate security criterion. In their analysis of covert timing channels, Moskowitz and Myong showed that zero-capacity covert channels could be designed by communicating a single symbol in exponentially increasing time periods. Their zero-capacity channel worked as follows: the first symbol was sent in one time period[23], the second symbol in two time periods, the third in four time periods, ... with the $n$th symbol being sent in $2^{n-1}$ time periods. After $n$ channel uses one of $2^n$ messages could therefore be transmitted over the channel (i.e., a maximum of $n$ bits could be transmitted); however, the capacity of this particular channel is zero (see [171] for the mathematical details). While this channel would not pose a risk for a continuous-source system, it could pose a serious risk for a fixed-source system. Moskowitz and Myong addressed this deficiency in capacity analysis by creating the SMC, which is based on three criteria: the maximum allowable length (in bits) of the information being leaked, the acceptable time frame in which the information can be leaked, and the acceptable fidelity of the information. For fixed-source systems, covert channels that violate the SMC can be classified as channels that violate the security of the system.

Determining the channel capacity of a covert channel in a continuous-source system allows the risk of the channel to be evaluated by comparing the calculated capacity to a set predefined rate based on the requirements of the secure system; however, there is no such agreed upon metric for assessing the risk of fixed-source systems, nor is there any generally accepted methodology for determining the capacity of covert channels when a secure system actively attempts to detect the channel through auditing.

### 3.5.2 Steganographic Capacity

The general detection of covert channels, i.e., measuring the *undetectability* of a covert channel, has been the topic of numerous studies and a wide array of general techniques have been documented in the literature. Researchers have used Kolmogorov-Smirnov testing to compare the statistical distributions of normal network traffic and covert network traffic in order to detect network covert channels [182]. The use of *regularity* tests has also been proposed to detect network covert channels that demonstrate traffic patterns that are too regular (e.g., the inter-packet delay of some network covert traffic algorithms is relatively constant) [29]. Similarly, some network covert timing channels can be identified through frequency analysis because they show disproportionate counts at the delays that are used to communicate symbols [30]. Additional tests that detect covert timing channels based on the regularity of covert network traffic include the Wilcoxon Signed-Rank Test and the Spearman Rho Test of Rezaei, et al. [193]. Empirically determined entropy has also been used to detect covert channels, where covert channels are identified by the measurable change they induce on the entropy of network traffic [74]. Techniques to identify specific network covert channels have also been discussed in the literature [32] (e.g., detection of

[23]Moskowitz and Myong referred to the basic time unit as a *tick*

the ICMP ping tunnel, Loki, [50], anomalous use of unused packet header fields [87], TCP header-based covert channels [218], and ICMP payload-based covert channels [217]). While these solutions all present detection metrics for either general or specific covert channel mechanisms, they do not provide a comprehensive metric that captures the amount of information that can be leaked via a covert channel before it is detected and thus do not appropriately quantify the risk of an audited covert channel.

Studying the capacity of information hiding channels in the presence of a passive adversary has been the ongoing focus of researchers both in the context of LPD communication systems and steganographic systems. Recently, a number of works outlining the theoretical limits of LPD communication for various channel models have been published, namely the additive white Gaussian noise channel (AWGN) [23, 24, 25], the wire-tap channel [98], and the binary symmetric channel (BSC) [40, 41, 42]. Bash, et al., proved the "square root law" for LPD signals transmitted over an AWGN channel, which demonstrated that at most $O(\sqrt{n})$ and $o(\sqrt{n})$ bits can be covertly communicated in $n$ channel uses while bounding the detector's probability of detection to some arbitrary threshold, when the detector's noise power is known by the covert communicators and when it is not, respectively [23, 24]. Their analysis gave asymptotic bounds on the number of channel uses; however, the researchers did not derive the exact number of channel uses that were possible under their assumptions. To address this, Wang, et al., studied the maximum amount of information that could be transmitted through the same channel and showed that the number of channel uses scaled with the square root of the Kullback-Leibler (KL) divergence between the distribution Eve observes when Alice is communicating and when she is not [241]. In contrast to the works of Bash, et al., and Wang, et al., in **Chapter 6**, the maximum amount of information that can be leaked over the AWGN channel in the presence of a passive adversary is derived.

Che, et al., examined the ability for Alice and Bob to communicate over a BSC while ensuring their communication is undetectable [40, 41]. In their analysis, Wendy observed Alice's transmissions through a noisier communication channel than Bob, i.e., the wire-tap channel [248], and were able to prove a similar "square root law" under this assumption. Prior to the works of Bash, et al., and Che, et al., a "square root law" was first observed in steganographic systems by Ker while analyzing the capacity of batch steganography [112]. Since this seminal work was first published, other steganographic systems have also been found to respect this same law, namely systems that rely on Markov chain covers [67] or covers composed of i.i.d. elements [114]. Similarly, the "square root law" has been demonstrated for a number of other covers under various assumptions [65, 66, 113, 116, 117]. While no universal theory proving the "square root law" exists in general, the law is composed of a "collection of theories for different mathematical models" [117].

This set of results provides strong evidence that repeated use of a covert channel under audit can lead to certain detection if the amount of information transmitted over the channel is not limited appropriately, e.g., at a rate proportional to $\sqrt{n}$, where $n$ is the number of channel uses. Suspicion of this result was first presented by Anderson and Petitcolas while studying the limits of steganography. The researchers argued that the more stego-objects Wendy has access to, the better model she has for the channel's cover and, as a result, the undetectable embedding rate might tend to zero [13]. These results have led steganography researchers to move away from using Shannon capacity for measuring

Table 3.1: Recommendations for Handling and Measuring Covert Channels by System Type

| | **System type** | |
|---|---|---|
| | **Continuous-source** | **Fixed-source** |
| **Recommended Countermeasure** | Bandwidth reduction | Auditing |
| **Security Criterion** | Predetermined rate | Small message criterion |
| **Relevant Metric for Covert Channels** | Channel capacity | Steganographic capacity |

steganographic channels, preferring instead the use of *steganographic capacity*, which is *the maximum amount of data that can be communicated covertly before an adversary's probability of detecting the communication reaches a given threshold*. In the context of covert channels, steganographic capacity provides a more appropriate measure for the *covertness* of a channel when the channel is being audited. Moreover, the collection of "square root laws" provides evidence that, by employing appropriate detection mechanisms, the amount of information being leaked can be capped to a fixed amount (possibly even zero using the analysis of steganographic capacity). This is of relevance to the design of secure fixed-source systems. A summary of the analysis in this section is presented in **Table 3.1**.

In this chapter, the history of covert channels was introduced and an updated perspective on this classical area of security was presented. In the next chapter, the problem statement that drives the research in this dissertation is presented.

# Chapter 4

# Problem Statement

Malware, in general, has proven effective at leaking highly sensitive information from government institutions and corporations in the past. Symantec estimates that over 552 million identities were exposed in 2013 alone by malware [225]. Moreover, there have been a seemingly endless stream of high-profile data breaches over the last few years, including: the data breach at the Office of Personnel Management in the US, which saw the social security numbers of 21.5 million individuals and the digital fingerprints of 1.1 million individuals leaked [179]; the data breach at Sony Pictures Entertainment, which saw their employee's personally identifiable information and confidential information leaked as well as their infrastructure destroyed [63]; and the data breach at the retail store Target which saw 40 million credit cards stolen [229].

A mitigating measure that corporations and government departments could follow to protect against this type of attack would be to move sensitive information offline to a system that is not accessible to the Internet. In fact, this is the strategy that is recommended by security experts (see Schneier [204] and the Head of the NSA's Tailored Access Operations department recommendations on protection [253]). Simply relying on this separation is potentially shortsighted, however, as there have been a number of real-world examples (e.g., Stuxnet [62], Gauss [107], and Fanny [109]) as well as research papers published [4, 11, 19, 20, 53, 61, 83, 89, 90, 93, 107, 109, 126, 134, 154, 175, 178, 181, 223, 232, 233] that demonstrate techniques to leak information from disconnected systems. It is the goal of this thesis to categorize these techniques, propose a methodology to evaluate the risk that they pose, and provide guidelines that can be followed to reduce their threat.

The specific problem that is addressed throughout the remainder of this dissertation is the risk that air-gap covert channels pose to the confidentiality of information stored on disconnected systems. This class of covert channel is currently a threat to systems deployed in the intelligence sector [151, 194], military sector [140, 194], critical infrastructure sector, including areas where SCADA and ICS systems are deployed [28], and in the financial sector [140]. In this work, the potential methods that malware could use to leak sensitive information from air-gapped systems are enumerated and a comprehensive catalogue of techniques is compiled (**Chapter 5**); a methodology is proposed to evaluate the risk of air-gap covert channels (**Chapter 6**); techniques from a specific class of air-gap covert

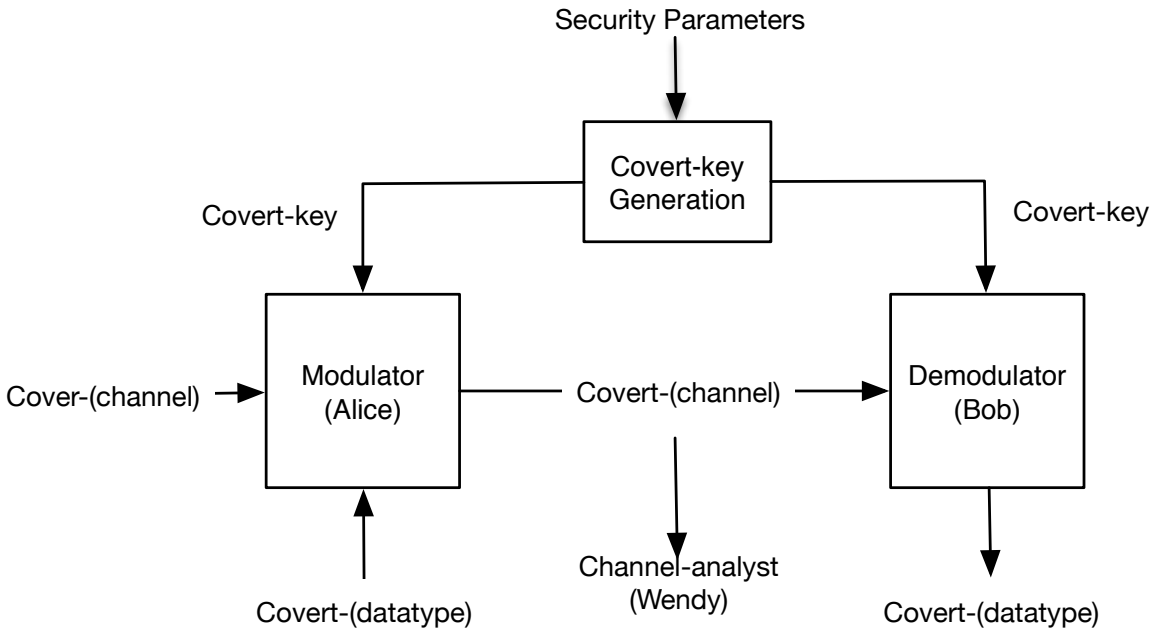



Figure 4.1: Basic Covert Channel Model with Terminology

channel, covert-acoustic channels, are developed and used to quantify the risk that this class of channel poses to secure systems (**Chapter 7** and **8**); appropriate countermeasures are developed (**Chapter 8**); and, lastly, appropriate guidelines that should be employed to protect against covert-acoustic channels are proposed (**Chapter 8**).

## 4.1 Terminology and Model

Beyond using the names of Alice and Bob to represent the parties interested in covertly communicating and the name of Wendy (or sometimes Eve) to represent the party interested in detecting their communication, no formal, comprehensive, agreed-upon terminology exists in the covert channel literature. The pioneers of information hiding, however, did define terminology for their area of study [187], which is adopted in this work and adapted to fit with the study of covert channels.

In this work, covert communication occurs in *simplex* or *duplex* mode between a *modulator* (Alice) and a *demodulator* (Bob). The *modulator* takes as input a *covert-(datatype)* message as well as *covert-key(s)* to modulate data symbols onto a *cover-(channel)* to produce a *covert-(channel)*. The *(datatype)* of the message is specific to the type of data being modulated (e.g., text, image, audio, etc. resulting in covert-text, covert-image, covert-audio, etc., respectively) and *(channel)* is named after the physical channel used to transmit *(datatype)* data symbols (e.g., acoustic, seismic, light, etc. resulting in covert-acoustic, covert-seismic, covert-light, etc., respectively). The *covert-key* used in the modulation process can either be the same as the key used during demodulation and results

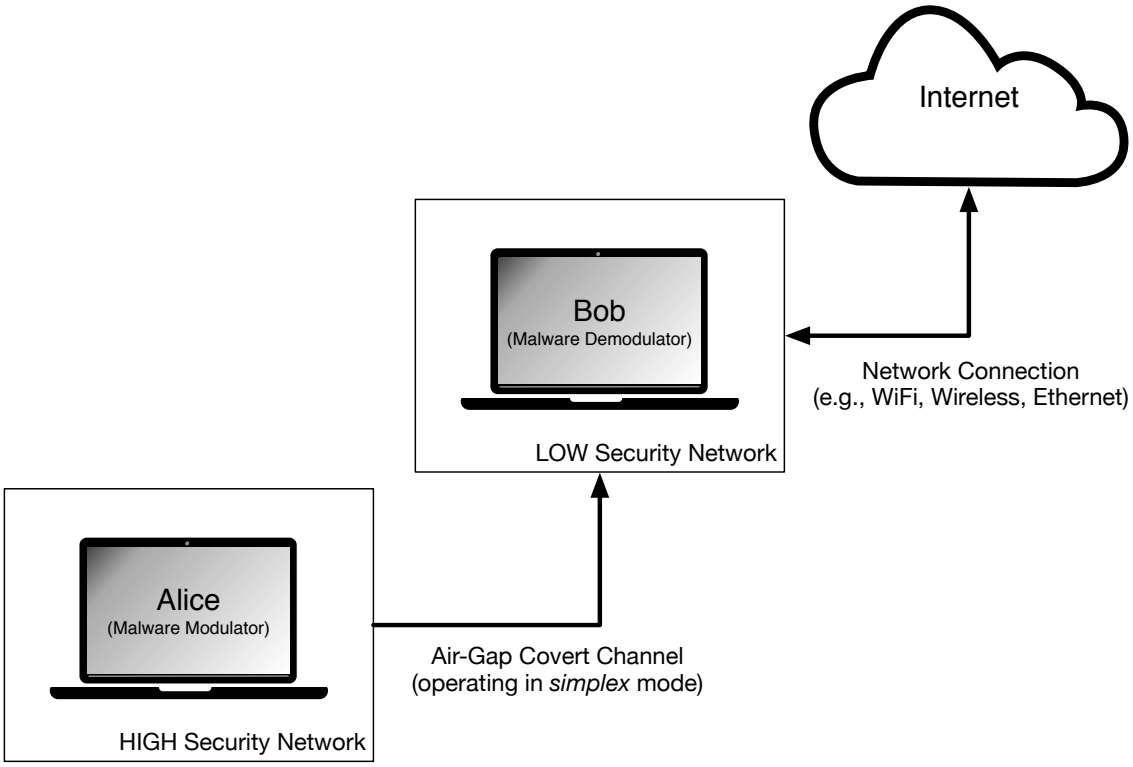



Figure 4.2: The *Prisoners Problem* in the Context of an Air-Gapped System

in a *symmetric-key covert channel*, or the *covert-keys* can be different resulting in an *asymmetric-key covert-channel*. Furthermore, the *covert-key(s)* generated are dependent on the *security parameters* of the system. Lastly, the *channel-analyst* (Wendy) has shared access to the *covert-(channel)* and, therefore, takes as input the messages that the *modulator* transmits on the *covert-(channel)*. This terminology is applied to the basic security model first introduced in **Chapter 1** in **Figure 4.1**.

This dissertation analyzes the solitary confinement problem in the context of two systems, HIGH and LOW, that are physically and electronically separated from each another. The modulator, Alice, and demodulator, Bob, both represent malware components operating on separate systems; Alice is a HIGH system component operating on a HIGH security network which contains sensitive information that must remain inaccessible to LOW system components and Bob is a LOW system component operating on a LOW security network (see **Figure 4.2**). As a reminder, the solitary confinement problem from the perspective of the modulator and demodulator is, therefore, to:

1. find a channel to communicate over such that:

   (a) the modulator, Alice, can modulate data symbols by effecting changes in the channel, and

   (b) the demodulator, Bob, can observe changes in and demodulate the changes into data symbols;

2. agree upon a modulation and demodulation scheme; and,

3. secure the channel such that the channel-analyst, Wendy, cannot detect that communication is taking place.

The problem from the perspective of the channel-analyst, conversely, is to detect or disrupt Alice and Bob's communication.

Summarizing the detection aspect of the problem mathematically, let $P_D$ be the probability that Wendy detects that Alice and Bob are communicating. The problem from the perspective of the prisoners is to secure their communication such that $P_D \to 0$, and the problem from the perspective of Wendy is to devise a scheme such that $P_D \to 1$. Moreover, given that Wendy is interested in eliminating or disrupting communication between the prisoners, let $P_E$ be the probability that the message that Alice transmits to Bob is not received by Bob. The problem for Alice and Bob is to ensure that $P_E \to 0$ and the problem from the perspective of Wendy is put in place a system such that $P_E \to 1$. Fundamentally, of course, Alice and Bob wish to be able to communicate at some positive rate, $R$, and Wendy is motivated to use whatever means possible (e.g., detection, elimination, or disruption), to ensure that $R = 0$.

## 4.2 Scope

This thesis focuses on the study of *air-gap covert channels* that are enabled by *semi-invasive* and *non-invasive covert exploits*, i.e., channels that are enabled by software modification or no modification at all. Throughout this work, channels that fit these criteria are referred to as *out-of-band covert channels* (OOB-CCs) because they provide communication outside of traditional network protocols:

**Definition 4.1.** An **out-of-band covert channel** is a covert channel that uses *semi-* and *non-invasive* covert exploits to enable communication between isolated systems (i.e., systems that are not able to communicate through traditional links).

The use of *invasive covert exploits* is a potential risk to air-gapped systems, however, the scope of this work is restricted to *semi-invasive* and *non-invasive covert exploits* for the following reasons:

First, the vast majority of studies on single-host and network covert channels assume that there is no physical modification to the systems that they are exploiting. In general, studies on covert channels assume that the communication endpoints are required to leverage existing system resources, communication, and cryptographic protocols in order to communicate. The analysis in this work, similarly, examines air-gap covert channels that can be established using existing hardware (e.g., system components, device sensors, and peripherals) found on commodity computing systems. This study thusly focuses on non-traditional methods of communication that are established using commodity hardware

(e.g., display, speaker, microphone, CPU, light emitting diodes (LEDs), ambient light sensor (ALS), magnetometer, etc.).

Second, while the analysis in this work does pull from the literature on LPD systems, the focus of this work is not on traditional LPD communication problems [184, 189]. Traditional LPD communication systems solutions are not restricted to using the hardware found in commodity devices in order to facilitate communication. Moreover, the application of techniques developed in the LPD literature, which usually require communication at low SNR (e.g., below 0 decibel (dB)), is not directly applicable to the study of OOB-CCs given that commodity hardware devices are not designed for communication in general, let alone low SNR communication. So while the application of LPD systems might appear to be a trivial solution to the solitary confinement problem from Alice and Bob's perspective, there are practical reasons why their direct application is not suitable.

Third, also outside the scope of this work are hardware Trojans deliberately added to integrated circuits for the purpose of leaking sensitive information [4, 119, 139]. Hardware Trojans cover modifications to the host system through either circuit manipulation [119, 139] or the addition of special-purpose circuitry [4]. Typically, hardware Trojans are added to cryptographic processing systems to leak plaintext, the secret key used for encryption, or intermediate values used in the encryption process. In the literature, there are a number of techniques that hardware Trojans use to leak information: modulated power fluctuations [121], temperature fluctuations [119], and radio-frequency signals [4, 119]. These leaked side-channel signals are typically picked up by specialized hardware at the demodulator: e.g., simple power analysis (SPA) [121] and differential power analysis (DPA) [121], thermal cameras [119], or radio-frequency (RF) receivers [4, 119], respectively. Hardware Trojans, in the context of covert channels, require invasive covert exploits to enable communication as they rely on hardware modification at the modulator and specialized hardware at the demodulator.

In order to comprehensively assess the impact of *covert-acoustic channels* enabled by *semi-* and *non-invasive covert exploits*, the basic security model shown in **Figure 4.1** is studied under a number of additional assumptions and constraints. First, it is assumed that, prior to being thrown into solitary confinement, the prisoners agreed upon a modulation and demodulation scheme. Additionally, the achievable data rate of the covert channel that the prisoners collude to establish is first measured under the assumption that the covert-analyst only uses her natural senses to detect the communication and then again under the assumption that the covert-analyst employs an optimal detection device to detect their communication. Second, the *covertness* (i.e., the amount of data communicated without detection) of the covert channel is measured under the assumption that Alice and Bob only pre-share a modulation and demodulation scheme and then again under the assumption that they are also able to pre-share a *covert-key(s)* in secret from the channel-analyst, which can be used, as needed, to secure the communication channel between them. Third, the achievable data rate of the covert channel is also assessed under scenarios where the channel-analyst is "active." In these scenarios the channel-analyst actively injects interference into the communication channel in an effort to make it more difficult for the prisoners to communicate.

Importantly, throughout the analysis in this work it is always assumed that the channel-analyst is able to monitor all possible channels that are accessible to the prisoners and that the channel-analyst also has knowledge of the modulation and demodulation scheme chosen by the prisoners. The solitary confinement problem from the perspective of the channel-analyst is, therefore, to reduce the *covertness* of Alice and Bob's communication channel given the medium and modulation scheme that they use. However, while it is assumed that the covert-analyst is fully knowledgeable of the medium and modulation scheme used by Alice and Bob, *Kerckhoff's Principle* is followed, i.e., the covert-analyst is *not* aware of the *covert-key(s)* that the prisoners have pre-shared. This assumption is in line with Auguste Kerckhoff's principles of communications security [118], in which he cautioned that secure systems should not rely on the method used to protect data for security, but rather systems should rely only on the choice of key.

An analysis of OOB-CC alternatives is presented in the next chapter, **Chapter 5**, where the devices and channels that could be used to bridge the air-gap are surveyed and general conclusions are drawn.

# Chapter 5

# Out-of-Band Covert Channels

In this chapter, a survey of the literature related to *out-of-band covert channels* (OOB-CCs) is presented in **Section 5.1**. As a result of this survey, general countermeasures are summarized and it is empirically shown that the previous studies on OOB-CCs have relied on an oblivious passive adversary in order to remain undetectable. In **Section 5.2**, a novel taxonomy of OOB-CCs is documented, which categorizes OOB-CCs based on their modulator and demodulator hardware requirements as well as their prevalence in commodity systems. The survey and conclusions drawn in this chapter help support the study of covert-acoustic channels in more depth in **Chapter 7** and **Chapter 8**.

In the next section, **Section 5.1**, the literature on covert channels, side channels and device pairing is summarized and channels that could be used as OOB-CCs are presented. The areas of side channel attacks (see [254] for an overview of the subject) and device pairing (see [120, 127] for an overview of the subject) were chosen because they have similar requirements, i.e., non-traditional forms of communication, to OOB-CCs. The research in the area of side channel attacks examines unintentional leakage of information (usually plain text or cryptographic keys) from secure systems, where the sender unintentionally leaks data and only the receiver is interested in successful reception of the communication; the relevant TEMPEST literature [238] is also reviewed as part of the survey. Additionally, given the vast number of side-channel attacks in the literature, only techniques that fit within the scope of this dissertation are reviewed, namely side channel attacks that do not require hardware modification (i.e., non-invasive side channels, see [16]). Furthermore, covert channels that fall within the definition of OOB-CCs but, to date, have not been categorized as such are also reviewed. Lastly, the literature on device pairing, which covers out-of-band channels as well as side channels (e.g., light, audio, seismic) is covered as well. These device pairing communication channels are used to bootstrap other protocols (e.g., secure sockets layer (SSL), network joining, etc.) as well as provide alternatives (e.g., audio communication) to traditional forms of communication (e.g., Bluetooth, near-field communication (NFC), etc.). These channels are all reviewed because their techniques could possibly be directly applied or slightly modified to satisfy the requirements of OOB-CCs.

There is a subtle yet clear distinction to be made between device pairing and OOB-

CCs. Work in the device pairing literature examines communication alternatives that are resistant to eavesdropping and man-in-the-middle attacks by creating authenticated out-of-band channels (A-OOB) [86]. Device pairing solutions rely on the fact that a human is a participant in the pairing process in order to ensure it is authentic, either actively, by participating in the protocol (e.g., clicking buttons, shaking devices, etc.), or, passively, by simply pointing their device at another device and letting the pairing protocol run. Furthermore, by utilizing out-of-band channels that are configured to communicate over short distances, the device pairing channel is assumed to also be secret, i.e., the assumption is that an eavesdropper cannot listen in on the exchange because of the attacker's distance from the transaction [86]. However, researchers have shown that in addition to humans being able to perceive these out-of-band device pairing channels, technical solutions can also be developed to eavesdrop on secret and authenticated out-of-band device pairing channels (AS-OOB) [86]. OOB-CCs, on the other hand, as defined, require no human intervention and are established to avoid both human perception as well as detection by a third party who has access to technical tools.

## 5.1 Survey of Out-of-Band Covert Channels

In this section, the different channels that possibly could be built upon to establish an OOB-CC are reviewed. Each channel's achievable data rate is noted, the limitations of each channel is discussed, and the hardware required for the modulator and demodulator to utilize the channel is documented. Moreover, relevant protection mechanisms that could be put in place to limit or eliminate the proposed covert channel are discussed and the *undetectability* of each channel is qualitatively presented. The survey in this section is separated into six sub-sections, each covering a specific *(channel)*:

1. Acoustic
2. Light
3. Seismic
4. Magnetic
5. Thermal
6. Radio-frequency

### 5.1.1 Out-of-Band Covert-Acoustic Channels

Utilizing covert audio signals for the purposes of leaking information from air-gapped systems has previously been discussed [53, 89, 90, 131, 181]. Hanspach, et al., built a proof-of-concept covert network with five identical Lenovo laptops and demonstrated that audio communication can be achieved in the near-ultrasonic range from 17 kHz to 20 kHz [89].

Their research demonstrated that frequency-hopping spread spectrum (FHSS) with 48 sub-channels can be used to effectively establish a covert channel capable of transmitting data at a rate of 20 bits per second (bps) up to a distance of 19.7 m. Hanspach, et al., documented the ability to communicate using two Lenovo T400 model laptops, over the ultrasonic range from 20.5 kHz to 21.5 kHz at a speed of 20 bps up to a range of 8.2 m [90]. O'Malley, et al., established a covert channel between a MacBook Pro and a Lenovo Tablet using Frequency Shift Keying (FSK) in the ultrasonic range between 20 kHz and 23 kHz; however, the authors used an external speaker at the transmitter to achieve their results [181]. Additionally, Deshotels demonstrated the ability to communicate information between mobile Android devices using audio signals between units separated by 100 feet. Deshotels was able to achieve over 300 bps using FSK in the 18 kHz to 19 kHz bandwidth [53]. Lastly, Lee, et al., demonstrated that a loudspeaker could be converted into a microphone and used for covert-acoustic communication at low bit rates [131].

The use of audio has also been researched as an alternative to traditional wireless communication (e.g., infrared (IR), Bluetooth, RF, Wi-Fi, and NFC); however, due to the relatively low bandwidth available in the channel when compared to IR and RF as well as the negative impacts of audio on humans and animals, this alternative solution has been primarily only studied in academic circles [73, 129]. Gerasimov, et al., studied the use of audio communication over-the-air for the purpose of device-to-device communication and were able to achieve a bit rate of 3.4 kbps using spread spectrum techniques in the 0 Hz to 20 kHz bandwidth [73]. Researchers also examined the ability to communicate using pleasant sounding audio signals in order to exchange pre-authorization information for joining wireless networks as well as uniform resource locators (URLs) [145, 146, 147]. The researchers synthesized audio signals using frequencies from musical scales, chords, and lullabies as well as from fictional characters (e.g., R2D2 from Star Wars) and insects. Similarly, Domingues, et al., studied the ability to communicate using audio signals that sound like musical instruments (e.g., piano, clarinet, and bells) [55]. Madhavapeddy, et al., examined audio communication as an alternative to Bluetooth wireless communication through the use of dual-tone multi-frequency (DTMF) signalling, on-off keying (OOK) and melodic sounds. Madhavapeddy, et al. also studied ultrasonic communication between two laptops with third-party speakers [149, 150]. Lastly, Nandakumar, et al., experimented with audio communication as an alternative to NFC [176]. In their work, the authors also presented *Jam Secure*, a self-interfering technique to provide information-theoretically secure communication. *Jam Secure*, however, uses audible signals to secure the communication which can easily be detected by both humans and technical equipment.

Side channel attacks that recover information from leaked acoustic signals have also been presented in the literature. Tromer demonstrated that CPUs in modern machines leak a specific acoustic signal related to the operation being performed [232, 233]. Using an external microphone, the researchers were able to pick up specific acoustic signatures during common CPU operations (e.g., HLT, MUL, FMUL, ADD, etc.) as well as common cryptographic operations (e.g., RSA decryption). The researchers found that the leaked audio signals emanated from capacitors on the motherboards that they studied. The work of Tromer was extended by LeMay and Tan in which they demonstrated that covert data could be leaked using acoustic signals by varying the algorithms executed on the CPU of

the modulator [134]. The acoustic signature generated by each algorithm could then be detected by a demodulator to recover the transmitted data. Recent work has demonstrated that not only can specific algorithms executed on remote machines be identified, but that the contents of RSA private keys can as well [72]. Genkin, et al., demonstrated that by performing a chosen plain-text attack against a target, the target's RSA private key can be recovered [72]. In their research, they were able to recover key material by analyzing the acoustic signals captured by the built-in microphone of a mobile device that was placed 30 cm from the target. Performing the same attack using specialized equipment (e.g., a parabolic microphone) allowed the researchers to recover the target's private key at a distance of over 4 m.

### Limitations

Interference in the context of acoustic communication can be caused by background ambient noise; however, the background noise in office environments is larger for frequencies below 3 kHz, and tapers off as frequency increases (see **Chapter 7**). Given that sound is a slow moving signal (about 340 m/s in air) the modulator and demodulator must account for delays as well as changes in the channel impulse response in time as well. Furthermore, Doppler effect must be accounted for if either the modulator, demodulator, or both are moving while communication is taking place. Lastly, reflections of audio signals off of objects in the environment can also cause significant echo (i.e., reverberations) which can result in inter-symbol interference.

### Device Requirements and Bandwidth

Given the research in the area, acoustic signals can be generated by a modulator either by sending audio signals to a speaker or by executing specific algorithms on its CPU. Producing audio signals by executing specific algorithms is a particularly insidious method for generating covert signals as all machines must have at least one CPU to operate and thus no additional hardware is required. On the other hand, speakers are either optional or can be physically removed. Audio signals can be produced using commodity speakers in at least the 0 Hz to 22 kHz range; some add-on speakers demonstrate frequency responses much higher than 22 kHz. Furthermore, the electronic components on motherboards (e.g., capacitors, coils) can produce signals at frequencies at least as high as 40 kHz. More research is required to determine the true low-pass frequency of CPU acoustic emanations and if all frequencies under 40 kHz are accessible to the modulator. On the demodulator end, commodity microphones installed in most laptops, mobiles, and USB headsets can detect audio signals upwards of 22 kHz with various degrees of fidelity and, therefore, acoustic communication between unmodified systems appears to be possible over the 0 Hz to 22 kHz bandwidth. In **Chapter 7**, however, it is demonstrated that the upperbound for frequency support can be pushed as high as 23 kHz on some systems.

### Detectability of Covert-Acoustic Communication

In this chapter, the detectability of audio signals is examined by qualitatively analyzing the ability of an adversary to detect covert communication given knowledge of the medium and modulation scheme. In the works that were studied in the preparation of this section, the authors' claims of creating a covert channel were based on their adversary's naïvety regarding the use of audio signals for communication. Techniques such as communicating via ultrasonic signals or audible signals, rely on the fact that humans are not able to perceive the signals using their natural ability to hear. Furthermore, the undetectability of audio signals generated by CPUs rests on the signals being of very low power and therefore only faintly audible to humans present in the environment. In other words, the reviewed covert channels relied on "security through obscurity." In all the cases that were studied, knowledge of the medium implied detection. Covert-analysts (i.e., Wendy) concerned with protecting themselves against this type attack could easily detect the covert communication by tuning their equipment to the correct frequency(ies). A number of the modulation schemes that were covered in this section were based on spread spectrum techniques (e.g., FHSS and DSSS); however, none of the authors presented results showing the use of spread spectrum techniques in low SNR configurations, where the signal power is constrained to be lower than the noise power in order to hide the signal. The use of spread spectrum techniques combined with low SNR signals is a known method for hiding communication from adversarial detection [189] and has previously been applied to audio signals in the area of underwater covert audio communication (see [135, 141, 239]). The result of applying spread-spectrum modulation to covert-acoustic signals is covered in **Chapter 8**.

### Defence Mechanisms

A number of defence mechanisms have been presented by various authors to either prevent or detect covert audio communication. Hanspach, et al., proposed the use of a low-pass filter to remove all ultrasonic signals from audio tracks before they are played by the system's speakers [89, 90]. The same authors also proposed the use of a host-based audio intrusion detection system (HIDS) tuned to detect the leakage of information via audio signals. While potentially effective, a HIDS suffers from the fact that all parameters of the attack must be known before a signature can be generated. This might be difficult, if not impossible, where spread spectrum techniques are used and the pseudorandom spreading sequence is generated in a sufficiently random fashion. All authors also proposed the obvious protection mechanism of physically removing the speakers and microphones from machines that do not require them or disabling them in software. Malware, however, could potentially enable the devices if they are simply disabled in software. Other defence mechanisms that should be further explored include wideband and narrowband jamming (see **Chapter 8**), depending on the modulation scheme used by the covertly communicating partners [189]. To protect against acoustic signals produced by devices on CPU motherboards, researchers have proposed placing the leaky devices in sound-proof chambers as well as covering the devices in acoustic shielding [232, 233]; however, the authors pointed out that the source of the acoustic signals was typically vent holes, which cannot be covered, as they are required

to prevent the machine from overheating. The introduction of random operations by the CPU is also a potential defence mechanism worth exploring.

### 5.1.2 Out-of-Band Covert-Light Channels

Light communication for the purposes of malware command and control has also been explored in the literature by Hasan, et al. [93]. In their work, the researchers performed two light-based communication experiments. First, a modulator was implemented to modify the intensity of a light source in a room such that a demodulator could detect the intensity changes using a mobile phone's ambient light sensor (ALS) [93]. Secondly, the authors displayed a "trigger" image on a liquid crystal diode (LCD) monitor, laptop display, and 47" LCD TV and used an ALS to pick up the trigger. The authors performed range and angle tests to determine the maximum bit rate they could achieve and determined that light-based signals can be used to establish a very low bit-rate covert channel.

To date, the use of light signals to pair devices has also been explored by many researchers. Balfanz, et al., used IR signals, a privileged side channel, between two devices to exchange pre-authentication information, i.e., commitments on public keys, to bootstrap key exchange in ad-hoc wireless networks [22]. The initial exchange of commitments was done over the IR channel since it was assumed that the channel provided "demonstrative identification," that is, channel authentication given IR's limited range and line of sight restriction. Additionally, McCune, et al., used barcodes, both printed and displayed on a screen, to communicate pre-authentication information, i.e., hashes [157]. In their *Seeing-is-Believing* protocol, the modulator displayed a barcode (or a series of barcodes) and the demodulator took a photo of the barcode to extract the hash from the captured image. Mutual entity authentication is supported, but requires both devices to have a display and a camera. Saxena, et al., created a device pairing scheme based on blinking light emitting diodes (LEDs). The modulator required two LEDs (or a display), one for data exchange and one for synchronization, while the demodulator required a camera [200]. Their scheme exchanged short authenticated strings (SAS) [240] to authenticate the communicating parties' public keys. Data is communicated by having one device modulate data by blinking its LEDs and the other capture and process images of the blinking LEDs. As a follow up to this work, Sexena, et al. created a protocol to attain mutual entity authentication with only one use of the out-of-band channel [202]. Their algorithm, however, required a human to interact with one of the devices to complete the protocol. Similar LED-based approaches are discussed to perform key assignment in ad-hoc wireless sensors networks as well [71, 183, 196].

Side channel attacks based on optical emissions, "Optical TEMPEST," has also received attention in the research community. Kuhn showed that the contents of cathode ray tube (CRT) monitors could be reconstructed by analyzing the light intensity of the display's diffuse reflection off a wall [126]. Reconstruction of the screen's contents was possible because the light intensity of the last few thousand pixels drawn by a CRT leaked a low-pass filtered version of the video signal. Using signal processing techniques and specialized hardware (e.g., photomultiplier and photosensor), a reading chart displayed on the screen

could be reconstructed by processing the screen's reflections. According to Kuhn however, LCD monitors are not susceptible to the same light intensity attack [123]. Backes, et al., showed that the contents of liquid crystal diode (LCD) screens could also be reconstructed by analyzing diffuse reflections off objects in the environment (e.g., teapots, eyeglasses, bottles, spoons, and a wine glass) [19]. The authors showed that 18 pt font displayed on a screen and reflected off a teapot could be reconstructed from up to 10 m away. Furthermore, by using telescopic lenses their attack could be extended to 30 m - a realistic distance between two buildings. Backes, et al. followed up their compromising reflections work by improving their attack through the use of a deconvolution algorithm and showed that reflections off more objects in the environment (e.g., human eye, shirt) could be used to reconstruct the screen's contents [20]. Similarly, Raguram, et al., were able to reconstruct characters typed on the LCD screen of an iPhone by analyzing reflections of the screen off objects in the environment [191]. Their work demonstrated that using a commodity camera, captured images of both the screen directly as well as its reflection could be analyzed to extract typed key sequences by looking for the "pop-out" keys displayed by the iPhone's virtual keyboard. Their attack was effective over distances up to 14 feet away. This work is significant because it represents a method of communication (or leakage) that is based on the normal function of the device, i.e., displaying an image on the screen, and not an unintended leakage produced by using the device. Lastly, Loughry and Umphress demonstrated that certain devices, namely network gear, leaked their internal state through the LEDs on their interfaces [148]. Given the speed at which LEDs can turn on and off, and the fact that a number of device manufactures tied their status LEDs to their devices' serial lines, the LEDs can be monitored by a simple photodiode, i.e., ALS, to read the data being processed.

### Limitations

Communicating via light intensity works best in low-light conditions where there is little to no ambient light in the room (e.g., overhead light, sun, television, etc.). Furthermore, a number of the results that were outlined in this section required the help of specialized hardware (e.g., astronomic telescopes in the works of Backes, et al., and a photomultiplier in the work of Kuhn), which are not found in commodity laptops, desktops or mobiles. Additionally, while IR transceivers were once typical in commodity hardware they are no longer as widely deployed as they used to be. Light communication also generally requires the receiving sensor to be unobstructed and therefore light communication will not work if the receiving device (e.g., camera, ALS) is stowed. Further research is required to determine if the cameras that are prevalent in today's mobile phones, laptops, and monitors are capable of capturing images that will allow reflections or off-angle views of the modulator's screen to be processed in order to facilitate communication.

### Device Requirements and Bandwidth

In order for light signals to be used, a light emitting device is required at the modulator, whether it be a screen (e.g., CRT, LCD, or LED) or status LEDs. On the other hand,

the demodulator either requires an ALS or a camera to pick up the transmitted signal. In the work of Hasan, et al., the authors were able to achieve a maximum bit rate of 0.5 bits per second with no bit errors using LEDs and an ALS [93]. McCune, et al., were able to achieve bit rates of around 580 bps using a screen and camera [157]. The bandwidth of their channel is highly governed by the choice of barcode displayed, i.e., the amount of data encoded in the barcode, and how long the barcode needs to be displayed in order for the demodulator to decode the message. Saxena, et al., required the LEDs to be lit for 250 ms in order for a bit to be communicated and, therefore, they were able to achieve a bit rate of approximately 4 bps using LEDs and a camera [200]. The goal of device pairing however is not necessarily to achieve the highest possible bit rate and it is often desirable for the communication to be slowed down so that the humans involved in the pairing process can visually validate what is going on. Gauger, et al., were able to achieve bit rates of up to 71 bps using the *sensor node lamp*, a specialized LED modulator, and 8 bps using the display of a mobile device [71]. Furthermore, Roman and Lopez achieved bit rates of 500 bps using their KeyLED scheme [196]. In general, the bit rate of light communication will be governed by the maximum rate that the modulator can update its display and the sampling rate of the demodulator. Further research is required to determine the maximum rate at which data can be communicated between commodity hardware using light communication in typical usage environments (e.g., office, home, etc.).

#### Detectability and Defence Mechanisms

The goal of Hasan, et al., was to create a covert command and control network based on light signals [93]. Communication was facilitated through small fluctuations in the overhead light to modulate data, which presumably were unnoticeable to any humans in the environment. This too is a form of "security through obscurity" as any entity monitoring the light intensity in the room would be able to detect that "covert" communication is taking place. Additionally, Gauger, et al., and Perkovic, et al., made the assumption that no adversary had access to the light-based communication channel [71, 183]. This is a weak security assumption, but one that is perhaps valid in the context of initial key assignment and shows that more research is required to develop ways to communicate using light in an undetectable way. The main defence against information transfer via light is to either reduce the brightness of the modulator, i.e., display, or shield it. Filters can also be added to displays to reduce their viewing angle and polarized filters that are 90° offset from each other can be placed on screens in the room as well as on the room's windows to prevent signals from leaking outside the room. Jamming, by ensuring high levels of ambient light, can also be used to reduce the risk of diffuse reflections. Additionally, to limit the channel's bandwidth, operating systems can either prevent access to the status LEDs on devices or limit the rate at which status LEDs can be turned on and off.

### 5.1.3 Out-of-Band Covert-Seismic Channels

Hasan, et al. also explored covert malware communication through vibration signals by describing two methods that a modulator could use to create vibrations: playing an audio

track with low-frequency content and activating the vibrator in a device [93]. Creating vibrations using audio equipment is especially effective if the machine under the control of the modulator has a sub-woofer or speakers with an ideal frequency response in the low-frequency range. Hasan, et al., hypothesized that low-frequency audio signals could be imperceptible to humans but detectable using commodity microphones at a distance of a few feet. The authors also described a method to transmit communication signals through enabling and disabling a mobile phone's vibrator; however, the vibration signals were shown to have a high latency and were only detectable from a few centimetres away. Subramanian, et al., similarly, demonstrated that malware communication could also be accomplished through vibrations [223]. Furthermore, researchers have shown that by utilizing the vibrator and accelerometer on the same device, a host-based covert channel can also be established [11, 53]. Deshotels demonstrated that Android devices, in contact with one another, could communicate using vibration signals lasting as little as 1 ms [53]. Interestingly, the vibration signals used in Deshotels' work were imperceptible to humans.

Seismic-based communication has also been used in device pairing applications. Saxena, et al., devised PIN-Vibra, a protocol between a vibrator-equipped mobile device and an accelerometer-equipped radio-frequency identification (RFID) tag [201]. The authors used OOK and a 200 ms symbol time, i.e., vibration time, to transmit information. Their scheme was built on the assumption that the vibration channel was authenticated (user pressed the vibrating mobile phone against a specific RFID tag) and secret (user could verify that no eavesdropper was also simultaneously in contact with the mobile phone), however, Halevi and Saxena demonstrated that the mobile phone's vibrations produced an acoustic signal which could be picked up by a commodity microphone from up to three feet away [86]. Additionally, Studer, et al., proposed an alternative to the widely popular Bump protocol [222, 245]. Bump is a protocol that allows users, having no pre-shared keys, to exchange information in a more secure manner by incorporating accelerometer readings taken while bumping their phones together. Studer, et al., were able to show that a man-in-the-middle attack could be launched against the protocol and proposed an alternative protocol, Shake on it (SHOT). Their protocol used the vibrator in one phone to send a pre-authenticator hash to another phone in contact with it. The pre-authenticator hash was then subsequently used to verify the transmitter's public key, which was exchanged over a traditional wireless link. Lastly, Marquardt, et al., were able to demonstrate a side-channel attack to reconstruct the keystrokes typed on a keyboard located in close proximity to an accelerometer-equipped cell phone [153]. The authors remarked that the mobile phone could only determine the keystrokes pressed if the mobile was within a couple of inches from the keyboard.

### Limitations

The biggest current limitation of the vibration channel, in the context of OOB-CCs, is that over-the-air communication has not been demonstrated to be possible. Additionally, as demonstrated by Marquardt, et al., the vibration signal can only be detected over a short distance [153]; however, more exhaustive testing is required to determine the maximum distance vibrations can travel given common mediums (e.g., desk, table). Path loss

in the vibration channel has been shown to be dependent on the distance between the communicating devices, the velocity of the vibrations, and the medium the vibrations are travelling through. Furthermore, Deshotels argued that vibrations induced by a speaker could be detected up to a few feet away [53]; however, the authors did not test their hypothesis. Lastly, as is the case with acoustic channels, vibration signals suffer from a high degree of latency, which must be taken into account at the demodulator.

### Device Requirements and Bandwidth

Seismic-based channels are transmitted by a modulator with commodity hardware through controlled vibrations using a speaker or vibrator, and are received by a demodulator through readings from an accelerometer. Subramanian, et al., demonstrated bit rates up to 65 bps using a vibrator and accelerometer [223]; however, the vibrations were not meant to be undetectable to users in the environment, but rather, were made to be covert by mimicking the same vibrations generated when an incoming call is received. Studer, et al., were able to achieve 17 bps using the same devices. In both cases, however, the vibrator and the accelerometer were in mobile devices that were placed in contact with one another [222]. Therefore, a bit rate of tens of bits per second most likely represents an upper bound on the amount of data that can be exchanged using the vibration channel established when commodity hardware is used.

### Detectability

As previously mentioned, Deshotels generated vibrations in such a way that the signals were not perceptible to humans because short signal periods were used, i.e., 1 ms. Similarly, the low-frequency audio signals hypothesized by Hasan, et al., were presumably of low enough amplitude and frequency that the amplitude of the signals fell below the human auditory threshold for a given frequency. Both of these solutions generated signals that were imperceptible to humans, but perceptible to correctly-tuned commodity hardware devices without reliance on a secret key. Further research is required to determine if vibration-based channels can even be established in an undetectable manner. Mimicking environmental vibrations, i.e., treating the channel as a *steganographic channel*, is an alternative that should be further explored to meet the undetectability requirement [223].

### Protection Mechanisms

To protect against covert vibrations generated through low-frequency sound, a high-pass filter could be applied to all audio tracks before they are amplified by the speaker. Furthermore, access to the vibrator and accelerometer could be monitored to ensure the device is not being abused. Additionally, systems that do not attach explicit user-controlled permissions to the vibrator and accelerometer should add mandatory access control policies that would limit liberal use of these components. Lastly, the sensitivity of the accelerometer should be reduced to the point where it still provides utility to generic application developers, but limits the covert communication bandwidth possible.

### 5.1.4 Out-of-Band Covert-Magnetic Channels

Hasan, et al. also explored malware command and control through magnetic signals [93]. The authors described a malware triggering method detectable by a demodulator equipped with a magnetometer (i.e., e-compass), which is a component that can be found in most modern-day mobile phones to provide compass functionality. The authors modulated signals by using a programmatically-controlled electro-magnet to induce changes in the detected magnetic field of the magnetometer and noticed that a 60 microtesla signal could be observed at a distance of five inches away from the demodulator device and error-free communication was possible over a distance of 3.5 inches. Their experiments also showed that triggering via magnetic field was not negatively impacted when the electro-magnet (modulator) was covered by clothing. Given this property, the authors concluded that a magnetic trigger could be covertly installed at a choke point where multiple magnetometer-equipped devices pass through (e.g., elevator, doorway).

A number of patents have also been filed documenting the ability to pair devices using magnetic signals. Libes proposed the use of add-on peripherals, capable of sending and receiving magnetic signals, in order to create an alternative wireless communication link between devices in close proximity to each other [138]. The authors also proposed using the magnetic wireless link for bootstrapping traditional wireless communication. Similarly, Hanna, et al. described a method for bootstrapping wireless communication by exchanging credentials over a magnetic wireless link [88]. The pairing protocol was designed to replace the traditional simple pairing protocol used to allow Bluetooth-enabled devices to communicate. Lastly, researchers have proposed the use of magnets to induce faults in cryptoprocessors in order to mount side-channel attacks [75, 198].

#### Limitations, Device Requirements, Bandwidth, Detectability, and Protection Mechanisms

There are a number of limitations to the magnetic channel. Firstly, a transmitting device (i.e., (electro-)magnet) is not typically found in commodity devices and therefore external hardware would be required to realize this channel. Secondly, magnetic field strength dissipates quickly as distance is increased because the field's strength is inversely proportional to the distance cubed. Thirdly, all the works covered in this section only describe communication over a distance of at most six inches (the distance achievable is proportional to the strength of the electro-magnet used for modulation). Magnetometers are also designed to monitor the earth's natural magnetic field (i.e., noise) and therefore any received magnetic signals from the channel must be stronger than those coming from the earth, which were measured at between 30 and 50 microtesla [93].Additionally, while magnetic fields can travel through non-metallic objects, the presence of metal will cause interference. Finally, in order for magnetic signals to be used, a large amount of current, 500 A, is required to induce a magnetic field even over a distance of just 1 m (note that 1 A is enough to cause electrocution) [81].

From a demodulator's perspective, magnetometers are prevalent in today's modern mobile phones and have a sampling rate of anywhere from 100 kHz to 400 kHz; however,

further research is required to determine realistic achievable bit rates using the magnetic channel. From a protection point of view, the most obvious physical safeguard would be to place the device in metal shielding; however, confining devices to a shielded room is most likely impractical in areas other than high security zones. Furthermore, generally applying metal shielding would cause interference to traditional RF signals. Lastly, none of the works studied explicitly took undetectability into account and it is presumed that a covert-analyst that has knowledge of the algorithms used in these works would be able to detect the channel using technical tools. Going forward, schemes such as spread-spectrum modulation [184] at power levels below that of the earth's magnetic field should be explored as a possible solution to hide covert-magnetic channels from a passive adversary.

### 5.1.5 Out-of-band Covert-Thermal Channels

While examining the problem of deanonymizing Tor hidden services, Murdoch first introduced the concept of temperature-based covert channels [175]. In his work, Murdoch demonstrated that a process (modulator) could increase the CPU load on a machine in order to cause a rise in the machine's internal temperature and, causally, an increase in the machine's clock skew (i.e., a delay in the clock signal). Furthermore, Murdoch showed that a machine's clock skew could be monitored by a remote process (demodulator) by observing the machine's TCP timestamps. Given the causal relationship between increased CPU load and clock skew, a covert channel could be created between two remote processes. Additionally, Murdoch showed that a server's CPU load could also be increased remotely by initiating additional network traffic to the server. By combining the abilities to remotely increase CPU load and observe timestamps, Murdoch was able to demonstrate a novel network covert channel. Murdoch finally demonstrated that hidden services on the Tor network could be exposed through the use of this covert channel.

Murdoch also hypothesized that two processes, running on two different machines, *Server A* and *Server B*, could covertly communicate: a modulator on *Server A* would increase the CPU load on its server which would in turn increase the temperature of *Server A*; a demodulator on *Server B* would then measure *Server B*'s clock skew to demodulate the information transferred by the modulator [175]. Although Murdoch presented this idea, which could be used as an OOB-CC, no bit rates were provided. Mirsky, et al., demonstrated how an Internet-connected air-conditioning system could be remotely controlled by an attacker to send commands to malware on an air-gapped system using a simplex covert-thermal channel [166]. By remotely increasing and decreasing the temperature of the physical spaces where air-gapped systems were present, the researchers showed that a low bit-rate channel could be established between systems on a public network and air-gapped systems. This work built on their previous research where they showed that a half-duplex covert-thermal channel could be established by increasing and decreasing the CPU load on one system and measuring the resulting temperature changes using the internal thermal sensors of nearby systems [84]. Lastly, while the work was not necessarily presented in a covert channel context, researchers have proposed the use of temperature-based proximity sensors to facilitate device pairing [45, 195] as well as the induction of temperature-based faults into crypto-processors to make side channel attacks possible [137].

#### Limitations, Device Requirements, Bandwidth, and Protection Mechanisms

The thermal communication channel that was measured in Murdoch's work [175] was shown to be of extremely low bandwidth, on the order of about $10^{-4}$ Hz [175, 251]. Similarly, the covert-thermal channels presented by Mirksky, et al. [166] and Guri, et al. [84], demonstrated bit rates of 40 and eight bits per hour, respectively. Therefore, the bit rates achievable using the covert-thermal channel range in the tens of bits per hour; however, low-bandwidth information, i.e., passwords, could still be leaked using a temperature-based channel over a long period of time (see the small message criterion [171]) and Guri, et al., where able to demonstrate bi-directional communication between air-gapped systems. In conclusion however, known thermal covert channels do not form a viable general-purpose covert communication channel and are more appropriate for basic signalling between networks. On the other hand, thermal channels do have one major advantage in that they do not require any additional hardware at the modulator or demodulator and thus there are no additional hardware requirements in order for the covert channel to be established.

Zander, et al. outlined a number of possible protection mechanisms for temperature-based covert channels [251]. They proposed the use of a clock crystal producing a regular clock signal that is not influenced by temperature. Additionally, they proposed throttling network traffic or CPU load to further reduce the bandwidth of the channel, removing all timestamps from network protocols (e.g., TCP timestamps), as well as introducing noise, by either running the CPU at 100% utilization at all times, or spiking the CPU to 100% utilization at random intervals. Mirksky, et al. proposed placing temperature sensors in all areas where air-gapped systems are present to monitor the environment for temperature fluctuations; however, the researchers did not provide detection rates using this method [166]. Moreover, the researchers also proposed protecting the heating, ventilation, and cooling (HVAC) system from remote attack by moving it off of the Internet.

### 5.1.6 Out-of-band Covert-RF Channels

According to Highland [95], government agencies have known about the possibilities of compromising electromagnetic emanations from electronic equipment since the 1980s and have focused their study of these possibilities under the program name TEMPEST. Electronic equipment (e.g., power supplies, microprocessor chips, cables, monitors, video display units, printers, keyboards, etc.), in general, generate high levels of radio frequency radiation when left unshielded. CRTs, specifically, have been shown to leak a significant amount of radio-frequency radiation to the extent that the displayed contents of a CRT monitor can be reconstructed by an eavesdropper from 1 km away [238]. In 1985, van Eck realized, through his research, that CRTs leaked their contents at harmonic frequencies of the CRT's clock and pixel rate (time between illuminating adjacent pixels) in a manner that resembled television broadcasting. By tuning his eavesdropping equipment to the specific frequencies of the leaked signals, van Eck was able to reconstruct images displayed by an unshielded (plastic) CRT from 1 km away as well as images displayed on a shielded (metal) CRT from up to 200 m away. In his attack, van Eck used no special signal processing techniques to enhance the signal, and instead relied on readily available RF communication equipment

(e.g., antenna, variable oscillator, television set). Since van Eck's work, many researchers have continued to exploit leaked-CRT electromagnetic emanations and have studied signal processing algorithms to improve their reception as well as focused their attack on different sources of CRT electromagnetic emanations [56, 96, 122, 142, 205]. In 2005, Kuhn demonstrated that LCD displays were also vulnerable to TEMPEST-style attacks [123, 124]. Kuhn was able to demonstrate that despite increased shielding becoming a requirement, pixel frequencies and video bandwidths increasing, and analog signals between computers and monitors approaching gigabit per second speeds, compromising emanations were still detectable at a distance of up to 10 m away using a wideband antenna. Furthermore, Kuhn was able to show that by controlling a display's foreground (text) and background colour, remote reconstruction of leaked images displayed on a monitor could be improved. Other researchers have also examined leakage from LCD monitors in an effort to quantitatively assess the amount of information leaked [227] and reduce the cost and space of the eavesdropping equipment [59]. Lastly, side channel attacks exploiting compromising RF emanations from cryptographic processing devices have been demonstrated [9, 39, 70].

Controlling electromagnetic emanations through software, specifically for the purposes of leaking sensitive information, has been the focus of "Soft TEMPEST" research [17, 125]. Kuhn and Anderson examined a scenario where malware installed on a secure "red" machine could egress data to an insecure "black" machine by controlling the contents of the secure machine's display [125]. Armed with knowledge of the display's pixel rate, horizontal and vertical frequencies, the authors were able to demonstrate two techniques, FSK and Amplitude Modulation (AM), to leak information from a secure system to an insecure system. In their first experiment, the authors demonstrated the ability to generate signals that could be picked up by a commodity AM radio by displaying a periodic pattern of solid black and white vertical bars on the screen. By controlling the width of the bars, specific frequencies could be detected by the AM radio thus allowing malware to leak signals using FSK. The screen displayed a very distinct visible pattern, but the researchers were able to achieve a data rate of 50 bps using this technique. Kuhn and Anderson improved their attack by using dithering techniques to embed recoverable images and text in the images that were displayed to the user, thus hiding the source of the leaked emanations. By hiding high frequency colours behind low frequency colours (the human eye is more sensitive to low frequency colours) malware could leak AM signals using this technique. As a countermeasure, the authors presented *TEMPEST Fonts* that consisted of filtered fonts whose high frequency components had been removed. Tanaka, et al., however, showed that even the use of *TEMPEST Fonts* could not prevent the leaking of compromising emanations and proposed the use of additional filtering techniques using Gaussian filters to reduce the leakage [228]. Similarly, Guri, et al. demonstrated that by modulating the video signals being sent to a display through different types of cables (e.g., VGA, DVI, and HDMI), FSK and DTMF data symbols could be communicated to the commodity FM radios that are found in popular mobile phone models [82].

### Limitations and Device Requirements

Electromagnetic emanations are able to travel long distances through non-metallic mediums with little interference. However, the biggest limitation to covert-RF channels is the lack of commodity hardware at the receiver capable of detecting or receiving covert-RF signals over long distances. The research of Kuhn and Anderson, [125], and Guri, et al., [82], is of particular relevance to this work because of the ability to receive signals using commodity AM and FM radios, which can be found in a number of modern mobile devices. The other side-channel attacks listed in this section, however, require a number of highly specialized probes, antennae, synchronization equipment, and filters, not all of which can be replicated in software. Furthermore, for a number of the side channel attacks discussed in the literature, there is a requirement for the probes to be placed either in contact or in close proximity to the leaky components embedded in crypto-processors in order to isolate the required signals. From a modulator device requirement perspective, the main system component studied in the literature capable of transmitting covert-RF signals has been monitors (e.g., CRTs, LCDs) and video display units; however, research has also shown that it is possible to recover signals from the cables used to connect a machine to other peripherals [216].

### Bandwidth and Detectability

Research into the capacity of signals leaked by LCDs has been analyzed from an information theory perspective [227]. Tanaka calculated that the information capacity of signals emanating from an LCD could be upwards of 100 megabits per second (Mbps) due the large SNR that the author measured using a near-field magnetic probe. There is potential for a large amount of data to be leaked by a video display unit, simply from the fact that a large amount of information is processed by the device. A 24-bit colour display at a pixel resolution of 1024x768 processes 18 megabits of information per frame. At a frame rate of 60 Hz the display will process about one gigabit of data per second. It remains to be seen, however, if all of the pixels and their colour values displayed to the user can be recovered by analyzing leaked electromagnetic radiation. Furthermore, the amount of information deliberately leaked through display emanations would presumably be much less once the covert-RF signals are hidden from both human perception as well as detection by a motivated passive adversary. Kuhn and Anderson were able to leak data at a rate of 50 bps; however, the frequencies that they needed to generate required a specific image to be displayed on the screen which was clearly visible to the user [125]. Kuhn and Anderson were able to hide their leaked signals using a dithering technique; however, the leaked signals were only hidden from human perception and could be reconstructed by any party with knowledge of their algorithm. Guri, et al., [82], were able to leak data at a rate of up to 60 bytes per second and demonstrated that signals could be leaked even when the monitor was turned off. Spread spectrum at low SNR should also be explored going forward as a possible technique to hide covert-RF communication.

#### Protection Mechanisms

In general, the countermeasures that can be put in place to protect against leaky devices are broken down into hardware protections and software protections. Shielding, both at the device and in rooms where sensitive material is processed, is an effective way to prevent electromagnetic signals from being leaked. Similarly, filters can be added to all cables as well as external devices to prevent them from amplifying signals. Jamming can also be used to increase the noise in the environment. Additionally, government organizations who are worried about compromising emanations have designated special zones, which have been specifically retrofitted to prevent leaks [124]. Using this zones scheme, both devices and locations in a building are assigned a zone. The location's zone indicates at what minimum distance an eavesdropper could have access to emanations leaked from electronic equipment in this zone. Similarly, a device is assigned to a zone based on how far its electromagnetic signals travel. A device is therefore restricted to a zone or zones to prevent its electromagnetic emanations from being accessed by an eavesdropper.

A number of software-based countermeasures have also been proposed in the literature. The use of *TEMPEST Fonts* were proposed to prevent Kuhn and Anderson's dithering attack. Similarly, the use of filters in general has also been proposed by researchers [227, 228] in order to reduce the possibility of leaking high frequency signals. Additionally, randomized displays, where pixels are not drawn in sequential order, have also been proposed. Kuhn also proposed using two digital video interface (DVI) standards to thwart eavesdropping [123]. By using *selective refresh* or *digital content protection*, the intelligible leaked signals can be reduced or completely eliminated.

### 5.1.7 Survey Summary

A summary of the channels covered in this section can be found in **Table 5.1**, **Table 5.2**, and **Table 5.3**. In general, the channels studied in this section are of relatively low bandwidth (kilobits per second and below) when compared to traditional communication links (e.g., Wi-Fi, mobile communication standards). This is not surprising, given that the channels that were examined are established by abusing sensors and devices that were never designed for communication. Additionally, while the use of the devices can be tailored for the optimal reception of covert signals, the bandwidth of the channels is still constrained by the limited power that can be vectored towards achieving covert communication. In saying that, general purpose, text-based communication is possible using the limited-bandwidth channels that have been presented. As an example, an individual typing 7-bit ASCII text at 80 words per minute at an average word length of 5.1 characters would produce data at an average rate of 47.6 bps, which could be communicated in real-time through a covert-acoustic, covert-light, or covert-RF channel and near real-time using the covert-seismic channel. Furthermore, using a low bit-rate codec (e.g., LPC-10 [132]), voice data could be communicated using covert-acoustic signals and, realistically, documents could also be transmitted using covert-acoustic, covert-RF and covert-light channels. A summary of popular document formats and their average page sizes is presented in **Table 5.4** to illustrate this more concretely.

Table 5.1: Out-of-Band Covert Channel Summary (Table 1 of 3)

| **Covert *-(channel)*** | Acoustic | | Light | | | | |
|---|---|---|---|---|---|---|---|
| **Modulator Requirements** | Speaker | CPU | Screen | Screen | LEDs | LEDs | Infrared transceiver |
| **Demodulator Requirements** | Microphone | Microphone | ALS | Camera | ALS | Camera | Infrared transceiver |
| **Order of Data Rate** | Kilobits per second | Data rates not provided in [134] | Bits per second | Hundreds of bits per second | Hundreds of bits per second | Hundreds of bits per second | Megabits per second |
| **Order of Distance** | Tens of meters | Tenths of a meter | Meters | Meters | Meters | Meters | Meters |
| **Channel Limitations** | • Relatively large ambient noise<br>• Relatively large signal delay<br>• Relatively large Doppler effect<br>• Reverberations<br>• Limited range (CPU modulator)<br>• Limited transmission power (CPU modulator) | | • Relatively large ambient noise (e.g., sun, room lighting)<br>• Signal does not travel through opaque objects<br>• Limited deployment of hardware in some cases (e.g., Infrared) | | | | |

Table 5.2: Out-of-Band Covert Channel Summary (Table 2 of 3)

| **Covert -*(channel)*** | Seismic | | Magnetic | Thermal | | |
|---|---|---|---|---|---|---|
| **Modulator Requirements** | Speaker | Vibrator | (Electro-)magnet | CPU load-inducing process | | HVAC System |
| **Demodulator Requirements** | Accelerometer | Accelerometer | Magnetometer | Clock monitoring process | On-board Thermal Sensor | |
| **Order of Data Rate** | Data rates were not provided in [93] | Tens of bits per second | Data rates were not provided in [93] | Tens of bits per hour | | |
| **Order of Distance** | Tens of meters | Tenths of a meter | Tenths of a meter | Contact is required | Tens of centimetres | Meters |
| **Channel Limitations** | • Cannot travel over the air<br>• Relatively large signal delay<br>• Path loss is dependent on the medium<br>• Limited range (vibrator) | | • Controllable electro-magnets (modulator) are not typically found in commodity devices<br>• Limited range<br>• Path loss is inversely proportional to the distance cubed<br>• Background noise from the earth's natural magnetic field | • Extremely low bandwidth<br>• Contact (or extremely close proximity) of modulator and demodulator required<br>• 100% CPU utilization required to increase temperature | | |

Table 5.3: Out-of-Band Covert Channel Summary (Table 3 of 3)

| **Covert *-(channel)*** | Radio-Frequency | | | | | |
|---|---|---|---|---|---|---|
| **Modulator Requirements** | CRT | CRT | LCD | Screen | Peripheral Cables | CPU |
| **Demodulator Requirements** | AM receiver | Specialized hardware | Specialized hardware | FM receiver | Specialized hardware | Specialized hardware |
| **Order of Data Rate** | Tens of bits per second | Data rates not provided | Data rates not provided | Hundreds of bits per second | Data rates not provided | Data rates not provided |
| **Order of Distance** | Tens of meters | Kilometres | Meters | Meters | Meters | Tenths of a meter |
| **Channel Limitations** | • Lack of hardware support at the demodulator in commodity devices (aside from AM/FM demodulator)<br>• Device-specific parameters (e.g., pixel rate, horizontal and vertical frequencies) affect modulated signals | | | | | |

Table 5.4: Average Sizes (kb) of Popular Document Types

| Document Type | Average Size (kb) per Page [177] |
|---|---|
| Microsoft Word | 15 |
| Microsoft Excel | 6 |
| Microsoft PowerPoint | 57 |
| Portable Document Format | 100 |
| Text | 1.5 |
| Email | 10 |
| Tagged Image File Format | 65 |

From the results of this survey, aside from some covert-RF configurations, out-of-band signals that were studied have limited transmission range and are, furthermore, typically constrained by common environmental obstacles (e.g., walls, doors, ceilings). This is due to the the physical properties of the signals and the fact that OOB-CCs are exploiting non-traditional modes of communication that have not been engineered for communication purposes. Additionally, the signals that were studied have limited transmit power available for communication and attenuate very quickly with increased distance. Lastly, for some channels (e.g., covert-magnetic, some covert-RF configurations), there is limited hardware support for communication and therefore, these channels are less likely to provide a good medium to use for general out-of-band covert communication. On the other hand, there are a number of viable existing physical channels available for OOB-CCs. Both covert-light and covert-acoustic channels as well as the covert-RF channels that allow demodulation using an AM/FM receiver benefit from widespread hardware support, increased distance when compared to the other alternatives, and the possibility of achieving higher-bandwidth channels (hundreds of bits per second and above). While a study to determine the highest-achievable bandwidth using covert-acoustic and covert-RF channels in common environments has been performed (see **Chapter 7** and [82], respectively) a similar study is required for covert-light channels.

All the OOB-CCs that were studied achieved undetectability by hiding their signals in the signal space above the sensitivity of on-board sensors and below human perception, thus relying on the fact that on-board sensors are more sensitive than our natural senses. The current adversarial model that researchers have been using assumes a passive adversary that is both unaware and unassuming of the covert communication, i.e., oblivious, and therefore the undetectability of the channels has only been measured by a human's natural ability to perceive the signals. This adversarial model needs to be expanded to include a passive adversary that is aware of both the channel and modulation scheme and is armed with technical tools developed specifically to detect covert communication in order to truly assess the covertness of these covert channels. Furthermore, the ability of an active adversary (e.g., ability to jam signals, inject messages, etc.) should be examined more closely. Going forward, out-of-band covert communication protocols should not rely on an oblivious passive adversary to remain undetectable if secure undetectable covert channels are to be realized. As discussed in **Chapter 3**, hiding strategies (e.g., hiding information

in background noise, utilizing diverse channels for communication) [43] could be employed to increase the undetectability of current OOB-CCs and should be considered by covert channel designers going forward.

The protection mechanisms that have been documented for each of the OOB-CCs above can be broken down into a number of general strategies. First, mediums that are used for computer-to-human communication (e.g., sound, light) should have the components of their signals that exist below the threshold of human perception filtered out so that they cannot be used for covert communication. Similarly, devices should be physically shielded whenever possible. If filtering or shielding is not possible, the covert signals should be deliberately jammed, i.e., increasing the ambient noise in the environment. Additionally, if the device sensors are superfluous, they can either be physically removed from the device or disabled in software. Furthermore, all sensors should be monitored for abuse (in terms of frequency of access), perhaps with the use of an intrusion detection system, and, whenever possible, the sensitivity of the sensor's readings should be reduced such that their legitimate use can continue, but not their abuse. From a secure systems development perspective, mandatory access control policies should be enforced to limit access to sensors, and application-specific manifests should be used to document all required sensor accesses. Lastly, as a general rule, all sensor accesses should be logged and periodically audited to help determine if a sensor is being used for covert communication.

## 5.2 Out-of-Band Covert Channel Taxonomy

A hierarchy showing the classification of OOB-CCs is presented in **Figure 5.1** and **Figure 5.2**. The survey in this chapter shows that modulation schemes, channel limitations, and protection mechanisms, at this point in the study of OOB-CCs, are directly related to the hardware used to realize each covert channel and, therefore, grouping by channel and hardware is the most representative view of the research at this point in time. As a result, OOB-CCs are first grouped along the general category of hardware that is required to realize channel, which is shown in *Tier 1* and *Tier 2*, respectively. Second, in *Tier 3*, modulator and demodulator hardware requirements are grouped based on the channel that they communicate over. Lastly, in *Tier 4*, the actual modulator and demodulator hardware devices are placed as the leaf nodes in the taxonomy tree.

Hardware devices are grouped into three general categories in the proposed taxonomy: *commodity - pervasive*, *commodity - limited*, and *specialized*. Hardware is placed in the *commodity - pervasive* category if the hardware can be found in most commodity systems (e.g., mobile phones, laptops and desktops); hardware is placed in the *commodity - limited* category if the hardware can only be found in a limited number of systems or only in a general category of systems (e.g., only mobile phones); and hardware is placed in the *specialized* category if the hardware is not found in commodity systems, but instead is specialized hardware constructed for a specific purpose (e.g., telescope, parabolic microphone, wideband antenna). The specific modulator and demodulator devices discussed in this chapter are grouped as follows:

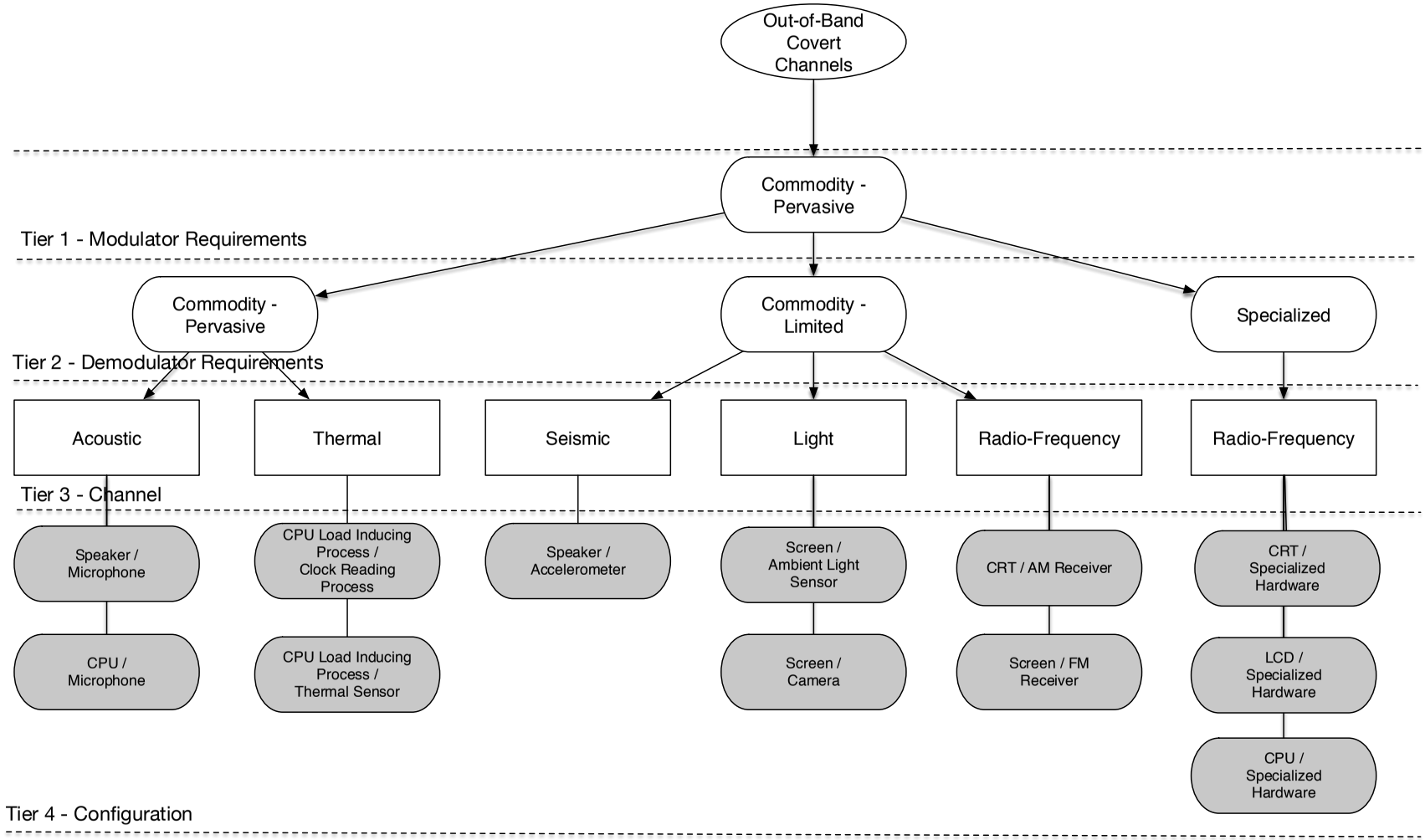



Figure 5.1: Out-of-Band Covert Channel Taxonomy (Part 1)

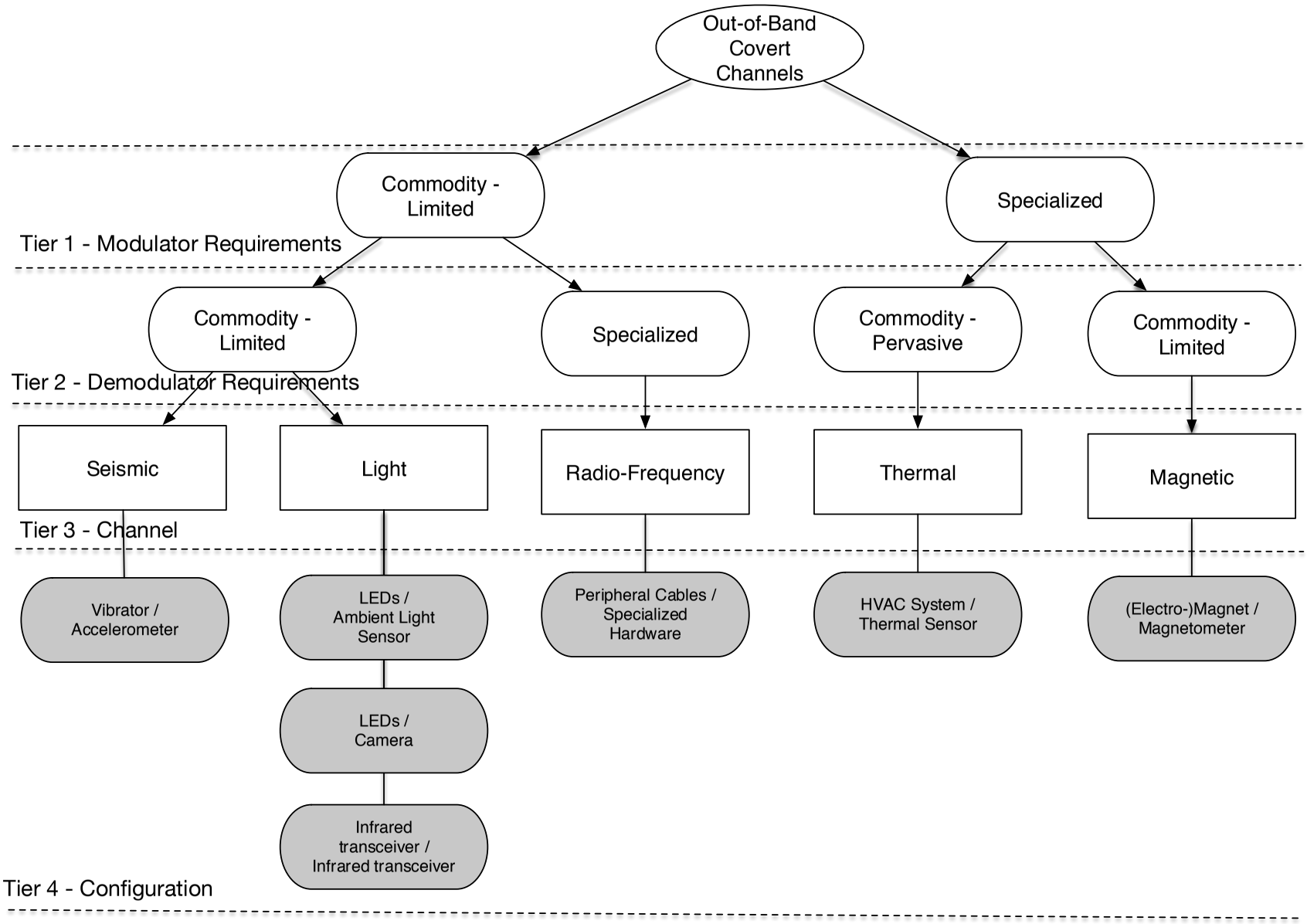



Figure 5.2: Out-of-Band Covert Channel Taxonomy (Part 2)

- **Commodity - Pervasive:** CPU, screen (including LCD, CRT), speaker, microphone, thermal sensor
- **Commodity - Limited:** Ambient light sensor, camera, light emitting diodes, infrared transceiver, vibrator, accelerometer, magnetometer, AM receiver, FM receiver, cables
- **Specialized:** Electro-magnet, specialized RF equipment, HVAC equipment

In general, the hardware that is required at the modulator and demodulator is grouped based on their availability for a couple of reasons. First, for secure system developers the prevalence of the required hardware for each covert channel maps directly to the risk posed by the covert channel to the secure system. Grouping based on prevalence provides a qualitative measure that secure system developers can use to prioritize the risk of the covert channel and thus the priority of the requirement to build appropriate countermeasures into their systems. Second, for covert channel designers, the prevalence of the covert channel's hardware provides a qualitative measure that allows developers to determine the general applicability of their covert channel to specific or general deployment scenarios, i.e., as the covert channel can be established using more *commodity - pervasive* hardware the utility of the covert channel increases.

Given the infancy of the study of OOB-CCs this taxonomy is presented as one such possible grouping. An alternative taxonomy would see OOB-CCs categorized based on their achievable data rate, and *covertness*; however, at this point in the research the achievable data rate of each covert channel is still an open question and, moreover, classifying channels based on their achievable data rate would be a moving target since presumably as OOB-CCs become more widely studied their rates would also increase.

In the next chapter, the generic measurement of OOB-CCs is presented.

# Chapter 6

# Measuring and Characterizing Out-of-Band Covert Channels

The survey in the previous chapter demonstrated that OOB-CCs exist between a number of commodity device pairs: e.g., microphone and speaker, CPU and microphone, light source and ambient light sensor or camera, speaker and accelerometer, vibration device and accelerometer, electromagnet and magnetometer, CPUs, CPU and thermometer, and display and AM/FM radio. These OOB-CCs can be classified as *open covert channels*, as opposed to *steganographic covert channels*, because they do not alter a cover protocol or object in order to communicate. Given this classification, from the perspective of a passive covert-analyst, the techniques and devices used to detect OOB-CC signals are more similar to the techniques used to detect LPD systems than those used to detect steganographic systems. In this chapter, the techniques that are used to detect LPD communications (e.g., the use of an energy detector) are applied to OOB-CCs.

OOB-CCs, in general, however, differ from both traditional and LPD communication systems in a number of ways. First, malware that rely on OOB-CCs for command and control are not necessarily concerned with general purpose communication. Often the main requirement for malware is to leak a limited amount of high-value data (e.g., passwords, encryption keys, keystrokes, documents, etc.) and, therefore, the designers of these channels are concerned with the amount of data that can be communicated before the channel is detected, i.e., the *covertness* of the channel, rather than the long-term average amount of information that can be transferred through the channel. Moreover, OOB-CCs are also constrained by the devices that are used for communication. Often the requirements for general-purpose communication in LPD systems call for communication at low SNR, which might not be possible given that commodity devices are not designed for communication at all and, therefore, perhaps lack the sensitivity required to communicate at low SNR. Furthermore, while the metrics used to measure traditional communication systems (e.g., data rate and bit error rate) and LPD communication systems (e.g., probability of detection) are useful measures for their respective systems, a more comprehensive metric is required for OOB-CCs that combines the amount of information that can be transferred over the channel and the detectability of the channel in order to evaluate the trade-off between the two.

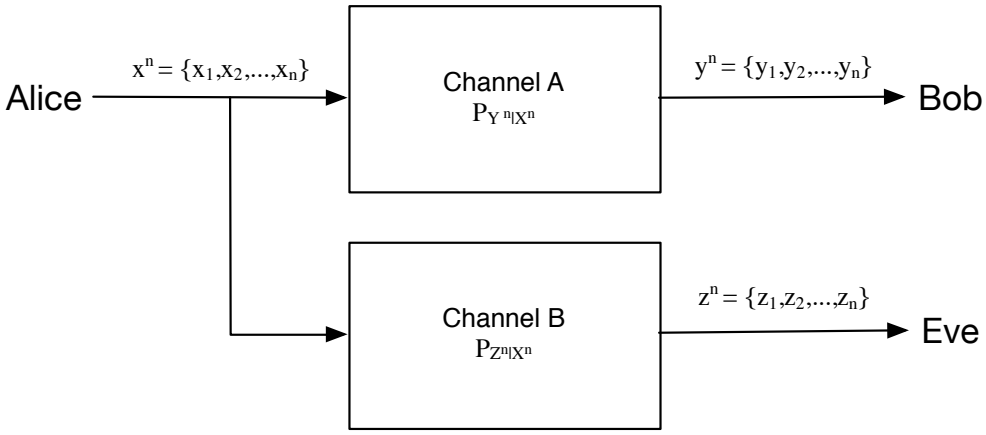



Figure 6.1: The system model analyzed in this chapter. Alice transmits a sequence of codewords $x^n = \{x_1, x_2, \ldots, x_n\} \in X^n$, $X^n \sim P_{X^n}$ through *Channel A* to Bob. Bob receives a sequence of codewords $y^n = \{y_1, y_2, \ldots, y_n\} \in Y^n$, $Y^n \sim P_{Y^n}$ where the sequence $y^n$ is a possibly corrupted version of $x^n$ and the distribution of $Y^n$ is dependent on the channel transition probability distribution $P_{Y^n|X^n}$. Wendy also receives a sequence of codewords $z^n = \{z_1, z_2, \ldots, z_n\} \in Z^n$, $Z^n \sim P_{Z^n}$ through *Channel B* where again the sequence $z^n$ is a possibly corrupted version of $x^n$ and Wendy's distribution of codewords is dependent on $P_{Z^n|X^n}$. Once Wendy observes $z^n$, she makes a decision and concludes whether or not Alice is communicating.

In the context of steganography, *steganographic capacity* is the largest payload that can be safely embedded in a cover object using a particular embedding method [117]. Researchers have used this measure to calculate the capacity of a number of steganographic channels and have empirically demonstrated, or mathematically proven, that their capacity is governed by a "square root law" (i.e., the maximum size of the embedded payload must be proportional to the square root of the size of the cover) [67, 112, 115, 117]. Moreover, results from the LPD research community also demonstrate a similar "square root law" governing their systems' capacity [23, 24, 25, 40, 41, 42, 98]. In both of these information hiding applications, the "square root law" demonstrates that the maximum amount of data that can be transmitted without detection is proportional to the square root of the size of the cover object or the number of channel uses, respectively. Furthermore, as a consequence of these results, the researchers also showed that the traditional rate used to measure communication systems, i.e., Shannon capacity [206], is ineffective as this rate for information hiding systems tends to zero when the square root law is respected. Given this review of previous results, in this chapter the performance of OOB-CCs is measured using *steganographic capacity*.

In the context of OOB-CCs, *steganographic capacity* is *the maximum amount of data that can be communicated between Alice and Bob before Wendy's probability of detection reaches an arbitrary threshold*. This measure is obtained by combining Alice and Bob's communication rate with the channel-analyst's probability of detection. The model analyzed in this chapter is an updated version of the basic model first introduced in **Chapter**

**1**; see **Figure 6.1**. The model is updated to reflect the more general scenario where Bob and Wendy both receive Alice's codewords through two separate channels. Moreover, it is assumed that Wendy is capable of monitoring the *covert-(channel)* between Alice and Bob and does so in order to answer the question: *Is Alice communicating?*

This is a stronger security assumption than the assumptions that have been made when evaluating previous OOB-CCs [53, 89, 90, 181]. In these previous works, it was assumed that the covert-analyst was an oblivious adversary and the analyzed OOB-CCs were deemed "covert" if the channel established between Alice and Bob was imperceptible to Wendy's natural senses (e.g., sight, hearing). The analysis in this chapter, conversely, assumes that Wendy is able to deploy technical solutions to detect if Alice and Bob are communicating. It is important to note that *detection* by a passive covert-analyst is evaluated in this chapter and not necessarily the *interception* of Alice's codewords. Thus, Alice is concerned with concealing the presence of her communication and not necessarily the confidentiality of the messages that she is sending as a result.

This chapter is organized as follows. Wendy's detection problem is framed as a statistical hypothesis test and the *steganographic capacity* of OOB-CCs is measured under a number of channel models: the channels between Alice and Bob as well as Alice and Wendy are memoryless channels (**Section 6.1**) and the channel between Alice and Bob is band-limited (**Section 6.2**). In both cases it is assumed that the channels are corrupted by additive white Gaussian noise (AWGN). In **Section 6.3**, the steganographic capacity of OOB-CCs is analyzed when Wendy uses an energy detector to detect Alice's transmissions and Alice transmits symbols in randomly selected symbol intervals. The analysis employed in **Section 6.3** is used again in **Chapter 8** to evaluate the *steganographic capacity* of covert-acoustic channels.

## 6.1 Measuring the Steganographic Capacity of Memoryless Channels

In this section, the steganographic capacity for OOB-CCs is derived when the channels between Alice and Bob as well as Alice and Wendy are modelled by memoryless channels and corrupted by AWGN. Thus, the analysis in this section is applicable to all OOB-CCs whose channels can be classified in this manner. To derive the OOB-CC steganographic capacity measure, Wendy's problem of detecting Alice's communications is modelled as a statistical hypothesis test. Results from the discussions on statistical hypothesis testing [46, 133] and information theory [46] are, therefore, used throughout this analysis.

### 6.1.1 Information-Theoretic Capacity for Memoryless Channels

Using statistical hypothesis testing, Wendy, upon making a sequence of observations, $\{z^n | z^n \in Z^n\}$ (where $z^n$ is shown in **Figure 6.1**), decides whether to either accept the null hypothesis, $H_0$ (i.e., conclude "Alice is not communicating"), or reject the null hypothesis

(i.e., conclude "Alice is communicating"). Wendy constructs the distributions $P_{H_0}$ and $P_{H_1}$ in such a way that when $H_0$ is true the sequence $z^n \sim P_{H_0}$ and when $H_1$ is true the sequence $z^n \sim P_{H_1}$. In order to make a decision, Wendy performs a *log-likelihood ratio test* (LLRT) and decides whether to accept or reject the null hypothesis. As a result of performing the LLRT, Wendy can make one of two types of errors: rejecting the null hypothesis when it is true (*Type I* error) or accepting the null hypothesis when it is false (*Type II* error). These two classes of errors are commonly referred to as false positive, whose probability is denoted by $\alpha$, and false negative, whose probability is denoted by $\beta$, respectively. By the Neyman-Pearson Theorem, the LLRT is optimal in the sense that for a given false positive, $\alpha$, $\beta$ is minimized.

A common performance measure for statistical hypothesis tests is the *sum of probability errors*, $\alpha + \beta$, which is used throughout this discussion to evaluate Wendy's performance when attempting to detect Alice's communications. Given that falsely accepting the alternate hypothesis represents falsely accusing Alice of covert communication, Wendy would like to fix her level of significance, $\alpha$, to an arbitrarily low value and, therefore, minimize $\beta$ for a set value of $\alpha$. Using **Theorem 13.1.1** from [133], the sum of probability errors can be expressed as

$$\alpha + \beta = 1 - \frac{1}{2} TV(P_{H_0}, P_{H_1}). \tag{6.1}$$

$TV(P_{H_0}, P_{H_1})$ is the *total variation distance* between $P_{H_0}$ and $P_{H_1}$ and can be expressed as

$$TV(P_{H_0}, P_{H_1}) = \int_{x \in \mathcal{X}} |P_{H_0}(x) - P_{H_1}(x)| \, \mathrm{d}x, \tag{6.2}$$

where $\mathcal{X}$ is the set of all possible $n$-length sequences of observations that Wendy can observe. Using **Lemma 11.6.1** in [46], $TV(P_{H_0}, P_{H_1})$ can be bounded by using the following inequality

$$\sqrt{2 \ln 2 D(P_{H_0} \| P_{H_1})} \geq TV(P_{H_0}, P_{H_1}), \tag{6.3}$$

where $D(P_{H_0} \| P_{H_1})$ is the KL divergence and is defined as

$$D(P \| Q) = \int_x P(x) \log \frac{P(x)}{Q(x)} \, \mathrm{d}x \tag{6.4}$$

for two probability distributions $P$ and $Q$. Given **Equation 6.3**, Wendy's sum of probability errors is thus lower bounded by $1 - \epsilon_1$, where

$$\epsilon_1 = \sqrt{\frac{\ln 2 D(P_{H_0} \| P_{H_1})}{2}}. \tag{6.5}$$

Based on these preliminaries, **Theorem 1** is presented:

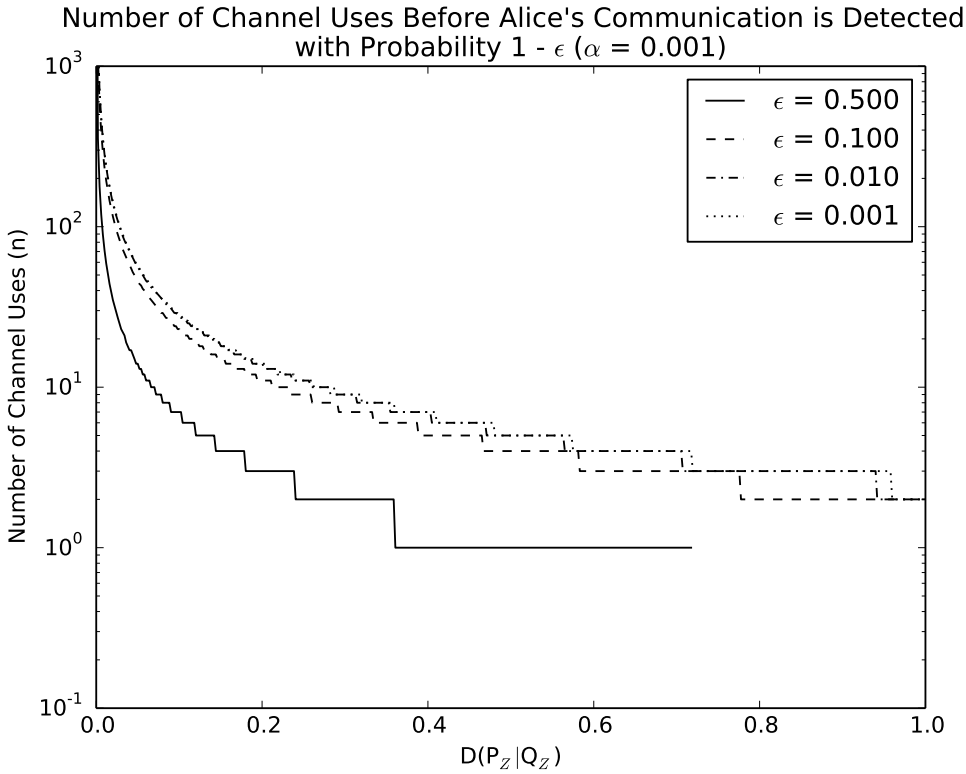



Figure 6.2: Number of Channel Uses, $n$, Before Wendy Detects Alice with Probability $> 1 - \epsilon$

**Theorem 1.** If the channel between Alice and Bob as well as Alice and Wendy are memoryless channels and Alice generates sequences of codewords $\{x^n | x^n \in X^n\}$ such that each $X_i \sim P_X$ in $X^n = \{X_1, X_2, \ldots, X_n\}$, $1 \leq i \leq n$, is i.i.d., then Alice can transmit $L$ bits of information to Bob while ensuring the upper bound on Wendy's probability of detection is $1 - \epsilon$, for some arbitrary $\epsilon \in (0, 1 - \alpha)$, where

$$\begin{aligned} &L \to \infty \text{ if } D(Q_Z \| P_Z) = 0, C > 0 \\ &L < nC \text{ if } D(Q_Z \| P_Z) > 0, C > 0 \\ &L = 0 \quad \text{if } C = 0 \end{aligned}$$

$C$ is the Shannon capacity of the channel between Alice and Bob in bits per channel use, $Q_Z$ is the probability distribution when Alice is not communicating, $P_Z$ is the probability distribution when Alice is communicating and

$$n = \left\lfloor \frac{2(1 - \alpha - \epsilon)^2}{\ln 2 D(Q_Z \| P_Z)} \right\rfloor. \tag{6.6}$$

*Proof.* Since Alice generates her symbols i.i.d., Wendy's observed sequence, $z^n = \{z_1, z_2, \ldots, z_n\}$, is also i.i.d and

$$P_{H_0} = Q_Z^n(z^n) = \prod_{i=1}^{n} Q_Z(z_i)$$
$$P_{H_1} = P_Z^n(z^n) = \prod_{i=1}^{n} P_Z(z_i).$$

Therefore,

$$\begin{aligned}\epsilon_1 &= \sqrt{\frac{\ln 2 D(P_{H_0} \| P_{H_1})}{2}} \\ &= \sqrt{\frac{\ln 2 D(Q_Z^n \| P_Z^n)}{2}} \\ &= \sqrt{\frac{n \ln 2 D(Q_Z \| P_Z)}{2}},\end{aligned}$$

since $D(P_{H_0} \| P_{H_1}) = nD(Q_Z \| P_Z)$ (i.e., the KL divergence is additive for sequences of i.i.d. random variables).

Under the assumptions that each $X_i$ is i.i.d and the channel between Alice and Wendy is a memoryless channel, Wendy constructs a model for $P_{Z|X}$ in order to determine an appropriate probability distribution for her received codewords, $P_Z$. Given Alice's construction of $P_X$, two different scenarios present themselves to Wendy. First, Alice generates $X \sim P_X$ such that Wendy generates $P_Z = Q_Z$ and Wendy calculates that $D(Q_Z \| P_Z) = 0$. Second, Alice generates $X \sim P_X$ such that Wendy generates $P_Z$ and Wendy calculates that $D(Q_Z \| P_Z) > 0$. In both cases it is assumed that Alice generates her symbols such that the capacity of the channel between Alice and Bob, $C$, is greater than zero since, if $C = 0$, the amount of data that Alice can covertly transmit to Bob is also zero (i.e., $L$ is zero).

When Wendy is forced to model $P_Z$ such that $Q_Z = P_Z$, $D(Q_Z \| P_Z) = 0$ and there is no measurable difference between the probability distributions $P_{H_0}$ and $P_{H_1}$ that Wendy can use to determine if Alice is communicating. Therefore, Wendy's sum of probability errors is one regardless of how many observations of the channel, $n$, Wendy makes. As pointed out by Hou and Kramer [98], in this case, Wendy's decision as to whether an observation was drawn from $P_{H_0}$ or $P_{H_1}$ is independent of Alice's transmission status and Wendy cannot reliably detect Alice's communications. Therefore, when the capacity, $C$, of the channel between Alice and Bob, $C > 0$, $L \to \infty$ as $n \to \infty$.

In the second case, when $D(Q_Z \| P_Z) > 0$; there is a measurable difference between the probability distributions $P_{H_0}$ and $P_{H_1}$ and $\alpha + \beta \geq 1 - \epsilon_1$. Let Wendy's probability of detection, $P_D$, be

$$P_D = Pr[\text{ Accepting } H_1 | \text{ Alice is communicating }]$$

$$= 1 - \beta,$$

and recall that the sum of errors equation is

$$\alpha + \beta = 1 - \frac{1}{2} TV(P_{H_0}, P_{H_1}).$$

After rearranging,

$$\begin{aligned} \alpha + (1 - P_D) &= 1 - \frac{1}{2} TV(P_{H_0}, P_{H_1}) \\ P_D &= \alpha + \frac{1}{2} TV(P_{H_0}, P_{H_1}), \end{aligned} \tag{6.7}$$

and, therefore, $P_D \leq \alpha + \epsilon_1$ (note that the lower bound for $P_D$ is $\alpha$ given **Equation 6.7**). Since $D(Q_Z \| P_Z) > 0$, $\epsilon_1 \to \infty$ as $n \to \infty$, which allows the upper bound on Wendy's $P_D \to 1$ (i.e., Wendy can improve her probability of detecting Alice's communications by increasing her number of observations in the event that $D(Q_Z \| P_Z) > 0$). Defining $n^*$ to be the maximum number of observations such that Wendy's upper bound on $P_D$ is $1 - \epsilon$, for some arbitrary $\epsilon \in (0, 1 - \alpha)$, it can be observed that

$$\begin{aligned} 1 - \epsilon &= \alpha + \epsilon_1 \\ \epsilon_1 &= 1 - \alpha - \epsilon \\ \sqrt{n^* \frac{\ln 2 D(Q_Z \| P_Z)}{2}} &= 1 - \alpha - \epsilon \\ n^* &= \left\lfloor \frac{2(1 - \alpha - \epsilon)^2}{\ln 2 D(Q_Z \| P_Z)} \right\rfloor, \end{aligned}$$

where the floor is taken to ensure that Wendy's probability of detection is upper bounded. The capacity of the channel between Alice and Bob in $n^*$ channel uses is therefore:

$$\begin{aligned} C^{n^*} &= \sup_{P_X} \left( I(X^{n^*} | Y^{n^*}) \right) \\ &= \sup_{P_X} \left( H(X^{n^*}) - H(X^{n^*} | Y^{n^*}) \right) \\ &\overset{(a)}{=} \sup_{P_X} \left( n^* H(X) - \sum_{i=1}^{n^*} H(X_i | Y_{n^*}, \ldots, Y_1, X_{i-1}, \ldots, X_1) \right) \\ &\overset{(b)}{=} \sup_{P_X} \left( n^* H(X) - \sum_{i=1}^{n^*} H(X_i | Y_i) \right) \\ &\overset{(a)}{=} \sup_{P_X} \left( n^* H(X) - n^* H(X|Y) \right) \end{aligned}$$

$$
\begin{aligned}
&= \sup_{P_X} \left(n^* I(X;Y)\right) \\
&\overset{(c)}{=} n^* C,
\end{aligned}
$$

where in (a) the fact that the sequence of $X_i$'s is chosen i.i.d by Alice has been used, in (b) the fact that the channel is a memoryless channel has been used, and in (c) $C$ is the capacity of a single use of the channel between Alice and Bob, in bits per channel use. Therefore, the maximum amount of data that Alice can transmit to Bob while ensuring Wendy's probability of detection, $P_D < 1 - \epsilon$, is $nC$ bits, where $n$ is defined in **Equation 6.6**.

Summarizing the analysis above, when Alice chooses her symbols i.i.d, the steganographic capacity, $L$, is

$$
\begin{aligned}
&L \to \infty \text{ if } D(Q_Z \| P_Z) = 0, C > 0 \\
&L < nC \text{ if } D(Q_Z \| P_Z) > 0, C > 0 \\
&L = 0 \quad \text{if } C = 0
\end{aligned}
$$

where $C$ is the capacity of the channel between Alice and Bob in bits per channel use, $Q_Z$ is the probability distribution when Alice is not communicating, $P_Z$ is the probability distribution when Alice is communicating and $n$ is given in **Equation 6.6**.

□

Given **Theorem 1**, $L$ is taken to be the steganographic capacity and a plot of $n$ versus $D(Q_Z \| P_Z)$ is shown in **Figure 6.2** for $\alpha = 0.001$ (see [35] for the source code that was used to generate all the plots in this chapter). Examining the plot in **Figure 6.2** as well as **Equation 6.6** it is clear that Alice's best strategy is to construct $P_X$ such that $P_Z$ matches Wendy's model when Alice is not communicating, $Q_Z$, as closely as possible. Or, more formally,

$$
\begin{aligned}
&\max_{P_X} C \\
&\min_{P_X} D(Q_Z \| P_Z).
\end{aligned}
$$

Conversely, Wendy's strategy is to model the distributions when Alice is communicating and when she is not as closely as possible in order to maximize the distance, in the KL divergence sense, between $P_Z$ and $Q_Z$.

### 6.1.2 Capacity for Memoryless Channels Corrupted by AWGN

The steganographic capacity of memoryless channels is now derived under the assumption that Alice is subject to an average power constraint (see **Equation 6.8**) and both channels are corrupted independently by AWGN. Alice is modelled under an average power

constraint because, as a result of the analysis that follows, her transmission power, $P_t$, must be controlled in order to limit her probability of being detected. In reality, Alice has a true average power constraint, $P$, due to the physical limitations of her transmitting device; however, it is assumed that the true average power constraint, $P \gg P_t$ and, therefore, $P_t$ is used in the calculations of this section. Furthermore, it is assumed that both *Channel A* and *Channel B* (shown in **Figure 6.1**) are corrupted by AWGN, with noise variances, $\sigma_B^2$ and $\sigma_W^2$, respectively. Under the AWGN noise assumption, Wendy's channel model when Alice is not transmitting can be expressed as $Z_1 = W_W$, where $W_W \sim \mathcal{N}(0, \sigma_W^2)$. Additionally, when Alice's transmit power is subject to an average power constraint, Alice and Bob's channel capacity is maximized by Alice distributing $X \sim \mathcal{N}(0, P_t)$ [46], which she can achieve through random coding (e.g., encrypting or compressing her data stream).

$$\frac{1}{n}\int_x x^2 \, \mathrm{d}x \leq P_t \tag{6.8}$$

Assuming Alice generates symbols with a normal distribution and variance $P_t$, Wendy's observation of the channel is $Z_2 = \alpha_W X + W_W$, $Z_2 \sim (0, \alpha_W^2 P_t + \sigma_W^2)$, where $\alpha_W$ is Wendy's attenuation factor. Similarly, Bob's observation of the channel is $Y = \alpha_B X + W_B$, where $W_B \sim \mathcal{N}(0, \sigma_B^2)$ and $Y \sim \mathcal{N}(0, \alpha_B^2 P_t + \sigma_B^2)$, where $\alpha_B$ is Bob's attenuation factor. Wendy's expected distributions, $Q_Z$ and $P_Z$, are, therefore $\mathcal{N}(0, \sigma_W^2)$ and $\mathcal{N}(0, \alpha_W^2 P_t + \sigma_W^2)$ to model when Alice is not communicating and when she is, respectively. Given these preliminaries, **Theorem 2** is presented:

**Theorem 2.** If the channel between Alice and Bob as well as Alice and Wendy are memoryless channels; both channels are corrupted by AWGN with distributions $\mathcal{N}(0, \sigma_B^2)$ and $\mathcal{N}(0, \sigma_W^2)$, respectively; Alice transmits symbols i.i.d. with distribution $\mathcal{N}(0, P_t)$; and Alice is subject to the average power constraint shown in **Equation 6.8**, then Alice can transmit $L$ bits of information to Bob while ensuring the upper bound on Wendy's probability of detection is $1 - \epsilon$, for some arbitrary $\epsilon \in (0, 1 - \alpha)$, where $L$ is

$$\begin{aligned} &L \to \infty \text{ if } D(Q_Z \| P_Z) = 0, C > 0 \\ &L < nC \text{ if } D(Q_Z \| P_Z) > 0, C > 0 \\ &L = 0 \quad \text{if } C = 0 \end{aligned}$$

$C$ is the Shannon capacity of the channel between Alice and Bob in bits per channel use, $Q_Z$ is the probability distribution when Alice is not communicating, $P_Z$ is the probability distribution when Alice is communicating,

$$n = \left\lfloor \frac{2(1 - \alpha - \epsilon)^2}{\ln 2 D(Q_Z \| P_Z)} \right\rfloor,$$

and $D(Q_Z \| P_Z)$ is

$$\frac{1}{2}\log\left(1 + \frac{\alpha_W^2 P_t}{\sigma_W^2}\right) + \frac{1}{2}\left(\frac{1}{1 + \frac{\alpha_W^2 P_t}{\sigma_W^2}} - 1\right). \tag{6.9}$$

*Proof.* Given **Theorem 1**, $L$ bits of information can be sent over a memoryless channel while bounding Wendy's probability of detection below some arbitrary threshold, $1-\epsilon$. The only remaining part of **Theorem 2** that has to be proven is the value for the KL divergence between $P_Z$ and $Q_Z$.

Generically, the KL divergence for two normally distributed random variables, $P_1 \sim \mathcal{N}(\mu_1, \sigma_1^2)$ and $P_2 \sim \mathcal{N}(\mu_2, \sigma_2^2)$ is

$$D(P_1 \| P_2) = \log \frac{\sigma_2}{\sigma_1} + \frac{\sigma_1^2 + (\mu_1 - \mu_2)^2}{2\sigma_2^2} - \frac{1}{2}. \tag{6.10}$$

Applying **Equation 6.10** to the distributions $Q_Z \sim \mathcal{N}(0, \sigma_W^2)$ and $P_Z \sim \mathcal{N}(0, \alpha_W^2 P_t + \sigma_W^2)$, the KL divergence is

$$\begin{aligned} D(Q_Z \| P_Z) &= \log \frac{\sigma_2}{\sigma_1} + \frac{1}{2}\left(\frac{\sigma_1^2}{\sigma_2^2} - 1\right) \\ &= \frac{1}{2}\log \frac{\sigma_2^2}{\sigma_1^2} + \frac{1}{2}\left(\frac{\sigma_1^2}{\sigma_2^2} - 1\right) \\ &= \frac{1}{2}\log \frac{\alpha_W^2 P_t + \sigma_W^2}{\sigma_W^2} + \frac{1}{2}\left(\frac{\sigma_W^2}{\alpha_W^2 P_t + \sigma_W^2} - 1\right) \\ &= \frac{1}{2}\log\left(1 + \frac{\alpha_W^2 P_t}{\sigma_W^2}\right) + \frac{1}{2}\left(\frac{1}{1 + \frac{\alpha_W^2 P_t}{\sigma_W^2}} - 1\right), \end{aligned}$$

as required.

□

Denoting $\mathrm{SNR}_W = \frac{\alpha_W^2 P_t}{\sigma_W^2}$ and $\mathrm{SNR}_B = \frac{\alpha_B^2 P_t}{\sigma_B^2}$ for Wendy and Bob's average power signal-to-noise ratio, respectively, the steganographic capacity is shown for all $\mathrm{SNR}_W$ and $\mathrm{SNR}_B$ combinations between -40 dB and 40 dB in **Figure 6.3**. In the figure, the channel capacity between Alice and Bob is [46]

$$C = \frac{1}{2}\log\left(1 + \mathrm{SNR}_B\right)\frac{\text{bits}}{\text{channel use}}.$$

The steganographic capacity surface plot is shown for the case where $\epsilon = 0.5$ to capture the maximum amount of data that Alice can transmit to Bob before Wendy has a better than guessing chance of detecting her communication after $n$ channel uses.

A number of conclusions can be drawn from **Figure 6.3**. First, at an $\mathrm{SNR}_W$ of 5 dB and above ($\mathrm{SNR}_W$ of 5 dB corresponds to a KL divergence of approximately 0.33), Wendy only needs one observation of Alice's communications in order to determine that she is communicating with probability 0.5. Hence, the steganographic capacity, $L$, is zero. Second, observing the line drawn in the plane $z = 0$, which represents the situation where

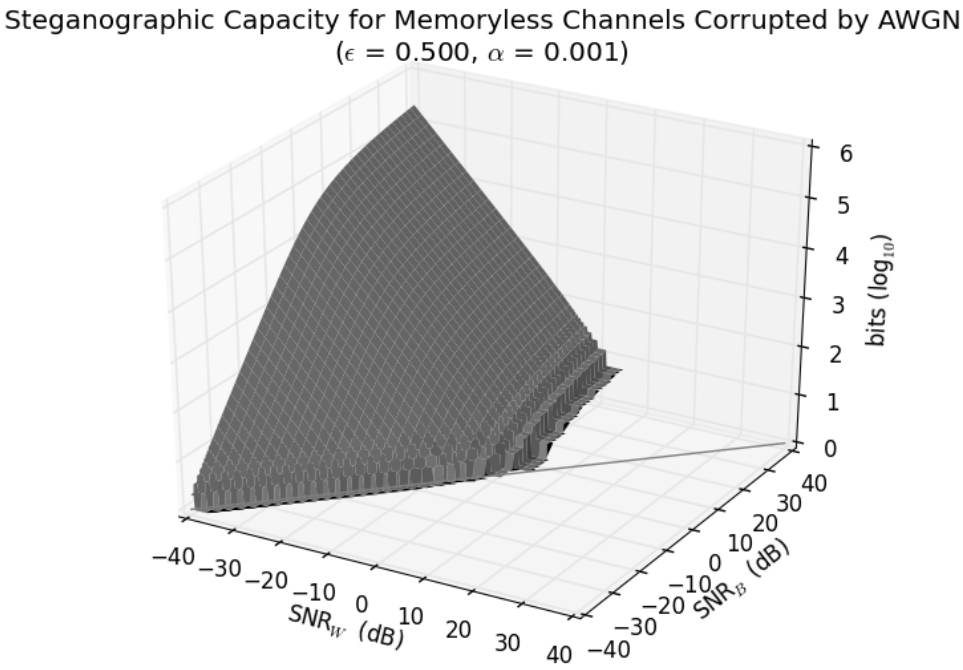



Figure 6.3: The Steganographic Capacity for Memoryless Channels in AWGN

$\text{SNR}_W = \text{SNR}_B$, a rule of thumb for Alice is to ensure that Wendy's SNR remains below that of Bob's in order to covertly communicate $L > 0$ bits. From these observations, it follows that if Alice wishes to communicate $L > 0$ bits while ensuring that Wendy is not able to detect her communication with a better than guessing chance, she must construct her signals such that:

1. Wendy's observed SNR, $\text{SNR}_W$, is less than 5 dB (in order to avoid detection) and
2. Wendy's observed SNR, $\text{SNR}_W$, is less than Bob's, $\text{SNR}_B$ (in order for $L > 0$ bits).

Additionally, from **Figure 6.2**, it can be observed that as $\epsilon \to 0$, $n$, and subsequently $L$, increases at the expense, for Alice, that Wendy can more definitively detect her communication. The assumptions made in this section represent the best case scenario for Wendy since she knows the exact distribution of Alice's symbols and performs an optimal Neyman-Pearson test in order to detect Alice. Conversely, this plot shows the worst case scenario for Alice when the channels are memoryless channels; however, it is clear that Alice can control her transmit power, $P_t$, in order to communicate a positive number of bits to Bob while limiting Wendy's probability of detection under certain circumstances. **Figure 6.3**, therefore, represents the theoretical lower bound for $L$. In the section that follows, it is shown that as real-world constraints are placed on Wendy, the steganographic capacity of OOB-CCs increases.

## 6.2 Measuring the Steganographic Capacity of Band-Limited Channels

In this section, the steganographic capacity is derived when the channel between Alice and Bob is band-limited to some bandwidth, $W$. Most real-world communication systems are band-limited to ensure that there is efficient use of the frequency spectrum that is available to them. However, in the case of OOB-CCs, these systems are band-limited due to the physical limitations of the devices that are used for transmitting and receiving. Given that the commodity devices exploited to create OOB-CCs were not designed for communication, oftentimes the bandwidth available for covert communication is constrained. The analysis in this section reflects this reality. Moreover, the analysis in this section assumes that Wendy must build a device, an energy detector, to detect Alice's communications. The steganographic capacity is again measured by modelling Wendy's detection problem as a statistical hypothesis test.

### 6.2.1 Information-Theoretic Capacity for Band-Limited Channels

**Theorem 3.** If the channels between Alice and Bob as well as Alice and Wendy are memoryless channels that are corrupted by AWGN; the channel between Alice and Bob is band-limited to some bandwidth $W > 0$; and Alice generates sequences of code words $\{x^n | x^n \in X^n\}$ such that each $X_i \sim P_X$ in $X^n = \{X_1, X_2, \ldots, X_n\}$, $1 \leq i \leq n$, is drawn i.i.d., then Alice can transmit $L$ bits of information to Bob while ensuring the upper bound on Wendy's probability of detection is $1 - \epsilon$, for some arbitrary $\epsilon \in (0, 1 - \alpha)$, where

$$L = nW \log \left(1 + \frac{\text{SNR}_B}{W}\right) T, \tag{6.11}$$

$T$ is the duration of each channel usage, in seconds, $W$ is Alice's bandwidth, in Hertz, $\text{SNR}_B$ is Bob's observed average power SNR, $\alpha$ is some arbitrary false positive rate,

$$n = \left\lfloor \frac{2(1 - \alpha - \epsilon)^2}{\ln 2 D(Q_Z \| P_Z)} \right\rfloor \tag{6.12}$$

$Q_Z$ is the probability distribution when Alice is not communicating, $P_Z$ is the probability distribution when Alice is communicating, and $D(Q_Z \| P_Z)$ is the KL divergence between $P_Z$ and $Q_Z$.

*Proof.* Given **Theorem 1**, $nC$ bits of information can be sent over a memoryless channel while bounding Wendy's probability of detection below some arbitrary threshold, $1 - \epsilon$. Furthermore, from the Shannon-Hartley theorem [46], the capacity for band-limited channels can be expressed as

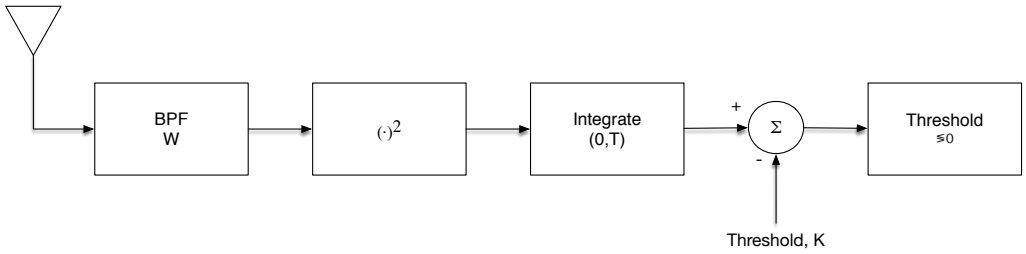



Figure 6.4: An energy detector. This image has been recreated from [184].

$$C = W \log\left(1 + \frac{\text{SNR}_B}{W}\right) \frac{\text{bits}}{\text{second}}, \tag{6.13}$$

where $\text{SNR}_B$ is Bob's received average power SNR in the bandwidth $W$. Letting $T$ denote the number of seconds per channel use, the steganographic capacity, $L$, is

$$L = nW \log\left(1 + \frac{\text{SNR}_B}{W}\right) T,$$

as required.

□

### 6.2.2 Estimating the KL Divergence

In the analysis in the previous section, it was assumed that Wendy was able to model the distributions when Alice is communicating, $P_Z$, and when she is not, $Q_Z$, perfectly. In reality, Wendy requires a device in order to detect Alice's communications and, from the research in LPD communication systems, the optimal device when only the covert signals' bandwidth, $W$, is known, is an energy detector [237]. An energy detector is a device that filters, squares, and sums a received signal before comparing the result to a pre-determined threshold (see **Figure 6.4** for the block diagram of an energy detector). If the signal's energy is above the threshold then the detector deems that communication has taken place; if it is below the threshold, the detector deems no communication has occurred. Moreover, the analysis in this section assumes that Wendy is able to perform coherent detection of Alice's communication, i.e., Wendy's reception of Alice's signal is coherent.

When using an energy detector, the distribution at its output when Alice is not communicating is modelled by a central chi-square distribution with $\eta = 2TW$ degrees of freedom, $\chi^2_\eta$, where $T$ is the per-channel-use time, in seconds [184]. Additionally, when Alice is communicating, the output from the energy detector is modelled by a non-central chi-square distribution with $\eta = 2TW$ degrees of freedom and a non-centrality parameter, $\lambda = \frac{\eta \text{SNR}_W}{W}$, $\chi^2_{\eta,\lambda}$, where $\text{SNR}_W$ is the average power SNR of the signal received by Wendy [184]. The KL divergence between $Q_Z$ and $P_Z$ is, therefore, between a central chi-square

distribution with $\eta$ degrees of freedom and a non-central chi-square distribution with $\eta$ degrees of freedom and non-centrality parameter $\lambda$. Expanding, $\lambda$

$$\begin{aligned}\lambda &= \frac{\eta \mathrm{SNR}_W}{W} \\ &= \frac{\mathrm{SNR}_W \ 2TW}{W} \\ &= 2 \ T \ \mathrm{SNR}_W\end{aligned}$$

it becomes evident that the non-centrality parameter does not depend on the band-limited channel's bandwidth and, therefore, the KL divergence between $\chi^2_\eta$ and $\chi^2_{\eta,\lambda}$ is not dependant on $W$.

Unfortunately, however, due to the complexity of the probability density functions (PDF) for $\chi^2_\eta$ and $\chi^2_{\eta,\lambda}$, calculating a closed-form expression for the KL divergence is unwieldy. Therefore, the KL divergence between a central chi-square distribution and a non-central chi-square distribution is estimated using the Wilson-Hilferty approximation [58] and Abdel-Aty approximation [7], respectively. Both approximations model the chi-square and non-central chi-square distributions' cumulative distribution function (CDF) by a modified version of a standard normal CDF, which makes the analysis of the KL divergence in this section more tractable. The approximated CDFs and PDFs for $\chi^2_\eta$ and $\chi^2_{\eta,\lambda}$ follow:

### Central Chi-Square ($\chi^2_\eta$)

The Wilson-Hilferty approximation for the CDF of $\chi^2_\eta$, $\Phi(x;\eta)$, $x \in [0,\infty)$, $\eta \in \mathbb{Z}^+$, is $\Psi(g(x;\eta))$, where

$$\begin{aligned}g(x;\eta) &= \frac{\left(\frac{x}{\eta}\right)^{\frac{1}{3}} - \left[1 - \frac{2}{9\eta}\right]}{\sqrt{\frac{2}{9\eta}}} \\ &= Ax^{\frac{1}{3}} - B,\end{aligned}$$

$A = \frac{1}{g_1 g_3}$, $B = \frac{g_2}{g_3}$, $g_1 = \eta^{\frac{1}{3}}$, $g_2 = 1 - \frac{2}{9\eta}$, $g_3 = \sqrt{\frac{2}{9\eta}}$ and $\Psi(x)$ is the CDF of $\mathcal{N}(0,1)$. Taking the derivative of $\Psi(g(x;\eta))$ with respect to $x$ yields the estimated PDF of $\chi^2_\eta$, $\phi(x;\eta)$,

$$\begin{aligned}\phi(x;\eta) &\approx \frac{d}{dx}\Psi(g(x;\eta)) \\ &\overset{(a)}{=} \psi(g(x;\eta)\frac{d}{dx}g(x;\eta)\end{aligned}$$

$$= \frac{Ax^{-\frac{2}{3}}}{3\sqrt{2\pi}} e^{-\frac{1}{2}\left(Ax^{\frac{1}{3}}-B\right)^2},$$

where

$$\psi(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$$

is the PDF of $\mathcal{N}(0,1)$ and the *Chain Rule* for differentiation has been used in step (a).

### Non-Central Chi-Square ($\chi^2_{\eta,\lambda}$)

Similarly, the Abdel-Aty approximation for the CDF of $\chi^2_{\eta,\lambda}$, $\Omega(x;\eta,\lambda)$, $x \in [0,\infty)$, $\eta \in \mathbb{Z}^+$, is $\Psi(h(x;\eta,\lambda))$, where

$$\begin{aligned} h(x;\eta,\lambda) &= \frac{\left(\frac{x}{a}\right)^{\frac{1}{3}} - \left[1 - \frac{2}{9}\left(\frac{1+b}{a}\right)\right]}{\sqrt{\frac{2}{9}\left(\frac{1+b}{a}\right)}} \\ &= Cx^{\frac{1}{3}} - D, \end{aligned}$$

$C = \frac{1}{h_1 h_3}$, $D = \frac{h_2}{h_3}$, $h_1 = a^{\frac{1}{3}}$, $h_2 = 1 - \frac{2}{9}\left(\frac{1+b}{a}\right)$, $h_3 = \sqrt{\frac{2}{9}\left(\frac{1+b}{a}\right)}$, $a = \lambda + \eta$ and $b = \frac{\lambda}{\eta+\lambda}$. Taking the derivative of $\Psi(h(x;\eta,\lambda))$ with respect to $x$ yields the estimated PDF of $\chi^2_{\eta,\lambda}$, $\omega(x;\eta,\lambda)$,

$$\begin{aligned} \omega(x;\eta,\lambda) &\approx \frac{d}{dx}\Psi(h(x;\eta,\lambda)) \\ &= \frac{Cx^{-\frac{2}{3}}}{3\sqrt{2\pi}} e^{-\frac{1}{2}\left(Cx^{\frac{1}{3}}-D\right)^2}. \end{aligned}$$

### KL Divergence

The KL divergence of $Q_Z = \phi(x;\eta) \approx \psi(g(x;\eta))$ and $P_Z = \omega(x;\eta,\lambda) \approx \psi(h(x;\eta,\lambda))$ is therefore,

$$\begin{aligned} &D(Q_Z \| P_Z) \\ &= D(\phi(x;\eta) \| \omega(x;\eta,\lambda)) \\ &\approx D(\psi(g(x;\eta)) \| \psi(h(x;\eta,\lambda))) \\ &= \int_0^\infty \psi(g(x;\eta)) \ln\left(\frac{\psi(g(x;\eta))}{\psi(h(x;\eta,\lambda))}\right) dx \end{aligned}$$

$$
\begin{aligned}
&= \int_0^\infty \frac{Ax^{-\frac{2}{3}}}{3\sqrt{2\pi}} e^{-\frac{1}{2}\left(Ax^{\frac{1}{3}}-B\right)^2} \ln\left(\frac{\frac{Ax^{-\frac{2}{3}}}{3\sqrt{2\pi}} e^{-\frac{1}{2}\left(Ax^{\frac{1}{3}}-B\right)^2}}{\frac{Cx^{-\frac{2}{3}}}{3\sqrt{2\pi}} e^{-\frac{1}{2}\left(Cx^{\frac{1}{3}}-D\right)^2}}\right) dx \\
&= \frac{A}{3\sqrt{2\pi}} \int_0^\infty x^{-\frac{2}{3}} e^{-\frac{1}{2}\left(Ax^{\frac{1}{3}}-B\right)^2} \ln\left(\frac{A}{C} e^{-\frac{1}{2}\left(Ax^{\frac{1}{3}}-B\right)^2+\frac{1}{2}\left(Cx^{\frac{1}{3}}-D\right)^2}\right) dx \\
&= \frac{A}{3\sqrt{2\pi}} \int_0^\infty x^{-\frac{2}{3}} e^{-\frac{1}{2}\left(Ax^{\frac{1}{3}}-B\right)^2} \\
&\qquad \left(\ln\left(\frac{A}{C}\right) - \frac{1}{2}\left[\left(Ax^{\frac{1}{3}}-B\right)^2 - \left(Cx^{\frac{1}{3}}-D\right)^2\right]\right) dx \\
&= \frac{A}{3\sqrt{2\pi}} \left[\frac{3e^{-\frac{1}{2}A^2x^{\frac{2}{3}}+ABx^{\frac{1}{3}}-\frac{B^2}{2}}}{2A^3}\right. \\
&\qquad \times \left(A^3x^{\frac{1}{3}} - A^2B - AC^2x^{\frac{1}{3}} + 2ACD - BC^2\right) \\
&\qquad -\frac{3\sqrt{\frac{\pi}{2}}\mathrm{erf}\left(\frac{B-Ax^{\frac{1}{3}}}{\sqrt{2}}\right)}{2A^3} \\
&\qquad \left.\times \left(2A^2\ln\left(\frac{A}{C}\right) + A^2D^2 - A^2 - 2ABCD + B^2C^2 + C^2\right)\right]\Bigg|_0^\infty \\
&= \frac{A}{3\sqrt{2\pi}} \left[\frac{3\sqrt{\frac{\pi}{2}}}{2A^3}\right. \\
&\qquad \times \left(2A^2\ln\left(\frac{A}{C}\right) + A^2D^2 - A^2 - 2ABCD + B^2C^2 + C^2\right) \\
&\qquad -\frac{\left(3e^{-\frac{B^2}{2}}\left[-A^2B + 2ACD - BC^2\right]\right)}{2A^3} \\
&\qquad +\frac{3\sqrt{\frac{\pi}{2}}\mathrm{erf}\left(\frac{B}{\sqrt{2}}\right)}{2A^3} \\
&\qquad \left.\times \left(2A^2\ln\left(\frac{A}{C}\right) + A^2D^2 - A^2 - 2ABCD + B^2C^2 + C^2\right)\right] \\
&= \frac{1}{2\sqrt{2\pi}A^2}\left[W_2 - \left(e^{-\frac{B^2}{2}}\left[-A^2B + 2ACD - BC^2\right] - \right.\right. \\
&\qquad \left.\left.\mathrm{erf}\left(\frac{B}{\sqrt{2}}\right)W_2\right)\right],
\end{aligned}
\tag{6.14}
$$

where

$$
W_2 = \sqrt{\frac{\pi}{2}}\left[2A^2\ln\left(\frac{A}{C}\right) + A^2D^2 - A^2 - 2ABCD + B^2C^2 + C^2\right]
$$

and $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$ is the error function.

Combining **Equation 6.14** with equations **6.11** and **6.12** a closed-form approximation for the steganographic capacity of band-limited channels can, therefore, be obtained.

### Approximation Error

The original works of Wilson-Hilferty [58] and Abdel-Aty [7] provided error results for their CDF approximations; however, they did not present error results for their corresponding PDF approximations. To address this, the percentage approximation error for the CDF of $\chi^2_\eta$ and $\chi^2_{\eta,\lambda}$, i.e., $\max\limits_x \frac{|\Psi(g(x;\eta))-\Phi(x;\eta)|}{\Phi(x;\eta)}$ and $\max\limits_x \frac{|\Psi(h(x;\eta,\lambda))-\Omega(x;\eta,\lambda)|}{\Omega(x;\eta,\lambda)}$, as well as the percentage approximation error for the PDF of both distributions, i.e., $\max\limits_x \frac{|\psi(g(x;\eta))-\phi(x;\eta)|}{\phi(x;\eta)}$ and $\max\limits_x \frac{|\psi(h(x;\eta,\lambda))-\omega(x;\eta,\lambda)|}{\omega(x;\eta,\lambda)}$ were calculated and can be found in **Appendix A** and **Appendix B**, respectively (see **Appendix C** for the algorithms that were used to populate these tables). To generate the values in the tables of **Appendix A** and **Appendix B**, the $\max\limits_x$ was taken over all $x$-values corresponding to each p-value, $p$, $\{p \in \mathbb{Z}^+ | 1 < p < 100\}$, i.e., $x = \Phi^{-1}(p;\eta)$ and $x = \Omega^{-1}(p;\eta,\lambda)$ for each distribution, respectively. Generally, in LPD radio systems the communicating parties attempt to communicate at the lowest SNR possible (a low $\text{SNR}_W$ results in a small non-centrality parameter, $\lambda$). **Appendix B** shows that the approximations derived in this section are most accurate under this condition, i.e., low values of $\lambda$, as well as high values of $\eta$.

### Analysis

Given that **Theorem 1** and **Theorem 2** presented results for $L$ that did not depend on the duration of each channel use, $T$, it would stand to reason that the value $nT$ for band-limited channels would not depend on the specific value of $T$, i.e., $n = \Theta(T^{-1})$, either. This hypothesis can be confirmed by examining **Figure 6.5**. **Figure 6.5** shows that for a given $\text{SNR}_W$ the value $nT$ is invariant for all values of $T$ where $n$ is not equal to zero. Letting the hypotenuse of the triangle in the diagram be $T_{\min}$, it follows that $T_{\min}$ denotes the observation time after which point Wendy can detect Alice with just one observation. Not surprisingly, as $\text{SNR}_W \to -\infty$, $T_{\min} \to \infty$ as well. Logically, this makes sense, in that for a given $\text{SNR}_W$ there is some observation time $T_{\min}$ at which point Wendy can detect Alice's communications with probability $1-\epsilon$ regardless of the particular per-channel-use observation time, $T > T_{\min}$. What this result says is that when Wendy performs an optimal LLRT on the output of an optimal energy detector her observation interval, $T$, is immaterial, the only time value of importance is $T_{\min}$ for each given $\text{SNR}_W$ and, as long as Wendy can observe $T_{\min}$ seconds of Alice's transmission she can detect Alice with some arbitrary probability $1-\epsilon$. Conversely, in order to remain undetected, Alice must only transmit for less than $T_{\min}$ seconds. See **Figure 6.6** for the graph of $\text{T}_{min}$ under various values of $\epsilon$ (**Figure 6.6** shows the hypotenuse of the triangle from **Figure 6.5**). Analyzing **Figure 6.6** allows the following straight-line extrapolations for $T_{\min}$ to be made:

$$nT_{(log_{10})} = -0.2\text{SNR}_{W(dB)} + 3.1 \text{ (for } \epsilon = 0.500) \tag{6.15}$$

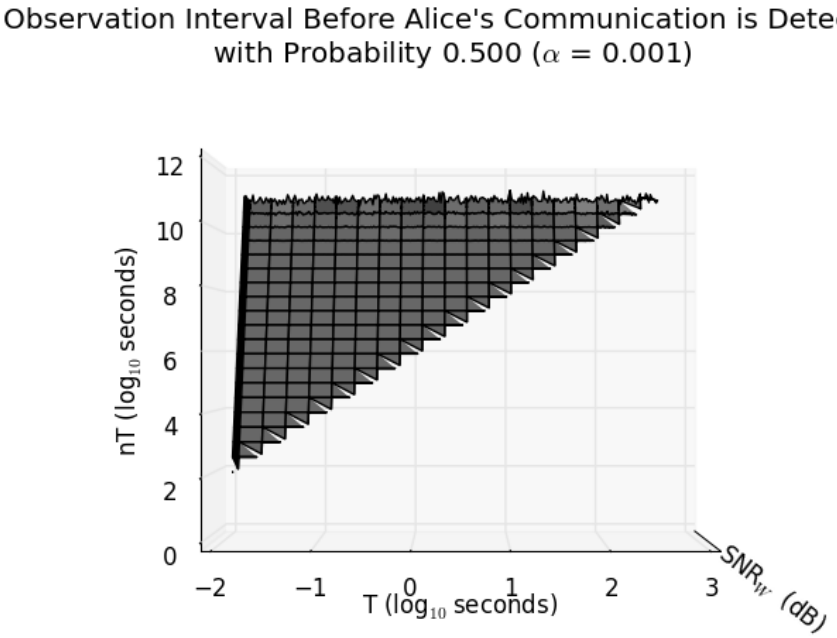



Figure 6.5: Observation Interval Before Wendy Detects Alice's Band-Limited Communications with Probability $> 0.500$

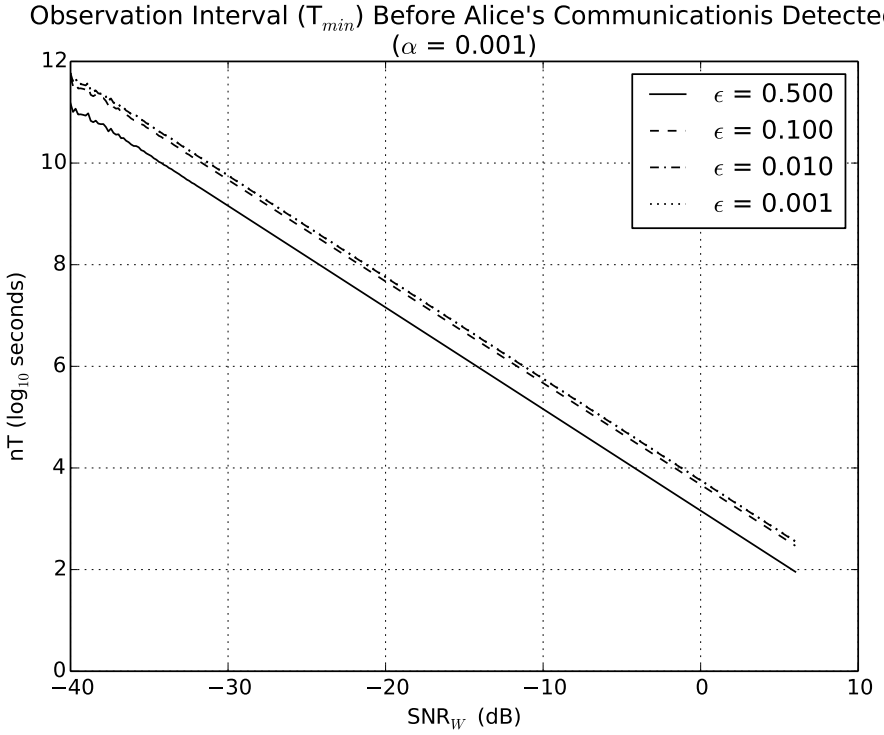



Figure 6.6: Observation Interval, $T_{min}$

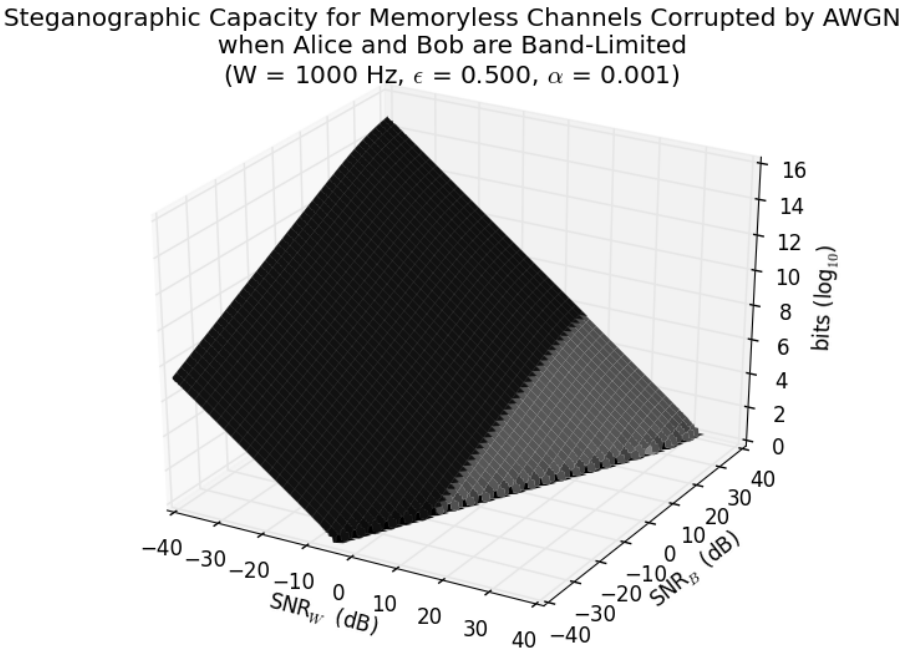



Figure 6.7: Steganographic Capacity for Band-Limited Systems

$$nT_{(log_{10})} = -0.2\text{SNR}_{W(dB)} + 3.7 \text{ (for } \epsilon = 0.001\text{)}.$$

Finally, the steganographic capacity is plotted for band-limited systems where $W = 1000$ Hz in **Figure 6.7**. Modifying the value for $W$, while leaving $\text{SNR}_B$ constant, simply increases the capacity, since the number of channel uses $n$ is not dependant on $W$, only the single channel use capacity, $C$, is. Despite performing an optimal LLRT after using an optimal energy detector, Wendy permits Alice to transmit significantly more bits of information than she did when she performed a theoretically optimal test in the previous section (see **Figure 6.3**). Additionally, Wendy requires a significantly higher SNR, $\text{SNR}_W$, in order to detect Alice with probability $1 - \epsilon$. In **Figure 6.7**, the black portion of the surface was generated using the estimated KL divergence calculated in this section whereas the grey portion of the surface was calculated using the straight-line extrapolation formula shown in **Equation 6.15**. The black portion of the surface is cut off around $\text{SNR}_W = 5$ dB because above this threshold the approximation error grows larger than 2 % (see the entry for $\eta = 25$, $\lambda = 0.100$ in **Appendix B**).

## 6.3 Steganographic Capacity with a Random Transmitter

In **Section 6.1**, it was demonstrated that in AWGN the steganographic capacity of the channel is zero when $\text{SNR}_W \geq 5$ dB and $\epsilon = 0.5$. As previously noted, this represents the best-case scenario for Wendy and thus a lower bound on the steganographic capacity since Wendy knows the exact statistical distribution both when Alice is communicating and

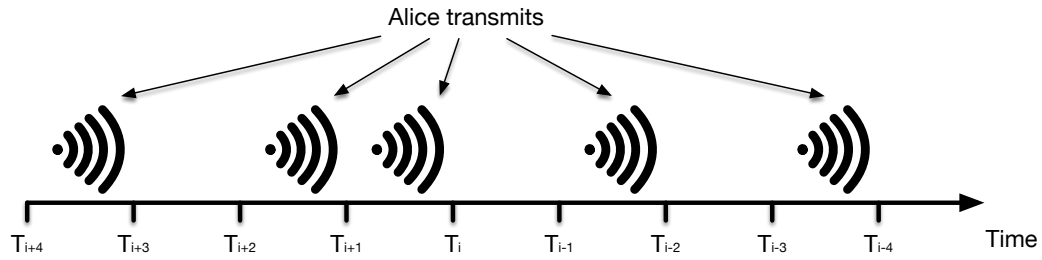



Figure 6.8: Alice chooses which time slot, $T_i$, to transmit in pseudorandomly. Wendy, on the other hand, attempts to detect Alice's communications by measuring for Alice's signal in each time slot.

when she is not and constructs an optimal test based on this information. Additionally, in **Section 6.2**, it was shown that the steganographic capacity is significantly higher under the same parameters when Wendy employs an optimal energy detector. Moreover, in **Section 6.2**, it was assumed that Wendy performed coherent detection of Alice's communications.

In this section, the steganographic capacity of OOB-CCs is evaluated when Wendy uses an optimal energy detector; however, it is no longer assumed that Wendy is able to perform coherent detection. Wendy's performance, as measured by steganographic capacity, is evaluated under the assumption that Alice and Bob have managed to share a covert-key and have used the covert-key to pseudorandomly determine which time slots, $T_i$, of length $T$ seconds, that they will transmit in; see **Figure 6.8** (this random transmission technique was previously explored in the context of the "square root" law by Bash, et al. [25]). In the previous section, it was assumed that Alice was continuously transmitting and, as a result, Wendy could simply listen until she had captured enough samples (i.e., $T_{\min}$). In this section, Wendy can no longer do so given that Alice now transmits in random time slots. In order to simplify the analysis in this section, however, it is assumed that Wendy and Alice are synchronized on the time boundaries that Alice could communicate on. That is, Wendy performs a test to determine if Alice is communicating at each time slot, $T_i$, aligned exactly to the beginning of the time slot. Under this new model, Wendy is thus forced to perform independent tests of duration $T$ seconds in each time slot since she does not know which time slots contain Alice's communication.

When using an energy detector, a false positive occurs if the output of the integrator, $k$, is above the threshold $K$, but there is no covert signal present (see **Figure 6.4**). Similarly, a missed detection error occurs when the output of the integrator, $k$, is below the threshold, $K$, but there is a covert signal present. The false positive probability, $\alpha$, therefore, is shown in **Equation 6.16**, and the missed detection probability, $\beta$, is shown in **Equation 6.17**, where $P_{\mathcal{X}^2_\eta}$ represents the PDF of the chi-squared distribution with $\eta$ degrees of freedom and $P_{\mathcal{X}^2_{\eta,\lambda}}$ represents the PDF of the non-central chi-squared distribution with $\eta$ degrees of freedom and a non-centrality parameter, $\lambda$.

$$\alpha = Pr[k > K | \text{ signal is not present}]$$

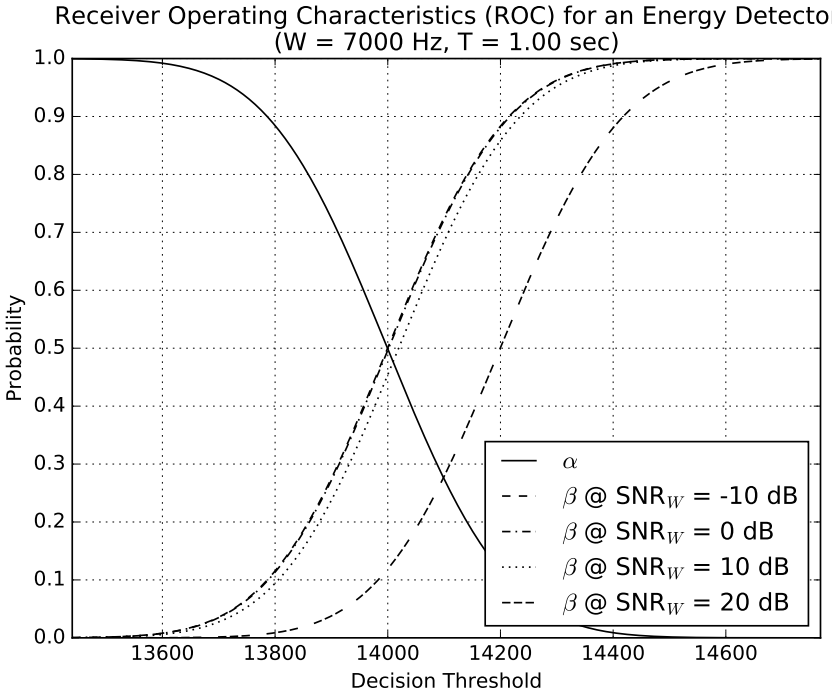



Figure 6.9: The receiver operating characteristics (ROC) for Wendy's energy detector. The probability of missed detection, $\beta$, is plotted for various values of $\text{SNR}_W$.

$$= \int_K^\infty P_{\mathcal{X}^2_\eta}(x)dx \tag{6.16}$$

$$\beta = Pr[k < K| \text{ signal is present }]$$

$$= \int_{-\infty}^K P_{\mathcal{X}^2_{\eta,\lambda}}(x)dx \tag{6.17}$$

The receiver operating characteristics (ROC), given this construction, for various values of $\text{SNR}_W$ are plotted in **Figure 6.9**. By examining the equal error rate (EER), i.e., the point where $\alpha = \beta$, for the various $\beta$ curves, it can be seen that as $\text{SNR}_W \to -\infty$, $\alpha + \beta \to 1$. Therefore, as $\text{SNR}_W \to -\infty$, Alice can communicate without being reliably detected, i.e., Alice approaches what is referred to in the study of steganography as *perfect steganography*. *Perfect steganography* is the condition where the KL divergence between stego object and cover object is zero [33]. In the context of OOB-CCs, the term relates to the condition where $\alpha + \beta = 1$. A proof showing that if $\alpha + \beta = 1$ then the KL divergence is equal to zero follows:

**Theorem 4.** If Wendy's sum of probability errors is equal to one (i.e., $\alpha + \beta = 1$), then Alice and Bob have achieved *perfect steganography.*

*Proof.*

$$\alpha + \beta \overset{(a)}{=} 1 - \frac{1}{2}TV(P_{H_0}, P_{H_1})$$

$$
\begin{aligned}
1 &= 1 - \frac{1}{2} TV(P_{H_0}, P_{H_1}) \\
TV(P_{H_0}, P_{H_1}) &= 0 \\
\int_{x \in \mathcal{X}} |P_{H_0}(x) - P_{H_1}(x)| \, \mathrm{d}x &\overset{(b)}{=} 0 \\
P_{H_0}(x) &\overset{(c)}{=} P_{H_1}(x) \; \forall x \in \mathcal{X},
\end{aligned}
$$

where in (a) **Equation 6.1** was used, in (b) **Equation 6.2** was used, and in (c) the fact that a sum of absolute values equals zero must mean that all individual values are zero, since $|x| \geq 0$, has been used.

Recalling the definition of KL divergence from **Equation 6.4**:

$$
\begin{aligned}
D(P_{H_0} \| P_{H_1}) &= \int_{x \in \mathcal{X}} P_{H_0}(x) \log \frac{P_{H_0}(x)}{P_{H_1}(x)} \, \mathrm{d}x \\
&= \int_{x \in \mathcal{X}} P_{H_0}(x) \log 1 \, \mathrm{d}x \\
&= \int_{x \in \mathcal{X}} 0 \, \mathrm{d}x \\
&= 0,
\end{aligned}
$$

and, therefore, if $\alpha + \beta = 1$, then the KL divergence is zero, which is the condition for *perfect steganography* [33].

□

Given the construction of an energy detector, in each time slot that Alice is transmitting, Wendy detects her communication with probability $p = 1 - \beta$, where the trade-off between $\alpha$ and $p$ is shown in **Figure 6.10**. This plot empirically confirms that as $\mathrm{SNR}_W \to -\infty$, $p \to \alpha$ and thus $\alpha + \beta \to 1$.

In order to improve her performance, it is assumed that Wendy performs multiple observations of the channel. Therefore, if Wendy detects Alice's communications with probability $p$ in each observation, and Wendy performs multiple observations, then the number of time slots that Wendy must observe before she can detect Alice's communications for the first time, is modelled by a geometric random variable, $M$, with parameter $p$ and probability mass function

$$
\begin{aligned}
Pr[M = m] &= (1 - p)^{m-1} p \\
&= \beta^{m-1} p.
\end{aligned}
$$

Moreover, the probability that Wendy detects Alice's communications at least once after $m$ observations is then $1 - (1 - p)^m = 1 - \beta^m$, i.e., one minus the probability of the event that

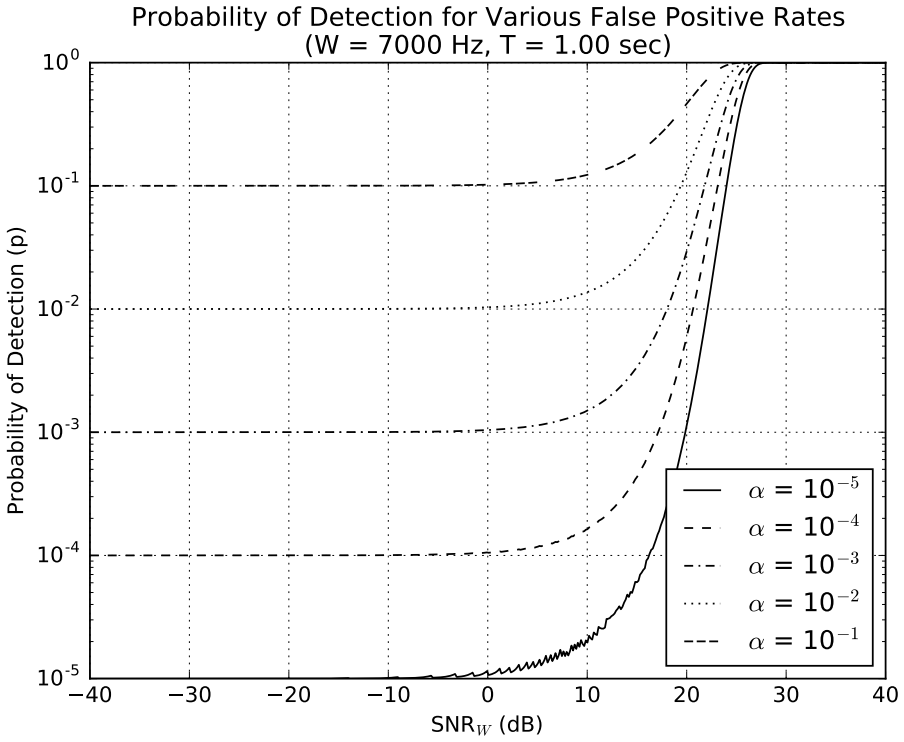



Figure 6.10: Plot of probability of detection, $p$, versus $\text{SNR}_W$, for various false alarm rates $\alpha$.

Wendy does not detect Alice's communications in any of the $m$ observations. If, again, $n$ is defined to be the maximum number of observations such that Wendy's upper bound on $P_D$ is $1 - \epsilon$, for some arbitrary $\epsilon \in (0, 1 - \alpha)$, then

$$\begin{aligned} 1 - (1-p)^n &= 1 - \epsilon \\ (1-p)^n &= \epsilon \\ n &= \left\lfloor \frac{\log \epsilon}{\log (1-p)} \right\rfloor \\ &= \left\lfloor \frac{\log \epsilon}{\log \beta} \right\rfloor, \end{aligned} \tag{6.18}$$

where the floor is taken to upper bound Wendy's probability of detection, $P_D$. The steganographic capacity is then $L = nCT$, where $T$ is the length of each time slot that Alice could communicate in, $n$ is shown in **Equation 6.18**, and $C$ is the Shannon-Hartley channel capacity for band-limited systems and, as a reminder, can be expressed as

$$C = W \log \left(1 + \frac{\text{SNR}_B}{W}\right) \frac{\text{bits}}{\text{second}}.$$

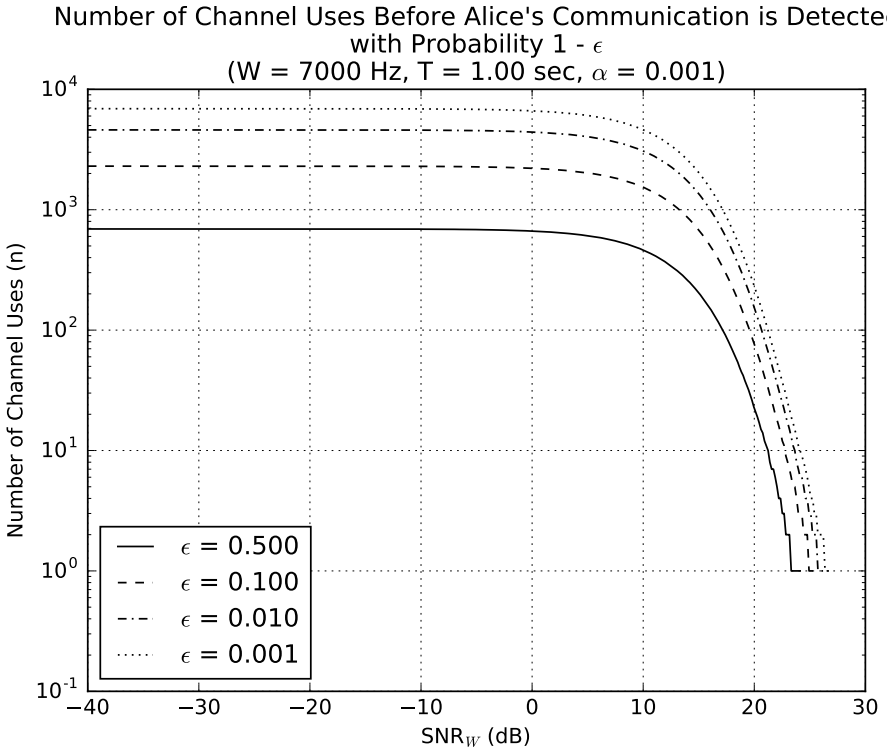



Figure 6.11: Plot of $n$ versus $\text{SNR}_W$ for various values of $\epsilon$.

Practically speaking, in order for Wendy to determine her threshold, $K$, she first must choose an acceptable level for her false positive rate, $\alpha$, then solve **Equation 6.16** for $K$. Once the value for $K$ is obtained, Wendy's per-observation probability of detection, $p$, can then be calculated by applying **Equation 6.17** and subtracting the result from one. This procedure is an application of the Neyman Pearson criterion for detection [184]. In **Figure 6.11**, various curves for different values of $\epsilon$ are plotted to highlight the maximum number of channel uses, $n$, that Alice can transmit in, while upper bounding Wendy's probability of detection to $1 - \epsilon$. Examining the figure, it can be see that below approximately $\text{SNR}_W =$ -10 dB, the number of channel uses that Alice has available for communication without being detected plateaus; this, again, reflects the situation where $\alpha + \beta \to 1$, and in reality below this threshold Alice approaches *perfect steganography*.

At this point, it should be highlighted that the duration of each time slot, $T$, is completely within the control of Alice and Bob. As a result, the effect of modifying the time slot interval time $T$ on the steganographic capacity is examined. It should be reiterated that despite the value for $T$ being chosen by Alice, it is assumed that Wendy knows the value for $T$ ahead of time, though not which of the $T_i$ time slots that Alice has chosen to transmit in. The effect of modifying the per-channel-use time, $T$, can be seen in **Figure 6.12**. The shaded region of the graph represents the $\text{SNR}_W$ and $T$ values where $|1 - (\alpha + \beta)| < 10^{-3}$. The effects of Alice varying her transmit time $T$ is clear. As Alice restricts her transmit time, $T$, Alice's sum of errors $\to 1$. It is clearly within Alice's best interest, therefore, to restrict how long she transmits for in each time slot since for fixed a $\text{SNR}_W$, as $T \to 0$,

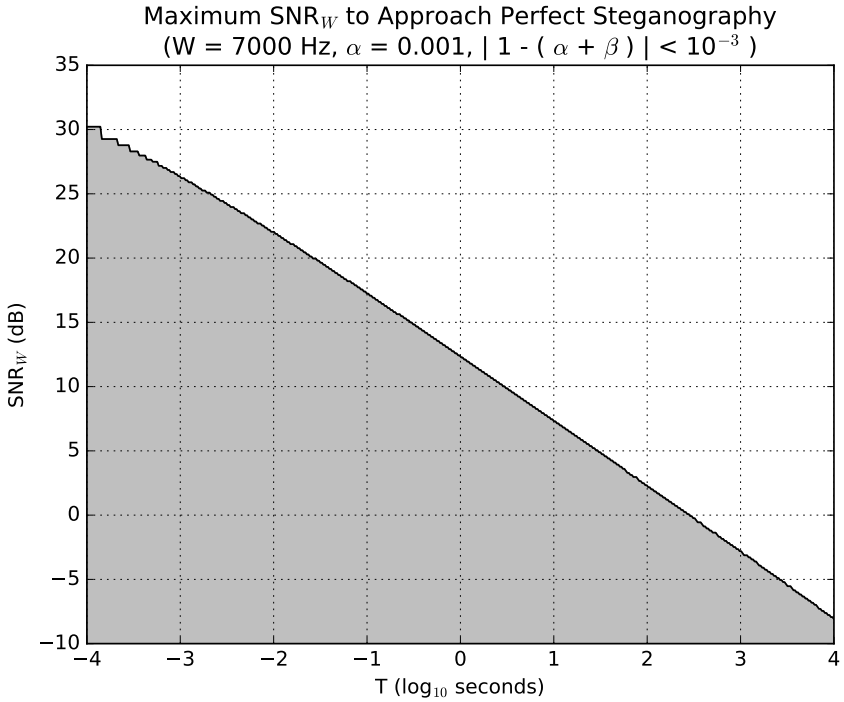



Figure 6.12: For each time slot interval value, $T$, the $\text{SNR}_W$ (dB) values at which point Wendy's sum of probability errors $|1 - (\alpha + \beta)| < 10^{-3}$ are coloured grey.

Wendy's sum of probability errors, $\alpha + \beta \to 1$.

The steganographic capacity when Wendy uses an energy detector to detect Alice's communications is shown in **Figure 6.13**. As demonstrated by **Figure 6.12**, the steganographic capacity for OOB-CC signals is highly dependant on T, which is reflected in **Figure 6.13**. Six sub-plots are provided, each with a different value for $T$ from $T = 10$ seconds to $T = 10^{-4}$ seconds. Moreover, in each of the sub-plots the region of the graph where $|1 - (\alpha + \beta)| < 10^{-3}$ is shaded black. These plots provide evidence that Alice's strategy is not only to ensure $\text{SNR}_W$ is a small as possible, but also to ensure that $T$ is as small as possible. Now, given this strategy, it appears Alice's requirement for undetectable communication is that she and Bob must be able to communicate with decreasing SNR and per-channel-use time, which is tantamount to saying that Alice must communicate undetectably by not communicating at all. As a result, in **Chapter 8**, the practical limits on both SNR and $T$ are explored for a real-world covert channel (e.g., a covert-acoustic channel) when Wendy employs an energy detector.

The last study in this section is the analysis of the attenuation factors $\alpha_W$ and $\alpha_B$. A plot of Wendy's sum of errors, $\alpha + \beta$, versus distance is shown in **Figure 6.14**. In the plot multiple curves are shown, each corresponding to different received SNR values at Bob, $\text{SNR}_B$. For each curve, the deleterious effect that distance has on Wendy's sum of errors can be seen. This plot shows that if Alice can make assumptions about Wendy's location and Alice knows Bob's location, then Alice has a better chance of approaching *perfect steganography* by ensuring some maximal $\text{SNR}_B$ and minimal $\text{SNR}_W$. Furthermore,

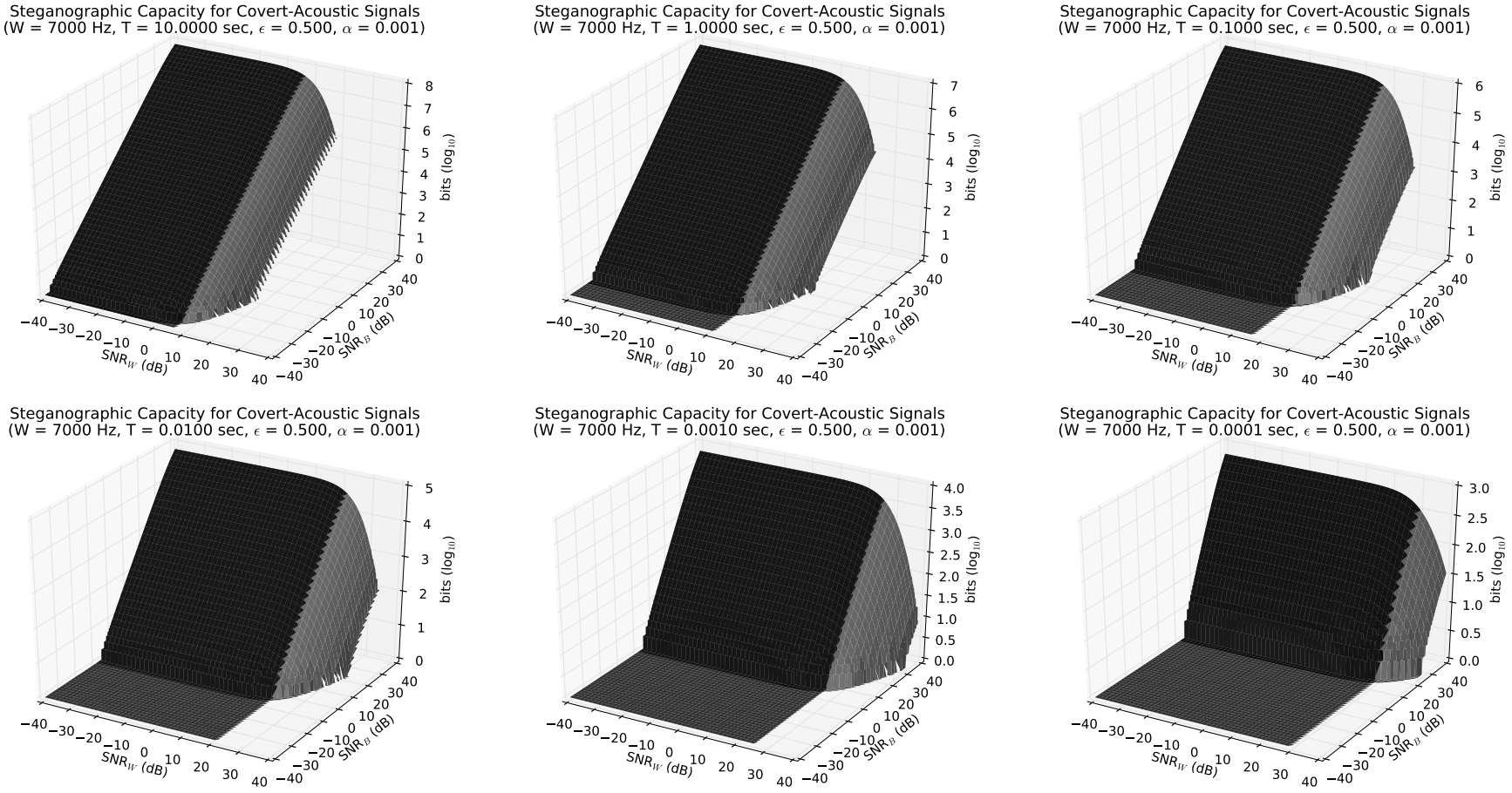



Figure 6.13: The steganographic capacity when Wendy uses an energy detector to detect Alice's OOB-CC communication.

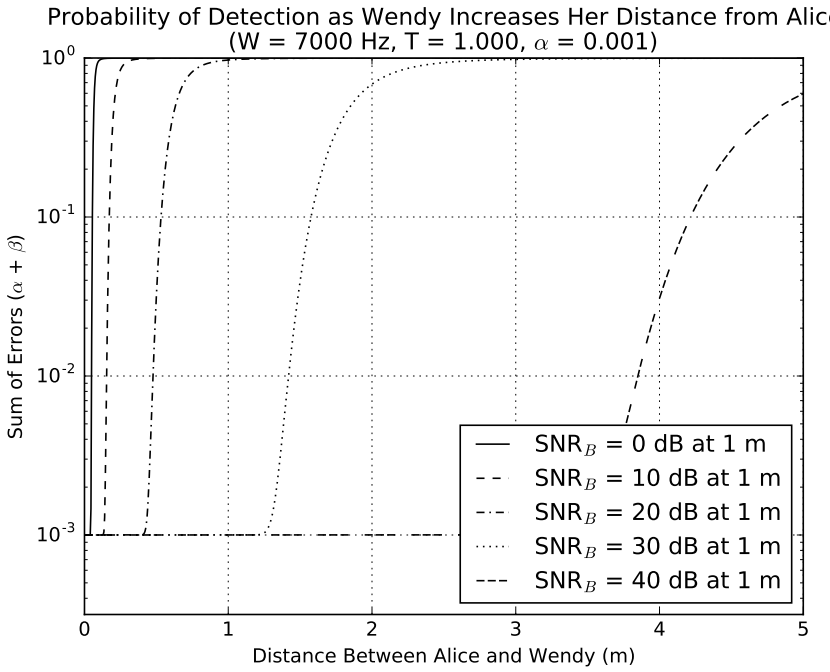



Figure 6.14: The relationship between Wendy's sum of errors, $\alpha + \beta$, is shown with respect to her distance from Alice. Multiple curves are shown, each of which corresponds to a received SNR at Bob, $\text{SNR}_B$, at a distance of 1 m.

it is clearly within Wendy's best interest to be as close to Alice as possible when she is transmitting.

From a detection perspective, more analysis is required to study the effects on the steganographic capacity when a detector is employed that takes more information into account than just the signal's bandwidth, $W$. While the energy detector that was studied in this chapter is optimal when only the signal's bandwidth is known, a motivated detector would try to employ a detection scheme that takes into account as much of the signal's information as possible in order to achieve the theoretical results presented in **Section 6.1** and **Section 6.2**. In order to validate the results presented in **Section 6.3**, in **Chapter 8**, a study where Wendy has knowledge of all the signal's properties except for some secret information that is shared between Alice and Bob, is presented.

Furthermore, the results of this chapter only analyzed the steganographic capacity when Wendy was a passive covert-analyst. In **Chapter 8**, the result of Wendy being an active covert-analyst is also studied. Logically, if Wendy has knowledge of the modulation scheme being used by Alice and Wendy knows the bandwidth of Alice's signals, Wendy can transmit noise on the same frequencies that Alice is using in order to jam Alice's signal, causing Bob's BER to increase, and thus the steganographic capacity of the channel to decrease. In the next chapter, **Chapter 7**, the covert-acoustic channel is studied in depth, and the achievable data rate of the channel is evaluated using commodity hardware.

# Chapter 7

# The Achievable Data Rate of Covert-Acoustic Channels

In this chapter, the achievable data rate of covert-acoustic channels is empirically evaluated in order to answer the question: *Can covert-acoustic channels capable of leaking sensitive information be enabled by* semi- *or* non-invasive covert exploits *between a modulator and a demodulator using only* commodity-pervasive *hardware*? To answer this question, modulators and demodulators are engineered and built in order to maximize the communication rate over covert-acoustic channels established between commodity desktops, laptops, and mobile devices, using only their built-in speakers and microphones. The information hiding strategy employed in this evaluation results in the channels being *imperceptible* to a passive adversary and, therefore, can be classified as *undetectable covert channels*. Furthermore, for the purposes of this initial study, the channel attacker model is *shared* and the adversary is considered to be an unaware and unassuming passive adversary.

Over the course of the next two chapters the covert-acoustic channel is evaluated in detail. In this chapter, the achievable data rate of covert-acoustic channels is evaluated in the presence of an oblivious passive adversary. Covert-acoustic channels are examined in a lab environment and their data rate is also measured in two real-world office settings: an open-concept office and a closed-door office under real-world conditions: humans present in the environment, humans absent from the environment, and a clock radio playing in the environment while data is being covertly communicated. In **Chapter 8**, the *covertness* of covert-acoustic-channels is evaluated in the presence of a passive adversary who uses technical tools to detect the covert-acoustic channel as well as an active adversary who tries to interfere with Alice and Bob's communication. The covert-acoustic channels presented in **Chapter 7** and **Chapter 8** were evaluated using a variation of the *pyCovertAudio* software, which is a python and C software tool that was written by the author to test the limitations of covert-acoustic channels. All *pyCovertAudio* software, documentation, and user guide are freely available for download [34].

This chapter is organized as follows. In **Section 7.1** the acoustic channel is introduced more formally and the effects of the channel on acoustic communication are explored. Additionally, the physical lab environment used in this study is introduced. In **Section**

**7.2**, it is proven that, given the acoustic channel's characteristics, orthogonal frequency-division multiplexing (OFDM) is a much more performant modulation scheme, in terms of achievable data rate, than the schemes that have been used in previous work. In **Section 7.3**, experimental results are presented in detail, which demonstrate that covert-acoustic signals can be used to leak sensitive information from a high-security network to a low-security network, in general. Lastly, in **Section 7.4**, the risk posed by covert-acoustic channels is demonstrated by using covert-acoustic OFDM signals to leak information in real-world environments under real-world scenarios.

## 7.1 Acoustic Channel

In this section, an in-depth look at the characteristics of the acoustic channel is presented and it is demonstrated, by way of measurement, that the over-the-air acoustic channel causes multipath delays and has a non-ideal frequency response. Furthermore, the ambient acoustic noise in the lab environment is characterized as *pink noise*.

Generally speaking, acoustic communication provides a number of benefits as compared to traditional modes of communication, e.g., radio-frequency (RF). First, the devices required for acoustic communication (e.g., speakers and microphones) are ubiquitous in today's computing systems (e.g., smart phones, laptops, desktops) and, therefore, no hardware modifications are required in order to enable communication. Second, ultrasonic communication above 20 kHz at low volumes appears to be harmless to humans [73]. Third, there are a number of security benefits to using acoustic communication: sounds can be localized to a room, the communication can be heard if it occurs in the audible range, and the transmission distance can be controlled by limiting the intensity, i.e., volume, of the transmitted signals. Fourth, acoustic communication is a valid communication alternative in situations where RF is not permitted (e.g., medical environments, airplanes) and it is not impacted by environmental factors such as sunlight, rain, or metal objects as compared to other channels.

Conversely, there are a number of drawbacks to using acoustic signals for communication. First, the achievable bit rates when using acoustic communication are much lower than RF and IR as sound waves travel slower (approximately 300 m/s versus 3 x $10^8$ m/s) than radio and light waves do. Second, the over-the-air channel has relatively large ambient noise, especially at low frequencies. Third, the acoustic modulation and demodulation schemes employed must take into account reverberations and the blurring of signals due to reflections of the originally transmitted signal off of objects in the environment. Fourth, there are medical concerns to using acoustic signals for communication: they can be annoying to bystanders, especially in cases where the sound is transmitted at high volumes; listening to audio in the 6 kHz to 16 kHz range can impact a bystander's degree of fatigue and wakefulness [129]; and noise below 100 kHz can be unpleasant to animals in the environment.

Table 7.1: The Systems Used in This Study

| ID | Make | Model | Operating System |
|---|---|---|---|
| Audio1 | Lenovo | Ideapad S10 | Windows 7 |
| Audio3 | Dell | Precision T3500 | Windows 7 |
| Audio4 | HP | HP Mini | Windows 7 |
| Audio5 | Acer | Aspire One | Windows 7 |
| Audio6 | Alienware | M15X | Windows 7 |
| Audio7 | Sony | Vaio | Windows 7 |
| Audio8 | Apple | MacBook Pro | Mac OS X 10.9 |
| Audio11 | Apple | iPhone 6 | iOS 8.4 |
| Audio12 | Apple | iPhone 4S | iOS 8.1 |
| Audio14 | Samsung | Galaxy Nexus | Android 4.4.4 |

### 7.1.1 Lab Environment and System Requirements

One of the goals of this chapter is to assess the risk that unauthorized acoustic channels pose to the security of air-gapped systems. Researchers have previously demonstrated the ability for acoustic signals to bridge the air-gap; however, they have only demonstrated limited bit rates [89, 90], on specific hardware [53, 89, 90, 131], and, in some cases, only in the near-ultrasonic band [53, 89]. This chapter, conversely, shows that, in general, covert-acoustic communication can be achieved using unmodified commodity systems, that the achievable bit rates are well above those previously reported, and that true ultrasonic communication is possible.

In order to prove these assertions, the covert-acoustic channel was first studied in a lab environment, whose layout can be seen in **Figure 7.1**. In total, ten systems were placed throughout the environment, each of which is described in **Table 7.1**. Each of the systems was labelled with the string **Audio** plus a numeric identifier and the distances between **Audio1** and each of the other machines can be seen in **Table 7.2** (0 ° can be understood as being directly in front of **Audio1** and positive offset angles are measured counter-clockwise from 0 °). The systems were chosen such that the heterogeneity of their hardware configuration represented that of a typical corporate environment, i.e., a desktop as well as a collection of laptops and mobile handsets.

The desktop and laptops used in this study were all configured with Windows 7, aside from **Audio8**, which was configured with Mac OS X 10.9. The two Apple iPhones were configured with iOS 8 and the Samsung Android phone was configured with Android 4.4 (KitKat). Additionally, none of the machines in this study had any hardware added or modified with the exception of **Audio3**, which had a USB headset (microphone and speaker) added because it did not have these devices installed by default. Moreover, some of the devices were configured, through software, via controls offered by the operating

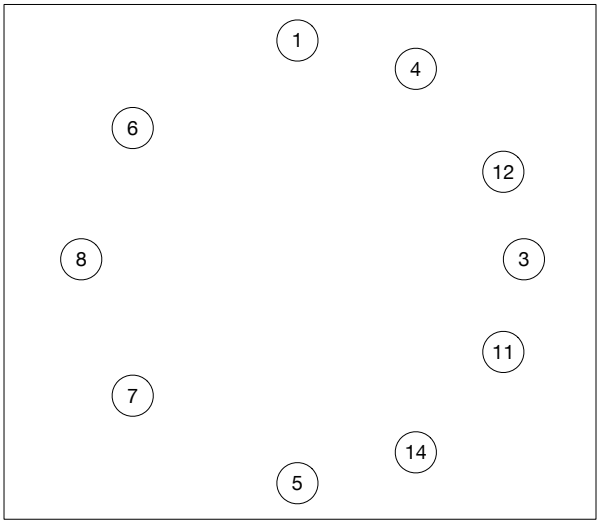



Figure 7.1: The lab environment used in this study. The circles labelled with numeric identifiers represent systems, i.e., "1" represents the "Audio1" system. The lab space used was approximately 2.06 m x 2.44 m x 1.98 m.

system, including the volume level of the speaker and the sensitivity level of the microphone being raised to their respective maximum levels. Such changes via the operating system's software controls would be well within the reasonable control of malware installed on a system. The tests run for this chapter were executed in *simplex* mode, i.e., uni-directional communication from the high-security system to the low-security systems, and, therefore, the detailed hardware and software configuration requirements for the systems can be summarized as follows:

- **High-Security System:**
    1. A speaker
    2. Software initially installed and updated online before the system is taken offline (as outlined in [204])
    3. No network connections to the low-security systems
- **Low-Security Systems:**
    1. A microphone

Lastly, given the slight modifications made to the operating system's sound settings and the uniform manner in which the systems were configured, this study's environmental model closely mimics that of a real-world corporate office where the same version of Windows is installed on most corporate machines and employees are permitted to bring their own devices to work under a "bring your own device" policy.

Table 7.2: Distance Between Audio1 and the Other Systems in the Lab Environment

| ID | Distance | Angle |
|---|---|---|
| Audio3 | 1.04 m | 41 ° |
| Audio4 | 0.48 m | 62 ° |
| Audio5 | 1.47 m | 0 ° |
| Audio6 | 1.52 m | 289 ° |
| Audio7 | 0.86 m | 334 ° |
| Audio8 | 1.24 m | 309 ° |
| Audio11 | 1.32 m | 16 ° |
| Audio12 | 0.81 m | 47 ° |
| Audio14 | 1.47 m | 11 ° |

The systems used in this study that were running the Windows and the Mac OS X operating systems did not require any further modification in order to allow access to their systems' speaker or microphone. As a result, the software that was developed to test the covert-acoustic channel was able to run without requiring any additional permissions and, therefore, the covert-acoustic channels established on systems running Windows and Mac OS X can be classified as covert channels that require a *non-invasive* covert-exploit. On the iOS and the Android operating systems, however, additional permissions were required by the developed software in order to record audio using their systems' microphone. While both operating systems allowed access to their systems' speakers without any special permissions, on Android the permission *android.permission.RECORD_AUDIO* was required to access the microphone [5] and on iOS permission to record audio had to be requested from the user through the API call *AVAudioSessionRecordPermission* [6]. Given these additional requirements, the covert-acoustic channels established using iOS and Android would require a *semi-invasive* covert exploit in order to enable the channel. The analysis going forward in this dissertation, however, does not look for ways in which these permissions can be obtained without user interaction, but rather assumes that these exploits exist and leaves finding an appropriate covert exploit to future researchers.

### 7.1.2 Measured Channel Characteristics

To properly engineer communication through the covert-acoustic channel, the following quantities were measured in the lab environment:

1. the power spectrum of the background noise,
2. the duration of reverberations caused by objects in the environment, and
3. the frequency response of the microphones and speakers built into the devices listed in **Table 7.1**.

In this section, the experiments that were used to measure each of these quantities are discussed and their results are presented.

### Background Noise

It has previously been reported that background acoustic noise drops off exponentially with increased frequency and that office environments contain equipment that generate noise at specific frequencies (e.g., monitors generate noise at their line frequencies) [230]. This was confirmed, through measurement, by observing the power spectral density (PSD), $S_x(f)$, of the noise in the lab environment. Measuring the PSD of a signal allows the distribution of power across the signal's frequency components to be evaluated and it was observed that the PSD, $|S_x(f)|$, roughly decreased in proportion to the frequency of the signal, $f$, i.e., $|S(f)| \propto \frac{1}{f^{\alpha}}$ in the lab environment. Therefore, the background noise can be roughly categorized as *pink noise* as opposed to *white noise*, which would have seen $|S_x(f)|$ as a constant across the signal's frequency spectrum [57].

Relatively speaking, the noise level in the lab environment was quite low at frequencies above 3 kHz and especially so for frequencies above 10 kHz, as compared to frequencies in the range from 0 Hz to 3 kHz. This is due to a combination of factors:

1. electrical and HVAC equipment in the environment were generating very little audible background noise at frequencies above 3 kHz, and
2. the frequency response of the microphones in the systems that were studied were not as sensitive to frequencies above 10 kHz as they were to frequencies between 0 Hz and 10 kHz (see the frequency response analysis that follows).

Ultrasonic communication, therefore, is not subject to the same degree of background noise that audible communication is subject to.

### Multipath Delay Spread

In order to quantify the effect of reverberations, i.e., echoes, in the acoustic channel, the *multipath delay spread* of the channel was calculated. The *multipath delay spread* measures the amount of time, as observed by the receiver, between the initial reception of a transmitted signal and the reception of the last copy of a transmitted signal. As an example, **Figure 7.2** visually shows the reception of three multipath components, $c_1$, $c_2$, and $c_3$. If the arrival times of the three components are $t_{c_1}$, $t_{c_2}$, and $t_{c_3}$, respectively, the *multipath delay spread* is $|\max(t_{c_1}, t_{c_2}, t_{c_3}) - \min(t_{c_1}, t_{c_2}, t_{c_3})|$. Where the *max* and *min* functions return the highest and lowest time values, respectively.

The *multipath delay spread* of the acoustic channel in the lab environment was measured by performing two experiments: one to test the reverberation of audible signals and the other to test the reverberation of near-ultrasonic signals. In the first experiment a 250 ms signal was transmitted from **Audio8**, consisting of a sinusoidal wave at 3 kHz (audible),

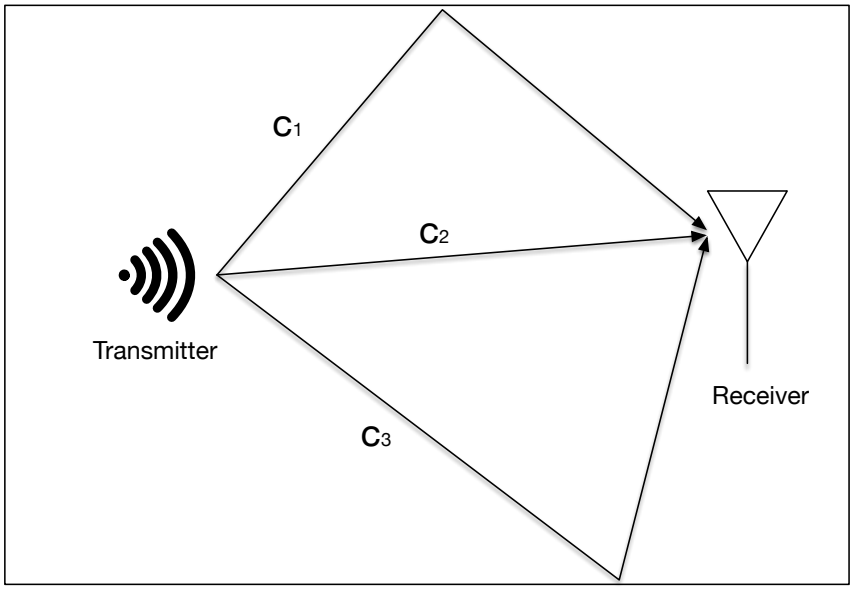



Figure 7.2: Visualizing Multipath in the Acoustic Channel

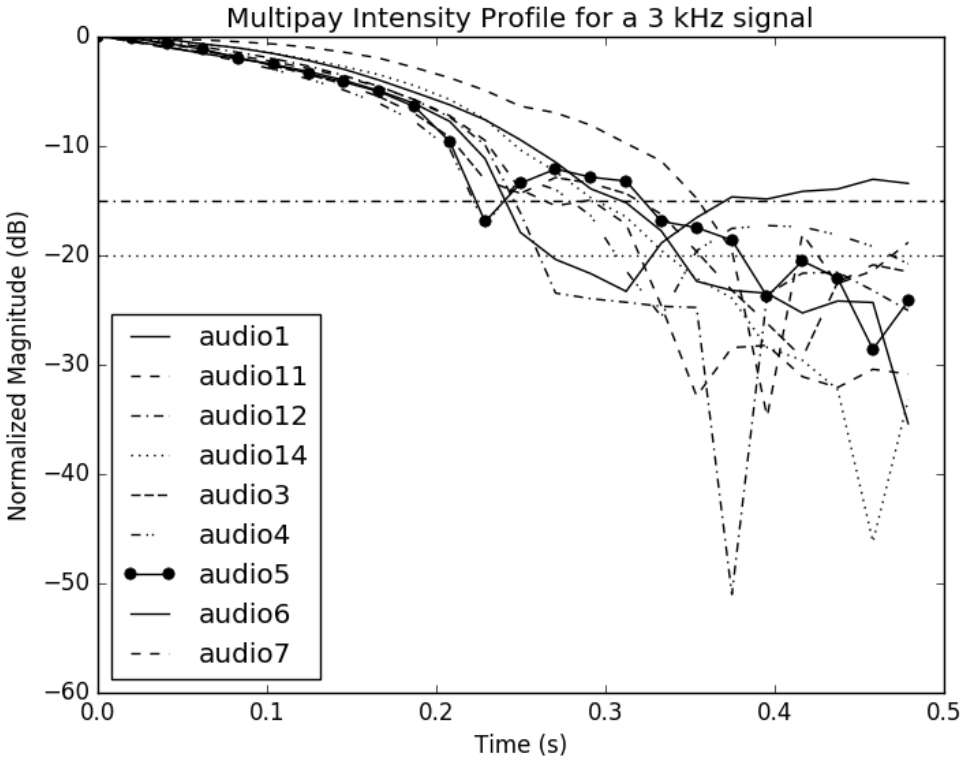



Figure 7.3: Normalized Multipath Intensity Profile in the Audible Spectrum

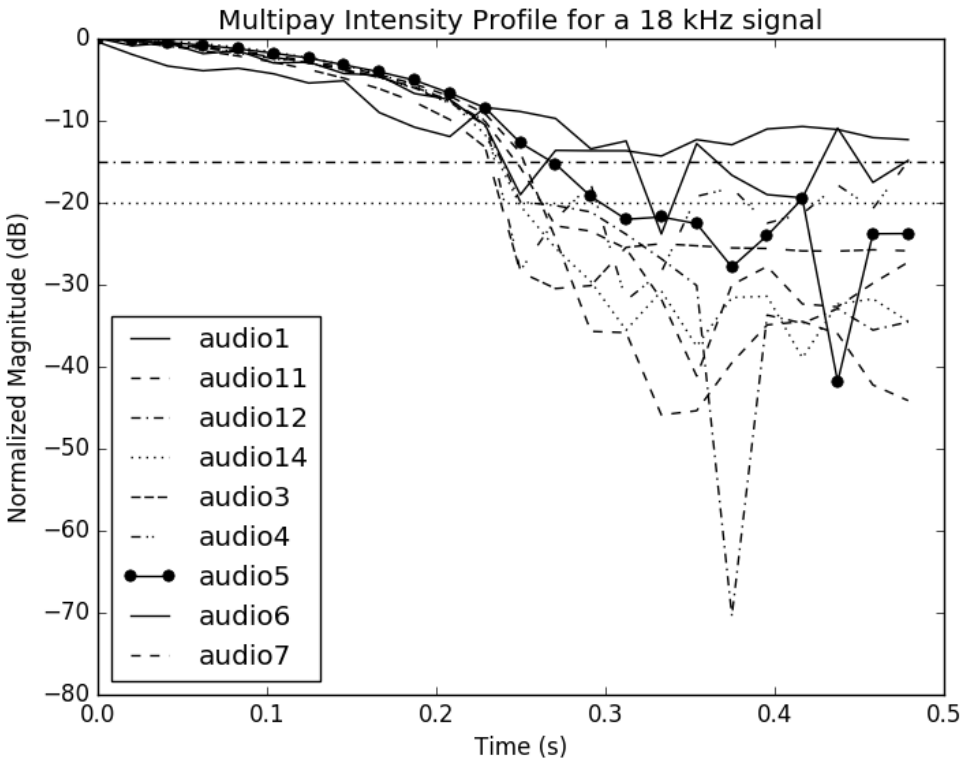



Figure 7.4: Normalized Multipath Intensity Profile in the Near-Ultrasonic Spectrum

and, in the second, a 250 ms signal was transmitted from **Audio8**, consisting of a sinusoidal wave at 18 kHz (near-ultrasonic). To measure the *multipath delay spread* of the channel, each of the received waveforms was first filtered to remove all frequencies outside of their respective passbands and then cross-correlated with their respective originally transmitted signal. This algorithm is an implementation of the algorithm documented by Proakis and Salehi [189] to determine the multipath delay spread of a channel. The normalized magnitude of the cross-correlated signals was then plotted over time to determine the *multipath delay spread* for two dB thresholds, -15 dB and -20 dB. The results can be seen in **Figure 7.3** and in **Figure 7.4** for the 3 kHz and 18 kHz pure-tones, respectively (see [36] for the source code that was used to generate all the plots in this chapter).

If no reverberations were present in the environment the magnitude of the cross-correlated signals would be very low at 250 ms, since a 250 ms signal was transmitted. **Figure 7.3** (audible case) shows that copies of the transmitted signal, however, were received for up to 100 ms at the -15 dB threshold after the first significant component of the transmitted signal was received and approximately 150 ms at the -20 dB threshold. The observed reverberations vary from system to system due to each system's distance from the transmitter, sensitivity to the specific frequency transmitted, and physical location in the lab. Interestingly, from **Figure 7.4** (near-ultrasonic case) it is clear that the reverberations at higher frequencies are much less persistent in the same environment. No system observed reverberations passed 250 ms at the -15 dB threshold, which is due to the sensitivity of the systems' microphones as well as the ability for **Audio 8**'s speakers to

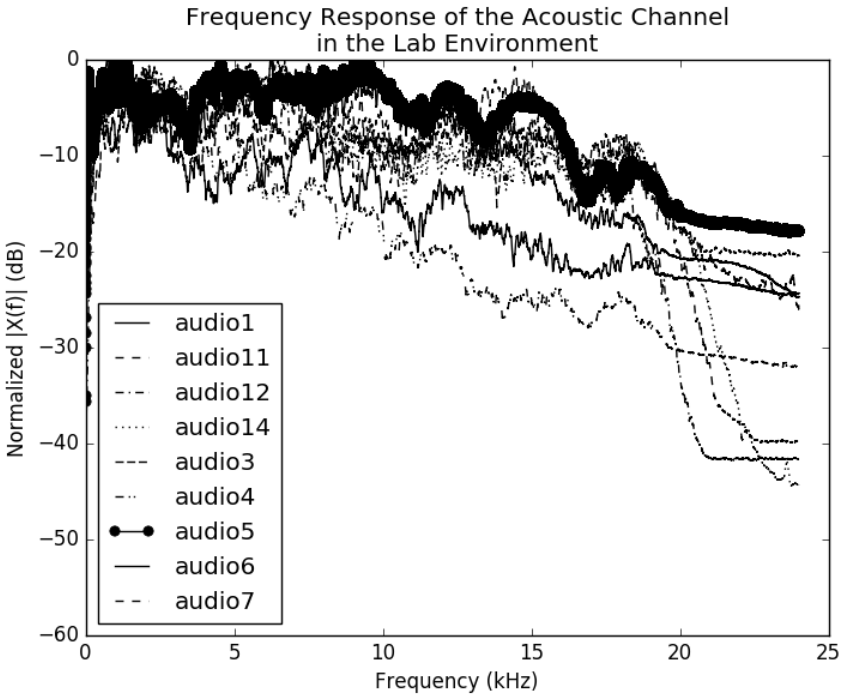



Figure 7.5: Frequency Response of Commodity Microphones and Speakers

output power at near-ultrasonic frequencies. In general, the curves shown in **Figure 7.3** and **Figure 7.4** differ because of the varying support by each systems' microphone and **Audio8**'s speakers for audible and ultrasonic frequencies.

Given these multipath intensity profiles, there is clearly the possibility of inter-symbol interference (ISI) if symbols are transmitted too closely (in time) to one another, especially when audible signals are transmitted. One way to avoid ISI caused by multipath spread is to introduce a *guard interval* between transmitted symbols, i.e., have the transmitter wait a period of time between transmitting symbols. Another popular technique to handle ISI is to use an *equalizer* at the receiver [189]. In **Section 7.3**, specific experiments are performed to determine the relationship between *guard interval* duration and bit error rate (BER) in the acoustic channel. The results from these experiments are then used to optimize the covert-acoustic channel in order to maximize its data rate.

### Frequency Response

The *frequency response* of a communication channel measures the output frequency spectrum of a channel with respect to some input. As an example, if a pure sinusoidal signal of frequency $f$ Hz is input into a channel, the *frequency response* of the channel is the magnitude and phase of the $f$ Hz component of the signal at the channel's output. Moreover, an *ideal channel* is one that introduces no magnitude change and only linear change in the phase of the input signal. In this study, in order to properly engineer the covert-acoustic channel, the *frequency responses* of the acoustic channel over the 0 Hz to 22 kHz was measured at each system.

Each systems' frequency response was measured in the lab environment by playing a broadband white noise signal, which consisted of all frequency components in the range 0 Hz to 22 kHz, from **Audio8**'s speakers. The broadband signal was then captured by each of the devices' microphones and their respective normalized magnitude frequency response was calculated by taking the Fourier transform of the received signal. The results of this experiment can be seen in **Figure 7.5**. The magnitudes shown in **Figure 7.5** are plotted on a decibel (dB) scale and are normalized to the highest amplitude for any received frequency component. If the channel were *ideal*, **Figure 7.5** would display as a horizontal line at the 0 dB level across all frequencies; however, from the figure it can be seen that the acoustic channel in the lab environment, given the systems tested, did not have an ideal frequency response. One other important observation to note is that the majority of the systems' measured frequency responses demonstrated a near-ideal response up to around 5 or 6 kHz. This is to be expected as the human voice consists primarily of frequencies between 300 Hz and 3.4 kHz [21] and it is reasonable to assume that the manufacturers of microphones would design their devices in such a way that they would have an ideal response in this range.

In general, the following conclusions can be drawn from the experiments presented in this section:

1. the ambient noise in the environments decreases proportionally with the frequency of the noise and can be categorized, in general, as pink noise;
2. the ambient noise in the near- and ultrasonic frequency bands is lower than the noise below 3 kHz;
3. the multipath delay spread in the environment is quite severe: 100 ms and up in the audible case;
4. the frequency response of the acoustic channel is non-ideal.

## 7.2 Modulation and Demodulation Schemes

Given the experimental results from the previous section, namely the non-ideal frequency response and multipath delay spread of the channel, modulation and demodulation schemes that take these channel effects into account are analyzed in this section. Multi-carrier modulation schemes, as opposed to single carrier modulation schemes, such as the M-ary Frequency Shift Keying (MFSK) solution used in [181], are bandwidth efficient solutions for channels with a non-ideal frequency response [189]. Frequency-hopping spread spectrum (FHSS) and OFDM are two such multi-carrier solutions. FHSS and OFDM gain their bandwidth efficiency by dividing the available channel (or passband) bandwidth, $W$, into a number of equal sub-channels, $N$, of bandwidth $\Delta f = \frac{W}{N}$, so that each sub-channel has an ideal frequency response.

As an example, in **Figure 7.6**, the passband from 3 kHz to 8 kHz is divided into 22 sub-channels, i.e., $W = 5000$ Hz, $N = 22$, and FHSS is used to modulate symbols. In the

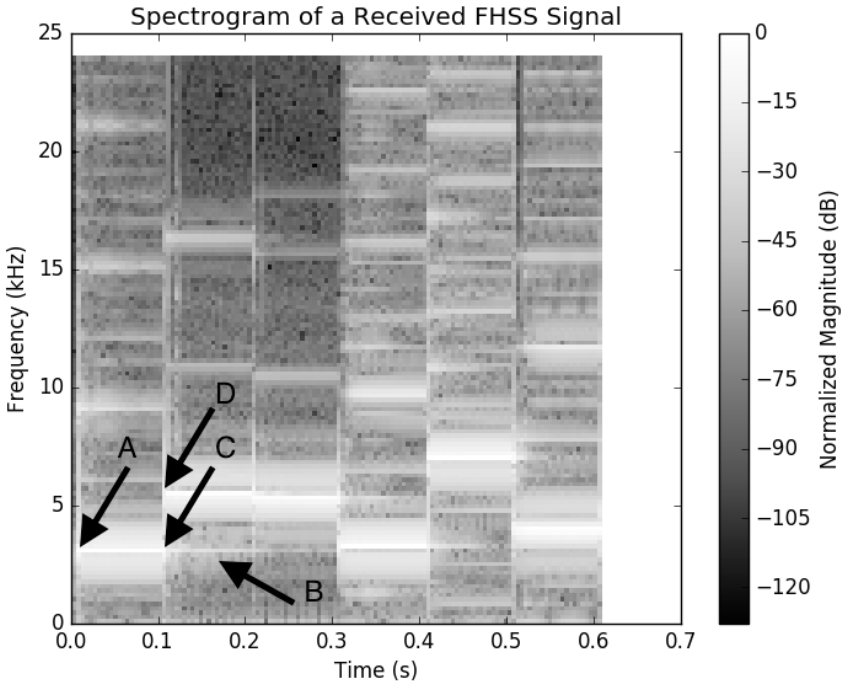



Figure 7.6: Spectrogram of a Received FHSS Signal

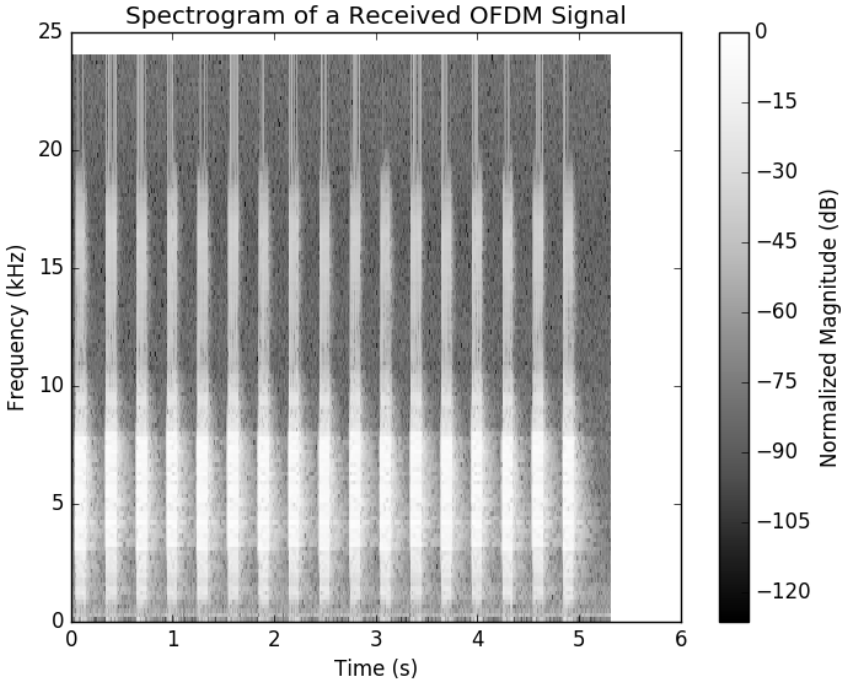



Figure 7.7: Spectrogram of a Received OFDM Signal

figure, it can be seen that symbols were transmitted with no delay between them; however, by hopping from channel to channel FHSS allows any reverberations in a previously used channel to dissipate before the sub-channel is reused. The first sub-channel used in **Figure 7.6**, with a sub-channel bandwidth from 3 kHz to 3.22 kHz, shows a symbol being received from time $t = 0.0$ s to $t = 0.1$ s (label **A**), while the reverberations (label **B**) from the symbol carry on from approximately $t = 0.1$ s (label **C**) well into the interval containing the symbol of the second sub-channel (label **D**). In **Figure 7.7**, the use of OFDM is shown, and again, the passband from 3 kHz to 8 kHz is used to transmit data on $N = 22$ sub-channels. Using OFDM, however, all 22 channels are used simultaneously to transmit data: one symbol on each sub-channel, and thus there is the potential for ISI if no *guard interval* is used. **Figure 7.7** shows that when using OFDM, a *guard interval* must be introduced in order to prevent ISI. For illustrative purposes, a 200 ms delay is used between each successive use of the channel.

In general, data can be sent in a bandwidth-efficient fashion in serial using FHSS, or in parallel using OFDM. By comparison, if data can be sent in a serial fashion at a rate of $R$ bits per second (bps) then, conceivably, if data is sent on $N$ sub-channels in parallel, information can be communicated at $NR$ bps. When sending data successively on different non-overlapping channels, the *guard interval* becomes less of an issue provided that reverberations in a previously used channel are allowed to dissipate before reusing the channel; however, when reusing the same channels to transmit data at subsequent transmit intervals, the *guard interval* of the channel must be respected in order to prevent ISI from occurring. Let $R_1$ represent the rate at which data can be sent using serial transmission on multiple non-overlapping channels and $R_2$ represent the rate at which data can be sent using parallel transmission on multiple non-overlapping channels. In the section that follows, it is shown that, despite the large *multipath delay spread* in the environment studied, the rate achievable using OFDM, $R_2$, is much higher than the bit rate achievable using FHSS, $R_1$, and, therefore, OFDM is a much more performant solution than FHSS, which is the modulation scheme that has been used by researchers in the past [73, 89, 90].

### 7.2.1 Analysis of the Data Rates for OFDM and FHSS

In this section, the data rates of both OFDM and FHSS are studied. In this analysis, it is assumed that a passband bandwidth of $W$ is available, which can be divided into $N$ sub-channels, and that on each of the sub-channels one of $M$ symbols is transmitted.

#### Frequency-Hopping Spread Spectrum

The achievable bit rate using FHSS is first calculated. Assuming that the channel can be sampled at a rate of at least $2W$, the theoretical maximum symbol rate, i.e., the Nyquist rate, that can be achieved for any one sub-channel, ignoring reverberations in the environment, is:

$$R_{sym} = \frac{W}{N}\left(\frac{\text{symbols}}{\text{second}}\right).$$

Assuming $k$ seconds are required between each reuse of the same sub-channel, the symbol interval, i.e., the duration of each symbol, is

$$\begin{aligned} T_{sym} &= \frac{N}{W} + \frac{k}{N} \\ &= \frac{N^2 + Wk}{WN}\left(\frac{\text{seconds}}{\text{symbol}}\right), \end{aligned}$$

where the *guard interval* is $\frac{k}{N}$ because it can be amortized over the number of sub-channels, $N$. Using FHSS, as the number of sub-channels, $N \to \infty$, the *guard interval*, $\frac{k}{N} \to 0$. Therefore, given $T_{sym}$, the bit rate, $R_{bits}$, after accounting for reverberations in the environment, is

$$\begin{aligned} R_{bits} &= \frac{\log M}{T_{sym}} \\ &= \frac{WN \log M}{N^2 + Wk}\left(\frac{\text{bits}}{\text{second}}\right). \end{aligned} \tag{7.1}$$

Examining **Equation 7.1** under three scenarios:

1. $N^2 \gg Wk$:

$$\begin{aligned} R_{bits} &= \frac{WN \log M}{N^2} \\ &= \frac{W \log M}{N}\left(\frac{\text{bits}}{\text{second}}\right), \end{aligned} \tag{7.2}$$

2. $Wk \gg N^2$:

$$\begin{aligned} R_{bits} &= \frac{WN \log M}{Wk} \\ &= \frac{N \log M}{k}\left(\frac{\text{bits}}{\text{second}}\right), \text{ and} \end{aligned}$$

3. $N^2 = Wk$:

$$\begin{aligned} R_{bits} &= \frac{WN \log M}{2N^2} \\ &= \frac{W \log M}{2N} \left( \frac{\text{bits}}{\text{second}} \right), \end{aligned} \tag{7.3}$$

it can be seen that by increasing $N$ to the point where $N^2 \gg Wk$, the highest bit rate for FHSS can be achieved (i.e., $\frac{W \log M}{N}$). The minimum number of channels, $N$, required to achieve the result shown in **Equation 7.3** is $N = \sqrt{Wk} = 55$ for a bandwidth of $W = 20,000$ and a guard interval of $k = 150$ ms, where $k = 150$ ms was taken from the multipath delay spread of the 3 kHz tone at the -20 dB threshold observed in **Figure 7.3**, as an example. Increasing the number of subchannels, $N$, from this point allows the attainable $R_{bits} \to \frac{W \log M}{N}$.

### Orthogonal Frequency-Division Multiplexing

Under the same assumptions (i.e., $W$ bandwidth available, $N$ sub-channels, and $M$ symbols) the achievable bit rate for OFDM in the presence of reverberations is calculated. Given these parameters as well as the Nyquist rate, the maximum symbol rate for any one sub-channel, $R_{sym}$, remains the same. The symbol interval, however, changes with OFDM since the effect of the *guard interval* in the channel cannot be reduced in the same way that it was in the analysis of FHSS and, therefore,

$$\begin{aligned} T_{sym} &= \frac{N}{W} + k \\ &= \frac{N + Wk}{W}. \end{aligned}$$

The benefit, however, of using a multi-carrier modulation scheme is that data can be transmitted on all sub-channels simultaneously in parallel and, therefore,

$$R_{\frac{bits}{channel}} = \frac{W}{N + Wk} \log M \left( \frac{\frac{\text{bits}}{\text{second}}}{\text{channel}} \right),$$

and

$$R_{bits} = N R_{\frac{bits}{channel}}$$

$$= \frac{WN \log M}{N + Wk} \left( \frac{\text{bits}}{\text{sec}} \right). \tag{7.4}$$

Examining **Equation 7.4** under three scenarios:

1. $N \gg Wk$:

$$\begin{aligned} R_{bits} &= \frac{WN \log M}{N} \\ &= W \log M \left( \frac{\text{bits}}{\text{second}} \right), \end{aligned} \tag{7.5}$$

2. $Wk \gg N$:

$$\begin{aligned} R_{bits} &= \frac{WN \log M}{Wk} \\ &= \frac{N \log M}{k} \left( \frac{\text{bits}}{\text{second}} \right), \text{ and} \end{aligned}$$

3. $N = Wk$:

$$\begin{aligned} R_{bits} &= \frac{WN \log M}{2N} \\ &= \frac{W \log M}{2} \left( \frac{\text{bits}}{\text{second}} \right), \end{aligned} \tag{7.6}$$

it can be seen that by increasing $N$ to the point where $N \gg Wk$ the highest bit rate for OFDM can be achieved (i.e., $W \log M$). The minimum number of channels required to achieve the result shown in **Equation 7.6** is $N = Wk = 3000$, when $W = 20,000$ and $k = 150$ ms, where $k = 150$ ms was taken from the multipath delay spread of the 3 kHz tone at the -20 dB threshold observed in **Figure 7.3**. Increasing the number of subchannels, $N$, from this point allows the attainable $R_{bits} \to W \log M$.

Comparing **Equation 7.2** and **Equation 7.5** it can be seen that when the number of sub-channels $N$ is increased to combat the effects of multipath the achievable bit rate using OFDM is larger by a factor of $N$. In **Table 7.3**, the bit rates for various values of $M$ are shown, where it is assumed $W = 20,000$, $k = 150$ ms, and $N$ is set to be the minimum number of channels required to satisfy the conditions $N^2 = Wk$ for FHSS and $N = Wk$ for OFDM, respectively. In conclusion, assuming that the channel is capable of handling the appropriate number of sub-channels, OFDM is the more performant modulation scheme for the acoustic channel.

Table 7.3: Data Rates for FHSS and OFDM ($\frac{\text{bits}}{\text{second}}$)

| | $M = 2$ | $M = 4$ | $M = 8$ | $M = 16$ |
|---|---|---|---|---|
| OFDM | 20,000 | 40,000 | 60,000 | 80,000 |
| FHSS | 363 | 727 | 1,090 | 1,454 |

### 7.2.2 Algorithms and Synchronization

In order to explore the limits of the covert-acoustic channels, two different modulation schemes were used to explore as well as empirically evaluate the data rate of the channel. First, FSK was used to test the channel's limitations and, second, OFDM was used to test its maximum data rate. The implementation of each of these schemes is now outlined.

#### Frequency Shift Keying

The FSK modulation algorithm used by the experiments discussed in this chapter worked as follows. First, for each information sequence of symbols that was to be transmitted through the acoustic channel, a sequence of symbols, commonly referred to as a *preamble*, known to both the transmitter and the receiver, was prepended to the sequence. As an aside, the combination of *preamble* and data symbols results in a *frame* of data where the *preamble* serves to synchronize the receipt of each *frame* at the receiver. Second, for each symbol in the *frame*, $m_i$, of $\log M$ bits in length, a signal was produced by first selecting a frequency, $f_{m_i}$, to represent the symbol, then taking inverse Fourier transform to create the symbol's time-domain representation. Finally, zero amplitude samples were appended to the resulting signal equal in duration to the desired *guard interval*. Once this process was completed for each symbol, the resulting symbols' signals were in-order concatenated to create the data frame's time sequence which was ultimately sent to the transmitter's speaker. The speaker then converted the frame's signal from a sequence of discrete amplitudes to analogue waveforms, which were then transmitted over the air to the receiver.

Demodulation at the receiver began by first converting the received analogue waveform into a sequence of discrete amplitudes or samples. Second, the received signal was then copied to create $M$ copies of the original signal, one for each of the $M$ symbols. Each copy was then filtered by a passband filter centred at $f_{m_i}$. The passband filters were designed to allow only frequency components close to $f_{m_i}$ through the filter while removing all other frequency components, including those at adjacent symbol frequencies. Each of the resulting filtered signals was then individually squared and low-pass filtered to leave only the amplitude of the signal component centred at their respective frequency, $f_{m_i}$. In the case of binary signalling, i.e., $M = 2$, which was used throughout the experiments in this chapter, the resulting two signals were then combined, downsampled, and normalized to produce a sequence of symbols with values of $\pm 1$. The start offset of each data frame was then found by taking the cross-correlation of the shared *preamble* and the recovered sequence of $\pm 1$'s in order to synchronize the receiver with the transmitter. Once synchronized, the

$\pm 1$'s were converted to a binary sequence by mapping the $+1$'s and $-1$'s back to 1's and 0's, respectively.

#### Orthogonal Frequency-Division Multiplexing

The OFDM modulation algorithm worked by simply performing FSK on each sub-channel. First, the information sequence of symbols was segmented into $N$ chunks before a preamble was prepended to each sub-channels' chunk of data. Second, each individual symbol, $m_{i,k}$, $i = 0, 1, 2, \ldots, M-1$, $k = 0, 1, 2, \ldots, N-1$, of $\log M$ bits, was modulated using FSK on a different orthogonal carrier, $f_{c_k}$. To accomplish this, the FSK modulation algorithm described above was executed on each sub-channel one symbol at a time and the resulting $N$ time-domain signals were combined. After the $N$ signals were combined, a delay was then added to the time sequence in the form of zero-amplitude samples equal in duration to the desired *guard interval* to form a time-domain signal for the $N$ symbols. Once all the signals were generated, they were in-order concatenated together and the resulting time sequence was transmitted on the acoustic channel using the transmitter's speaker.

To facilitate demodulation at the receiver, the FSK demodulation algorithm described above was executed on each sub-channel and each of the resulting binary sequences was serialized back together in order to reconstitute an estimate of the transmitted sequence of symbols. All the systems studied in this chapter allowed audio samples to be produced and captured at a sample rate of 48 kHz, which theoretically allowed acoustic signals up to 24 kHz to be transmitted and received, respectively, given Nyquist's Law. Moreover, all samples collected were 16 bits in depth and all devices supported stereo audio (i.e., two channels) recording and playback with the exception of the Samsung Galaxy Nexus which only supported mono audio (i.e., one channel). These configuration parameters were all natively supported on the equipment that was tested, which is to say that they were supported in hardware by all the systems.

## 7.3 Lab Experiments and Results

In this section, the acoustic channel is studied by measuring the effect of tweaking various system parameters on a number of different metrics:

1. probability of synchronizing a frame of data,
2. BER, and
3. data transfer rate.

In total, six channel parameters were examined in order to determine the limits of the channel (as realized using the systems listed in **Table 7.1**) and, ultimately, to maximize the data transfer rate. All systems, with the exception of **Audio3**, were used as a *modulator*

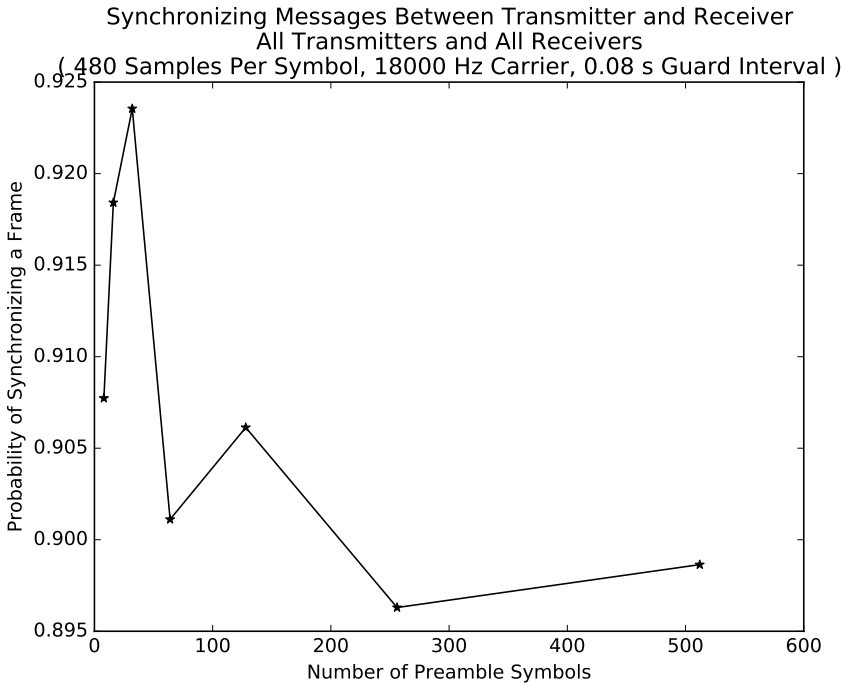
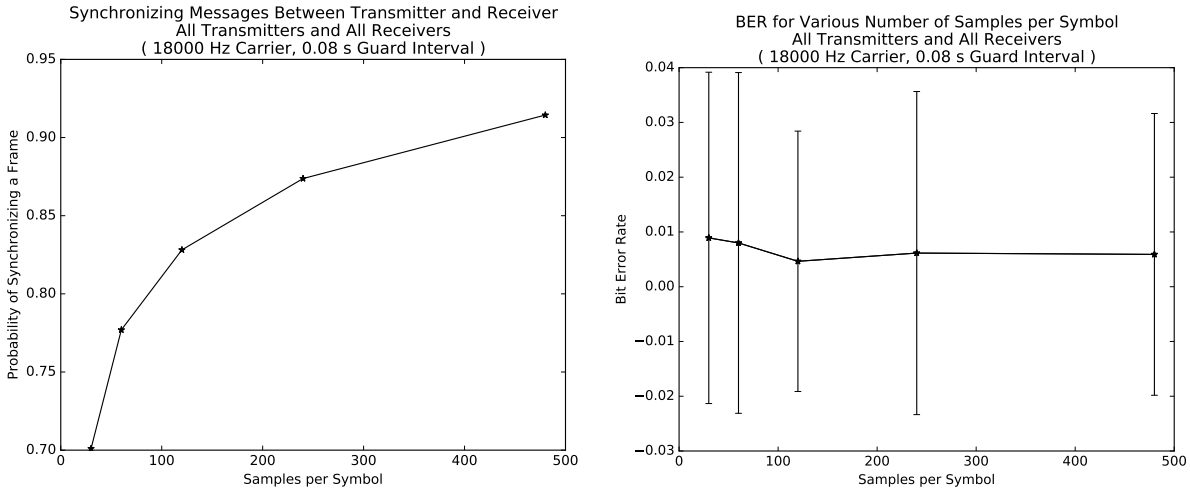



Figure 7.8: Synchronization Probability versus Number of Preamble Symbols

in all experiments in order to capture results for each system acting as the high-security, air-gapped system. Similarly, each system was also used as a *demodulator* in all experiments as well in order to capture results for each machine acting as the low-security system. In all of the experiments documented in this chapter it was assumed that the *modulator* was the only machine that resided on the high-security network and all other machines were *demodulators* residing on the low-security network. A description of each of the six experiments that were performed and their aggregate results follow. The detailed results for all tests, showing their breakdown by individual transmitter and individual receiver can be seen in **Appendix D**.

### Preamble Length

As mentioned in **Section 7.2.2**, all information sequences were prepended by a *preamble*, which was known by both the modulator and the demodulator, before being transmitted over the channel. This first experiment analyzed the effect of varying the length of the *preamble* on the probability of a data frame being synchronized. From a data transfer perspective, if a long *preamble* is required for synchronization, the effective data transfer rate is lowered because more symbols must be allocated to the function of synchronization as opposed to transferring information. It stands to reason that the longer the *preamble* the higher the probability of synchronizing a given frame and in **Figure 7.8** the effect of increasing the length of the *preamble* can be seen. Surprisingly, as more symbols were used for synchronization the probability of synchronizing remained within the bounds $0.895 \leq P_{sync} \leq 0.925$. The preamble lengths that were tested were 8, 16, 32, 64, 128,



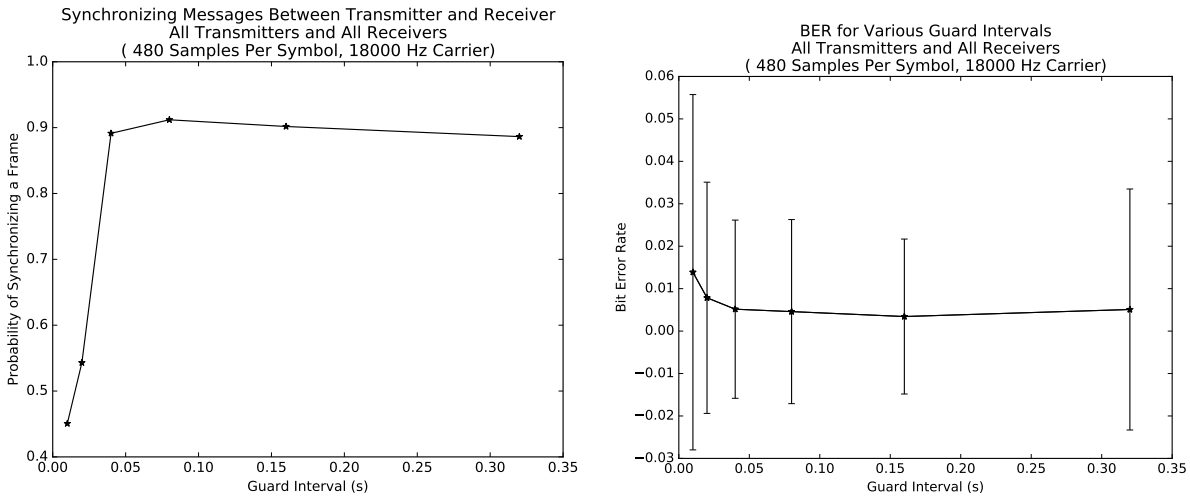

(a) (b)

Figure 7.9: Synchronization Probability versus Transmitted Samples per Symbol (a) and Bit Error Rate versus Transmitted Samples per Symbol (b)

256, and 512 symbols and since the modulator and demodulator are interested in the shortest *preamble* that provides the highest probability of synchronizing, a *preamble* length of 8 symbols would allow Alice and Bob to synchronize data frames with a probability of $0.905 \leq P_{sync} \leq 0.910$, on average.

### Number of Transmitted Samples per Symbol

The second experiment examined the effect of varying the number of transmitted samples per symbol on both the probability of synchronizing a frame as well as the BER. The number of transmitted samples per symbol affects both the data rate achievable and the SNR of each symbol. As the number of transmitted samples per symbol increases so too does the SNR per symbol, while at the same time the data transfer rate decreases, since fewer symbols can be transferred per unit of time. It is in the best interest of the modulator and demodulator, therefore, from an efficacy perspective, to reduce the number of transmitted samples per symbol so that more symbols can be transmitted per second at lower SNR. Similarly, from a covertness perspective, it is in the modulator and demodulator's best interest to reduce the number of samples as well. The probability of synchronizing a given frame is shown in **Figure 7.9a** for various counts of transmitted samples per symbol. Clearly, as the number of samples per symbol increases so too does the probability of synchronization. Conversely, as the number of samples increases the BER decreases, which can be seen in **Figure 7.9b**. The number of transmitted samples per symbol that were tested was 30, 60, 120, 240, and 480 samples per symbol. In the remainder of the experiments, 480 samples per symbol were used.




(a) (b)

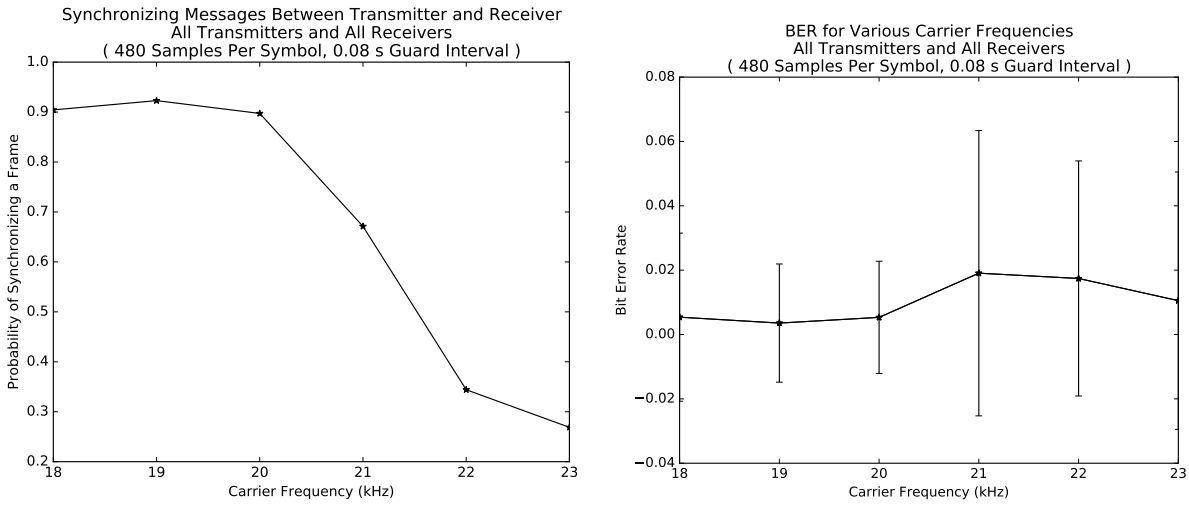
Figure 7.10: Synchronization Probability versus Guard Interval (a) and Bit Error Rate versus Guard Interval (b)

### Guard Interval Duration

The third experiment looked at the effect of increasing the duration of the guard interval. The guard interval, as previously mentioned, affects ISI, and, consequently, both the probability of synchronizing a frame as well as the BER. Whereas increasing the guard interval to an arbitrarily long duration would reduce both ISI and the BER, an arbitrarily high duration effectively reduces the data rate achievable, since fewer symbols can be transmitted per unit of time. It is, therefore, in the best interest of the modulator and demodulator to choose a minimal guard interval that also minimizes the BER and maximizes the probability of synchronizing each frame at the same time. From **Figure 7.10a** and **Figure 7.10b**, it can be seen that a guard interval of 80 ms maximizes the probability of synchronizing while minimizing the BER below 1 %. The guard intervals that were tested were 10, 20, 40, 80, 160, and 320 ms. For most experiments that follow, unless otherwise stated, a guard interval of 80 ms was used.

### Ultrasonic Frequency Support

The fourth experiment tested for the highest supported frequency that could be used to communicate data symbols. Frequencies over 20 kHz are inaudible to humans and as humans age that threshold decreases. It is for this reason that a number of researchers consider frequencies over 18 kHz (i.e., near-ultrasonic) as inaudible and, therefore, undetectable by an oblivious passive adversary. Moreover, given the frequency response of the acoustic channel shown in **Figure 7.5** it is unclear as to what degree near- and ultrasonic frequencies are supported in general by commodity hardware. Therefore, in order to test the support for ultrasonic frequencies, information was transferred using FSK on carrier frequencies: 18 kHz, 19 kHz, 20 kHz, 21 kHz, 22 kHz, and 23 kHz. The results for the




(a) (b)

Figure 7.11: Synchronization Probability versus Frequency (a) and Bit Error Rate versus Frequency (b)

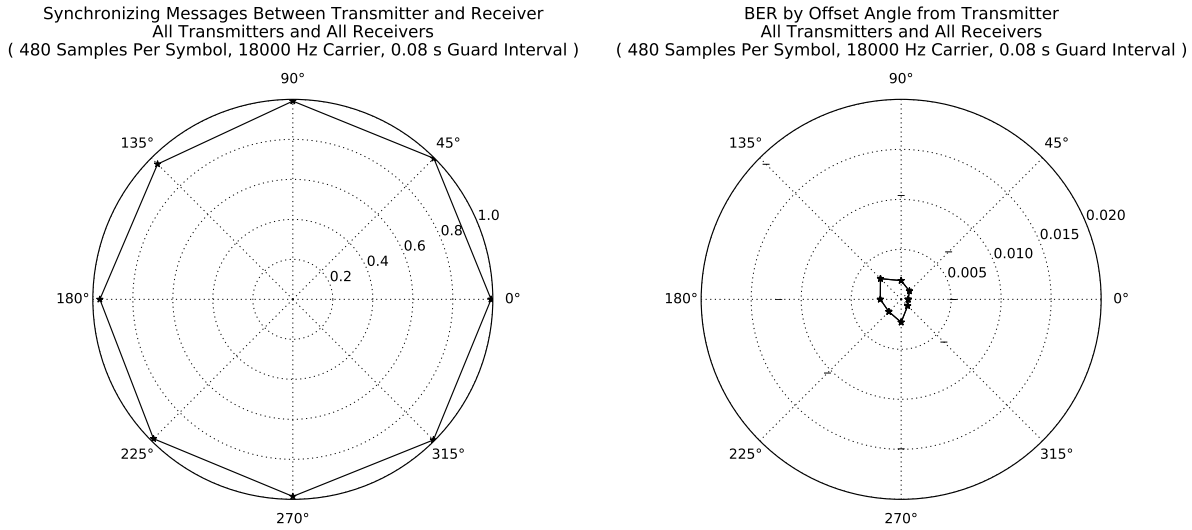
probability of synchronizing a frame and the BER can be seen in **Figure 7.11a** and **Figure 7.11b**, respectively. Surprisingly, there is support at carrier frequencies all the way up to and including 23 kHz on some devices. From the detailed results, which can be seen in **Figure D.23** and **Figure D.26**, about half of the systems were capable of transmitting at frequencies up to 23 kHz and all systems except for the iOS systems and the Mac OS X system could receive audio signals up to and including 23 kHz.

### Angle Between Transmitter and Receiver

The fifth experiment examined the effect that the angle between the transmitter and receiver had on the BER and probability of synchronizing. Given that all the machines in the lab environment were positioned in a circle (see **Figure 7.1**) an earlier reviewer of this work pointed out that the angle between modulator and demodulator could affect the results of the experiments documented in this chapter. From **Figure 7.12a** and **Figure 7.12b**, however, it can be seen that there is minimal, if any, effect on the offset angle between the machines at the distances and angles (i.e., angles from 0 ° to 90 ° and from 270 ° to 360 °) tested and, therefore, the positioning of the machines, for the experiments outlined in this chapter, are not adversely affected by their orientation around the circle. Given these results, the transmitters can be considered *isotropic* sources at the distance and volume level tested, since it appears that all transmitters radiate equivalent power in all directions.

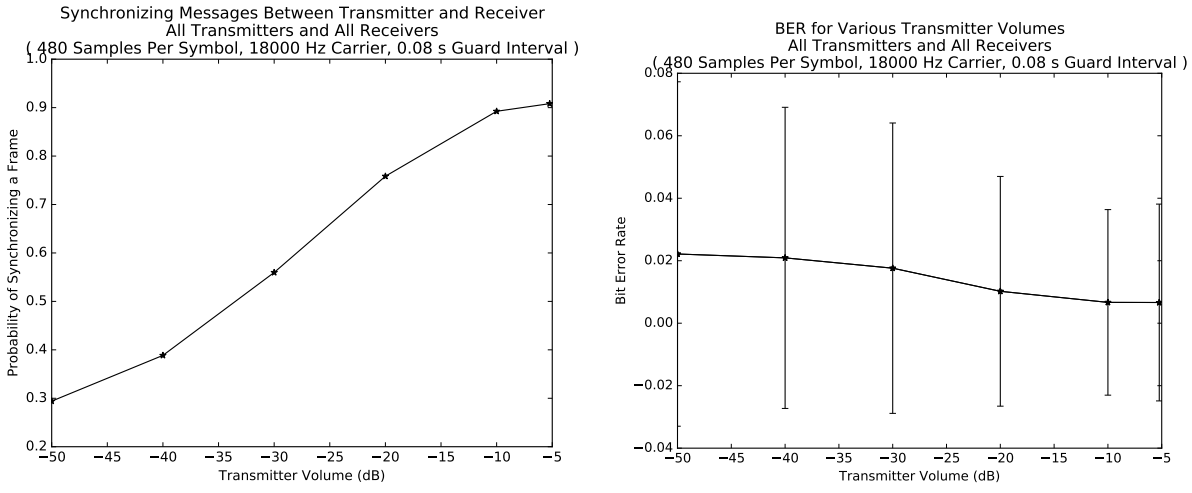
### Transmitter Volume

The final controlled experiment that was performed examined the effect of reducing the transmitter's volume. Lowering the transmitter's volume effectively lowers the SNR of




(a) (b)

Figure 7.12: Synchronization Probability versus Offset Angle (a) and Bit Error Rate versus Offset Angle (b)




(a) (b)

Figure 7.13: Synchronization Probability versus Volume (a) and Bit Error Rate versus Volume (b)

each symbol, which makes transmitted signals even more difficult to detect by a passive covert-analyst. Furthermore, from an covertness perspective, as outlined in the previous chapter, it is in the modulator and demodulator's best interest to communicate at the lowest possible SNR to avoid detection by an energy detector. Results for the transmitter reducing the volume to levels as low as -50 dB can be seen in **Figure 7.13a** and **Figure 7.13b** (i.e., the transmitter, Alice, reduces her transmit volume to a level of $\frac{1}{10^5}$ of her maximum transmit volume). The greatest impact to lowering the transmitter's volume can be seen on the probability of synchronizing a frame; however, surprisingly, the BER, on average, remains low and relatively constant. This provides an interesting trade off: while synchronizing becomes less probable, on average, the resulting SNR that would be observed by a passive adversary is also lowered and, therefore, detecting the transmission is more difficult for the adversary. The effect of lowering the transmitter's volume is analyzed in more depth in **Chapter 8** where the *steganographic capacity* of the channel is studied.

In summary, given the experimental results of this section, the following observations can be derived, on average, when FSK modulation is used to communicate data over the acoustic channel:

1. using eight or more symbols for synchronization results in a probability of synchronization, $P_{sync} \geq 0.900$;
2. using 120 samples per symbol and above results in $P_{sync} \geq 0.800$ and a BER $\leq 0.01$;
3. using a guard interval of 0.04 s and above results in $P_{sync} \geq 0.900$ and a BER $\leq 0.01$;
4. all systems can transmit and receive FSK signals with a carrier frequency up to and including 21 kHz;
5. all Windows systems tested can transmit and receive FSK signals with a carrier frequency up to and including 23 kHz;
6. in the lab environment the angle between the transmitter and receiver, in general, did not adversely affect the probability of synchronizing a frame of data and only minimally affects the BER; and
7. restricting the transmitter's volume to as low as -30 dB (i.e., to $\frac{1}{10^3}$ of the maximum volume) still results in a $P_{sync} \geq 0.500$ and a BER $\leq 0.02$.

### 7.3.1 Effective Data Transfer Rate

Given the experimental results presented in this section as well as the mathematical analysis from the previous section, test transmissions were performed using OFDM modulation in order to maximize the data transfer rate over the near- and ultrasonic acoustic channel. In total, six different tests were performed and their results are shown in **Table 7.4**, where $f_1$ and $f_2$ are the lower and upper bound frequencies of the available bandwidth, i.e., $W = f_2 - f_1$, $N$ is the number of sub-channels, $T_{guard}$ is the guard interval, in seconds,

Table 7.4: OFDM Results for All Transmitters and All Receivers

| $f_1$ **(Hz)** | $f_2$ **(Hz)** | $N$ | $T_{guard}(s)$ | $P_{sync}$ | $\mu_{errors}$ | $\sigma_{errors}$ | $R$ ($\frac{\textbf{bits}}{\textbf{sec}}$) |
|---|---|---|---|---|---|---|---|
| 18000 | 19600 | 4 | 0.08 | 0.8181 | 0.0248 | 0.0549 | 44.4444 |
| 18000 | 19600 | 8 | 0.04 | 0.7424 | 0.0591 | 0.0661 | 160.0000 |
| 18000 | 20500 | 6 | 0.08 | 0.7775 | 0.0373 | 0.0619 | 66.6667 |
| 18000 | 20500 | 12 | 0.04 | 0.6304 | 0.0693 | 0.0687 | 240.0000 |
| 20000 | 21000 | 2 | 0.08 | 0.7312 | 0.0264 | 0.0619 | 22.2222 |
| 20000 | 21000 | 5 | 0.04 | 0.6147 | 0.0643 | 0.0776 | 100.0000 |

$P_{sync}$ is the probability of synchronizing a frame, $\mu_{errors}$ is the average BER, $\sigma_{errors}$ is the standard deviation of the BER, and $R$ is the achievable bit rate for the test. As a comparison, using FSK and 480 samples per symbol with a guard interval of 80 ms results in a data transfer rate of 11.1 bps. Moreover, using FHSS with 480 samples per symbol, six sub-channels, and a guard interval of 15 ms, a data transfer rate of 40 bps can be achieved. The results in **Table 7.4** show that bit rates well above those achievable using FSK and FHSS are possible while keeping the signals imperceptible to an oblivious passive adversary.

These results demonstrate that, in general, acoustic communication in the ultrasonic range is possible using commodity hardware at data rates that allow the leakage of sources of sensitive information that require low bit rates to communicate. Previous to this result being made available it had not been shown that commodity hardware in general could be used to both transmit and receive ultrasonic communication, let alone at bit rates of 100 bps. In the next section, **Section 7.4**, these results are built upon and the data rates are pushed even higher for specific real-world scenarios to demonstrate the risk that covert-acoustic channels can pose to secure systems.

### Distribution of Errors

In the analysis of the relationship between BER and carrier frequency (see **Figure 7.11b**), it was pointed out that while synchronization became less probable as the carrier frequency was increased the BER remained relatively constant. Given this result, it would, therefore, be expected that when using OFDM the BER conditioned on sub-channel would be consistent with this result, i.e., the BER, when conditioned on a given sub-channel, would be independent of the sub-channel. **Figure 7.14** shows a bar chart of the conditional BER by sub-channel and it is clear that this assumption does not hold. As the sub-channel carrier frequency increases so too do the BERs for symbols transmitted on sub-channels that have higher carrier frequencies. Further analysis of this situation revealed the fact that while each sub-channel was allocated bandwidth according to Carson's Rule (i.e., the passband bandwidth, $W$, was allocated such that each sub-channel's bandwidth, $B < W$, contained 98 % of the sub-channel's power) the 2 % of a sub-channel's power that spilled over into adjacent sub-channels negatively affected the adjacent sub-channel's BER. This was especially pronounced on sub-channels at higher frequencies whose power was relatively lower than their adjacent lower-frequency sub-channel. This spillover effect could of

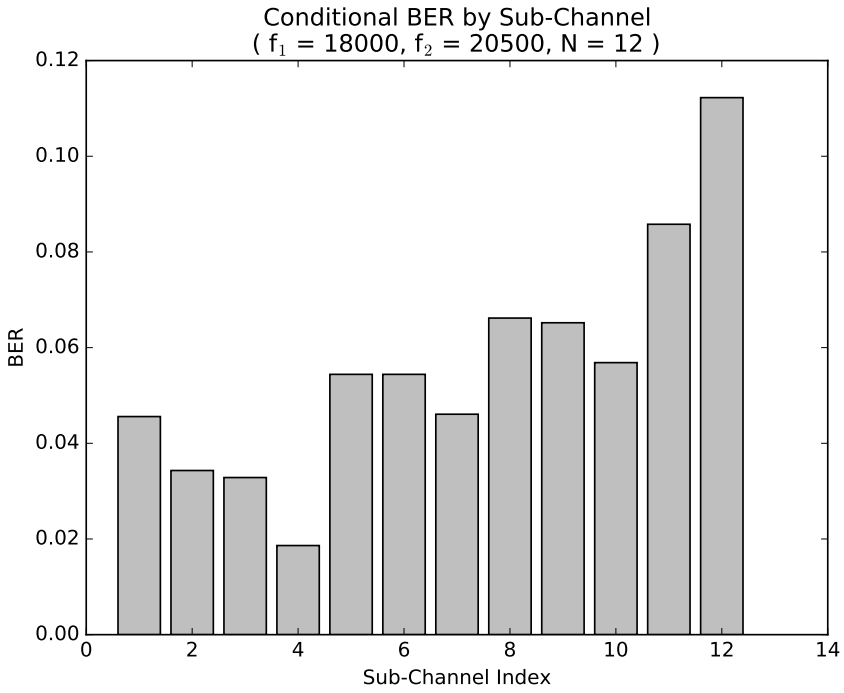



Figure 7.14: BER by OFDM Sub-Channel

course be limited further by increasing each sub-channel's bandwidth; however, this would consequently reduce the number of sub-channels and, therefore, reduce the effective data rate of the channel as a whole.

While **Figure 7.14** shows results for only one of the tested OFDM configurations, this conditional BER distribution was observed in all of the OFDM tests that were performed. These results demonstrate that while OFDM can be used to establish performant covert-acoustic channels, careful consideration must be paid to the manner in which these channels are constructed and that there is a trade-off to be had between effective data rate and BER. Moreover, appropriate error correction techniques that take this conditional distribution of errors into account should be employed in order to maximize the throughput, i.e., rate of messages successfully transmitted over the channel, of the acoustic channel.

Additionally, **Figure 7.15** shows the distribution of bit errors when single-carrier FSK is used. This result is meant to validate the assumption that errors occur in uniform fashion across all bit positions. Or, conversely, that no bit positions demonstrate an abnormally high BER. In contrast to the previous result, which showed that BER was not independent of sub-channel, the result graphed in **Figure 7.15** demonstrates that the BER is in fact independent of bit position and thus errors occur in the acoustic channel with uniform random probability. Given this result, error correction that is designed to correct uniform random errors should be applied to FSK signals transmitted over the acoustic channel. Combining this error distribution observation with that of OFDM, error correcting codes should be applied on a per-channel basis to account for random errors in transmission at different rates depending on the carrier frequency by the sub-channel. In concluding that, however, the application of error correcting codes to covert-acoustic signals would be highly

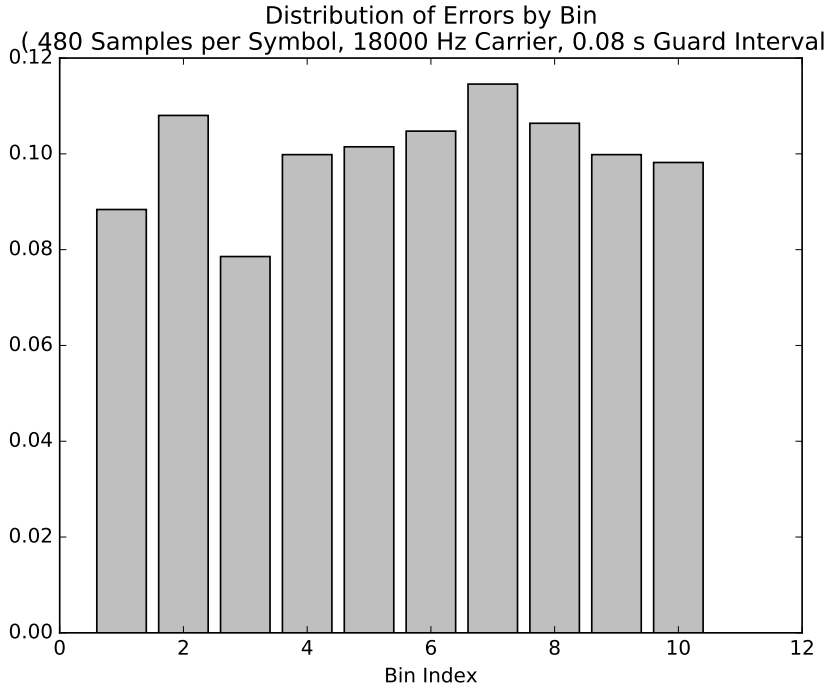



Figure 7.15: Distribution of Errors when using FSK

dependant on the communication mode, e.g., duplex or simplex, between the high-security, air-gapped systems and the low-security systems.

## 7.4 Covert-Acoustic Channel Attacks

In the previous section it was shown that covert-acoustic channels can be established between air-gapped systems in the presence of an oblivious covert-analyst in a lab setting. Where the focus was on demonstrating that covert-acoustic communication is possible in general using commodity hardware, this section focuses on demonstrating that covert-acoustic channels can be used by malware to leak sensitive information from a high-security system to disconnected systems on a low-security network under real-world conditions. To demonstrate this, the covert-acoustic channel is studied in two traditional office environments:

1. a closed-door office containing a single desk and multiple systems, and
2. an open-concept office containing four desks, each holding multiple systems;

as well as under two real-world scenarios:

1. data is leaked from the high-security system when there are humans present in the environment (e.g., during regular business hours), and

Table 7.5: Distance Between Audio8 and the Other Systems in Both Environments

| | Closed-Door Office | | Open-Concept Office | |
|---|---|---|---|---|
| **ID** | **Distance** | **Angle** | **Distance** | **Angle** |
| Audio1 | 1.19 m | 310 ° | 3.89 m | 356 ° |
| Audio3 | 1.88 m | 327 ° | 3.68 m | 339 ° |
| Audio4 | 1.50 m | 322 ° | 1.47 m | 270 ° |
| Audio5 | 1.91 m | 5 ° | 3.33 m | 25 ° |
| Audio6 | 2.36 m | 30 ° | 1.45 m | 55 ° |
| Audio7 | 2.11 m | 20 ° | 3.84 m | 313 ° |

2. data is leaked from the high-security system when there are no humans present in the environment (e.g., after regular business hours),

where the latter attack has been termed the **overnight attack**. For each of these scenarios, different modulation parameters were used to establish communication, including:

1. the use of near- and ultrasonic acoustic signals in the frequency range from 18 kHz to 24 kHz in the former attack, and
2. the use of audible and inaudible acoustic signals in the frequency range from 0 Hz to 24 kHz in the **overnight attack.**

The results of this study show that, in general, captured keystrokes, encryption key material (e.g., private keys, shared keys), authentication credentials (e.g., passwords), documents, and even recorded audio can effectively be leaked from compromised air-gapped systems in real-time using *semi-* and *non-invasive* covert exploits through *commodity-pervasive* hardware in the presence of an oblivious covert-analyst.

The closed-door office environment used in this section consisted of a single room approximately 3 m x 3 m x 2.8 m in dimension with a single desk that was approximately 0.75 m off of the ground. The open-concept office consisted of four desks, each of which was 0.75 m off of the ground, spread out over a space approximately 4.25 m x 4.25 m x 2.8 m in dimension. All of the Windows laptops (e.g., **Audio1**, **Audio3**, **Audio4**, **Audio5**, **Audio6**, and **Audio7**) as well as **Audio8**, the Mac OS X laptop, were used in this study and the distances and angles between **Audio8** and each of the other systems in both environments can be seen in **Table 7.5**, where 0 ° can be interpreted as being directly in front of **Audio8** and positive offset angles are measured counter-clockwise from 0 °. Furthermore, in all of the experiments described in this section, **Audio8**, was used as the air-gapped system and the remaining six systems were connected to the low-security network.

### 7.4.1 Real-World Experiments and Results

In order to demonstrate that covert-acoustic channels pose a threat to secure systems and secure facilities, a number of experiments were performed in both environments to mea-

Table 7.6: Configuration Parameters for the Experiments

| Test # | $W(kHz)$ | $T_{guard}(s)$ | $N$ | Description |
|---|---|---|---|---|
| 1 | 18 to 20.5 | 0.020 | 17, 34, 69, 139, 278 | Near ultrasonic |
| 2 | 18 to 20.5 | 0.040 | 17, 34, 69, 139, 278 | Near ultrasonic |
| 3 | 20 to 20.5 | 0.015 | 5, 11, 23, 46, 92 | Ultrasonic |
| 4 | 20 to 20.5 | 0.025 | 5, 11, 23, 46, 92 | Ultrasonic |
| 5 | 0.5 to 20.5 | 0.055 | 232, 464, 928, 1857 | Audible |
| 6 | 0.5 to 20.5 | 0.125 | 232, 464, 928, 1857 | Audible |
| 7 | 0.5 to 18 | 0.055 | 203, 406, 812 | Audible |
| 8 | 0.5 to 18 | 0.125 | 203, 406, 812 | Audible |

sure the data rate of the channel under real-world conditions. The covert-analyst was once again considered to be an unaware and unassuming passive adversary and the maximum achievable data transfer rate as well as the corresponding BER of the channel were measured. The data rate was measured in order to better quantify the threat that malware poses to the security of *continuous source systems*. Moreover, by quantifying the achievable data rates, the type of sensitive data that could be leaked in real-world scenarios can also be characterized. To quantify this risk, the channel was evaluated in real-world environments (e.g., open-concept office, closed-door office) under real-world conditions (e.g., radio playing, people talking) in real-world scenarios (e.g., humans present in the environment, humans absent from the environment). In all, the following experiments were performed:

1. the channel parameters: bandwidth, $W$, guard interval, $T_{guard}$, and number of subchannels, $N$, were all varied to determine the maximum data rate that could be achieved in both environments;

2. given the optimal values for the channel parameters $W$, $T_{guard}$, and $N$, communication was attempted using the ultrasonic spectrum, i.e., $>$ 20 kHz, while a clock radio was playing a local radio station in the closed-door environment;

3. similarly, given the optimal values for the channel parameters $W$, $T_{guard}$, and $N$, communication was attempted using the ultrasonic spectrum while conversations were taking place in the closed-concept environment; and

4. the maximum distance that ultrasonic acoustic signals could be communicated over was evaluated.

The configuration parameters that were tested can be seen in **Table 7.6**. Results for configurations one and two were obtained in order to compare this work against the results initially presented by Hanspach, et al. [89]; configurations three and four were designed to confirm that ultrasonic communication was possible in the two real-world environments; and, experiments five through eight were designed to determined the maximum achievable data rate of the **overnight attack**.

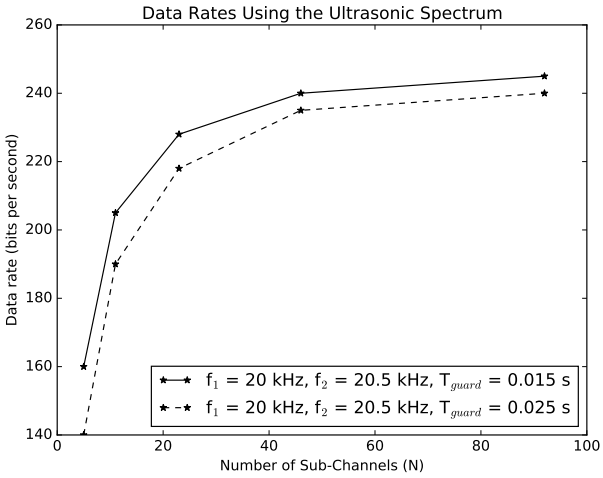



Figure 7.16: Data rates for the ultrasonic tests, namely tests three and four from **Table 7.6**.

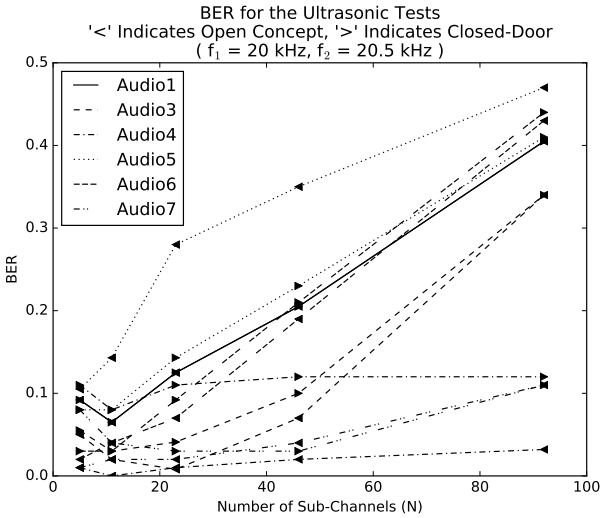



Figure 7.17: BER for the ultrasonic tests, namely tests three and four from **Table 7.6**.

Table 7.7: Average Time (s/page) to Leak Popular Document Types

| Document Type | Average Size (kb) per Page [177] | Leak Time Using **Overnight Attack** |
|---|---|---|
| Microsoft Word | 15 | 3.27 |
| Microsoft Excel | 6 | 1.31 |
| Microsoft PowerPoint | 57 | 12.42 |
| Portable Document Format | 100 | 21.79 |
| Text | 1.5 | 0.33 |
| Email | 10 | 2.18 |
| Tagged Image File Format | 65 | 14.16 |

The achievable data rates corresponding to tests three and four are shown in **Figure 7.16**. From the figure it is evident that as the number of sub-channels, $N$, was increased the data rate also increased, as designed. Correspondingly, in **Figure 7.17**, the BER for the same tests are shown. From the figure it can be seen that as the number of channels in the ultrasonic experiments increased, the BER increased as well. In the closed-door office environment a BER of 10 % or less for all machines with $N = 5$ and $N = 11$ was achieved and in the open-concept environment a BER of 10 % with $N = 5$ was achieved. With $N = 11$ all machines had a BER below 10 % except **Audio5** in the open-concept environment. This was due to the increased distance between **Audio8** and **Audio5** between the two environments, i.e., 1.91 m in the closed-door environment versus 3.33 m in the open-concept environment. The corresponding data rates for $N = 5$ and $N = 11$ were 140 bps and 189 bps respectively. It should also be noted that in the closed-door environment, a data rate of 229 bps and BER below 15 % for all machines was achievable.

Although not shown, communication using the combined near-ultrasonic and ultrasonic ranges (i.e., 18 kHz and above) using $N = 17$ sub-channels was possible, achieving an effective data rate of over 500 bps and BERs of 10 % and 15 % in the closed-door office and the open-concept office environments, respectively. As a comparison, previous researchers were only able to achieve a data rate of 20 bps with a BER of 0 % using the same bandwidth. Furthermore, the best BER results obtained for experiments five through eight were 10 % and 15 % and below for the closed-door and open-concept environments respectively, with the exception again being **Audio5**, which achieved a BER of 19 % in the open-concept tests. $N = 812$ sub-channels were used to achieve these results, which produce a data rate of over 6.7 kbps. Through experimentation it was also confirmed that transmission at a data rate over 8.7 kbps could also be achieved using $W = 500$ Hz to 20.5 kHz and $N = 1857$ with BERs below 25 % and 30 % in the closed-door and open-concept office environments, respectively.

In order to reduce these error rates to acceptable levels, an $[n, k, d]$ block code (where $n$ is the block length, $k$ is the message length, and $d$ is the distance), capable of correcting

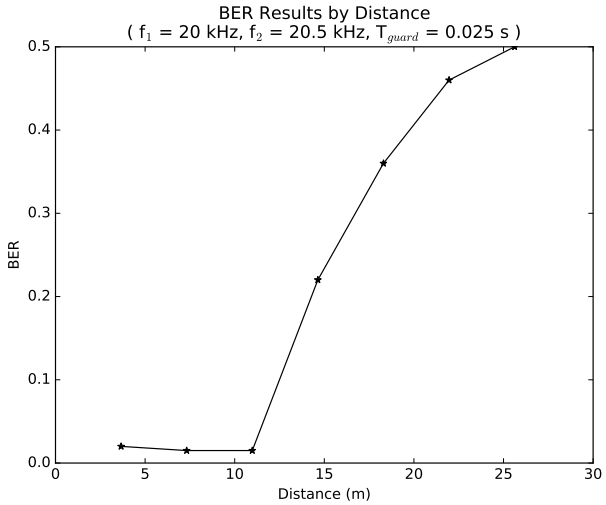



Figure 7.18: BER for the distance experiment. **Audio8**'s ability to communicate with **Audio7** over increasing distances was tested. The parameters for the distance tests were $W = 20$ kHz to 20.5 kHz, $T_{guard} = 0.025$ s, and $N = 46$.

$\lfloor \frac{d-1}{2} \rfloor$ random errors, such as $[n, k, n-k+1]$ Reed-Solomon Codes [192], could be used. To correct up to 10% and 15% bit errors using Reed-Solomon codes, an overheard of approximately 20% and 30% is respectively required. Given the experimental results of this section, the measured data rates after error correcting would be reduced to 112 bps and 4.7 kbps using the ultrasonic and audible frequency ranges, respectively. To put these data rates into perspective, an individual typing 7-bit ASCII text at 80 words per minute and an average word length of 5.1 characters would produce data at an average rate of 47.6 bps. Similarly, voice can be streamed using the LPC-10 codec at 2.4 kbps [132]. Given these data rates, the **overnight attack** could be used to effectively leak buffered keystrokes collected throughout regular business hours during off-hours as well as recorded audio. Additionally, using the ultrasonic frequency range, keystrokes could also be leaked in real-time. Data, such as text files or private keys, can be leaked at a rate of $x/112$ seconds and $x/4700$ seconds, where $x$ is the size of the data in bits, using the ultrasonic and **overnight attacks** respectively. **Table 7.7** again provides average document sizes but now includes the amount of time that would be required in order to leak each document type using the **overnight attack**. Lastly, both attacks are effectively able to leak cryptographic key material such as 256-bit Advanced Encryption Standard [49] keys within seconds.

Using the parameters $W = 20$ kHz to 20.5 kHz, $k = 25$ ms, and $N = 11$, the ultrasonic attack was tested with both a clock radio playing in the background as well as conversations taking place in the room while data was being leaked. The result was that the BER only increases marginally. This was due to the fact that while the human voice is predominantly composed of frequencies below 4 kHz there are still some near-ultrasonic frequencies present which interfered with the data symbols. It was observed that the majority of the acoustic energy from the radio as well as the conversations was in the 0 Hz to 15 kHz bandwidth and, in general, did not adversely affect the ultrasonic communication.

Lastly, an experiment was performed to determine the maximum distance over which

ultrasonic signals could be transmitted as a means to compare these results to those of previous work. To determine the maximum transmission range **Audio8** was set up to transmit to **Audio7** over increasing distances in 3.66 m (12') increments from 3.66m to 25.60m (84'). The results are graphed in **Figure 7.18**. The ultrasonic communication attack is, therefore, able to effectively communicate up to distances of 11 m with BERs under 2 % and up to a distance of 15 m with BERs around 20 %. With $W = 20$ kHz to 20.5 kHz, $T_{guard} = 25$ ms and $N = 46$, communication was possible at over 230 bps. With error correcting it is, therefore, possible to communicate at a distance of 15 m with an effective data rate of 138 bps. As a comparison, the researchers in [90] were only able to communicate at 20 bps up to a maximum distance of 8.2 m with a BER of 0 %.

The experiments preformed in this section, therefore, demonstrate the following:

1. malware can leak sensitive data using ultrasonic communication to systems on a low-security network at data rates up to 140 bps (112 bps after error correction) with a BER of 10 % or less;

2. malware can leak sensitive data using the **overnight attack** to systems on a low-security network at data rates up to 6.7 kbps (4.7 kbps after error correction) with a BER of 15 % or less (the exception being **Audio5**, which experienced a BER of 19 %, at least 4 % higher than all other machines);

3. the ultrasonic attack is not affected by either a clock radio playing a local radio station in the environment or by conversations taking place while the covert communication is taking place; and

4. the ultrasonic attack is capable of leaking sensitive information at distances up to 11 m and data rates up to 230 bps. Furthermore, ultrasonic communication can be used to leak sensitive information at a distance of 15 m and a data rates up to 138 bps.

In summary, in this chapter it was shown that by measuring the acoustic channel and by engineering an appropriate communication system, data rates of hundreds of bits per second could be achieved in the near- and ultrasonic ranges that are *imperceptible* to an oblivious passive adversary in both the lab environment as well as under real-world conditions. Moreover, the **overnight attack** was shown to be effective at leaking sensitive data at rates above 6 kbps. In the next chapter, it is shown that with appropriate technical tools these channels can be detected under certain circumstances. And, furthermore, algorithms for increasing the *covertness* of covert-acoustic signals in the face of a capable passive adversary are explored.

# Chapter 8

# The Covertness of Covert-Acoustic Channels

In the previous chapter, it was assumed that a passive covert-analyst was present in the environment, but that she was oblivious to any communication that was taking place. As a result, the covert-acoustic channel was considered *covert* if it was *imperceptible* to the analyst given only the analyst's natural ability to hear. In this chapter, the *covertness* of covert-acoustic channels is empirically evaluated by measuring the *steganographic capacity* of the channel when the covert-analyst, Wendy, uses technical tools to detect the near- and ultrasonic signals being communicated. Moreover, given Wendy's new technical ability, various *secure undetectable covert channel* techniques that Alice and Bob could employ to actively avoid detection are also evaluated. The evaluation in this chapter empirically measures the amount of information, as opposed to data rate, that could be leaked from high-security, air-gapped systems to low-security systems before a covert-analyst can detect the communication and, thus, is relevant to the security of *fixed source systems*.

The analysis in this chapter continues to assume that the *modulator* and *demodulator* use *semi-* and *non-invasive* covert-exploits to establish communication. Moreover, given the nature of the acoustic channel, the channel attacker model continues to be a *shared* model. Given this model, Wendy is capable of adding signals to the environment in addition to being able to passively listen for communication. As a reminder, in the former case Wendy is referred to as an "active covert-analyst" and in the latter case she is referred to as a "passive covert-analyst." In addition to evaluating the covert-acoustic channel when Wendy is passive, the BER and probability of synchronizing a frame of data is also evaluated in this chapter when Wendy is active.

This chapter is organized as follows. In **Section 8.1**, *undetectable* covert-acoustic channels, established through FSK as well as OFDM modulation, are evaluated to determine the *steganographic capacity* of the resulting channels. In **Section 8.2**, *secure undetectable* covert-acoustic channels, established using FHSS modulation, as well as channels established by transmitting during randomly selected symbol intervals are also evaluated. The performance of the covert-acoustic channel is also measured in the face of an "active covert-analyst" in **Section 8.3**. And, lastly, in **Section 8.4**, recommendations on how to reduce

the threat of covert-acoustic channels are provided to secure system developers.

## 8.1 Detection of Undetectable Covert-Acoustic Channels

In the previous chapter, FSK was used to modulate data onto carriers that were in the near- and ultrasonic frequency ranges, i.e., 18 kHz and above. With FSK modulation, each symbol, $m_i$, is modulated using the following equation:

$$u_i(t) = \begin{cases} A\cos\left(2\pi\left[f_c + m_i\Delta f\right]t\right) & 0 \leq t \leq T_{sym} \\ 0 & \text{otherwise} \end{cases}, \tag{8.1}$$

where $A$ is the amplitude of the transmitted signal, $m_i = 0, 1, 2, \ldots, M-1$, is the transmitted symbol, $\Delta f$ is the frequency separation between successive symbol frequencies, i.e., $\Delta f = f_m - f_{m-1}$, where $f_m = f_c + m\Delta f$, $0 \leq t \leq T_{sym}$, $T_{sym}$ is the transmission duration of a symbol, in seconds, and $f_c$ is the carrier frequency of the channel. Given this construction, the result of FSK modulating a sequence of data symbols, $\mathbf{s}$, of length $|\mathbf{s}|$, produces a time-domain signal of the form:

$$\begin{aligned} u_{\text{FSK}}(t) &= \sum_{i=1}^{|\mathbf{s}|} u_i(t - iT_{sym}) \\ &= \sum_{i=1}^{|\mathbf{s}|} A\cos\left[2\pi\left(f_c + m_i\Delta f\right)\left(t - iT_{sym}\right)\right], \end{aligned} \tag{8.2}$$

where $m_i \in \mathbf{s}$ and the *guard interval* is not shown.

OFDM was also used in the previous chapter to establish communication over the acoustic channel at higher data rates. OFDM signals can be constructed as a combination of FSK signals by modulating data onto $N$ sub-channels. To accomplish this, the sequence of transmitted data symbols, $\mathbf{s}$, is divided amongst the sub-channels by transforming $\mathbf{s}$ into a matrix, $\mathbf{S}$, of size $N$ rows by $\left\lceil \frac{|\mathbf{s}|}{N} \right\rceil$ columns. This transformation allows each row, $k \in 1, 2, \ldots N$, of the matrix to be used as the data sequence for the $k^{\text{th}}$ sub-channel and, thus, each column, $i \in 1, 2, \ldots, \left\lceil \frac{|\mathbf{s}|}{N} \right\rceil$, contains the data symbols transmitted on the $N$ sub-channels during the $i^{\text{th}}$ symbol interval. OFDM signals that modulate data using FSK on each sub-channel take the form:

$$u_{\text{OFDM}}(t) = \sum_{k=1}^{N} u_{\text{FSK},k}(t)$$

$$
\begin{aligned}
&= \sum_{k=1}^{N} \sum_{i=1}^{\left\lceil \frac{|\mathbf{s}|}{N} \right\rceil} u_{k,i}(t) \\
&= \sum_{k=1}^{N} \sum_{i=1}^{\left\lceil \frac{|\mathbf{s}|}{N} \right\rceil} A \cos\left[2\pi \left(f_{c_k} + m_{k,i}\Delta f\right)\left(t - iT_{sym}\right)\right], \qquad (8.3)
\end{aligned}
$$

where $f_{c_k}$ is the carrier frequency on the $k^{\text{th}}$ sub-channel and $m_{k,i}$ is the symbol transmitted on k$^{\text{th}}$ sub-channel in the i$^{\text{th}}$ symbol interval, i.e., $m_{k,i} \in \mathbf{S}$ is the $(k, i)$ element of $\mathbf{S}$.

OFDM sub-channels were allocated a near non-overlapping portion of the passband bandwidth, $W$, using Carson's Rule [188], which, given a frequency modulated signal, produces a bandwidth, $B$, such that 98 % of the signal's power is contained within the bandwidth. Carson's Rule can be calculated using the following formula:

$$B = 2(\Delta f + f_{peak}),$$

where $f_{peak}$ is the peak frequency deviation from the carrier frequency, and $\Delta f$ is equal to $\frac{1}{T_{sym}}$. Given Carson's Rule, the bandwidth requirements for the modulation schemes used in this work are $B$ and $NB$ for FSK and OFDM, respectively. Lastly, the number of OFDM sub-channels was determined by the equation $N = \left\lfloor \frac{W}{B} \right\rfloor$, and each sub-channel's carrier frequency was chosen such that all of the sub-channels' signal's bandwidth, $B$, remained within the passband bandwidth $W$.

### 8.1.1 Detection of Covert-Acoustic FSK and OFDM Signals

The steganographic capacity of the acoustic channel is measured, in this chapter, when Wendy uses an energy detector to detect the transmission of near- and ultrasonic covert-acoustic signals. As a reminder, an energy detector is a device that takes a received waveform, $r(t)$, and determines whether the waveform contained a transmitted signal plus noise, i.e., $r(t) = u(t) + n(t)$, or simply noise, i.e., $r(t) = n(t)$, where $n(t)$ is a noise signal. In order to make this determination, the energy detector device carries out the following algorithm:

1. the continuous received signal, $r(t)$, is sampled and filtered to remove all signal components and noise outside of the bandwidth $W$ (note that for FSK, $W = B$, and for OFDM, $W = NB$). This processes produces a new, discrete signal, $r_{filt}(t)$.

2. $r_{filt}(t)$ is then squared and summed to produce a reading, $K$, where

$$K = \sum_{t}^{T_{obs}} r_{filt}(t)^2,$$

and $T_{obs}$, in this context, is the length of time the channel is observed for, i.e., $0 \leq t \leq T_{obs}$, $t \in \mathbb{Z}$.

3. Lastly, $K$ is then compared against a pre-computed threshold, $K_0$, and if $K \geq K_0$, Wendy concludes that covert communication had taken place, and if $K < K_0$, Wendy concludes that the original signal, $r(t)$, simply contained noise and that no covert communication has taken place.

A key requirement of the energy detector's algorithm is for Wendy to measure the background noise signal, $n(t)$, so that an appropriate threshold, $K_0$, can be set. To do so, Wendy empirically estimates the distribution of the energy contained in $n(t)$ within the bandwidth $W$ by directly measuring the channel when she reasonably believes there is no communication taking place. Once the PDF of the energy in $n(t)$, $P_n$, has been calculated, Wendy then sets the threshold, $K_0$, such that her probability of false positive, $\alpha$, is set to some acceptable value, where $\alpha$ is calculated as follows:

$$\alpha = \int_{K_0}^{\infty} P_n(x)\,\mathrm{d}x.$$

In this section, the ability for Wendy to detect covert-acoustic signals is determined when Alice communicates with Bob using both FSK and OFDM modulation. When FSK is used, $r_{\mathrm{FSK}}(t) = u_{\mathrm{FSK}}(t) + n(t)$, where $u_{\mathrm{FSK}}(t)$ is defined in **Equation 8.2**, and, therefore, Wendy's probability of detecting Alice and Bob's communication is

$$P_D = \int_{K_0}^{\infty} P_{r_{\mathrm{FSK}}}(x)\,\mathrm{d}x,$$

where $P_{r_{\mathrm{FSK}}}$ is the PDF of the energy contained in $r_{\mathrm{FSK}}$. Similarly, when OFDM is used, $r_{\mathrm{OFDM}}(t) = u_{\mathrm{OFDM}}(t) + n(t)$, where $u_{\mathrm{OFDM}}(t)$ is defined in **Equation 8.3**, and Wendy's probability of detecting Alice's communication is

$$P_D = \int_{K_0}^{\infty} P_{r_{\mathrm{OFDM}}}(x)\,\mathrm{d}x,$$

where $P_{r_{\mathrm{OFDM}}}$ is the PDF of the energy contained in $r_{\mathrm{OFDM}}$.

Whereas in the previous chapter commodity hardware was used by the modulator and demodulator to transmit and receive signals, in this chapter, Wendy attempts to detect the covert-acoustic communication using a specialized, ultrasonic microphone. The microphone used to perform the experiments outlined in this chapter was the Ultramic200K USB ultrasonic microphone from Dodotronic. This particular microphone was chosen because it has a near ideal frequency response in the ultrasonic range, is capable of sample rates up to 200,000 samples per second, and, therefore, is also able to observe audio signals up to a frequency of 100 kHz. The use of a specialized device to detect covert communication is in-line with the security model studied in this dissertation; the modulator and demodulator are restricted to the built-in microphones and speakers found natively on their systems, but Wendy is under no such hardware restriction. Furthermore, it is also reasonable to assume that Wendy is motivated to detect (and disrupt) the covert-acoustic channel and will, therefore, modify her environment to best do so.

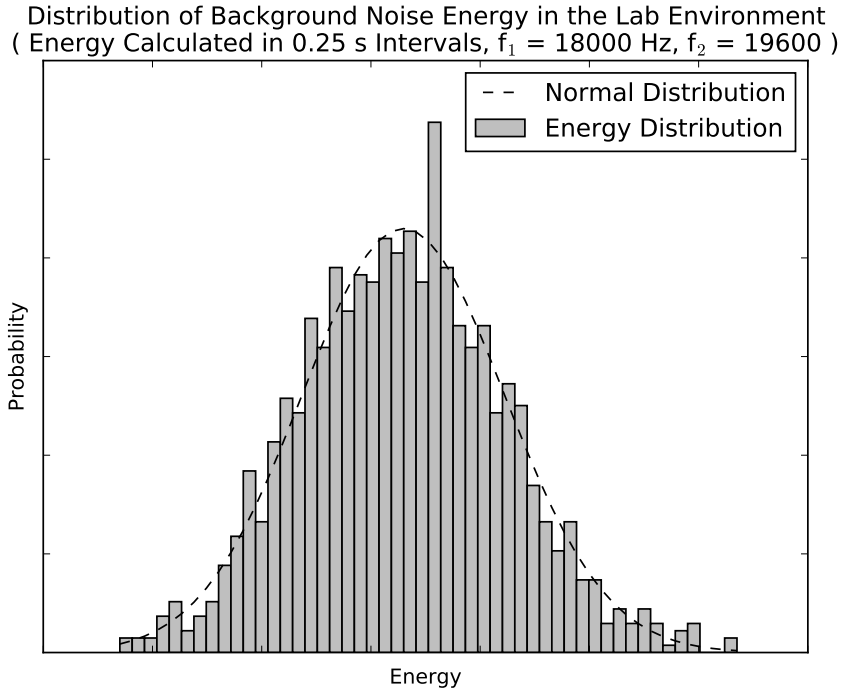



Figure 8.1: PDF of the Background Noise Energy Captured in the Lab Environment

The steganographic capacity of the covert-acoustic channel was measured in the lab environment by using **Audio7** as the transmitter and connecting the UltraMic200K to **Audio8** and using **Audio8** as the covert-analyst. The two machines were separated by 1 m and test transmissions were sent from **Audio7** using both FSK and OFDM modulation at various transmission volumes from 0 dB to -40 dB (i.e., experiments were performed with **Audio7** transmitting at max volume all the way down to $\frac{1}{10^4}$ of max volume) in -20 dB increments. The transmission volume was successively reduced in the tests in order to:

1. observe the relationship between the SNR at the covert-analyst and the steganographic capacity of the channel, and
2. model the effect of increasing the distance between the transmitter and the covert-analyst on the steganographic capacity of the channel.

As a reminder, ultrasonic acoustic signals attenuate at a rate of approximately $0.5\frac{\text{dB}}{\text{m}}$. The two scenarios that were initially tested were:

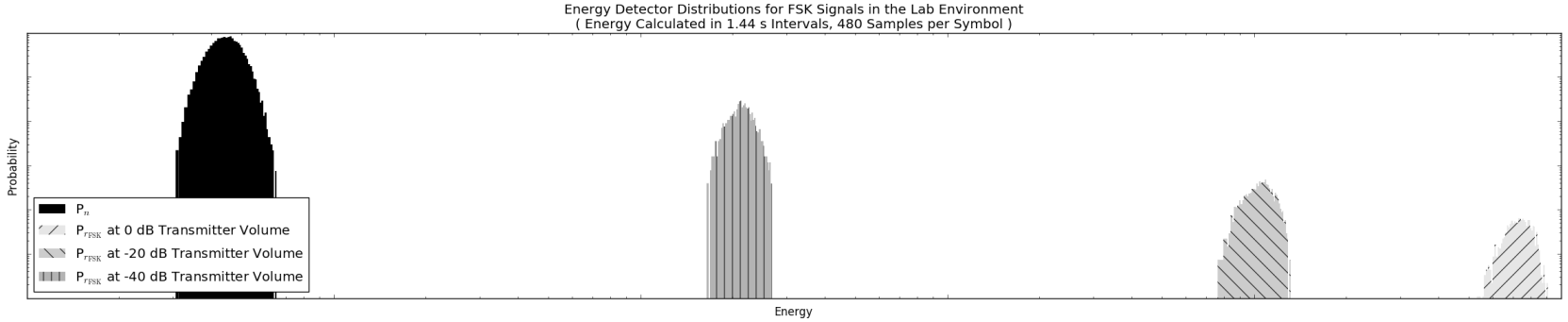
1. FSK modulation with an 18.2 kHz carrier and 480 samples per symbol (W = B = 400 Hz), and
2. OFDM modulation in the 18 kHz to 19.6 kHz bandwidth, $N = 4$ sub-channels, and 480 samples per symbol (B = 400 Hz, W = NB = 1600 Hz).

Before executing each of the test scenarios, the threshold for Wendy's energy detector, $K_0$, was set by observing the background noise without any covert communication taking place. In both scenarios, the background noise over the bandwidths evaluated closely followed a normal distribution, which was verified via a Kolmogorov-Smirnov test. The PDF of the energy contained in the background noise over the bandwidth from 18 kHz to 19.6 kHz can be seen in **Figure 8.1** (see [37] for the source code that was used to generate all the plots in this chapter). In the figure, the normal PDF that closely models the background noise is also shown.

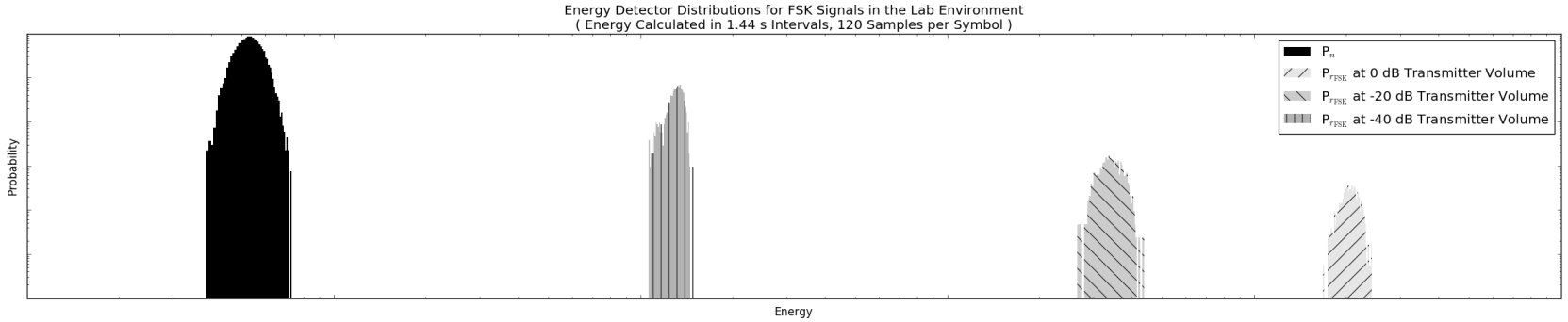
In **Figure 8.2**, Wendy's observed PDFs are shown when Alice and Bob use FSK as well as OFDM modulation (i.e., the plots show $P_n$ versus $P_{FSK}$ and $P_{OFDM}$, respectively, at various transmission volumes). The distributions are plotted on a log-log scale in order to allow all of the distributions to be shown on one graph, which was done to make them more visually comparable. From the FSK (**Figure 8.2a**) and OFDM (**Figure 8.2c**) plots, in which 480 samples per symbol were used, it appears that Wendy can choose a threshold, $K_0$, such that she can easily determine when Alice is communicating, i.e., Wendy can easily distinguish between $P_n$ and $P_{FSK}$ as well as $P_{OFDM}$. This was confirmed by calculating the steganographic capacity of the covert-acoustic channel, which, in both scenarios, came out to zero bits. In **Figure 8.2b**, the energy detector's distributions are again shown, but this time FSK modulation is used with only 120 samples per symbol and a carrier of 18.8 kHz (B = 1600 Hz). As mentioned in the previous chapter, this lowers Alice's signals' SNR, which is reflected in this plot, first visually, by observing that all of the energy distributions are shifted closer to the background noise distribution, as compared **Figure 8.2a**, but most notably by recognizing that the received SNR at -40 dB dropped from 17 dB to 14 dB when 120 samples per symbol were used. Despite this drop in SNR, however, with a false positive rate of $\alpha = 0.001$ and an $\epsilon = 0.5000$, i.e., Wendy detects the covert communication with at least a probability 0.500, the steganographic capacity of the channel is still zero bits.

## 8.2 Detection of Secure Undetectable Covert-Acoustic Channels

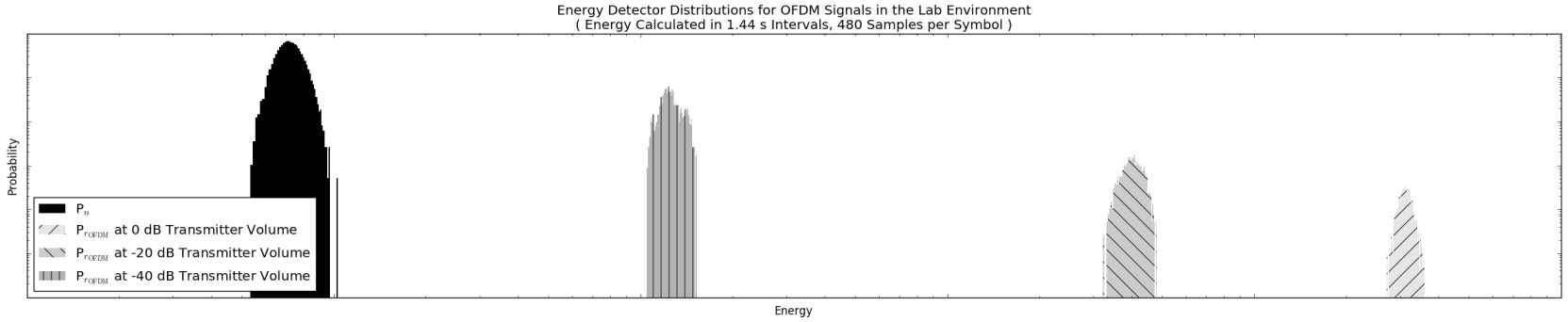
In **Chapter 6**, the theoretical analysis of the steganographic capacity of OOB-CCs led to the conclusion that, by transmitting in short bursts during randomly selected symbol intervals, the covertly communicating parties, Alice and Bob, could communicate more information before being detected, i.e., they could increase the steganographic capacity of the channel by changing their behaviour. When Alice and Bob continuously communicate, i.e., they do not introduce random delays between symbols, Wendy can observe their communication for as long a duration as she needs to in order to maximize her probability of detection. In **Figure 8.2**, an observation interval of $T_{obs} = 1.44$ s was used, which, with a guard interval of 80 ms and 480 samples per symbol, results in a $T_{obs}$ equivalent to 16 symbols. If, however, Alice and Bob use the alternative approach of random inter-symbol delays, then Wendy can no longer simply listen to their communication continuously for as long as she would like before making a decision. Rather, she is forced to make a number of




(a)

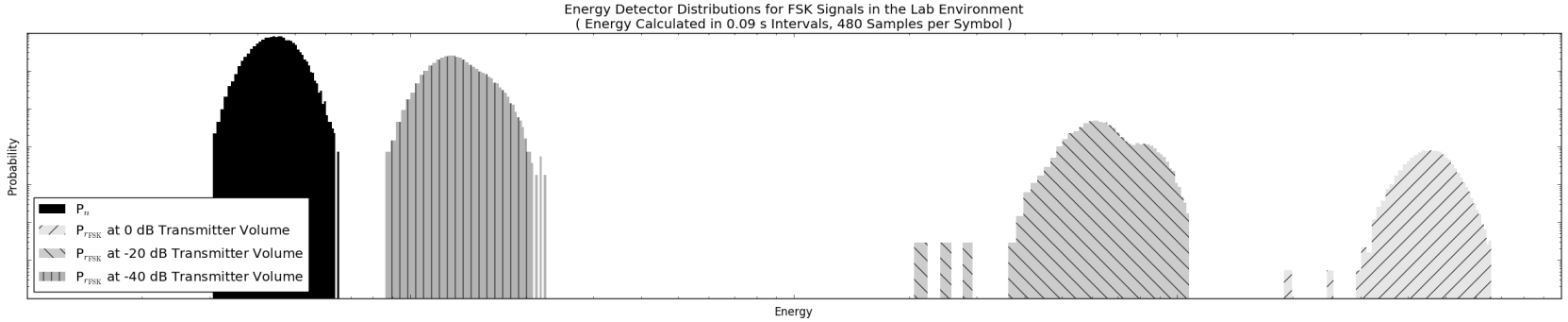



(b)

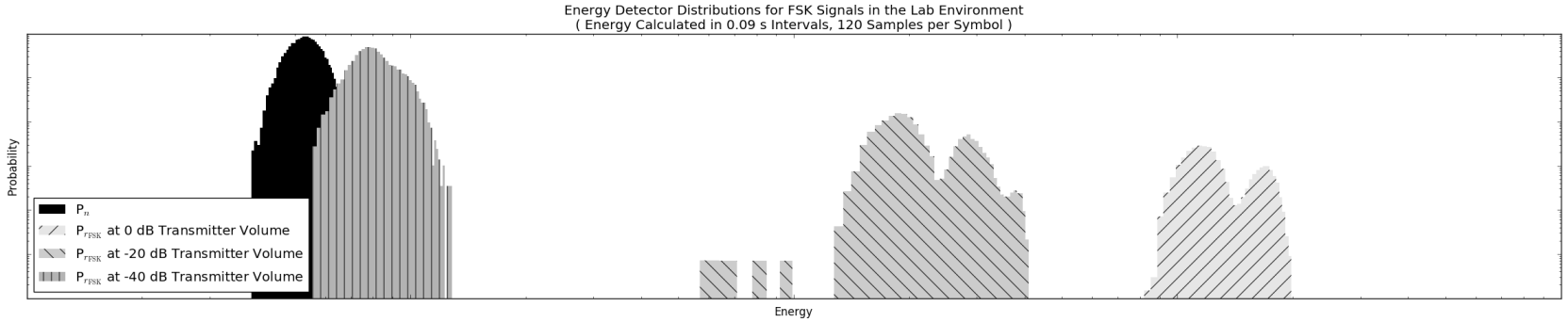



(c)

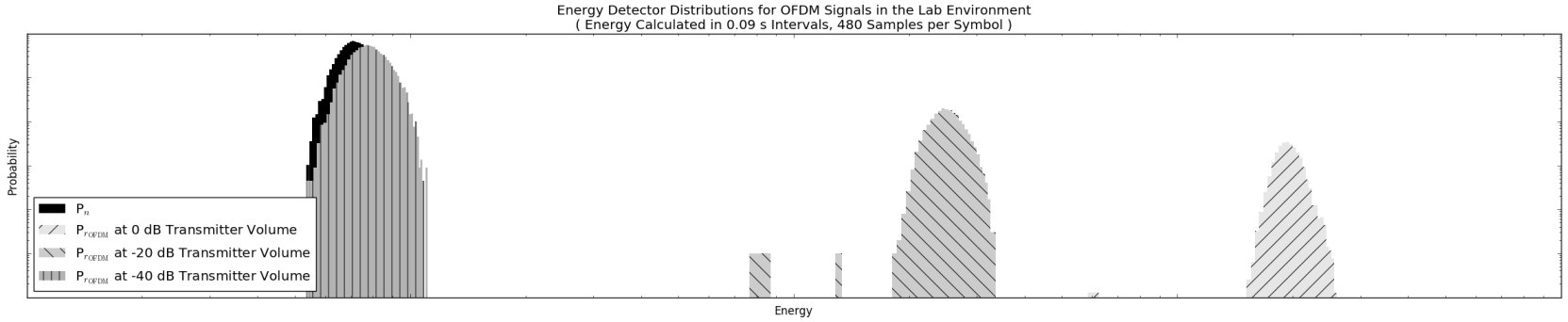
Figure 8.2: Energy Detector Distribution for FSK Signals at Various Transmitter Volumes using 480 Samples per Symbol (a), Energy Detector Distribution for FSK Signals at Various Transmitter Volumes using 120 Samples per Symbol (b), and for OFDM Signals at Various Transmitter Volumes (c)




(a)




(b)




(c)

Figure 8.3: Energy Detector Distribution for FSK Signals and Random Delays at Various Transmitter Volumes using 480 Samples per Symbol (a), Energy Detector Distribution for FSK Signals and Random Delays at Various Transmitter Volumes using 120 Samples per Symbol (b), and for OFDM Signals and Random Delays at Various Transmitter Volumes (c)

shorter duration, independent observations and somehow combine them in order to come to a determination regarding Alice's transmission status.

In **Figure 8.3**, the energy detector distributions are plotted again for the FSK and OFDM test scenarios mentioned above; however, these plots show the results when Alice and Bob transmit one symbol at a time and introduce random delays between each symbol. The results for FSK when 480 samples per symbol and 120 samples per symbol are used can be seen in **Figure 8.3a** and **Figure 8.3b**, respectively. When 120 samples per symbol are used, the distribution at the -40 dB transmission volume level does overlap with the background noise distributions and the received SNR drops from 5 dB to 2 dB; however, at a false positive rate of $\alpha = 0.001$ and $\epsilon = 0.500$ the steganographic capacity remains zero. When OFDM is used, on the other hand (see **Figure 8.3c**), the received SNR at -40 dB is 0.37 dB and the steganographic capacity becomes non-zero, climbing to a modest 40 bits. This result is not entirely unexpected because with OFDM Alice's transmit power, $P_t$, is less than or equal to her transmission power when FSK is used, given the non-ideal frequency response of the channel; however, the passband bandwidth is $N = 4$ times larger, and, thus, the SNR at the covert-analyst is consequently lower which produces the result shown.

Another technique that Alice and Bob could use to improve their steganographic capacity, in the face of a powerful passive adversary, is to spread their signals out in the frequency domain in addition to the time domain. FHSS is one such technique that allows them to do so. Recalling the equation used to modulate FSK symbols shown in **Equation 8.1**, FHSS uses the same basic equation but spreads the transmitted signal's power out in the frequency domain by changing the carrier frequency each time a symbol is transmitted. This results in each symbol's signal component taking the following form:

$$u_{\text{FHSS},i}(t) = \begin{cases} A\cos\left(2\pi\left[f_{c_i} + m_i\Delta f\right]t\right) & 0 \leq t \leq T_{sym} \\ 0 & \text{otherwise} \end{cases},$$

where $f_{c_i}$ is the carrier frequency chosen to transmit the i$^{\text{th}}$ symbol, $f_{c_i} \in \{f_{c_k}\}$, $k \in 1, 2, \ldots N$, $\{f_{c_k}\}$ is the set of possible carrier frequencies, and the passband bandwidth $W$ is divided into $N$ sub-channels of width $B$ Hz, in the same way it was previously for OFDM. Combining each symbol's signal produces the transmitted signal

$$\begin{aligned} u_{\text{FHSS}}(t) &= \sum_{i=1}^{|\mathbf{s}|} u_{\text{FHSS},i}(t - iT_{sym}) \\ &= \sum_{i=1}^{|\mathbf{s}|} A\cos\left[2\pi\left(f_{c_i} + m_i\Delta f\right)\left(t - iT_{sym}\right)\right]. \end{aligned} \tag{8.4}$$

As a result, Wendy then observes $r_{\text{FHSS}}(t) = u_{\text{FHSS}}(t) + n(t)$, which has a probability density, $P_{r_{\text{FHSS}}}$, and, therefore, a probability of detection of

$$P_D = \int_{K_0}^{\infty} P_{r_{\text{FHSS}}}(x)\,\mathrm{d}x.$$

The important difference between the FSK and FHSS scenarios, from Wendy's perspective, is that when FHSS is used Wendy is forced to observe a much larger bandwidth than when FSK is used in order to observe all of Alice's transmission. Therefore, Wendy also must observe more noise as a result. When Alice uses FSK the passband bandwidth that Wendy filters $r_{\text{FSK}}(t)$ by is $W = B$ Hz, however, when FHSS is used, Wendy's passband filter bandwidth for $r_{\text{FHSS}}(t)$ is $W = NB$ Hz, because data is transmitted on random carriers spread out through the larger bandwidth, $W = NB$ Hz. Furthermore, the important difference between FHSS and OFDM, in the context of calculating steganographic capacity, is that, while the passband bandwidths are the same for both modulation schemes, FHSS modulation only transmits on one sub-channel per symbol interval, whereas OFDM modulation transmits on all sub-channels. Assuming, however, that the modulator outputs an average power of $P_t$ within the passband $W$, regardless of modulation scheme, there should not be a significant difference between the two, in terms of how many channel observations Wendy requires in order to detect the channel.

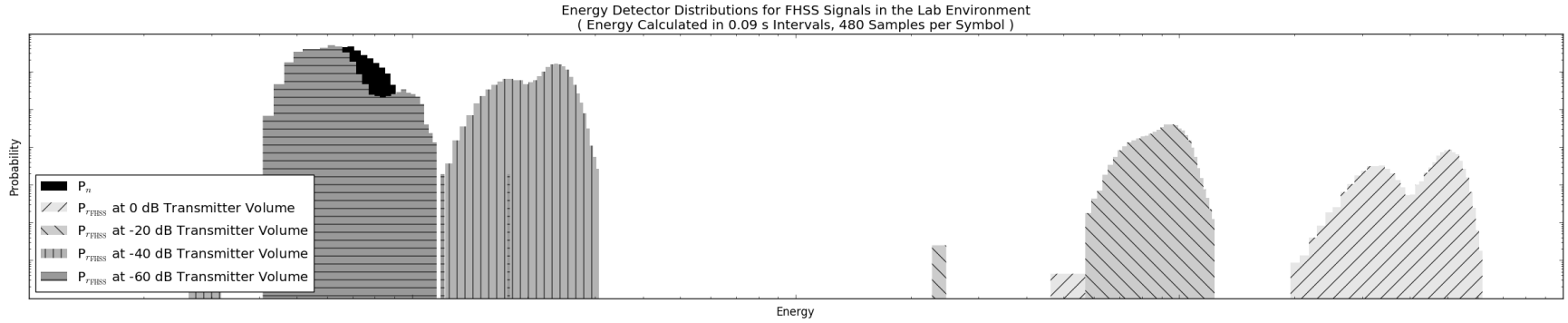
In order to measure any difference in steganographic capacity between OFDM and FHSS, the following test was performed:

1. FHSS modulation in the 18 kHz to 19.6 kHz bandwidth, $N = 4$ sub-channels and 480 samples per symbol (B = 400 Hz, W = NB = 1600 Hz).

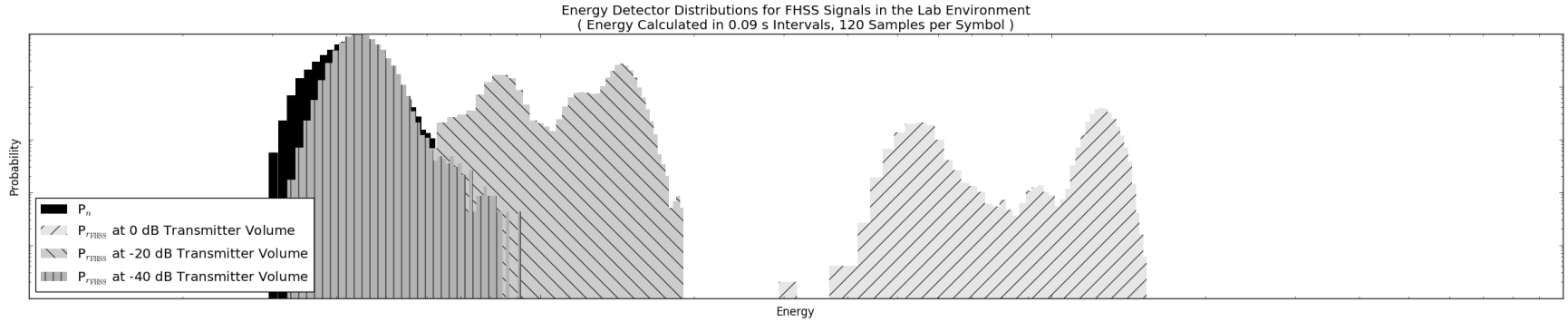
**Figure 8.4a** shows the resulting energy distributions, as observed by Wendy, which are directly comparable to the energy distributions for OFDM shown in **Figure 8.3c**. Comparing both figures shows that when OFDM is used there is overlap between the PDF at the -40 dB volume level and the PDF of the background noise energy; however, when FHSS is used there is no overlap at the -40 dB level. Upon further investigation, it was confirmed that OFDM signals are not received with the same power as signals transmitted using FHSS. As a comparison, the SNR at the receiver when OFDM was used was 0.37 dB at the -40 dB level, whereas when FHSS was used it was 5.13 dB. In order to match the received power of the OFDM signals at the -40 dB level, FHSS signals would have to roughly be transmitted at around -60 dB transmitter volume. This was confirmed by measuring the steganographic capacity of the channel using the technique outlined in **Section 6.3** at the -40 dB level for OFDM and the -60 dB level for FHSS, which came out to 40 bits and 30 bits, respectively.

The effect of widening the passband bandwidth, $W$, on the steganographic capacity of FHSS signals was also measured by performing the following test:

1. FHSS modulation in the 18 kHz to 23 kHz bandwidth, $N = 3$ sub-channels and 120 samples per symbol (B = 1600 Hz, W = NB = 4800 Hz).




(a)




(b)

Figure 8.4: Energy Detector Distribution for FHSS Signals and Random Delays at Various Transmitter Volumes using 480 Samples per Symbol (a), and for FHSS Signals and Random Delays at Various Transmitter Volumes using 120 Samples per Symbol (b)

From **Figure 8.4b**, it can be seen that the energy distributions of the received wave forms, $r_{\text{FHSS}}$, have a much wider variance when FHSS is used as compared to when FSK or OFDM were used. This is due to the fact that FHSS transmits information on multiple sub-channels and, given the non-ideal frequency response of the channel, signals transmitted on sub-channels at higher carrier frequencies are transmitted and received with less power than those transmitted at lower frequencies. Moreover, by transmitting using FHSS over a wider bandwidth the steganographic capacity can be increased because the SNR observed by Wendy is decreased. As an example, when FHSS is used over the bandwidth from 18 kHz to 23 kHz with 120 samples per symbol, the steganographic capacity climbed to 120 bits (at a false positive rate of $\alpha = 0.001$ and $\epsilon = 0.500$) again using the method to calculate steganographic capacity outlined in **Section 6.3**.

While the steganographic capacity of the channel has been increased by randomly choosing which symbol intervals to transmit in, by using multi-carrier modulation, and by widening the spread-spectrum bandwidth, there is now an additional requirement for random data to be shared between Alice and Bob. If Alice and Bob agree to transmit one symbol out of every $n$ symbol intervals, then the two must share $\log n$ bits of information per symbol. Additionally, if Alice and Bob choose a different carrier frequency each symbol interval then they must also share an additional $\log N$ bits of information. Thus, in order to transmit one symbol Alice and Bob must share at least

$$\begin{aligned} v &= \log N + \log n \\ &= \log nN \text{ bits.} \end{aligned}$$

And, thus, for a sequence of length $|\mathbf{s}|$ symbols, $|\mathbf{s}| \log nN$ bits of random information are required. A practical way of ensuring that Alice and Bob are effectively able to share this degree of random information is for the two parties to initially share a sufficiently random seed that they can both use to initialize their own internal random number generate (RNG). This way, they can produce the same sequence of random values required to communicate without having to directly share the random bits.

The result of switching from an *undetectable* covert channel to a *secure undetectable* covert channel resulted in the steganographic capacity increasing from zero bits to potentially hundreds of bits. While this is a small amount of information, it provides evidence that the modulator and demodulator can implement measures in order to increase the steganographic capacity of their channel, even in the presence of a capable passive covert-analyst under certain conditions. This seminal, practical result should provide motivation for covert channel designers to continue down the path of enhancing practical secure undetectable covert-acoustic channels through the development of novel algorithms with the goal of increasing the steganographic capacity of the channel.

On the other hand, the results presented so far in this chapter are a promising outcome for the designers of secure systems and secure facilities. By installing energy detection devices in environments where air-gapped systems are installed, covert-acoustic channels can be detected, and subsequently compromised systems can be removed. It is recommended

that the energy detector devices be installed as external system components so that they are less likely to be tampered with by the malware installed on the low- and high-security systems. As an interesting aside, when configured to produce five nine's reliability, i.e., a false positive rate of 0.00001 and a probability of detection of 0.99999, the steganographic capacity of the channel when FHSS modulation is used with 120 samples per symbol is less than four kilobytes of data, which, after accounting for synchronization and error correction, results in what amounts to a very low practical goodput (i.e., the amount of data that can be successfully communicated by applications that use the channel) for malicious applications that are looking to leak data.

## 8.3 Disruption of Secure Undetectable Covert-Acoustic Channels

An alternative defence strategy to detecting covert-acoustic channels is to preemptively disrupt them. In the literature on low-probability of detection communication systems this particular technique is referred to as *jamming* and it is studied under the *electronic counter measures* (ECM) field of research [184]. In the context of covert channels, *jamming* translates to Wendy being an "active covert-analyst" and in the *shared* channel model Wendy jams Alice's transmissions by adding signals to the environment in an effort to cause Bob to fail when synchronizing a frame of data or to cause Bob to demodulate symbols incorrectly, i.e., increase Bob's BER.

There are two general, classical jamming strategies that exist in the literature [184]: *tone jamming* and *barrage jamming*. With *tone jamming*, the jammer, (i.e., the active covert-analyst), transmits power on a specific frequency in the hopes of disrupting the synchronization phase of the covertly communicating parties or introducing demodulation and decoding errors into their communication. *Tone jamming* techniques include transmitting power on a single frequency or multiple frequencies and have also been documented in *repeater* mode where the jammer attempts to determine which carrier frequency is being used to communicate data and transits jamming power on the estimated frequency. The *repeater* technique is especially effective against parties that use FHSS to communicate.

In *barrage jamming*, power is transmitted at an equal level across a given bandwidth, $W$, in the hopes of increasing the background noise level at the receiver to consequently reduce the communicating parties' probability of synchronizing as well as increase their BER. *Barrage jamming* techniques include *wideband jamming*, which transmits power across the whole bandwidth, $W$, used for communication, and *partial-band jamming*, which transmits power across a portion of the bandwidth, $\rho W$, $0.0 < \rho < 1.0$, used for communication. Furthermore, in general, jammers can operate in *continuous* or *pulse* mode, where in the latter case the jammer oscillates between being "on" and "off", i.e., transmitting noise and not, respectively, according to some duty factor $0 < \rho_{pulse} \leq 1$. The benefit of *pulse jamming* as well as *partial-band jamming* is that a greater amount of power can be concentrated into a shorter time window or into a more restricted bandwidth window, respectively.

The literature on jamming (or ECM) and anti-jamming (or *electronic counter counter measure*) techniques is extensive. In the area of *electronic counter counter measures*, for instance, there are a number of known techniques, such as error correcting codes and symbol interleavers that can be used to reduce the effectiveness of certain classes of jammers. However, while these solutions are itemized here for completeness, they are not studied any further in this dissertation. Rather, their study and application to covert-acoustic channels is left to future researchers. This section, therefore, is meant to be used as a starting point for future research into jamming and associated countermeasures in the acoustic channel. Furthermore, all of the background theory presented and discussed in this section is sourced from the works of Peterson, et al. [184] and Torrieri [231].

In this section, the effect of *wideband barrage jamming* as well as *tone jamming* are studied. In all of the experiments outlined in this section, **Audio7** was configured to be the modulator and **Audio8** was configured to be the demodulator. The **Audio3** system was updated to include an external set of speakers and acted as the "active covert-analyst." KEF X300A external speakers were added to **Audio3** and used for jamming communication between **Audio8** and **Audio7** because they possess a near-ideal frequency response up to 28 kHz. Moreover, the speakers support sample rates up to 96 kHz and are, therefore, ideally suited for jamming near- and ultrasonic acoustic signals. In order to measure the effect of each of the jamming algorithms, the probability of synchronizing a frame and the BER were measured using three different modulation schemes:

1. FSK modulation with an 18.2 kHz carrier and 480 samples per symbol (W = B = 400 Hz);
2. OFDM modulation in the 18 kHz to 19.6 kHz bandwidth, $N = 4$ sub-channels and 480 samples per symbol (B = 400 Hz, W = NB = 1600 Hz); and
3. FHSS modulation in the 18 kHz to 19.6 kHz bandwidth, $N = 4$ sub-channels and 480 samples per symbol (B = 400 Hz, W = NB = 1600 Hz).

All three modulation schemes were tested against two different jamming techniques:

1. *wideband barrage jamming*, and
2. *tone jamming* with a frequency of 18.1 kHz,

which were both administered in *continuous* mode. Furthermore, the *wideband barrage jamming* tests were configured to transmit noise across the full bandwidth used by each of the modulation schemes. Moreover, the *tone jamming* frequency of 18.1 kHz was chosen because all schemes used this particular frequency to transmit information.

Given the theoretical literature on jamming, it would be expected that the FSK as well as FHSS modulation results would show less adverse effects in the presence of a *barrage jammer* than a scheme like OFDM would. The reason being that with FSK and FHSS, each symbol's chosen frequency is transmitted with maximum power since only one symbol

Table 8.1: Jamming Results with the Covert Analyst at Full Power

| | **No Jamming** | | **Tone Jamming** | | **Barrage Jamming** | |
|---|---|---|---|---|---|---|
| **Modulation Scheme** | $\mathbf{P}_{sync}$ | **BER** | $\mathbf{P}_{sync}$ | **BER** | $\mathbf{P}_{sync}$ | **BER** |
| FSK | 1.00 | 0.00 | 0.00 | | 0.30 | 0.09 |
| OFDM | 1.00 | 0.00 | 1.00 | 0.15 | 0.00 | |
| FHSS | 1.00 | 0.00 | 0.00 | | 0.00 | |

Table 8.2: Jamming Results with the Covert Analyst at Half Power

| | **No Jamming** | | **Tone Jamming** | | **Barrage Jamming** | |
|---|---|---|---|---|---|---|
| **Modulation Scheme** | $\mathbf{P}_{sync}$ | **BER** | $\mathbf{P}_{sync}$ | **BER** | $\mathbf{P}_{sync}$ | **BER** |
| FSK | 1.00 | 0.00 | 0.52 | 0.14 | 1.00 | 0.00 |
| OFDM | 1.00 | 0.00 | 1.00 | 0.05 | 0.90 | 0.10 |
| FHSS | 1.00 | 0.00 | 1.00 | 0.30 | 1.00 | 0.00 |

is transmitted per interval, whereas with OFDM, individual symbols transmitted on sub-channels are transmitted with less power given that the total power of the transmitter is necessarily spread across all symbols' signals. Furthermore, it would also be expected that FHSS would perform well in the presence of a *tone jammer* since, on each symbol transmission, the carrier frequency changes and, therefore, the *tone jammer* only affects one symbol for every $N$ symbols transmitted, on average.

The results of the jamming tests can be seen in **Table 8.1** and **Table 8.2**. To generate the results shown in **Table 8.1**, the covert-analyst transmitted each of the jamming signals at maximum power, whereas to generate the results shown in **Table 8.2**, the covert-analyst transmitted the jamming signals at half power, or at a level 3 dB lower than the full power experiments. As expected, when FSK was used the channel could not reliably be synchronized, regardless of jamming method when jamming was performed at full power. This was due to the fact that both jamming methods induced a sufficient number of random errors to the extent that the demodulator could not reliably find the preamble in the received signal. Also, as expected, when OFDM was used, the demodulator was able to reliably synchronize data frames in the presence of a tone jammer, but did suffer from a much higher BER (15 % and 5 % for full and half-power, respectively, as opposed to 0 %). Moreover, surprisingly, neither OFDM nor FHSS were as resilient as one would expect in the presence of the barrage jammer at full power. This result, combined with barrage jamming results for the half power jammer, were due to the fact that the signal power generated by the KEF X300A speakers at full power was sufficient to overpower each of the modulation schemes' transmitted symbols. This result is consistent with the literature and confirms that when using active methods to disrupt communication, jamming power at the receiver is of utmost importance.

## 8.4 Defence Mechanisms

Given the experimental observations from this chapter, as well as those from the previous chapter, **Chapter 7**, the following recommendations are provided to developers of secure systems as well as to designers of secure facilities:

### 8.4.1 Prevention

- Systems that contain microphones and speakers but do not require them to perform their intended function should have them removed.
- In the event that a system's speakers or microphones cannot be removed, they should be disabled in software. Moreover, acoustic dampening material should be placed over top of the devices so that their effectiveness can be reduced.
- All secure systems should require applications to request and obtain permission to use any speaker and microphone installed on their systems. Moreover, any permissions granted should also be logged so that they can be audited.
- All secure systems should use mandatory access control policies to restrict access to speakers and microphones [178].
- Systems with different security requirements, that also require speakers and microphones to perform their intended function, should be physically separated from each other by distance and by acoustic shielding.
- Secure systems, and vendors of speakers for high-security systems, should filter out inaudible frequencies before audio signals are transmitted or manufacture speakers such that they cannot produce inaudible frequencies. Similarly, audio signals captured by microphones on secure systems should be filtered so that inaudible frequencies are removed or microphones should be manufactured in such a way that they cannot observe inaudible frequencies [53, 89, 90].

### 8.4.2 Detection

- Energy detection devices, tuned to the inaudible frequency range, i.e., 18 kHz and above, should be configured and placed as close as possible to systems that require speakers and microphones to perform their intended function. Moreover, energy detection devices tuned to the audible frequency range should be active outside of business hours to detect the **overnight attack**.
- All secure systems should log any accesses by applications to the speakers and microphones on their systems so that the access can be audited for abuse [89].

### 8.4.3 Disruption

- Barrage jamming devices, tuned to the inaudible frequency range, i.e., 18 kHz and above, should be configured and placed as close as possible to systems that require microphones to perform their intended function.
- The jamming device must be capable of outputting noise power above the power level that nearby systems can output.

Given these recommendations, a judicious implementation for secure facilities would be to implement all of the *prevention* recommendations as well as the *detection* recommendations. Moreover, the *disruption* recommendations should also be implemented, but instead of constantly flooding the environment with barrage jamming noise, the barrage jamming devices should be enabled when the energy detection devices in the environment detect that covert-acoustic communication is taking place, as a means to conserve power.

# Chapter 9

# Conclusion

A fresh perspective on covert channels has been presented in this work. A new class of covert channel, *air-gap covert channels*, was defined as *an unintentional communication channel that circumvents the security of systems protected by the* total isolation *principle*. Secure systems were also categorized as either *fixed-source systems* or *continuous-source systems*, and the analysis of these classes led to the conclusion that the relevant security criterion for evaluating covert channels in *continuous-source systems* continues to be an acceptable predefined communication rate, but that the security criterion of paramount importance to *fixed source systems* is Moskowitz and Myong's *small message criterion* [105]. Correspondingly, the traditional metric used to measure the risk that covert channels pose to secure systems, *Shannon capacity*, was challenged, and a new metric, *steganographic capacity*, was proposed to accurately evaluate the risk posed by covert channels to *fixed-source systems*.

An extension of Simmons' classical *prisoners' problem*, the *solitary confinement problem*, was also presented: two prisoners placed in solitary confinement are unable to communicate with one another by traditional means, i.e., message passing. Their goal, however, is to establish a covert, out-of-band communication channel, that is undetectable to the guards who are watching them so that they can communicate an escape plan. The goal for the guards, on the other hand, is to devise a scheme to detect the covert communication and take corrective action against the prisoners. Given the *solitary confinement problem*, a novel sub-class of *air-gap covert channels*, out-of-band covert channels (OOB-CCs), was defined as *communication channels established between disconnected systems that use* semi- *and* non-invasive *covert exploits to enable the communication*, i.e., air-gap covert channels that require no hardware modification to be realized.

The pre-existing sub-categories of covert channels, namely single-host, physical, and network covert channels, were compared and contrasted with OOB-CCs, and it was demonstrated that OOB-CCs are a new category of covert channel on their own that, to date, has not been studied in a systematic fashion. Through the analysis of state-of-the-art OOB-CCs, it was qualitatively shown that current OOB-CC techniques rely on an unaware and unassuming passive adversary. As a result, a more comprehensive adversarial model was proposed where a *passive adversary* is present and no longer oblivious, but aware of both

the communication channel and modulation scheme used for covert communication. Moreover, it was proposed that covert channel techniques also be evaluated in the presence of an *active adversary* when measuring the data transfer rate of covert channel techniques going forward.

The survey of OOB-CCs in **Chapter 5**, categorized the existing techniques in the covert channel, device pairing and side channel literature that share similar requirements with OOB-CCs, i.e., techniques that use non-traditional forms of communication and do not require hardware modification, but instead leverage the set of sensors commonly found in commodity hardware. Additionally, a taxonomy based on the physical channels used by OOB-CCs, e.g., acoustic, light, seismic, magnetic, thermal, and radio-frequency, as well as the hardware requirements of the modulator (transmitter) and demodulator (receiver) were also presented to categorize OOB-CC techniques. The review of the literature also showed that OOB-CCs, in general, are not as high-bandwidth as conventional radio-frequency channels; however, they are capable of transferring up to hundreds and in some cases thousands of bits per second, e.g., covert-acoustic, covert-RF. In general, OOB-CCs have limited transmission range, and are typically constrained by common environmental obstacles (e.g., walls, doors). Additionally, in some cases (e.g., covert-magnetic, some covert-RF configurations), there is limited hardware support at the demodulator for out-of-band communication and, therefore, these classes of OOB-CC are less likely to provide out-of-band covert communication on a wide array of systems. Both covert-light and covert-acoustic channels, as well as some covert-RF channels, on the other hand, benefit from widespread hardware support, increased sender-receiver distance when compared to other alternatives, and the possibility for higher-bandwidth channels (hundreds of bits per second and above).

The overall objective of this thesis was to show that covert channels could be established between systems separated by an air-gap without physically modifying the transmitting and receiving systems. Moreover, technical solutions and best practices were sought to detect, eliminate, or reduce the achievable data rate of these covert channels. In order to demonstrate this, the amount of information, in bits per second, that could be communicated over a covert-acoustic communication channel was measured and the *covertness* of the channels was measured by the amount of information that could be leaked through the channel before being detected. This dissertation showed that while covert channels capable of leaking sensitive information could be built without physical modification to the target systems, the covert-analyst could also detect the constructed channels under reasonable circumstances and, furthermore, that there is a trade off for the prisoners between achieving a channel capable of leaking information at a high data rate and achieving a covert channel that is more difficult to detect.

Previous researchers and certification bodies have relied on bandwidth or channel capacity to determine the security threat that covert channels pose to secure systems. The research in this dissertation showed that while these measures are useful, they do not evaluate how effective the channel is at communicating fixed amounts of data without being detected. The *steganographic capacity* metric was proposed as a solution to this problem and was used to measure and characterize OOB-CCs. *Steganographic capacity*, in the context of OOB-CCs, is *the maximum amount of data that can be communicated through a channel before a passive adversary detects the channel with some arbitrary probability.* The

metric provides a more accurate account of the amount of data that can be leaked in situations where there is a passive adversary who is attempting to detect the communication as well as when the security of *fixed source systems* is being evaluated.

The *steganographic capacity* of multiple, classical communication channels was also studied in detail. In the case where the channels between Alice and Bob as well as Alice and Wendy are memoryless channels, it was shown that in order for Alice to maximize the *steganographic capacity* of the channel she must maximize the Shannon channel capacity with her intended receiver, Bob, while minimizing Wendy's ability to measure a difference between the probability distribution of symbols when Alice is transmitting and when she is not. Furthermore, the steganographic capacity of memoryless channels corrupted by additive white Gaussian noise was also evaluated and it was shown that the most important parameter for Alice to control in order to maximize *steganographic capacity* is her transmit power, $P_t$. Additionally, a closed-form expression for the *steganographic capacity* of OOB-CCs was also derived when Wendy employs an energy detector to uncover Alice and Bob's covert communication over a band-limited channel. Lastly, it was demonstrated that Alice can increase the amount of data that she can undetectably communicate by sending transmissions in short bursts and at the lowest tolerable SNR that allows Bob to demodulate her signal.

To complement the theoretical work done in **Chapter 6**, the ability for malware to leak sensitive information from a high-security system to low-security systems using near- and ultrasonic acoustic signals was also studied in a lab environment. To properly engineer this covert communication channel using commodity hardware, the acoustic channel was first measured and categorized. In summary, the background noise that was present in the acoustic channel can be categorized as *pink noise*, there is significant multipath delay spread when acoustic signals are transmitted in the audible range, and, lastly, the frequency responses of the systems tested were non-ideal. Given these channel properties, two multichannel modulation schemes were evaluated for their performance, namely, OFDM and FHSS. The analysis of these two schemes led to the conclusion that OFDM was the modulation scheme better able to leak information at higher data rates.

Various modulation parameters were also tested, including the number of samples per symbol, the duration of the guard interval, the supported ultrasonic carrier frequencies, the transmitter volume, and the number of preamble symbols required for synchronization. The result of these experiments showed that a sufficient guard interval is required between successive symbols to prevent ISI, that commodity hardware can communicate using ultrasonic signals, in general, and that the transmitter can limit its transmission power and still communicate. Given these results, an OFDM solution was built that is capable of using both the near- and ultrasonic bandwidths to communicate hundreds of bits per second with a low BER as well as over a hundred bits per second using ultrasonic signals. Lastly, it was demonstrated that errors occur uniformly at random in the acoustic channel when single-carrier modulation is used for communication, and that the BER is dependent on sub-channel when multi-carrier OFDM is used.

The achievable data rate and BER of the covert-acoustic channel was also studied in two real-world environments: a closed-door office and an open-concept office. The study

showed that data can be communicated using ultrasonic communication at data rates up to 140 bps with BERs below 10 %. Furthermore, it was demonstrated that malware can leak information when nobody is around to hear it, using an attack called the **overnight attack**, at data rates up to 6.7 kpbs with a BER below 15 %. Additionally, the ultrasonic attack that was demonstrated is not affected by ambient conversations taking place at the same time as the covert-acoustic communication, nor is it negatively affected when a clock radio is also playing. Lastly, data can be covertly communicated using ultrasonic signals across distances up to 11 m and bit rates up to 230 bps with a BER of 2 %. Given these achievable data rates, the channels presented in this work are able to leak captured keystrokes in real-time using the ultrasonic attack and both buffered keystrokes and recorded audio using the **overnight attack**.

Two practical defensive techniques were also explored in **Chapter 8**: the detection of covert-acoustic signals using an energy detector, and the disruption of covert-acoustic signals using various jamming techniques. The *covertness* of covert-acoustic channels was measured by calculating the *steganographic capacity* of the channel when a passive covert-analyst, Wendy, attempted to detect the communication. It was shown that the *steganographic capacity* of the channel in the lab environment is significantly less than the theoretical results calculated in **Chapter 6**; however, it was also demonstrated that hundreds of bits could be communicated without being detected using FHSS modulation with random delays between symbols under certain circumstances. This outcome demonstrates that when placed appropriately in a secure environment, the steganographic capacity of the covert-acoustic channel, currently, can be greatly reduced, though perhaps not eliminated, by an acoustic energy detector tuned to the correct bandwidth. Active jamming techniques were also evaluated and it was demonstrated that while certain jamming techniques are effective against specific modulation schemes, finding a single jamming technique that can render all the modulation schemes that were tested ineffective is most likely not feasible without the use of jamming equipment that outputs a sufficient amount of wideband noise, i.e., barrage jamming with sufficient power. Lastly, additional protection mechanisms, over and above active jamming and passive monitoring, were also recommended.

## 9.1 Contributions

### Chapter 3

As a result of the literature review in **Chapter 3**, the following contributions were made to the covert channel literature:

1. the different classes of covert channels were defined in the context of access control and a novel class, *air-gap covert channels*, was documented;
2. recommendations on how to design *secure undetectable covert channels* were presented;

3. secure systems were separated into the classes of *continuous source* and *fixed source* systems based on their security requirements;

4. the proper criterion that should be used to evaluate the risk posed by covert channels to *fixed source* systems was recommended and a new metric, *steganographic capacity*, was shown to be more appropriate for measuring covert channels in *fixed source* systems; and

5. novel extensions to the traditional covert channel taxonomy were proposed (e.g., channel cover model, channel attacker model, modulation type, modulation mode, covert exploit, and reference monitor).

**Chapter 5**

As a result of the survey of covert channel techniques and related disciplines in **Chapter 5**, the following contributions were made to the covert channel literature:

1. the class of covert channels, *out-of-band covert channels* (OOB-CCs), was defined[1] and characterized;

2. it was demonstrated that OOB-CCs, to date, have relied on "security through obscurity" and it was proposed that a more standard passive and active adversarial model be adopted to evaluate all OOB-CCs going forward;

3. a comprehensive survey of the techniques that could be used to build OOB-CCs was presented and the data rates as well as the *covertness* of each medium used for communication was discussed. This particular survey is useful for:

   (a) secure system developers who build systems that require protection against OOB-CCs, and

   (b) covert channel designers who build communication systems using existing commodity hardware and must avoid detection by a third-party;

4. the first taxonomy of OOB-CCS based on their physical channel as well as their modulator and demodulator hardware requirements was presented.

**Chapter 6**

As a result of the mathematical analysis of the *steganographic capacity* of OOB-CCs in **Chapter 6**, the following contributions were made to the covert channel literature:

1. using information theory and statistical hypothesis testing the *steganographic capacity* of OOB-CCs built on memoryless channels was derived;

[1] OOB-CCs were initially defined in **Chapter 4**, but were described fully in **Chapter 5**.

2. relatedly, the *steganographic capacity* when both channels are also corrupted by additive white Gaussian noise was also derived;

3. the *steganographic capacity* of OOB-CCs under the constraint that the channel between the communicating parties is also band-limited, in addition to being subject additive white Gaussian noise, was also derived when the passive detector uses an optimal energy detector to attempt to reveal the covert communication; and

4. it was shown that by transmitting symbols with random inter-symbol delays the *steganographic capacity* of OOB-CCs can be increased.

**Chapter 7**

As a result of the mathematical analysis and experimental work done in **Chapter 7**, the following contributions were made to the covert channel literature:

1. properties of the acoustic channel were measured and it was demonstrated mathematically that the OFDM modulation scheme performs better than FHSS, from the perspective of achievable data rate, for covert-acoustic communication;

2. in general, unmodified commodity systems are capable of the following:

   (a) bidirectional communication in the near-ultrasonic, i.e., above 18 kHz, and ultrasonic, i.e., above 20 kHz, frequency ranges,

   (b) communication at data rates above 200 bps in the near-ultrasonic range and above 100 bps in the ultrasonic range; and,

   (c) on average, able to communicate acoustic signals at -30 dB transmit power;

3. certain systems, e.g., the Windows systems tested, are capable of transmitting and receiving ultrasonic signals as high as 23 kHz.

The latter part of **Chapter 7** was dedicated to testing the limits of the covert-acoustic channel in real-world environments under real-world conditions. The results obtained in **Section 7.4** of **Chapter 7** contribute the following to the covert channel literature:

1. the concept of the **overnight attack** was introduced and it was demonstrated that, given the achievable data rate and BER, the threat of the overnight attack challenges the traditional threat model that is based on the assumption that covert audio communication is strictly low-bandwidth [89, 90];

2. covert ultrasonic audio communication is a capable channel for leaking sensitive data, including captured keystrokes in real-time, from air-gapped systems in real-world environments (e.g., open-concept office, closed-door office) under real-world settings (e.g., people conversing and a radio playing nearby); and

3. ultrasonic communication can be used to leak data from compromised systems over distances up to 11 m at data rates up to 230 bps.

**Chapter 8**

As a result of the work in **Chapter 8**, the following contributions were made to the covert channel literature:

1. an acoustic energy detector was demonstrated to be able detect covert-acoustic signals;
2. through the use of an energy detector the steganographic capacity can be limited to zero bits if the covert signals are observed with adequate SNR;
3. by using spread-spectrum modulation, e.g., FHSS, and inserting random delays between transmitting symbols, the steganographic capacity of the acoustic channel can be increased for a given SNR at the detector; and,
4. various jamming techniques can be used to disrupt covert-acoustic communication; however, in order to effectively disrupt covert communication in the acoustic channel the jamming noise power must be greater than the covert signal's power at the demodulator.

## 9.2 Future Work

This dissertation has laid the groundwork to allow air-gap covert channels to be more formally characterized and measured going forward. Moreover, a systematic approach was followed to measure the data rate and covertness of out-of-band covert-acoustic channels. Combining the methodology outlined in **Chapter 7** and **Chapter 8** to evaluate these metrics, with the survey of OOB-CCs in **Chapter 5**, there are a number of OOB-CCs that should be studied in a similar fashion, e.g., covert-light, covert-seismic, and covert-magnetic. Understanding the limitations of these covert channels would better allow secure systems developers and secure facility designers to protect sensitive information.

The covert-acoustic channels engineered and analyzed in this dissertation used a guard interval in between transmitted symbols in order to avoid inter-symbol interference. While this allowed for certain data types to be effectively communicated, the data rates reported in this work can be improved by removing the guard interval and transmitting data on each symbol interval. The trade-off is a more complex receiver. Taking the acoustic channel as an example, without a guard interval the receiver would have to deal with the multipath delay spread of the channel by using a more sophisticated device, such as a RAKE receiver. Similarly, more bandwidth efficient modulation schemes exist that have improved performance over non-coherent FSK. The trade-off, again, is that the receiver is more complex. And, while a more bandwidth efficient scheme could be adopted to improve the data rate results reported in this dissertation, it remains to be seen if they can practically be realized on commodity hardware.

This dissertation also studied the steganographic capacity of OOB-CCs by modelling the channels as memoryless channels corrupted by additive white Gaussian noise. Moreover, the steganographic capacity of OOB-CCs was also determined when the channel was band-limited and the passive adversary used an energy detector to detect the covert communication. There are a number of additional common channel models that exist in digital communications. As an example, acoustic channels as well as RF channels follow a fading model, where the receiver receives multiple copies of the transmitted signal and, therefore, steganographic capacity analysis of these types of channels would move the analysis of OOB-CCs forward.

# APPENDICES

# Appendix A

# Maximum Percentage Error for Approximating $\chi^2_\eta$

Table A.1: Maximum Percentage Error for Approximating $\chi^2_\eta$

| $\eta$ | CDF Error | PDF Error | $\eta$ | CDF Error | PDF Error | $\eta$ | CDF Error | PDF Error | $\eta$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 25.1874 | 523.3595 | 31 | 0.4040 | 1.5144 | 61 | 0.1980 | 0.6613 | 91 | 0.1305 | 0.4141 |
| 2 | 12.6579 | 117.3043 | 32 | 0.3906 | 1.4549 | 62 | 0.1946 | 0.6487 | 92 | 0.1290 | 0.4089 |
| 3 | 8.1040 | 52.3972 | 33 | 0.3781 | 1.3997 | 63 | 0.1914 | 0.6365 | 93 | 0.1276 | 0.4039 |
| 4 | 5.2470 | 30.9063 | 34 | 0.3663 | 1.3482 | 64 | 0.1883 | 0.6247 | 94 | 0.1262 | 0.3989 |
| 5 | 3.6439 | 21.0051 | 35 | 0.3552 | 1.3002 | 65 | 0.1853 | 0.6134 | 95 | 0.1248 | 0.3941 |
| 6 | 2.6818 | 15.5312 | 36 | 0.3448 | 1.2553 | 66 | 0.1823 | 0.6024 | 96 | 0.1234 | 0.3894 |
| 7 | 2.0630 | 12.1374 | 37 | 0.3349 | 1.2133 | 67 | 0.1795 | 0.5918 | 97 | 0.1221 | 0.3848 |
| 8 | 1.7697 | 9.8615 | 38 | 0.3256 | 1.1738 | 68 | 0.1767 | 0.5816 | 98 | 0.1208 | 0.3803 |
| 9 | 1.5489 | 8.2459 | 39 | 0.3168 | 1.1367 | 69 | 0.1741 | 0.5717 | 99 | 0.1196 | 0.3759 |
| 10 | 1.3757 | 7.0485 | 40 | 0.3085 | 1.1017 | 70 | 0.1715 | 0.5621 | 100 | 0.1183 | 0.3716 |
| 11 | 1.2364 | 6.1306 | 41 | 0.3005 | 1.0687 | 71 | 0.1689 | 0.5528 | 101 | 0.1171 | 0.3673 |
| 12 | 1.1220 | 5.4076 | 42 | 0.2930 | 1.0376 | 72 | 0.1665 | 0.5438 | 102 | 0.1159 | 0.3632 |
| 13 | 1.0273 | 4.8254 | 43 | 0.2858 | 1.0081 | 73 | 0.1641 | 0.5351 | 103 | 0.1147 | 0.3592 |
| 14 | 0.9479 | 4.3478 | 44 | 0.2790 | 0.9801 | 74 | 0.1618 | 0.5266 | 104 | 0.1136 | 0.3552 |
| 15 | 0.8796 | 3.9498 | 45 | 0.2724 | 0.9536 | 75 | 0.1596 | 0.5184 | 105 | 0.1125 | 0.3514 |
| 16 | 0.8203 | 3.6137 | 46 | 0.2662 | 0.9284 | 76 | 0.1574 | 0.5105 | 106 | 0.1114 | 0.3476 |
| 17 | 0.7684 | 3.3265 | 47 | 0.2603 | 0.9045 | 77 | 0.1552 | 0.5027 | 107 | 0.1103 | 0.3439 |
| 18 | 0.7225 | 3.0786 | 48 | 0.2546 | 0.8817 | 78 | 0.1532 | 0.4952 | 108 | 0.1092 | 0.3402 |
| 19 | 0.6816 | 2.8627 | 49 | 0.2491 | 0.8599 | 79 | 0.1512 | 0.4879 | 109 | 0.1082 | 0.3367 |
| 20 | 0.6451 | 2.6732 | 50 | 0.2439 | 0.8392 | 80 | 0.1492 | 0.4808 | 110 | 0.1072 | 0.3332 |
| 21 | 0.6122 | 2.5056 | 51 | 0.2388 | 0.8194 | 81 | 0.1473 | 0.4739 | 111 | 0.1062 | 0.3298 |
| 22 | 0.5824 | 2.3564 | 52 | 0.2340 | 0.8004 | 82 | 0.1454 | 0.4672 | 112 | 0.1052 | 0.3264 |
| 23 | 0.5553 | 2.2229 | 53 | 0.2294 | 0.7823 | 83 | 0.1436 | 0.4607 | 113 | 0.1042 | 0.3231 |
| 24 | 0.5306 | 2.1029 | 54 | 0.2249 | 0.7649 | 84 | 0.1418 | 0.4543 | 114 | 0.1033 | 0.3199 |
| 25 | 0.5080 | 1.9943 | 55 | 0.2207 | 0.7483 | 85 | 0.1401 | 0.4481 | 115 | 0.1024 | 0.3168 |
| 26 | 0.4872 | 1.8957 | 56 | 0.2165 | 0.7323 | 86 | 0.1384 | 0.4421 | 116 | 0.1015 | 0.3137 |
| 27 | 0.4680 | 1.8059 | 57 | 0.2125 | 0.7170 | 87 | 0.1367 | 0.4362 | 117 | 0.1006 | 0.3106 |
| 28 | 0.4502 | 1.7237 | 58 | 0.2087 | 0.7023 | 88 | 0.1351 | 0.4305 | 118 | 0.0997 | 0.3076 |
| 29 | 0.4337 | 1.6482 | 59 | 0.2050 | 0.6881 | 89 | 0.1335 | 0.4249 | 119 | 0.0988 | 0.3047 |
| 30 | 0.4183 | 1.5786 | 60 | 0.2014 | 0.6745 | 90 | 0.1320 | 0.4194 | 120 | 0.0980 | 0.3018 |

# Appendix B

# Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$

Table B.1: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 1 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 100.0000 | 94.2213 | 97.3212 | 6 | 100.0000 | 93.1346 | 96.7033 | 11 | 100.0000 | 92.0026 | 96.0353 |
| 1 | 10.0000 | 99.2046 | 99.7782 | 6 | 10.0000 | 88.6517 | 93.9426 | 11 | 10.0000 | 76.4481 | 84.8629 |
| 1 | 1.0000 | 78.3771 | 68.3157 | 6 | 1.0000 | 31.0153 | 32.9481 | 11 | 1.0000 | 18.6967 | 21.1360 |
| 1 | 0.1000 | 25.5817 | 511.0392 | 6 | 0.1000 | 2.6408 | 15.4569 | 11 | 0.1000 | 1.2374 | 6.1145 |
| 1 | 0.0100 | 25.1923 | 523.2128 | 6 | 0.0100 | 2.6813 | 15.5304 | 11 | 0.0100 | 1.2364 | 6.1304 |
| 1 | 0.0010 | 25.1875 | 523.3580 | 6 | 0.0010 | 2.6818 | 15.5312 | 11 | 0.0010 | 1.2364 | 6.1306 |
| 2 | 100.0000 | 94.0082 | 97.2019 | 7 | 100.0000 | 92.9114 | 96.5735 | 12 | 100.0000 | 91.7718 | 95.8962 |
| 2 | 10.0000 | 97.7897 | 99.2042 | 7 | 10.0000 | 86.1080 | 92.2029 | 12 | 10.0000 | 74.2398 | 83.0446 |
| 2 | 1.0000 | 61.2329 | 55.8455 | 7 | 1.0000 | 27.4404 | 29.6951 | 12 | 1.0000 | 17.3065 | 19.6998 |
| 2 | 0.1000 | 12.1960 | 115.8592 | 7 | 0.1000 | 2.0647 | 12.0872 | 12 | 0.1000 | 1.1228 | 5.3947 |
| 2 | 0.0100 | 12.6528 | 117.2885 | 7 | 0.0100 | 2.0627 | 12.1369 | 12 | 0.0100 | 1.1220 | 5.4075 |
| 2 | 0.0010 | 12.6578 | 117.3042 | 7 | 0.0010 | 2.0630 | 12.1374 | 12 | 0.0010 | 1.1220 | 5.4076 |
| 3 | 100.0000 | 93.7928 | 97.0805 | 8 | 100.0000 | 92.6865 | 96.4418 | 13 | 100.0000 | 91.5397 | 95.7554 |
| 3 | 10.0000 | 95.8666 | 98.2708 | 8 | 10.0000 | 83.5916 | 90.3959 | 13 | 10.0000 | 72.1243 | 81.2588 |
| 3 | 1.0000 | 49.8694 | 47.3644 | 8 | 1.0000 | 24.5855 | 26.9921 | 13 | 1.0000 | 16.1062 | 18.4436 |
| 3 | 0.1000 | 7.8995 | 51.9406 | 8 | 0.1000 | 1.7727 | 9.8257 | 13 | 0.1000 | 1.0284 | 4.8149 |
| 3 | 0.0100 | 8.1018 | 52.3923 | 8 | 0.0100 | 1.7697 | 9.8612 | 13 | 0.0100 | 1.0273 | 4.8253 |
| 3 | 0.0010 | 8.1039 | 52.3972 | 8 | 0.0010 | 1.7697 | 9.8615 | 13 | 0.0010 | 1.0273 | 4.8254 |
| 4 | 100.0000 | 93.5754 | 96.9568 | 9 | 100.0000 | 92.4601 | 96.3081 | 14 | 100.0000 | 91.3064 | 95.6129 |
| 4 | 10.0000 | 93.6155 | 97.0364 | 9 | 10.0000 | 81.1320 | 88.5546 | 14 | 10.0000 | 70.1012 | 79.5123 |
| 4 | 1.0000 | 41.6559 | 41.6461 | 9 | 1.0000 | 22.2575 | 24.7214 | 14 | 1.0000 | 15.0599 | 17.3360 |
| 4 | 0.1000 | 5.1399 | 30.6948 | 9 | 0.1000 | 1.5510 | 8.2193 | 14 | 0.1000 | 0.9487 | 4.3391 |
| 4 | 0.0100 | 5.2459 | 30.9041 | 9 | 0.0100 | 1.5490 | 8.2456 | 14 | 0.0100 | 0.9479 | 4.3477 |
| 4 | 0.0010 | 5.2470 | 30.9063 | 9 | 0.0010 | 1.5489 | 8.2459 | 14 | 0.0010 | 0.9479 | 4.3478 |
| 5 | 100.0000 | 93.3559 | 96.8311 | 10 | 100.0000 | 92.2321 | 96.1726 | 15 | 100.0000 | 91.0720 | 95.4689 |
| 5 | 10.0000 | 91.1770 | 95.5719 | 10 | 10.0000 | 78.7473 | 86.7041 | 15 | 10.0000 | 68.1684 | 77.8098 |
| 5 | 1.0000 | 35.6029 | 36.8921 | 10 | 1.0000 | 20.3251 | 22.7924 | 15 | 1.0000 | 14.1397 | 16.3526 |
| 5 | 0.1000 | 3.5804 | 20.8866 | 10 | 0.1000 | 1.3772 | 7.0281 | 15 | 0.1000 | 0.8803 | 3.9425 |
| 5 | 0.0100 | 3.6432 | 21.0038 | 10 | 0.0100 | 1.3757 | 7.0483 | 15 | 0.0100 | 0.8796 | 3.9498 |
| 5 | 0.0010 | 3.6439 | 21.0050 | 10 | 0.0010 | 1.3757 | 7.0485 | 15 | 0.0010 | 0.8796 | 3.9498 |

Table B.2: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 2 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 100.0000 | 90.8365 | 95.3232 | 21 | 100.0000 | 89.6460 | 94.5730 | 26 | 100.0000 | 88.4392 | 93.7904 |
| 16 | 10.0000 | 66.3230 | 76.1542 | 21 | 10.0000 | 58.2783 | 68.6088 | 26 | 10.0000 | 51.8563 | 62.2239 |
| 16 | 1.0000 | 13.3244 | 15.4737 | 21 | 1.0000 | 10.3347 | 12.1897 | 26 | 1.0000 | 8.4342 | 10.0511 |
| 16 | 0.1000 | 0.8209 | 3.6075 | 21 | 0.1000 | 0.6124 | 2.5024 | 26 | 0.1000 | 0.4873 | 1.8939 |
| 16 | 0.0100 | 0.8203 | 3.6136 | 21 | 0.0100 | 0.6122 | 2.5055 | 26 | 0.0100 | 0.4872 | 1.8957 |
| 16 | 0.0010 | 0.8203 | 3.6137 | 21 | 0.0010 | 0.6122 | 2.5056 | 26 | 0.0010 | 0.4872 | 1.8957 |
| 17 | 100.0000 | 90.6001 | 95.1760 | 22 | 100.0000 | 89.4056 | 94.4189 | 27 | 100.0000 | 88.1966 | 93.6304 |
| 17 | 10.0000 | 64.5617 | 74.5471 | 22 | 10.0000 | 56.8785 | 67.2436 | 27 | 10.0000 | 50.7292 | 61.0716 |
| 17 | 1.0000 | 12.5972 | 14.6837 | 22 | 1.0000 | 9.8897 | 11.6925 | 27 | 1.0000 | 8.1344 | 9.7100 |
| 17 | 0.1000 | 0.7688 | 3.3212 | 22 | 0.1000 | 0.5826 | 2.3536 | 27 | 0.1000 | 0.4681 | 1.8042 |
| 17 | 0.0100 | 0.7684 | 3.3265 | 22 | 0.0100 | 0.5824 | 2.3564 | 27 | 0.0100 | 0.4680 | 1.8059 |
| 17 | 0.0010 | 0.7684 | 3.3265 | 22 | 0.0010 | 0.5824 | 2.3564 | 27 | 0.0010 | 0.4680 | 1.8059 |
| 18 | 100.0000 | 90.3628 | 95.0274 | 23 | 100.0000 | 89.1648 | 94.2635 | 28 | 100.0000 | 87.9536 | 93.4694 |
| 18 | 10.0000 | 62.8804 | 72.9892 | 23 | 10.0000 | 55.5397 | 65.9240 | 28 | 10.0000 | 49.6478 | 59.9573 |
| 18 | 1.0000 | 11.9444 | 13.9698 | 23 | 1.0000 | 9.4810 | 11.2341 | 28 | 1.0000 | 7.8550 | 9.3912 |
| 18 | 0.1000 | 0.7228 | 3.0740 | 23 | 0.1000 | 0.5555 | 2.2205 | 28 | 0.1000 | 0.4503 | 1.7221 |
| 18 | 0.0100 | 0.7225 | 3.0786 | 23 | 0.0100 | 0.5553 | 2.2229 | 28 | 0.0100 | 0.4502 | 1.7236 |
| 18 | 0.0010 | 0.7225 | 3.0786 | 23 | 0.0010 | 0.5553 | 2.2229 | 28 | 0.0010 | 0.4502 | 1.7237 |
| 19 | 100.0000 | 90.1246 | 94.8773 | 24 | 100.0000 | 88.9234 | 94.1070 | 29 | 100.0000 | 87.7104 | 93.3074 |
| 19 | 10.0000 | 61.2754 | 71.4805 | 24 | 10.0000 | 54.2586 | 64.6485 | 29 | 10.0000 | 48.6096 | 58.8796 |
| 19 | 1.0000 | 11.3554 | 13.3217 | 24 | 1.0000 | 9.1046 | 10.8101 | 29 | 1.0000 | 7.5941 | 9.0927 |
| 19 | 0.1000 | 0.6819 | 2.8587 | 24 | 0.1000 | 0.5308 | 2.1006 | 29 | 0.1000 | 0.4338 | 1.6468 |
| 19 | 0.0100 | 0.6816 | 2.8627 | 24 | 0.0100 | 0.5306 | 2.1028 | 29 | 0.0100 | 0.4337 | 1.6482 |
| 19 | 0.0010 | 0.6816 | 2.8627 | 24 | 0.0010 | 0.5306 | 2.1029 | 29 | 0.0010 | 0.4337 | 1.6482 |
| 20 | 100.0000 | 89.8856 | 94.7258 | 25 | 100.0000 | 88.6815 | 93.9492 | 30 | 100.0000 | 87.4670 | 93.1444 |
| 20 | 10.0000 | 59.7426 | 70.0207 | 25 | 10.0000 | 53.0318 | 63.4156 | 30 | 10.0000 | 47.6122 | 57.8369 |
| 20 | 1.0000 | 10.8213 | 12.7307 | 25 | 1.0000 | 8.7567 | 10.4168 | 30 | 1.0000 | 7.3498 | 8.8124 |
| 20 | 0.1000 | 0.6453 | 2.6696 | 25 | 0.1000 | 0.5081 | 1.9923 | 30 | 0.1000 | 0.4184 | 1.5774 |
| 20 | 0.0100 | 0.6451 | 2.6731 | 25 | 0.0100 | 0.5080 | 1.9943 | 30 | 0.0100 | 0.4183 | 1.5786 |
| 20 | 0.0010 | 0.6451 | 2.6731 | 25 | 0.0010 | 0.5080 | 1.9943 | 30 | 0.0010 | 0.4183 | 1.5786 |

Table B.3: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 3 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 31 | 100.0000 | 87.2234 | 92.9805 | 36 | 100.0000 | 86.0045 | 92.1482 | 41 | 100.0000 | 84.7876 | 91.2980 |
| 31 | 10.0000 | 46.6534 | 56.8278 | 36 | 10.0000 | 42.3699 | 52.2401 | 41 | 10.0000 | 38.7899 | 48.3071 |
| 31 | 1.0000 | 7.1206 | 8.5489 | 36 | 1.0000 | 6.1591 | 7.4364 | 41 | 1.0000 | 5.4252 | 6.5795 |
| 31 | 0.1000 | 0.4041 | 1.5132 | 36 | 0.1000 | 0.3448 | 1.2545 | 41 | 0.1000 | 0.3006 | 1.0682 |
| 31 | 0.0100 | 0.4040 | 1.5144 | 36 | 0.0100 | 0.3448 | 1.2553 | 41 | 0.0100 | 0.3005 | 1.0687 |
| 31 | 0.0010 | 0.4040 | 1.5144 | 36 | 0.0010 | 0.3448 | 1.2553 | 41 | 0.0010 | 0.3005 | 1.0687 |
| 32 | 100.0000 | 86.9797 | 92.8157 | 37 | 100.0000 | 85.7608 | 91.9795 | 42 | 100.0000 | 84.5449 | 91.1262 |
| 32 | 10.0000 | 45.7311 | 55.8510 | 37 | 10.0000 | 41.6034 | 51.4054 | 42 | 10.0000 | 38.1438 | 47.5879 |
| 32 | 1.0000 | 6.9052 | 8.3006 | 37 | 1.0000 | 5.9970 | 7.2477 | 42 | 1.0000 | 5.2987 | 6.4312 |
| 32 | 0.1000 | 0.3907 | 1.4538 | 37 | 0.1000 | 0.3350 | 1.2125 | 42 | 0.1000 | 0.2930 | 1.0370 |
| 32 | 0.0100 | 0.3906 | 1.4549 | 37 | 0.0100 | 0.3349 | 1.2133 | 42 | 0.0100 | 0.2930 | 1.0376 |
| 32 | 0.0010 | 0.3906 | 1.4549 | 37 | 0.0010 | 0.3349 | 1.2133 | 42 | 0.0010 | 0.2930 | 1.0376 |
| 33 | 100.0000 | 86.7359 | 92.6500 | 38 | 100.0000 | 85.5173 | 91.8101 | 43 | 100.0000 | 84.3024 | 90.9538 |
| 33 | 10.0000 | 44.8434 | 54.9050 | 38 | 10.0000 | 40.8634 | 50.5958 | 43 | 10.0000 | 37.5184 | 46.8889 |
| 33 | 1.0000 | 6.7024 | 8.0663 | 38 | 1.0000 | 5.8431 | 7.0682 | 43 | 1.0000 | 5.1780 | 6.2895 |
| 33 | 0.1000 | 0.3781 | 1.3987 | 38 | 0.1000 | 0.3257 | 1.1731 | 43 | 0.1000 | 0.2858 | 1.0076 |
| 33 | 0.0100 | 0.3781 | 1.3996 | 38 | 0.0100 | 0.3256 | 1.1738 | 43 | 0.0100 | 0.2858 | 1.0081 |
| 33 | 0.0010 | 0.3781 | 1.3997 | 38 | 0.0010 | 0.3256 | 1.1738 | 43 | 0.0010 | 0.2858 | 1.0081 |
| 34 | 100.0000 | 86.4921 | 92.4835 | 39 | 100.0000 | 85.2739 | 91.6400 | 44 | 100.0000 | 84.0602 | 90.7809 |
| 34 | 10.0000 | 43.9884 | 53.9887 | 39 | 10.0000 | 40.1486 | 49.8102 | 44 | 10.0000 | 36.9128 | 46.2095 |
| 34 | 1.0000 | 6.5110 | 7.8449 | 39 | 1.0000 | 5.6969 | 6.8975 | 44 | 1.0000 | 5.0627 | 6.1538 |
| 34 | 0.1000 | 0.3664 | 1.3473 | 39 | 0.1000 | 0.3168 | 1.1360 | 44 | 0.1000 | 0.2790 | 0.9797 |
| 34 | 0.0100 | 0.3663 | 1.3482 | 39 | 0.0100 | 0.3168 | 1.1367 | 44 | 0.0100 | 0.2790 | 0.9801 |
| 34 | 0.0010 | 0.3663 | 1.3482 | 39 | 0.0010 | 0.3168 | 1.1367 | 44 | 0.0010 | 0.2790 | 0.9801 |
| 35 | 100.0000 | 86.2483 | 92.3162 | 40 | 100.0000 | 85.0306 | 91.4693 | 45 | 100.0000 | 83.8184 | 90.6075 |
| 35 | 10.0000 | 43.1644 | 53.1008 | 40 | 10.0000 | 39.4578 | 49.0476 | 45 | 10.0000 | 36.3261 | 45.5489 |
| 35 | 1.0000 | 6.3302 | 7.6352 | 40 | 1.0000 | 5.5577 | 6.7347 | 45 | 1.0000 | 4.9523 | 6.0239 |
| 35 | 0.1000 | 0.3553 | 1.2993 | 40 | 0.1000 | 0.3085 | 1.1011 | 45 | 0.1000 | 0.2725 | 0.9532 |
| 35 | 0.0100 | 0.3552 | 1.3002 | 40 | 0.0100 | 0.3085 | 1.1017 | 45 | 0.0100 | 0.2724 | 0.9536 |
| 35 | 0.0010 | 0.3552 | 1.3002 | 40 | 0.0010 | 0.3085 | 1.1017 | 45 | 0.0010 | 0.2724 | 0.9536 |

Table B.4: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 4 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 46 | 100.0000 | 83.5769 | 90.4337 | 51 | 100.0000 | 82.3757 | 89.5588 | 56 | 100.0000 | 81.1871 | 88.6766 |
| 46 | 10.0000 | 35.7574 | 44.9063 | 51 | 10.0000 | 33.1579 | 41.9407 | 56 | 10.0000 | 30.9061 | 39.3346 |
| 46 | 1.0000 | 4.8467 | 5.8993 | 51 | 1.0000 | 4.3791 | 5.3463 | 56 | 1.0000 | 3.9933 | 4.8879 |
| 46 | 0.1000 | 0.2662 | 0.9280 | 51 | 0.1000 | 0.2389 | 0.8190 | 56 | 0.1000 | 0.2165 | 0.7321 |
| 46 | 0.0100 | 0.2662 | 0.9284 | 51 | 0.0100 | 0.2388 | 0.8194 | 56 | 0.0100 | 0.2165 | 0.7323 |
| 46 | 0.0010 | 0.2662 | 0.9284 | 51 | 0.0010 | 0.2388 | 0.8194 | 56 | 0.0010 | 0.2165 | 0.7323 |
| 47 | 100.0000 | 83.3358 | 90.2595 | 52 | 100.0000 | 82.1369 | 89.3828 | 57 | 100.0000 | 80.9511 | 88.4995 |
| 47 | 10.0000 | 35.2059 | 44.2810 | 52 | 10.0000 | 32.6820 | 41.3929 | 57 | 10.0000 | 30.4915 | 38.8510 |
| 47 | 1.0000 | 4.7454 | 5.7797 | 52 | 1.0000 | 4.2961 | 5.2479 | 57 | 1.0000 | 3.9242 | 4.8055 |
| 47 | 0.1000 | 0.2603 | 0.9041 | 52 | 0.1000 | 0.2340 | 0.8001 | 57 | 0.1000 | 0.2126 | 0.7167 |
| 47 | 0.0100 | 0.2603 | 0.9045 | 52 | 0.0100 | 0.2340 | 0.8004 | 57 | 0.0100 | 0.2125 | 0.7170 |
| 47 | 0.0010 | 0.2603 | 0.9045 | 52 | 0.0010 | 0.2340 | 0.8004 | 57 | 0.0010 | 0.2125 | 0.7170 |
| 48 | 100.0000 | 83.0951 | 90.0848 | 53 | 100.0000 | 81.8986 | 89.2066 | 58 | 100.0000 | 80.7156 | 88.3222 |
| 48 | 10.0000 | 34.6709 | 43.6725 | 53 | 10.0000 | 32.2194 | 40.8588 | 58 | 10.0000 | 30.0877 | 38.3789 |
| 48 | 1.0000 | 4.6482 | 5.6649 | 53 | 1.0000 | 4.2162 | 5.1530 | 58 | 1.0000 | 3.8573 | 4.7258 |
| 48 | 0.1000 | 0.2546 | 0.8813 | 53 | 0.1000 | 0.2294 | 0.7820 | 58 | 0.1000 | 0.2087 | 0.7020 |
| 48 | 0.0100 | 0.2546 | 0.8817 | 53 | 0.0100 | 0.2294 | 0.7823 | 58 | 0.0100 | 0.2087 | 0.7023 |
| 48 | 0.0010 | 0.2546 | 0.8817 | 53 | 0.0010 | 0.2294 | 0.7823 | 58 | 0.0010 | 0.2087 | 0.7023 |
| 49 | 100.0000 | 82.8548 | 89.9098 | 54 | 100.0000 | 81.6609 | 89.0302 | 59 | 100.0000 | 80.4808 | 88.1448 |
| 49 | 10.0000 | 34.1517 | 43.0800 | 54 | 10.0000 | 31.7696 | 40.3381 | 59 | 10.0000 | 29.6944 | 37.9179 |
| 49 | 1.0000 | 4.5549 | 5.5546 | 54 | 1.0000 | 4.1392 | 5.0615 | 59 | 1.0000 | 3.7927 | 4.6487 |
| 49 | 0.1000 | 0.2491 | 0.8596 | 54 | 0.1000 | 0.2250 | 0.7646 | 59 | 0.1000 | 0.2050 | 0.6879 |
| 49 | 0.0100 | 0.2491 | 0.8599 | 54 | 0.0100 | 0.2249 | 0.7649 | 59 | 0.0100 | 0.2050 | 0.6881 |
| 49 | 0.0010 | 0.2491 | 0.8599 | 54 | 0.0010 | 0.2249 | 0.7649 | 59 | 0.0010 | 0.2050 | 0.6881 |
| 50 | 100.0000 | 82.6151 | 89.7345 | 55 | 100.0000 | 81.4237 | 88.8535 | 60 | 100.0000 | 80.2467 | 87.9673 |
| 50 | 10.0000 | 33.6476 | 42.5029 | 55 | 10.0000 | 31.3320 | 39.8301 | 60 | 10.0000 | 29.3111 | 37.4677 |
| 50 | 1.0000 | 4.4653 | 5.4484 | 55 | 1.0000 | 4.0650 | 4.9732 | 60 | 1.0000 | 3.7302 | 4.5741 |
| 50 | 0.1000 | 0.2439 | 0.8388 | 55 | 0.1000 | 0.2207 | 0.7480 | 60 | 0.1000 | 0.2014 | 0.6742 |
| 50 | 0.0100 | 0.2439 | 0.8392 | 55 | 0.0100 | 0.2207 | 0.7483 | 60 | 0.0100 | 0.2014 | 0.6745 |
| 50 | 0.0010 | 0.2439 | 0.8392 | 55 | 0.0010 | 0.2207 | 0.7483 | 60 | 0.0010 | 0.2014 | 0.6745 |

Table B.5: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 5 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 61 | 100.0000 | 80.0131 | 87.7895 | 66 | 100.0000 | 78.8557 | 86.9003 | 71 | 100.0000 | 77.7163 | 86.0110 |
| 61 | 10.0000 | 28.9375 | 37.0278 | 66 | 10.0000 | 27.2023 | 34.9727 | 71 | 10.0000 | 25.6616 | 33.1309 |
| 61 | 1.0000 | 3.6698 | 4.5018 | 66 | 1.0000 | 3.3945 | 4.1721 | 71 | 1.0000 | 3.1574 | 3.8873 |
| 61 | 0.1000 | 0.1980 | 0.6611 | 66 | 0.1000 | 0.1823 | 0.6023 | 71 | 0.1000 | 0.1689 | 0.5527 |
| 61 | 0.0100 | 0.1980 | 0.6613 | 66 | 0.0100 | 0.1823 | 0.6024 | 71 | 0.0100 | 0.1689 | 0.5528 |
| 61 | 0.0010 | 0.1980 | 0.6613 | 66 | 0.0010 | 0.1823 | 0.6024 | 71 | 0.0010 | 0.1689 | 0.5528 |
| 62 | 100.0000 | 79.7803 | 87.6118 | 67 | 100.0000 | 78.6264 | 86.7224 | 72 | 100.0000 | 77.4908 | 85.8335 |
| 62 | 10.0000 | 28.5731 | 36.5980 | 67 | 10.0000 | 26.8796 | 34.5883 | 72 | 10.0000 | 25.3740 | 32.7853 |
| 62 | 1.0000 | 3.6112 | 4.4318 | 67 | 1.0000 | 3.3443 | 4.1119 | 72 | 1.0000 | 3.1139 | 3.8350 |
| 62 | 0.1000 | 0.1946 | 0.6485 | 67 | 0.1000 | 0.1795 | 0.5917 | 72 | 0.1000 | 0.1665 | 0.5437 |
| 62 | 0.0100 | 0.1946 | 0.6487 | 67 | 0.0100 | 0.1795 | 0.5918 | 72 | 0.0100 | 0.1665 | 0.5438 |
| 62 | 0.0010 | 0.1946 | 0.6487 | 67 | 0.0010 | 0.1795 | 0.5918 | 72 | 0.0010 | 0.1665 | 0.5438 |
| 63 | 100.0000 | 79.5481 | 87.4340 | 68 | 100.0000 | 78.3977 | 86.5445 | 73 | 100.0000 | 77.2659 | 85.6558 |
| 63 | 10.0000 | 28.2178 | 36.1779 | 68 | 10.0000 | 26.5645 | 34.2122 | 73 | 10.0000 | 25.0927 | 32.4467 |
| 63 | 1.0000 | 3.5545 | 4.3639 | 68 | 1.0000 | 3.2955 | 4.0534 | 73 | 1.0000 | 3.0716 | 3.7840 |
| 63 | 0.1000 | 0.1914 | 0.6363 | 68 | 0.1000 | 0.1767 | 0.5814 | 73 | 0.1000 | 0.1641 | 0.5349 |
| 63 | 0.0100 | 0.1914 | 0.6365 | 68 | 0.0100 | 0.1767 | 0.5816 | 73 | 0.0100 | 0.1641 | 0.5351 |
| 63 | 0.0010 | 0.1914 | 0.6365 | 68 | 0.0010 | 0.1767 | 0.5816 | 73 | 0.0010 | 0.1641 | 0.5351 |
| 64 | 100.0000 | 79.3166 | 87.2561 | 69 | 100.0000 | 78.1698 | 86.3667 | 74 | 100.0000 | 77.0419 | 85.4783 |
| 64 | 10.0000 | 27.8710 | 35.7672 | 69 | 10.0000 | 26.2566 | 33.8441 | 74 | 10.0000 | 24.8176 | 32.1150 |
| 64 | 1.0000 | 3.4995 | 4.2980 | 69 | 1.0000 | 3.2482 | 3.9965 | 74 | 1.0000 | 3.0303 | 3.7344 |
| 64 | 0.1000 | 0.1883 | 0.6246 | 69 | 0.1000 | 0.1741 | 0.5715 | 74 | 0.1000 | 0.1618 | 0.5265 |
| 64 | 0.0100 | 0.1883 | 0.6247 | 69 | 0.0100 | 0.1741 | 0.5717 | 74 | 0.0100 | 0.1618 | 0.5266 |
| 64 | 0.0010 | 0.1883 | 0.6247 | 69 | 0.0010 | 0.1741 | 0.5717 | 74 | 0.0010 | 0.1618 | 0.5266 |
| 65 | 100.0000 | 79.0858 | 87.0783 | 70 | 100.0000 | 77.9427 | 86.1888 | 75 | 100.0000 | 76.8186 | 85.3009 |
| 65 | 10.0000 | 27.5326 | 35.3655 | 70 | 10.0000 | 25.9557 | 33.4837 | 75 | 10.0000 | 24.5483 | 31.7899 |
| 65 | 1.0000 | 3.4462 | 4.2341 | 70 | 1.0000 | 3.2021 | 3.9412 | 75 | 1.0000 | 2.9902 | 3.6860 |
| 65 | 0.1000 | 0.1853 | 0.6132 | 70 | 0.1000 | 0.1715 | 0.5619 | 75 | 0.1000 | 0.1596 | 0.5183 |
| 65 | 0.0100 | 0.1853 | 0.6134 | 70 | 0.0100 | 0.1715 | 0.5621 | 75 | 0.0100 | 0.1596 | 0.5184 |
| 65 | 0.0010 | 0.1853 | 0.6134 | 70 | 0.0010 | 0.1715 | 0.5621 | 75 | 0.0010 | 0.1596 | 0.5184 |

Table B.6: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 6 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 76 | 100.0000 | 76.5961 | 85.1236 | 81 | 100.0000 | 75.4958 | 84.2395 | 86 | 100.0000 | 74.4159 | 83.3602 |
| 76 | 10.0000 | 24.2848 | 31.4712 | 81 | 10.0000 | 23.0471 | 29.9682 | 86 | 10.0000 | 21.9286 | 28.6010 |
| 76 | 1.0000 | 2.9511 | 3.6389 | 81 | 1.0000 | 2.7701 | 3.4203 | 86 | 1.0000 | 2.6098 | 3.2264 |
| 76 | 0.1000 | 0.1574 | 0.5103 | 81 | 0.1000 | 0.1473 | 0.4738 | 86 | 0.1000 | 0.1384 | 0.4420 |
| 76 | 0.0100 | 0.1574 | 0.5105 | 81 | 0.0100 | 0.1473 | 0.4739 | 86 | 0.0100 | 0.1384 | 0.4421 |
| 76 | 0.0010 | 0.1574 | 0.5105 | 81 | 0.0010 | 0.1473 | 0.4739 | 86 | 0.0010 | 0.1384 | 0.4421 |
| 77 | 100.0000 | 76.3744 | 84.9465 | 82 | 100.0000 | 75.2781 | 84.0632 | 87 | 100.0000 | 74.2025 | 83.1850 |
| 77 | 10.0000 | 24.0268 | 31.1588 | 82 | 10.0000 | 22.8144 | 29.6845 | 87 | 10.0000 | 21.7177 | 28.3422 |
| 77 | 1.0000 | 2.9131 | 3.5930 | 82 | 1.0000 | 2.7365 | 3.3796 | 87 | 1.0000 | 2.5800 | 3.1902 |
| 77 | 0.1000 | 0.1552 | 0.5026 | 82 | 0.1000 | 0.1454 | 0.4671 | 87 | 0.1000 | 0.1367 | 0.4361 |
| 77 | 0.0100 | 0.1552 | 0.5027 | 82 | 0.0100 | 0.1454 | 0.4672 | 87 | 0.0100 | 0.1367 | 0.4362 |
| 77 | 0.0010 | 0.1552 | 0.5027 | 82 | 0.0010 | 0.1454 | 0.4672 | 87 | 0.0010 | 0.1367 | 0.4362 |
| 78 | 100.0000 | 76.1535 | 84.7695 | 83 | 100.0000 | 75.0613 | 83.8871 | 88 | 100.0000 | 73.9899 | 83.0100 |
| 78 | 10.0000 | 23.7742 | 30.8525 | 83 | 10.0000 | 22.5864 | 29.4061 | 88 | 10.0000 | 21.5108 | 28.0881 |
| 78 | 1.0000 | 2.8760 | 3.5482 | 83 | 1.0000 | 2.7037 | 3.3400 | 88 | 1.0000 | 2.5508 | 3.1548 |
| 78 | 0.1000 | 0.1532 | 0.4951 | 83 | 0.1000 | 0.1436 | 0.4606 | 88 | 0.1000 | 0.1351 | 0.4304 |
| 78 | 0.0100 | 0.1532 | 0.4952 | 83 | 0.0100 | 0.1436 | 0.4607 | 88 | 0.0100 | 0.1351 | 0.4305 |
| 78 | 0.0010 | 0.1532 | 0.4952 | 83 | 0.0010 | 0.1436 | 0.4607 | 88 | 0.0010 | 0.1351 | 0.4305 |
| 79 | 100.0000 | 75.9335 | 84.5927 | 84 | 100.0000 | 74.8454 | 83.7113 | 89 | 100.0000 | 73.7781 | 82.8354 |
| 79 | 10.0000 | 23.5268 | 30.5520 | 84 | 10.0000 | 22.3628 | 29.1328 | 89 | 10.0000 | 21.3078 | 27.8384 |
| 79 | 1.0000 | 2.8398 | 3.5045 | 84 | 1.0000 | 2.6717 | 3.3012 | 89 | 1.0000 | 2.5223 | 3.1202 |
| 79 | 0.1000 | 0.1512 | 0.4878 | 84 | 0.1000 | 0.1418 | 0.4542 | 89 | 0.1000 | 0.1335 | 0.4248 |
| 79 | 0.0100 | 0.1512 | 0.4879 | 84 | 0.0100 | 0.1418 | 0.4543 | 89 | 0.0100 | 0.1335 | 0.4249 |
| 79 | 0.0010 | 0.1512 | 0.4879 | 84 | 0.0010 | 0.1418 | 0.4543 | 89 | 0.0010 | 0.1335 | 0.4249 |
| 80 | 100.0000 | 75.7142 | 84.4160 | 85 | 100.0000 | 74.6302 | 83.5356 | 90 | 100.0000 | 73.5671 | 82.6609 |
| 80 | 10.0000 | 23.2845 | 30.2573 | 85 | 10.0000 | 22.1436 | 28.8644 | 90 | 10.0000 | 21.1086 | 27.5931 |
| 80 | 1.0000 | 2.8045 | 3.4619 | 85 | 1.0000 | 2.6404 | 3.2634 | 90 | 1.0000 | 2.4944 | 3.0864 |
| 80 | 0.1000 | 0.1492 | 0.4807 | 85 | 0.1000 | 0.1401 | 0.4480 | 90 | 0.1000 | 0.1320 | 0.4194 |
| 80 | 0.0100 | 0.1492 | 0.4808 | 85 | 0.0100 | 0.1401 | 0.4481 | 90 | 0.0100 | 0.1320 | 0.4194 |
| 80 | 0.0010 | 0.1492 | 0.4808 | 85 | 0.0010 | 0.1401 | 0.4481 | 90 | 0.0010 | 0.1320 | 0.4194 |

Table B.7: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 7 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 91 | 100.0000 | 73.3570 | 82.4868 | 96 | 100.0000 | 72.3194 | 81.6206 | 101 | 100.0000 | 71.3030 | 80.7621 |
| 91 | 10.0000 | 20.9130 | 27.3520 | 96 | 10.0000 | 19.9867 | 26.2068 | 101 | 10.0000 | 19.1385 | 25.1530 |
| 91 | 1.0000 | 2.4671 | 3.0532 | 96 | 1.0000 | 2.3390 | 2.8977 | 101 | 1.0000 | 2.2236 | 2.7572 |
| 91 | 0.1000 | 0.1305 | 0.4141 | 96 | 0.1000 | 0.1234 | 0.3893 | 101 | 0.1000 | 0.1171 | 0.3673 |
| 91 | 0.0100 | 0.1305 | 0.4141 | 96 | 0.0100 | 0.1234 | 0.3894 | 101 | 0.0100 | 0.1171 | 0.3673 |
| 91 | 0.0010 | 0.1305 | 0.4141 | 96 | 0.0010 | 0.1234 | 0.3894 | 101 | 0.0010 | 0.1171 | 0.3673 |
| 92 | 100.0000 | 73.1478 | 82.3129 | 97 | 100.0000 | 72.1144 | 81.4482 | 102 | 100.0000 | 71.1022 | 80.5915 |
| 92 | 10.0000 | 20.7210 | 27.1151 | 97 | 10.0000 | 19.8111 | 25.9891 | 102 | 10.0000 | 18.9774 | 24.9522 |
| 92 | 1.0000 | 2.4403 | 3.0208 | 97 | 1.0000 | 2.3150 | 2.8685 | 102 | 1.0000 | 2.2018 | 2.7308 |
| 92 | 0.1000 | 0.1290 | 0.4089 | 97 | 0.1000 | 0.1221 | 0.3847 | 102 | 0.1000 | 0.1159 | 0.3632 |
| 92 | 0.0100 | 0.1290 | 0.4089 | 97 | 0.0100 | 0.1221 | 0.3848 | 102 | 0.0100 | 0.1159 | 0.3632 |
| 92 | 0.0010 | 0.1290 | 0.4089 | 97 | 0.0010 | 0.1221 | 0.3848 | 102 | 0.0010 | 0.1159 | 0.3632 |
| 93 | 100.0000 | 72.9394 | 82.1394 | 98 | 100.0000 | 71.9103 | 81.2762 | 103 | 100.0000 | 70.9023 | 80.4212 |
| 93 | 10.0000 | 20.5324 | 26.8822 | 98 | 10.0000 | 19.6386 | 25.7749 | 103 | 10.0000 | 18.8190 | 24.7546 |
| 93 | 1.0000 | 2.4142 | 2.9891 | 98 | 1.0000 | 2.2914 | 2.8399 | 103 | 1.0000 | 2.1805 | 2.7048 |
| 93 | 0.1000 | 0.1276 | 0.4038 | 98 | 0.1000 | 0.1208 | 0.3802 | 103 | 0.1000 | 0.1147 | 0.3591 |
| 93 | 0.0100 | 0.1276 | 0.4039 | 98 | 0.0100 | 0.1208 | 0.3803 | 103 | 0.0100 | 0.1147 | 0.3592 |
| 93 | 0.0010 | 0.1276 | 0.4039 | 98 | 0.0010 | 0.1208 | 0.3803 | 103 | 0.0010 | 0.1147 | 0.3592 |
| 94 | 100.0000 | 72.7319 | 81.9662 | 99 | 100.0000 | 71.7070 | 81.1045 | 104 | 100.0000 | 70.7033 | 80.2512 |
| 94 | 10.0000 | 20.3473 | 26.6533 | 99 | 10.0000 | 19.4691 | 25.5642 | 104 | 10.0000 | 18.6631 | 24.5601 |
| 94 | 1.0000 | 2.3886 | 2.9580 | 99 | 1.0000 | 2.2684 | 2.8118 | 104 | 1.0000 | 2.1596 | 2.6793 |
| 94 | 0.1000 | 0.1262 | 0.3989 | 99 | 0.1000 | 0.1196 | 0.3758 | 104 | 0.1000 | 0.1136 | 0.3552 |
| 94 | 0.0100 | 0.1262 | 0.3989 | 99 | 0.0100 | 0.1196 | 0.3759 | 104 | 0.0100 | 0.1136 | 0.3552 |
| 94 | 0.0010 | 0.1262 | 0.3989 | 99 | 0.0010 | 0.1196 | 0.3759 | 104 | 0.0010 | 0.1136 | 0.3552 |
| 95 | 100.0000 | 72.5252 | 81.7932 | 100 | 100.0000 | 71.5045 | 80.9332 | 105 | 100.0000 | 70.5051 | 80.0816 |
| 95 | 10.0000 | 20.1654 | 26.4282 | 100 | 10.0000 | 19.3024 | 25.3569 | 105 | 10.0000 | 18.5098 | 24.3686 |
| 95 | 1.0000 | 2.3636 | 2.9275 | 100 | 1.0000 | 2.2457 | 2.7842 | 105 | 1.0000 | 2.1391 | 2.6543 |
| 95 | 0.1000 | 0.1248 | 0.3940 | 100 | 0.1000 | 0.1183 | 0.3715 | 105 | 0.1000 | 0.1125 | 0.3513 |
| 95 | 0.0100 | 0.1248 | 0.3941 | 100 | 0.0100 | 0.1183 | 0.3716 | 105 | 0.0100 | 0.1125 | 0.3514 |
| 95 | 0.0010 | 0.1248 | 0.3941 | 100 | 0.0010 | 0.1183 | 0.3716 | 105 | 0.0010 | 0.1125 | 0.3514 |

Table B.8: Maximum Percentage Error for Approximating $\chi^2_{\eta,\lambda}$ (Table 8 of 8)

| $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error | $\eta$ | $\lambda$ | CDF Error | PDF Error |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 106 | 100.0000 | 70.3078 | 79.9123 | 111 | 100.0000 | 69.3338 | 79.0718 | 116 | 100.0000 | 68.3807 | 78.2410 |
| 106 | 10.0000 | 18.3590 | 24.1801 | 111 | 10.0000 | 17.6402 | 23.2792 | 116 | 10.0000 | 16.9753 | 22.4426 |
| 106 | 1.0000 | 2.1189 | 2.6297 | 111 | 1.0000 | 2.0237 | 2.5135 | 116 | 1.0000 | 1.9366 | 2.4071 |
| 106 | 0.1000 | 0.1114 | 0.3475 | 111 | 0.1000 | 0.1062 | 0.3297 | 116 | 0.1000 | 0.1015 | 0.3136 |
| 106 | 0.0100 | 0.1114 | 0.3476 | 111 | 0.0100 | 0.1062 | 0.3298 | 116 | 0.0100 | 0.1015 | 0.3137 |
| 106 | 0.0010 | 0.1114 | 0.3476 | 111 | 0.0010 | 0.1062 | 0.3298 | 116 | 0.0010 | 0.1015 | 0.3137 |
| 107 | 100.0000 | 70.1113 | 79.7435 | 112 | 100.0000 | 69.1415 | 78.9048 | 117 | 100.0000 | 68.1926 | 78.0761 |
| 107 | 10.0000 | 18.2106 | 23.9944 | 112 | 10.0000 | 17.5031 | 23.1069 | 117 | 10.0000 | 16.8482 | 22.2825 |
| 107 | 1.0000 | 2.0992 | 2.6056 | 112 | 1.0000 | 2.0056 | 2.4915 | 117 | 1.0000 | 1.9200 | 2.3869 |
| 107 | 0.1000 | 0.1103 | 0.3438 | 112 | 0.1000 | 0.1052 | 0.3264 | 117 | 0.1000 | 0.1006 | 0.3106 |
| 107 | 0.0100 | 0.1103 | 0.3439 | 112 | 0.0100 | 0.1052 | 0.3264 | 117 | 0.0100 | 0.1006 | 0.3106 |
| 107 | 0.0010 | 0.1103 | 0.3439 | 112 | 0.0010 | 0.1052 | 0.3264 | 117 | 0.0010 | 0.1006 | 0.3106 |
| 108 | 100.0000 | 69.9156 | 79.5750 | 113 | 100.0000 | 68.9500 | 78.7383 | 118 | 100.0000 | 68.0053 | 77.9115 |
| 108 | 10.0000 | 18.0646 | 23.8115 | 113 | 10.0000 | 17.3681 | 22.9372 | 118 | 10.0000 | 16.7231 | 22.1245 |
| 108 | 1.0000 | 2.0798 | 2.5820 | 113 | 1.0000 | 1.9879 | 2.4698 | 118 | 1.0000 | 1.9038 | 2.3670 |
| 108 | 0.1000 | 0.1092 | 0.3402 | 113 | 0.1000 | 0.1042 | 0.3231 | 118 | 0.1000 | 0.0997 | 0.3076 |
| 108 | 0.0100 | 0.1092 | 0.3402 | 113 | 0.0100 | 0.1042 | 0.3231 | 118 | 0.0100 | 0.0997 | 0.3076 |
| 108 | 0.0010 | 0.1092 | 0.3402 | 113 | 0.0010 | 0.1042 | 0.3231 | 118 | 0.0010 | 0.0997 | 0.3076 |
| 109 | 100.0000 | 69.7208 | 79.4069 | 114 | 100.0000 | 68.7594 | 78.5721 | 119 | 100.0000 | 67.8189 | 77.7476 |
| 109 | 10.0000 | 17.9209 | 23.6314 | 114 | 10.0000 | 17.2352 | 22.7700 | 119 | 10.0000 | 16.5997 | 21.9688 |
| 109 | 1.0000 | 2.0607 | 2.5587 | 114 | 1.0000 | 1.9705 | 2.4486 | 119 | 1.0000 | 1.8878 | 2.3474 |
| 109 | 0.1000 | 0.1082 | 0.3366 | 114 | 0.1000 | 0.1033 | 0.3199 | 119 | 0.1000 | 0.0988 | 0.3047 |
| 109 | 0.0100 | 0.1082 | 0.3367 | 114 | 0.0100 | 0.1033 | 0.3199 | 119 | 0.0100 | 0.0988 | 0.3047 |
| 109 | 0.0010 | 0.1082 | 0.3367 | 114 | 0.0010 | 0.1033 | 0.3199 | 119 | 0.0010 | 0.0988 | 0.3047 |
| 110 | 100.0000 | 69.5269 | 79.2391 | 115 | 100.0000 | 68.5696 | 78.4064 | 120 | 100.0000 | 67.6333 | 77.5839 |
| 110 | 10.0000 | 17.7795 | 23.4540 | 115 | 10.0000 | 17.1042 | 22.6051 | 120 | 10.0000 | 16.4782 | 21.8153 |
| 110 | 1.0000 | 2.0420 | 2.5359 | 115 | 1.0000 | 1.9534 | 2.4276 | 120 | 1.0000 | 1.8721 | 2.3282 |
| 110 | 0.1000 | 0.1072 | 0.3332 | 115 | 0.1000 | 0.1024 | 0.3167 | 120 | 0.1000 | 0.0980 | 0.3018 |
| 110 | 0.0100 | 0.1072 | 0.3332 | 115 | 0.0100 | 0.1024 | 0.3168 | 120 | 0.0100 | 0.0980 | 0.3018 |
| 110 | 0.0010 | 0.1072 | 0.3332 | 115 | 0.0010 | 0.1024 | 0.3168 | 120 | 0.0010 | 0.0980 | 0.3018 |

# Appendix C

# Algorithm for Calculating Maximum Percentage Error

## C.1 Algorithm to Calculate $\chi^2_\eta$ Error

**Algorithm 1** Calculating max percentage error for $\chi^2_\eta$

▷ *For each degree of freedom, $\eta$, output the largest CDF and PDF estimation error.*
**for** $dofRange \leftarrow 1, dofMax$ **do**
  $\eta \leftarrow 2^{dofRange}$
  $\delta_{max,CDF} \leftarrow 0$
  $\delta_{max,PDF} \leftarrow 0$
  **for** $p \leftarrow 1, 100$ **do**
    $pValue \leftarrow p/100$
    $x_{true} \leftarrow \Phi^{-1}(pValue; \eta)$
    $x_{adjusted} \leftarrow \frac{\left(\frac{x_{true}}{\eta}\right)^{\frac{1}{3}} - \left[1 - \frac{2}{9\eta}\right]}{\sqrt{\frac{2}{9\eta}}}$
    $pValue_{estimated} = \Psi(x_{adjusted})$
    $CDF_{error} = 100 * \frac{|pValue_{estimated} - pValue|}{pValue}$
    **if** $CDF_{error} > \delta_{max,CDF}$ **then**
      $\delta_{max,CDF} \leftarrow CDF_{error}$
    **end if**
    $g_1 \leftarrow \eta^{\frac{1}{3}}$
    $g_2 \leftarrow \sqrt{\frac{2}{9\eta}}$
    $A \leftarrow \frac{1}{g_1 g_3}$
    $PDF_{true} = \phi(x_{true}; \eta)$
    $PDF_{estimated} = \frac{A x_{adjusted}^{-\frac{2}{3}}}{3} \psi(x_{adjusted})$
    $PDF_{error} = 100 * \frac{|PDF_{estimated} - PDF_{true}|}{PDF_{true}}$
    **if** $PDF_{error} > \delta_{max,PDF}$ **then**
      $\delta_{max,PDF} \leftarrow PDF_{error}$

**end if**
**end for**
**output** $\delta_{max,CDF}, \delta_{max,PDF}$
**end for**

## C.2 Algorithm to Calculate $\chi^2_{\eta,\lambda}$ Error

**Algorithm 2** Calculating max percentage error for $\chi^2_{\eta,\lambda}$

▷ *For each degree of freedom, $\eta$, and non-centrality, $\lambda$, output the largest CDF and PDF estimation error.*
**for** $dofRange \leftarrow 1, dofMax$ **do**
  $\eta \leftarrow 2^{dofRange}$
  **for** $lambdaRange \leftarrow 1, lambdaMax$ **do**
    $\lambda = 10^{-lambdaRange}$
    $\delta_{max,CDF} \leftarrow 0$
    $\delta_{max,PDF} \leftarrow 0$
    **for** $p \leftarrow 1, 100$ **do**
      $pValue \leftarrow p/100$
      $x_{true} \leftarrow \Omega^{-1}(pValue; \eta, \lambda)$
      $x_{adjusted} \leftarrow \frac{\left(\frac{x_{true}}{a}\right)^{\frac{1}{3}} - \left[1 - \frac{2}{9}\left(\frac{1+b}{a}\right)\right]}{\sqrt{\frac{2}{9}\left(\frac{1+b}{a}\right)}}$
      $pValue_{estimated} = \Psi(x_{adjusted})$
      $CDF_{error} = 100 * \frac{|pValue_{estimated} - pValue|}{pValue}$
      **if** $CDF_{error} > \delta_{max,CDF}$ **then**
        $\delta_{max,CDF} \leftarrow CDF_{error}$
      **end if**
      $a \leftarrow \eta + \lambda$
      $b \leftarrow \frac{\lambda}{a}$
      $h_1 \leftarrow a^{\frac{1}{3}}$
      $h_3 \leftarrow \sqrt{\frac{2}{9\eta}\frac{1+b}{a}}$
      $C \leftarrow \frac{1}{g_1 g_3}$
      $PDF_{true} = \omega(x_{true}; \eta)$
      $PDF_{estimated} = \frac{C x_{adjusted}^{-\frac{2}{3}}}{3} \psi(x_{adjusted})$
      $PDF_{error} = 100 * \frac{|PDF_{estimated} - PDF_{true}|}{PDF_{true}}$
      **if** $PDF_{error} > \delta_{max,PDF}$ **then**
        $\delta_{max,PDF} \leftarrow PDF_{error}$
      **end if**
    **end for**
    **output** $\delta_{max,CDF}, \delta_{max,PDF}$
  **end for**
**end for**

# Appendix D

# Detailed Results for Chapter 7

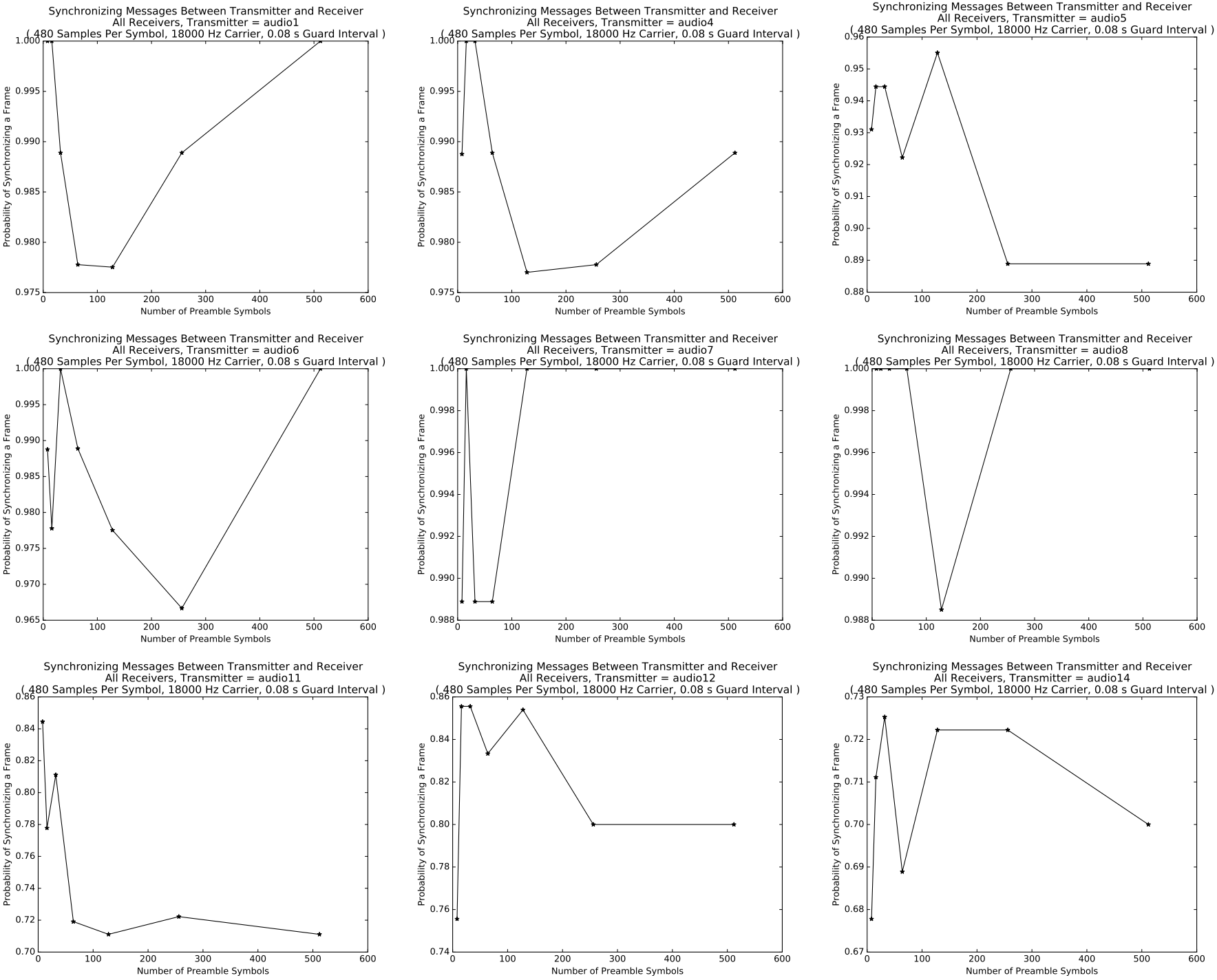



Figure D.1: Probability of Synchronization versus Number of Preamble Bytes for Each Device as Transmitter

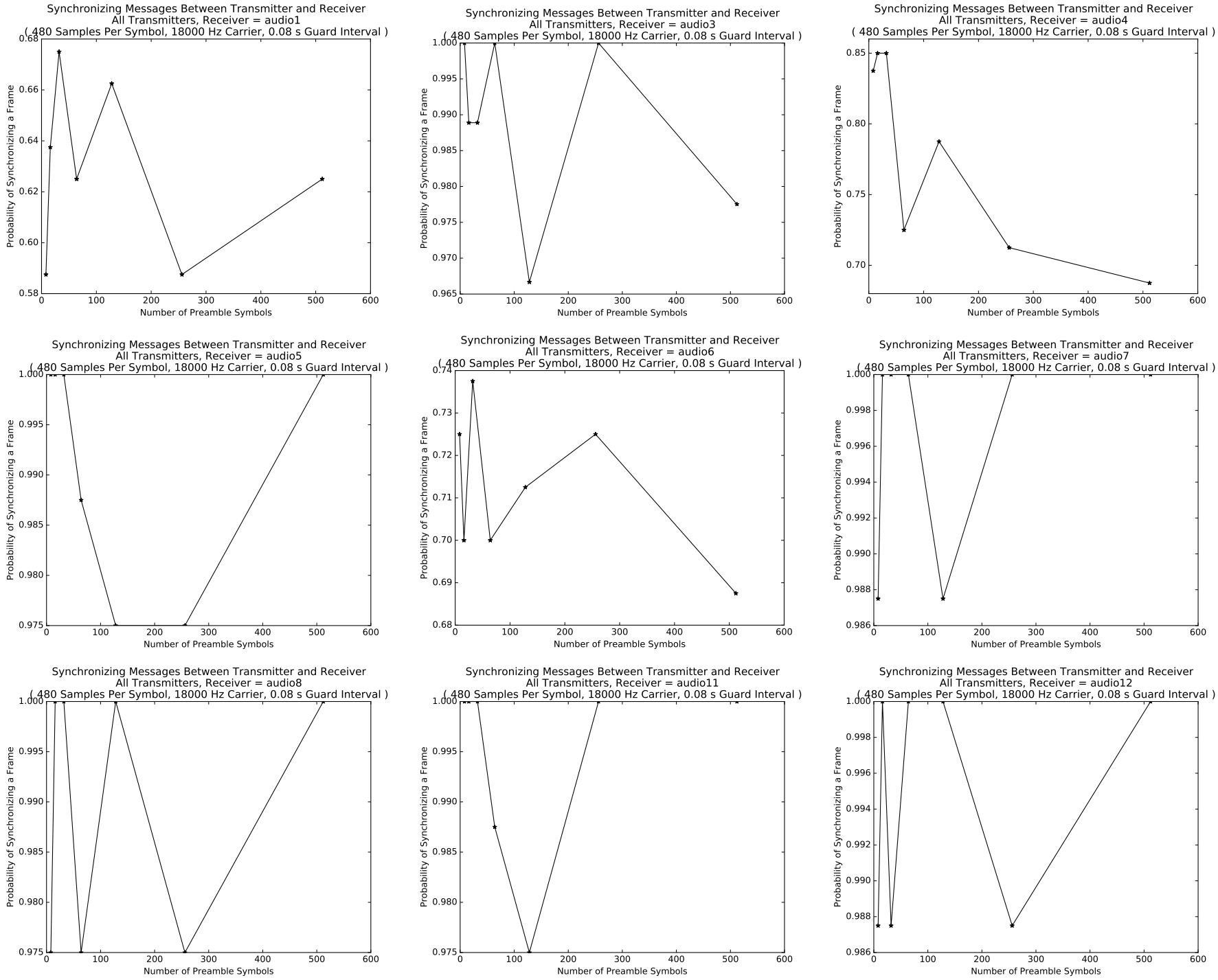



Figure D.2: Probability of Synchronization versus Number of Preamble Bytes for Each Device as Receiver (Part 1)

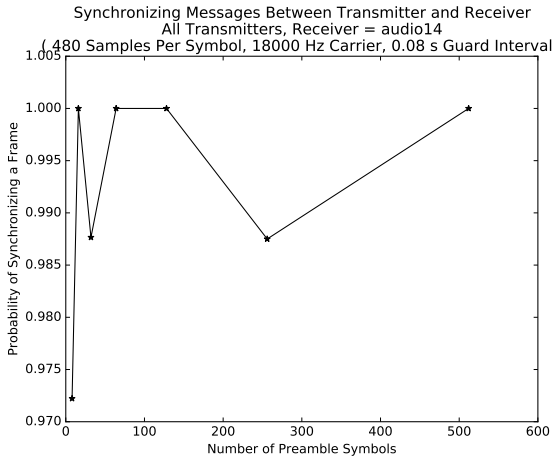



Figure D.3: Probability of Synchronization versus Number of Preamble Bytes for Each Device as Receiver (Part 2)

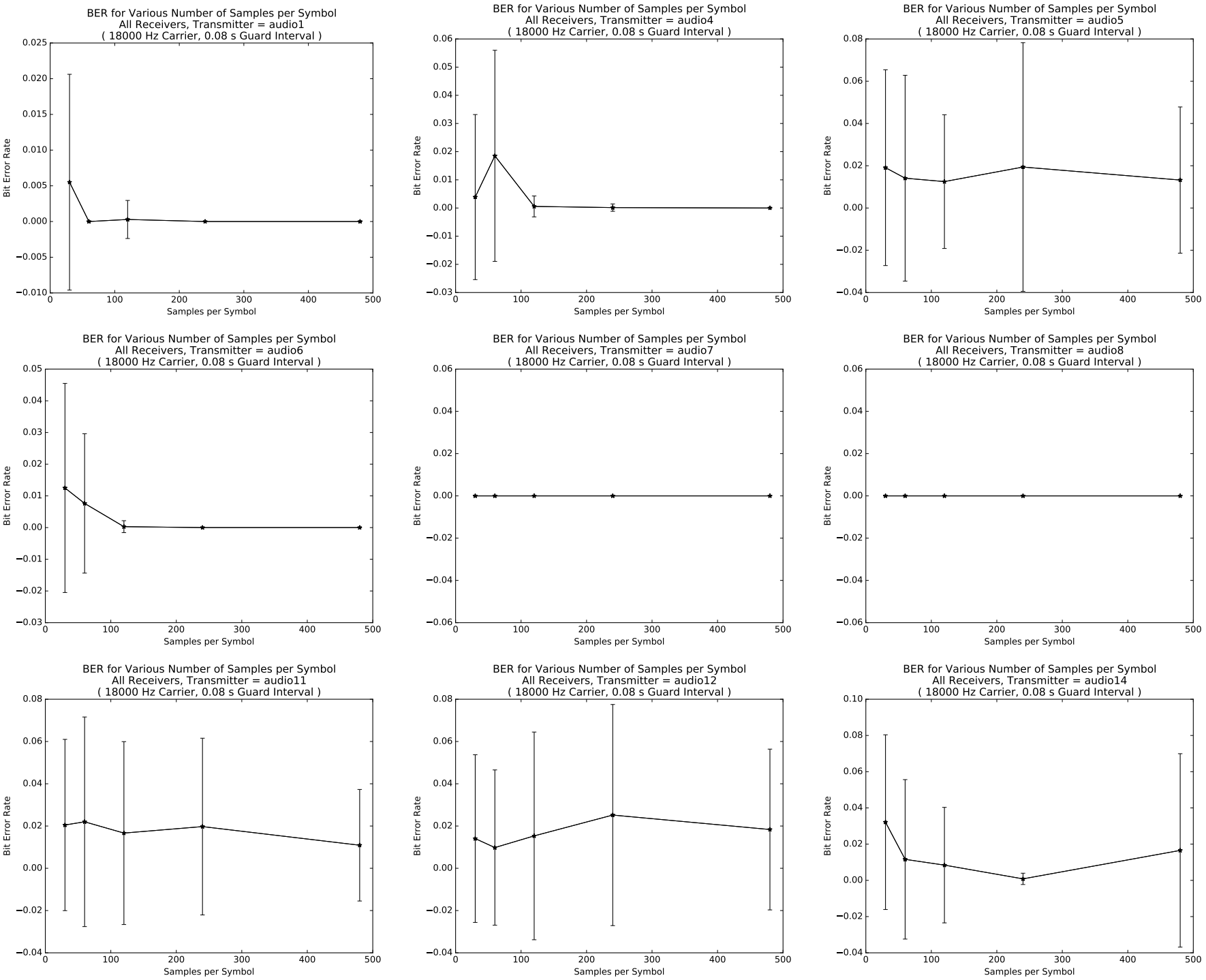



Figure D.4: Bit Error Rate versus Transmitted Samples per Symbol for Each Device as Transmitter

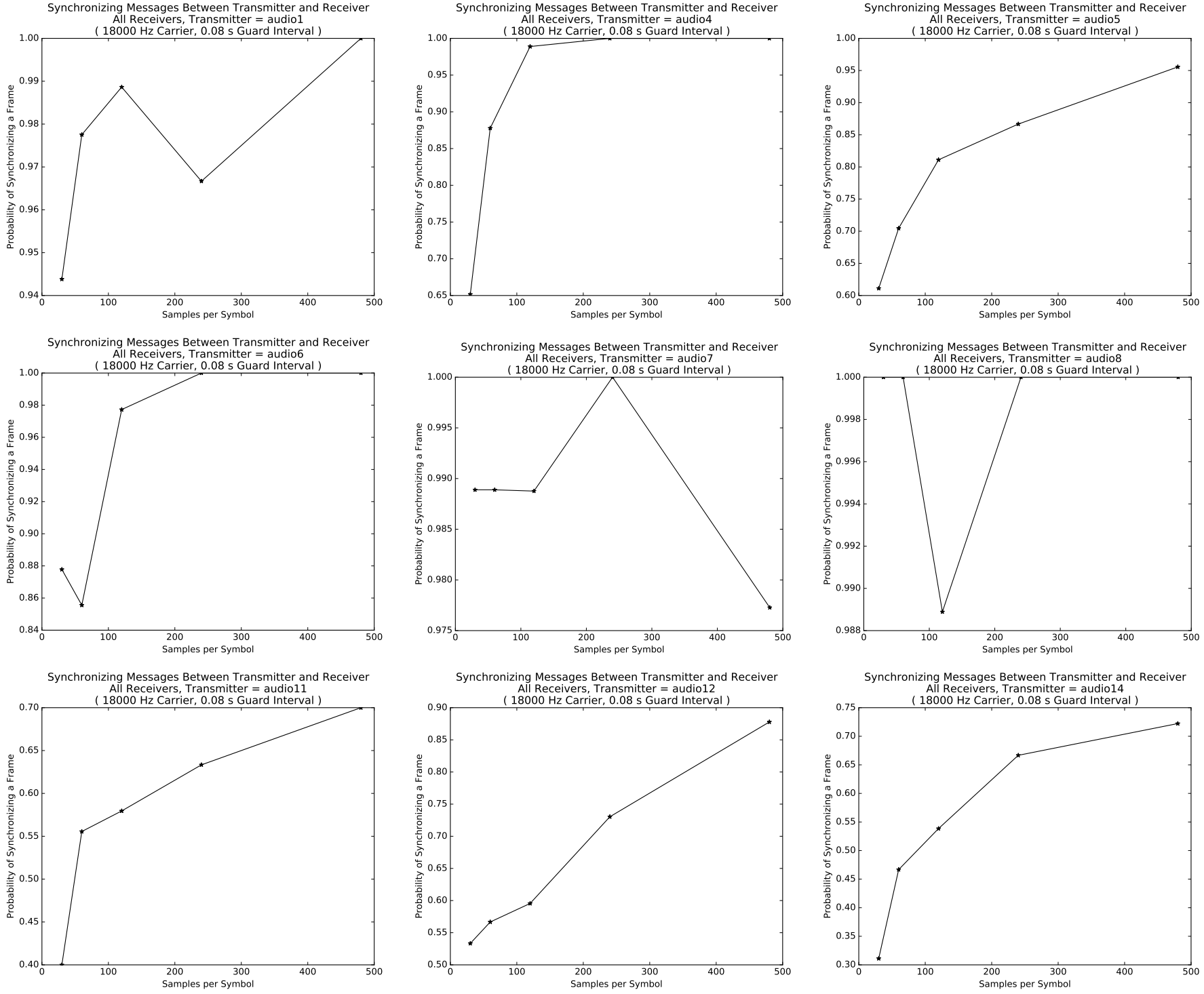



Figure D.5: Probability of Synchronization versus Transmitted Samples per Symbol for Each Device as Transmitter

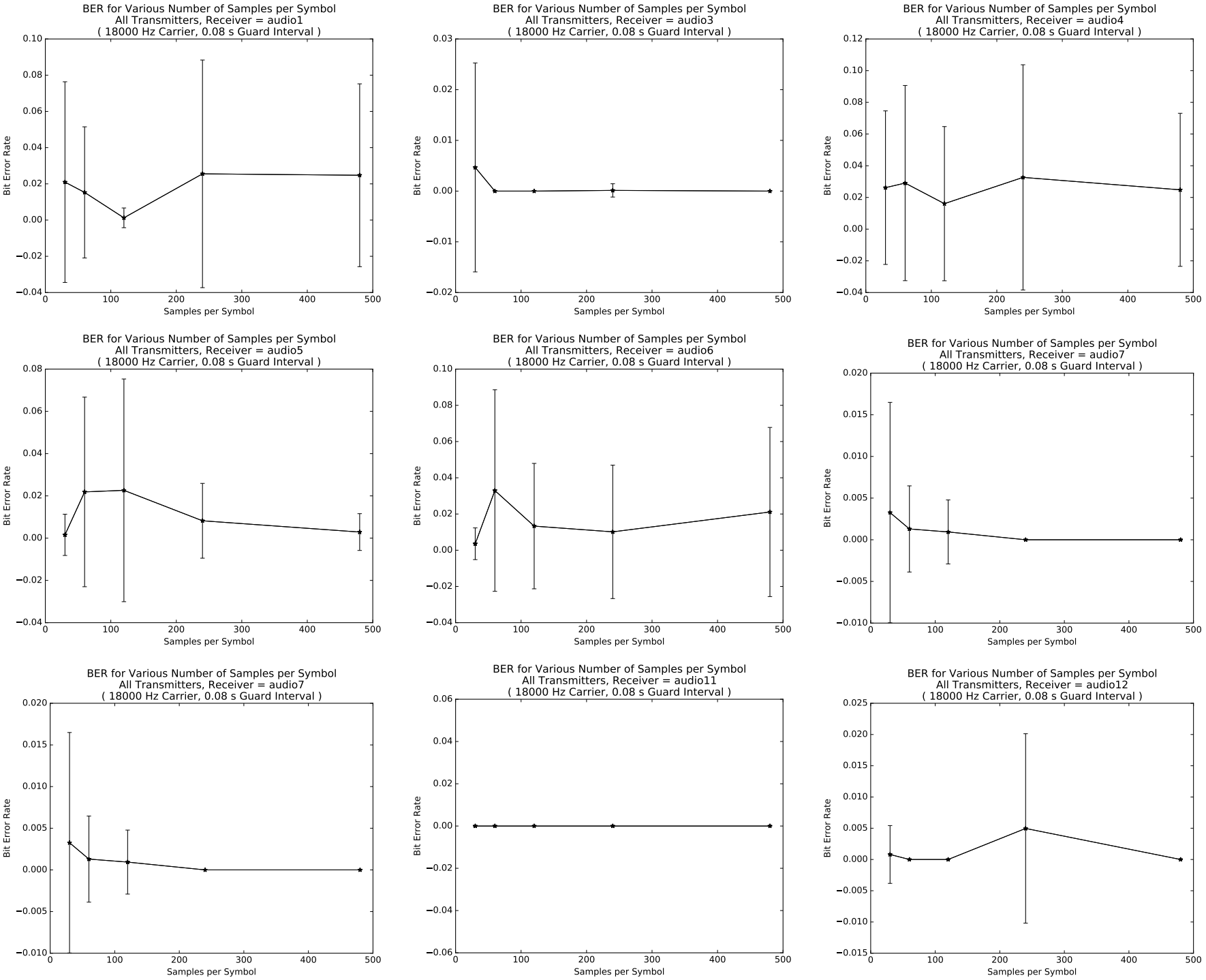



Figure D.6: Bit Error Rate versus Transmitted Samples per Symbol for Each Device as Receiver (Part 1)

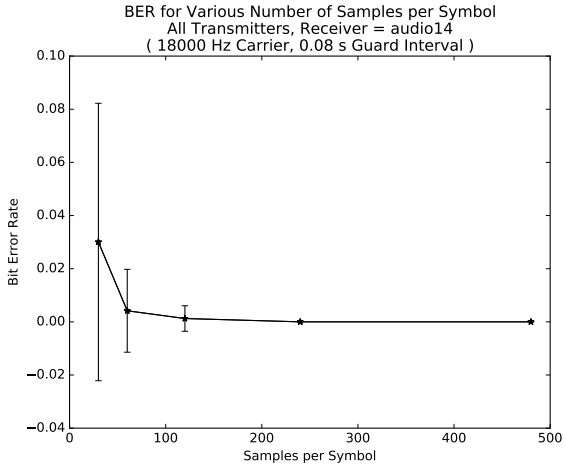



Figure D.7: Bit Error Rate versus Transmitted Samples per Symbol for Each Device as Receiver (Part 2)

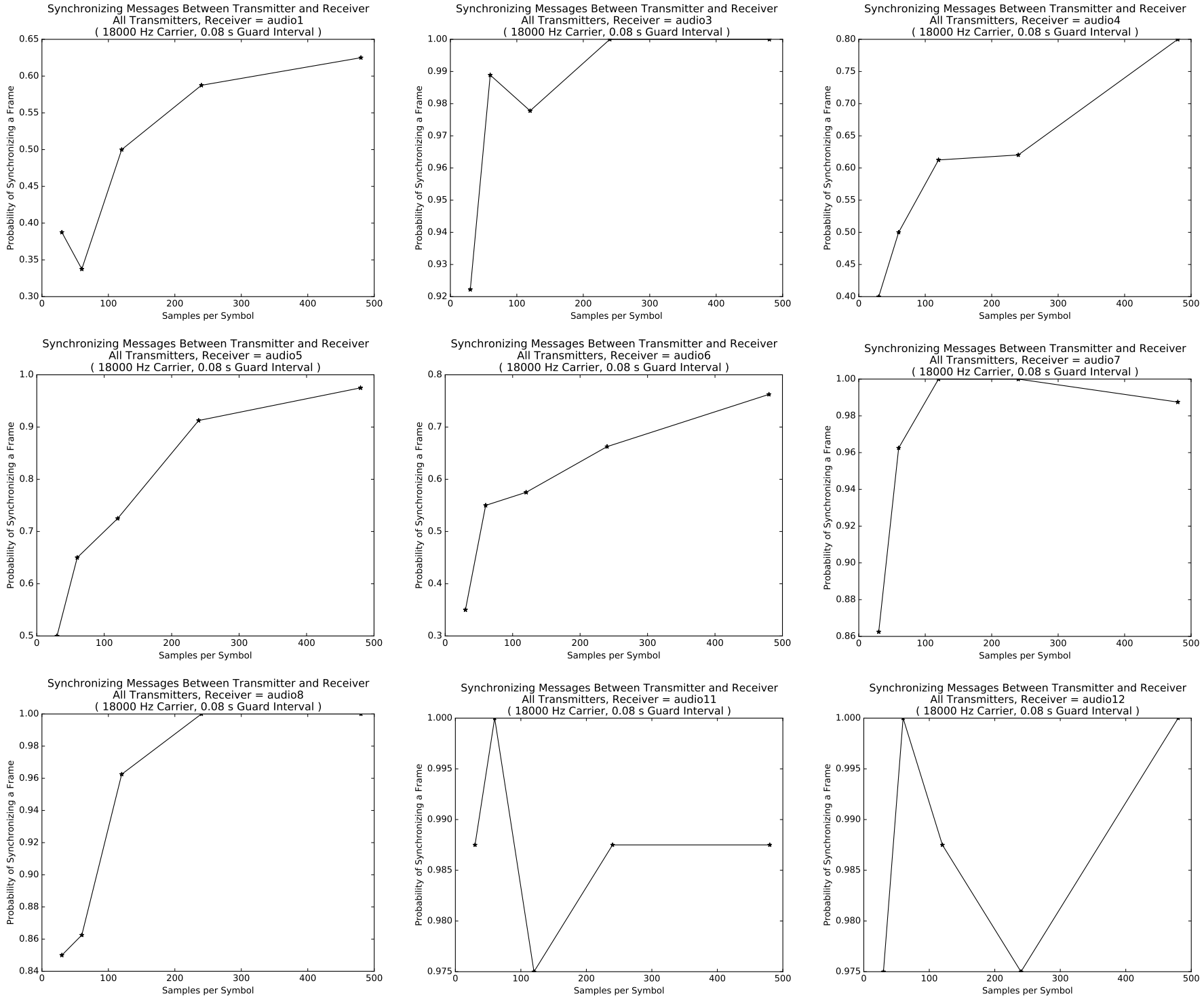



Figure D.8: Probability of Synchronization versus Transmitted Samples per Symbol for Each Device as Receiver (Part 1)

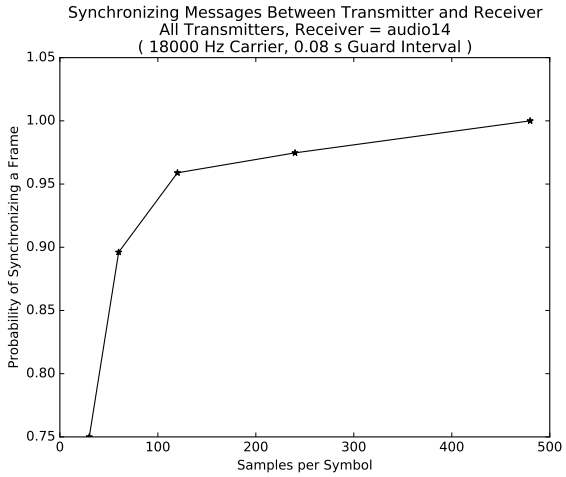



Figure D.9: Probability of Synchronization versus Transmitted Samples per Symbol for Each Device as Receiver (Part 2)

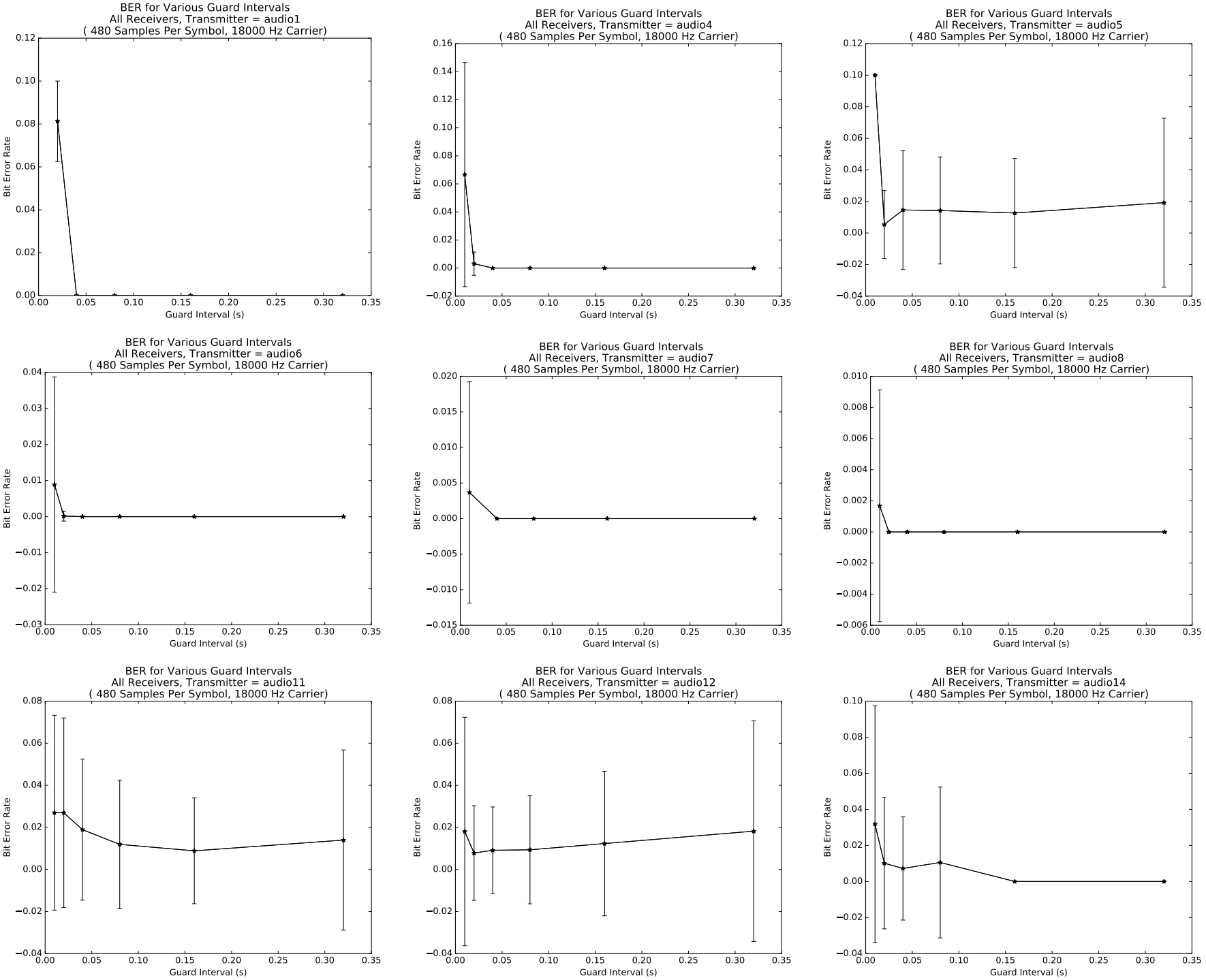



Figure D.10: Bit Error Rate versus Guard Interval for Each Device as Transmitter

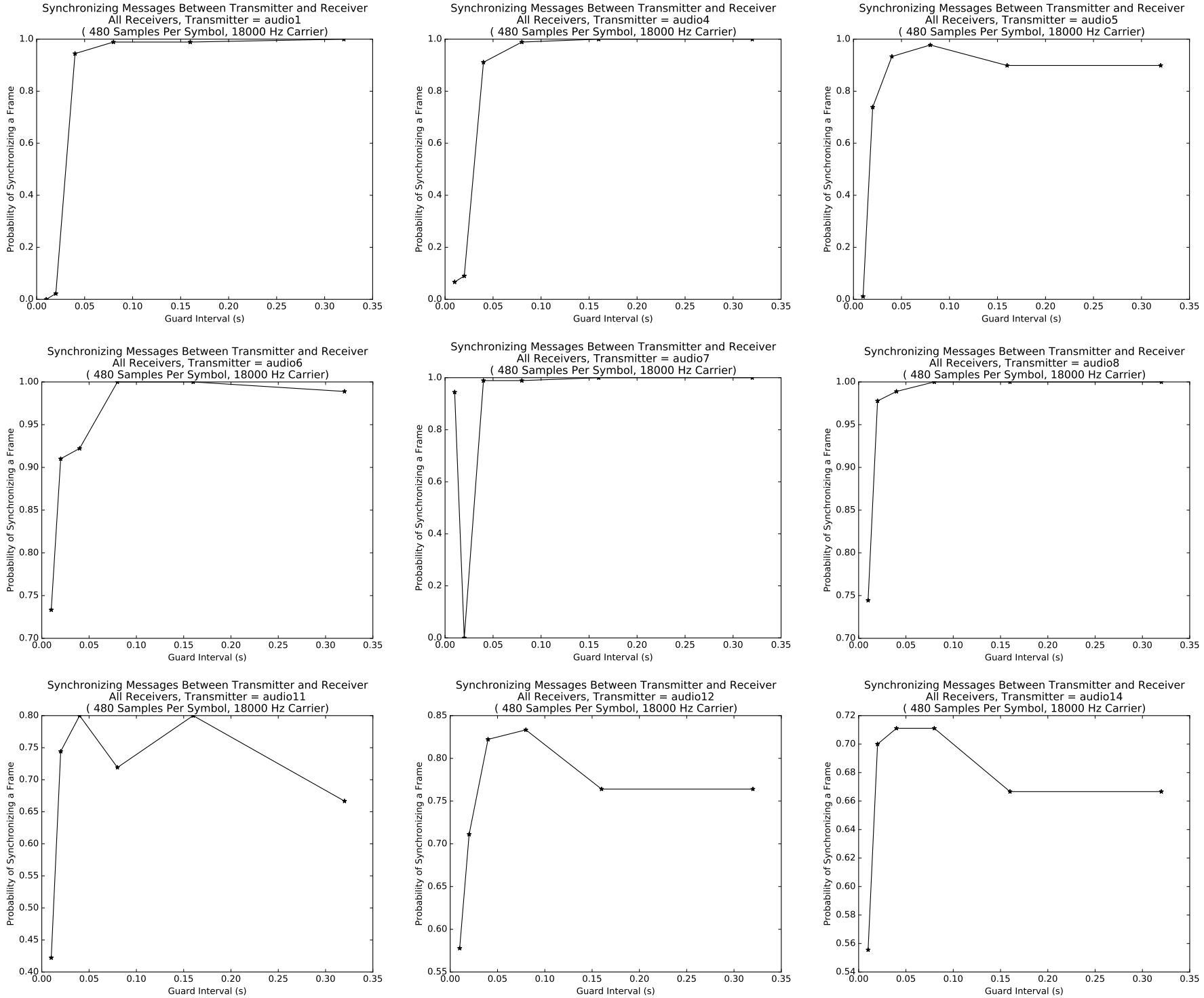



Figure D.11: Probability of Synchronization versus Guard Interval for Each Device as Transmitter

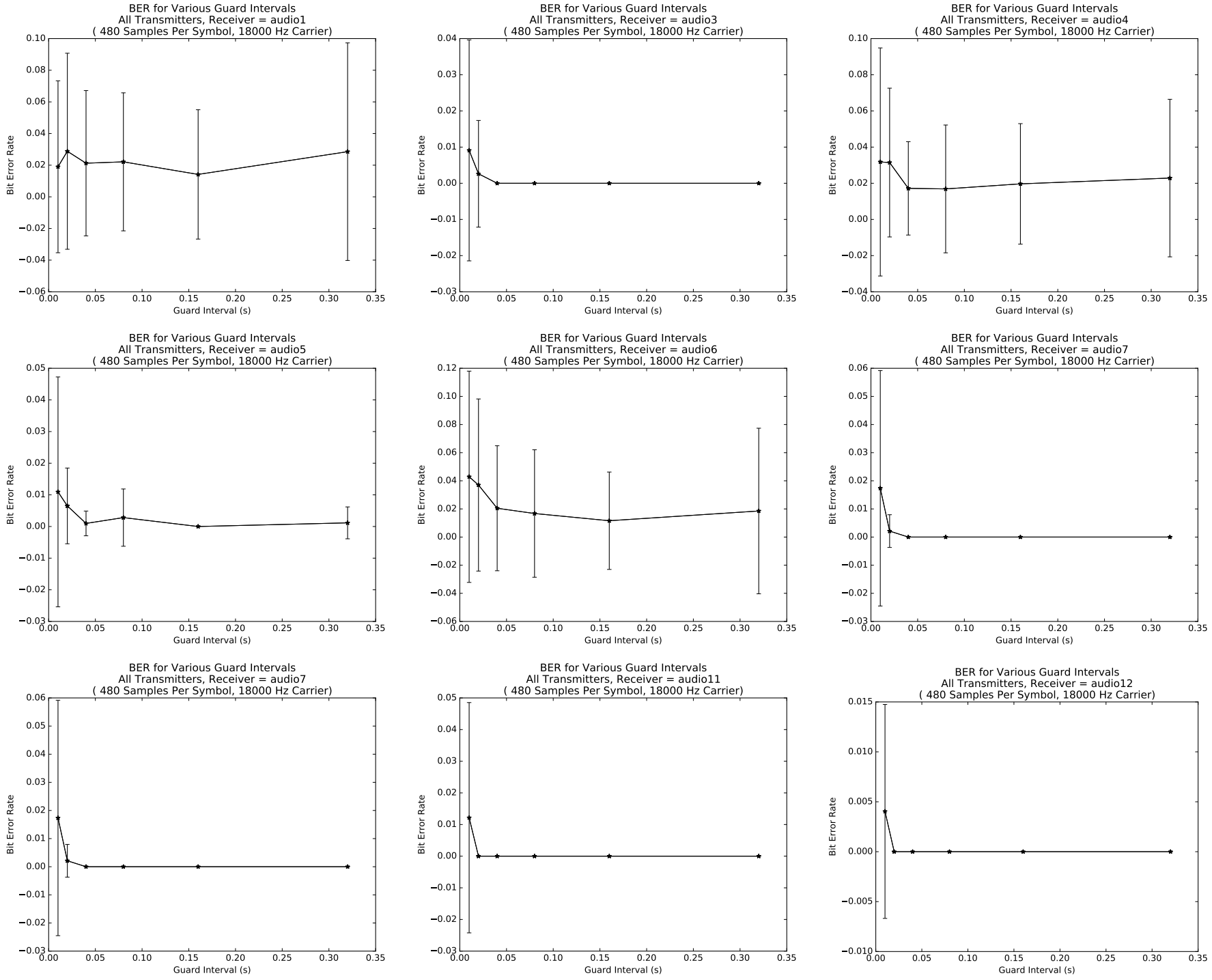



Figure D.12: Bit Error Rate versus Guard Interval for Each Device as Receiver (Part 1)

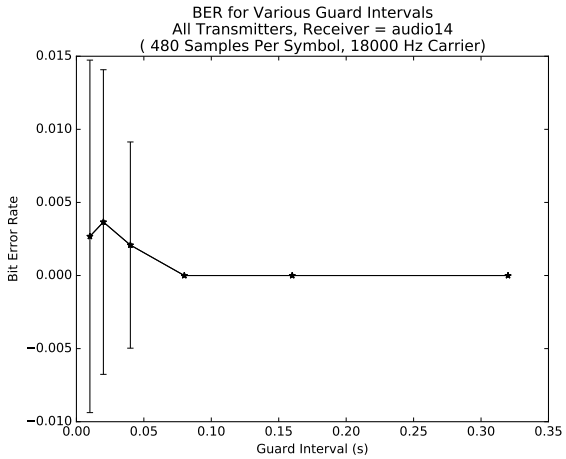



Figure D.13: Bit Error Rate versus Guard Interval for Each Device as Receiver (Part 2)

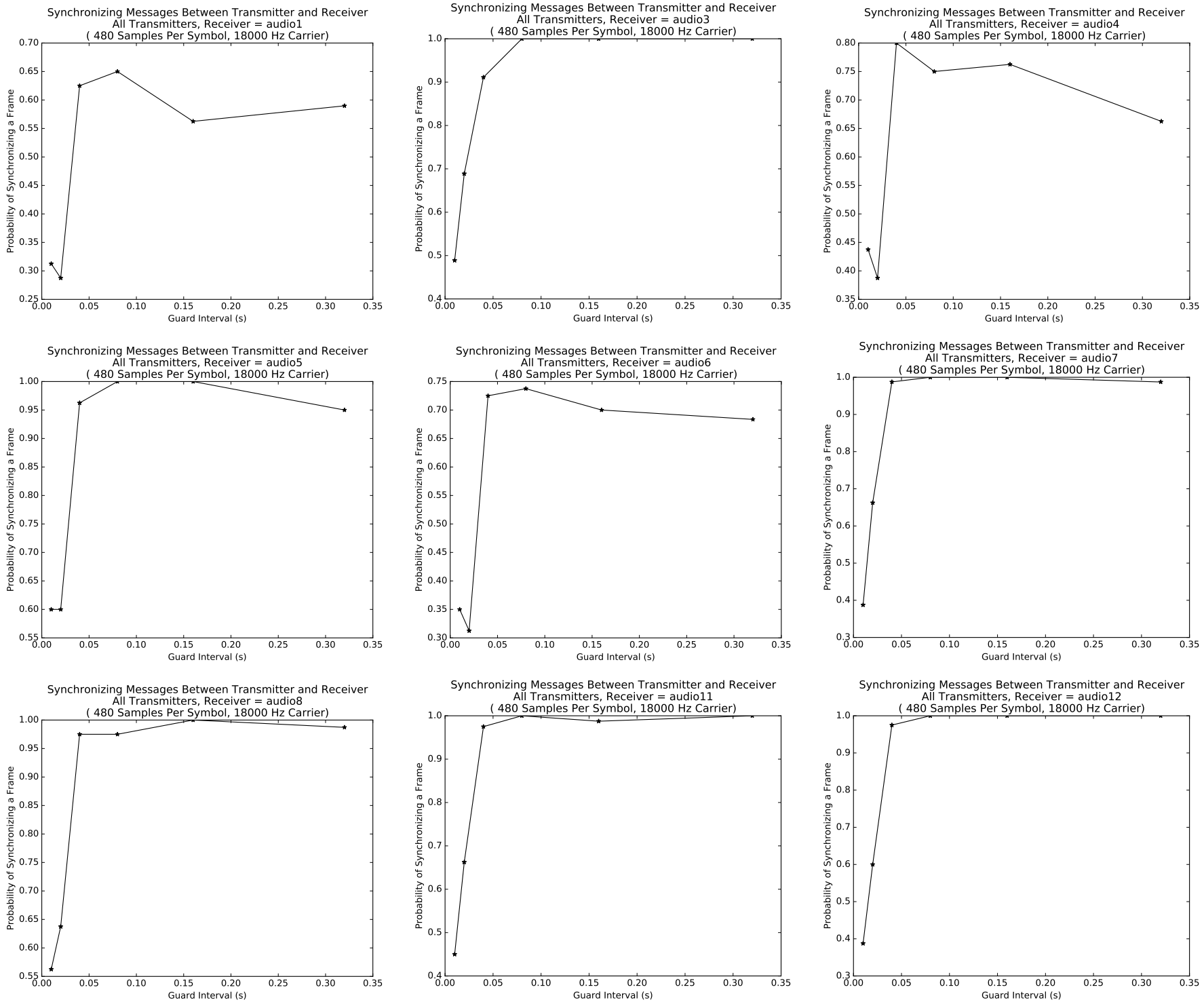



Figure D.14: Probability of Synchronization versus Guard Interval for Each Device as Receiver (Part 1)

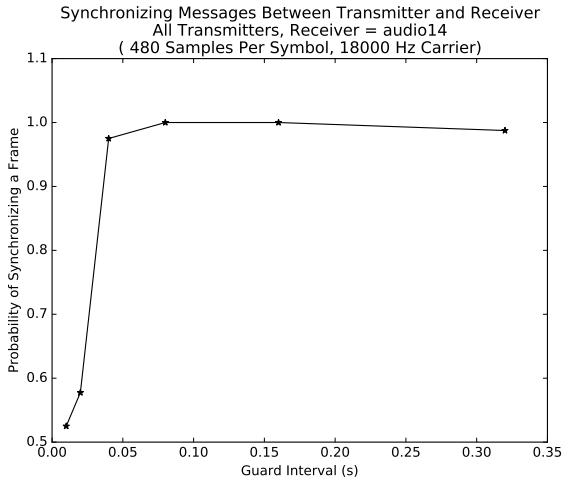



Figure D.15: Probability of Synchronization versus Guard Interval for Each Device as Receiver (Part 2)

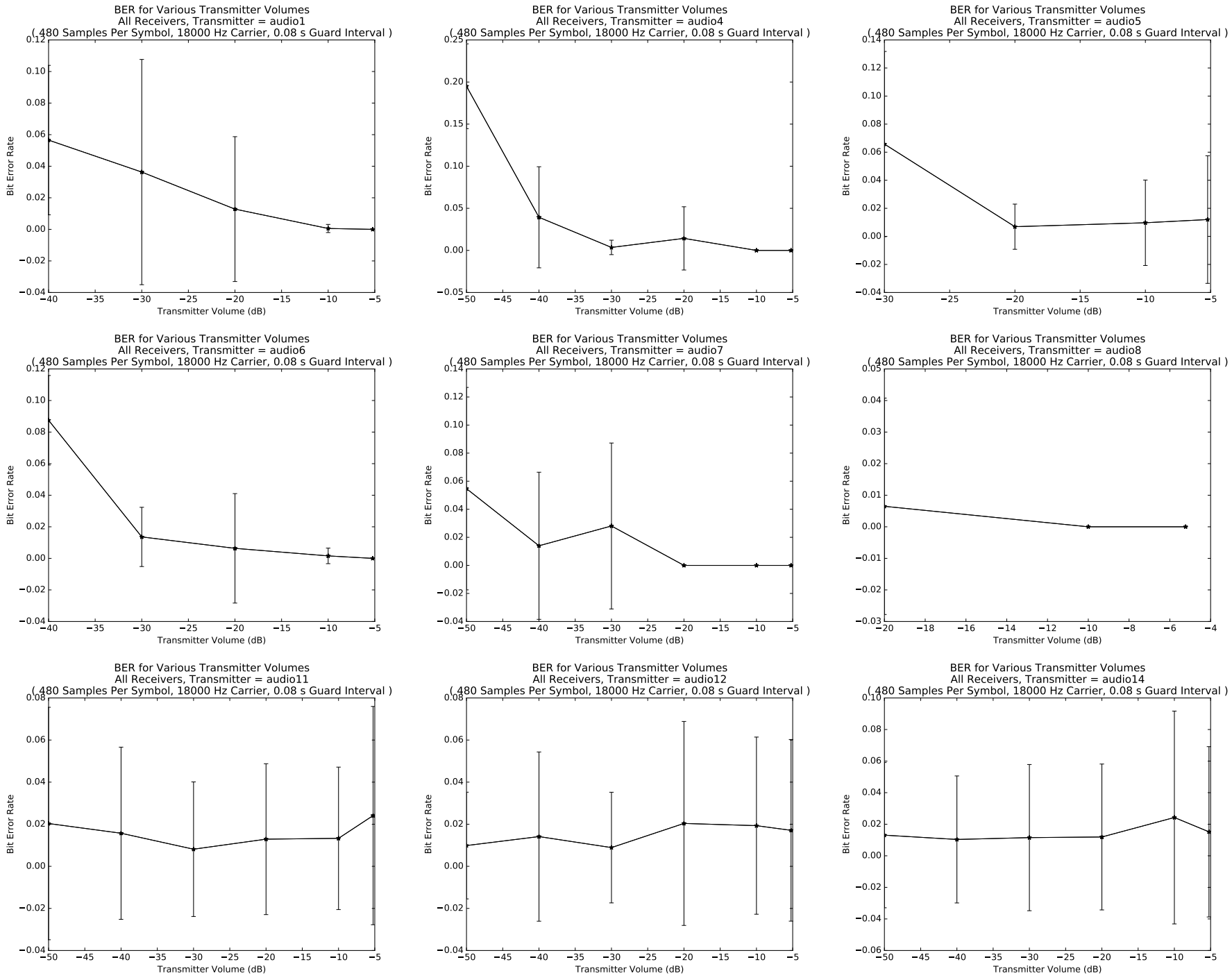



Figure D.16: Bit Error Rate versus Volume for Each Device as Transmitter

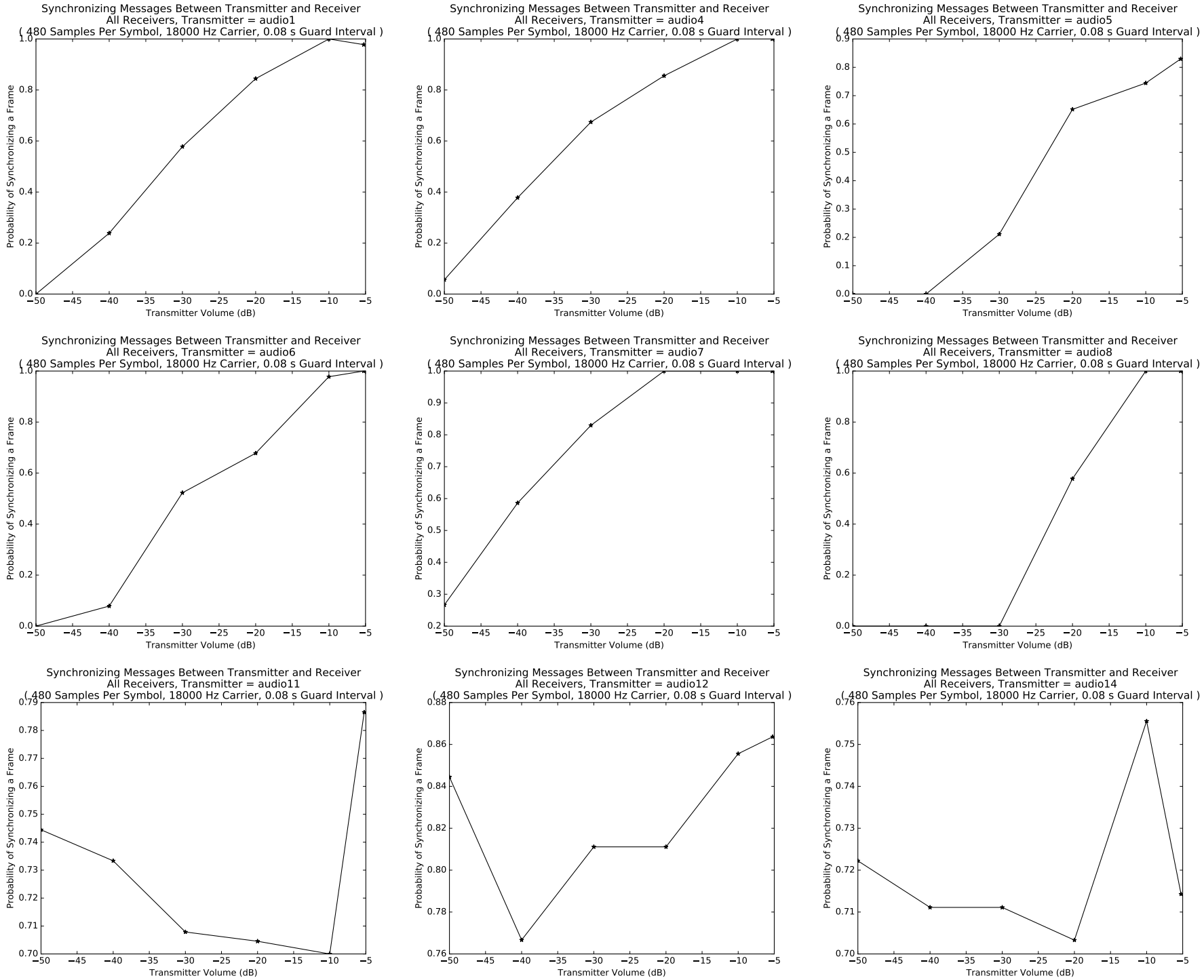



Figure D.17: Probability of Synchronization versus Volume for Each Device as Transmitter

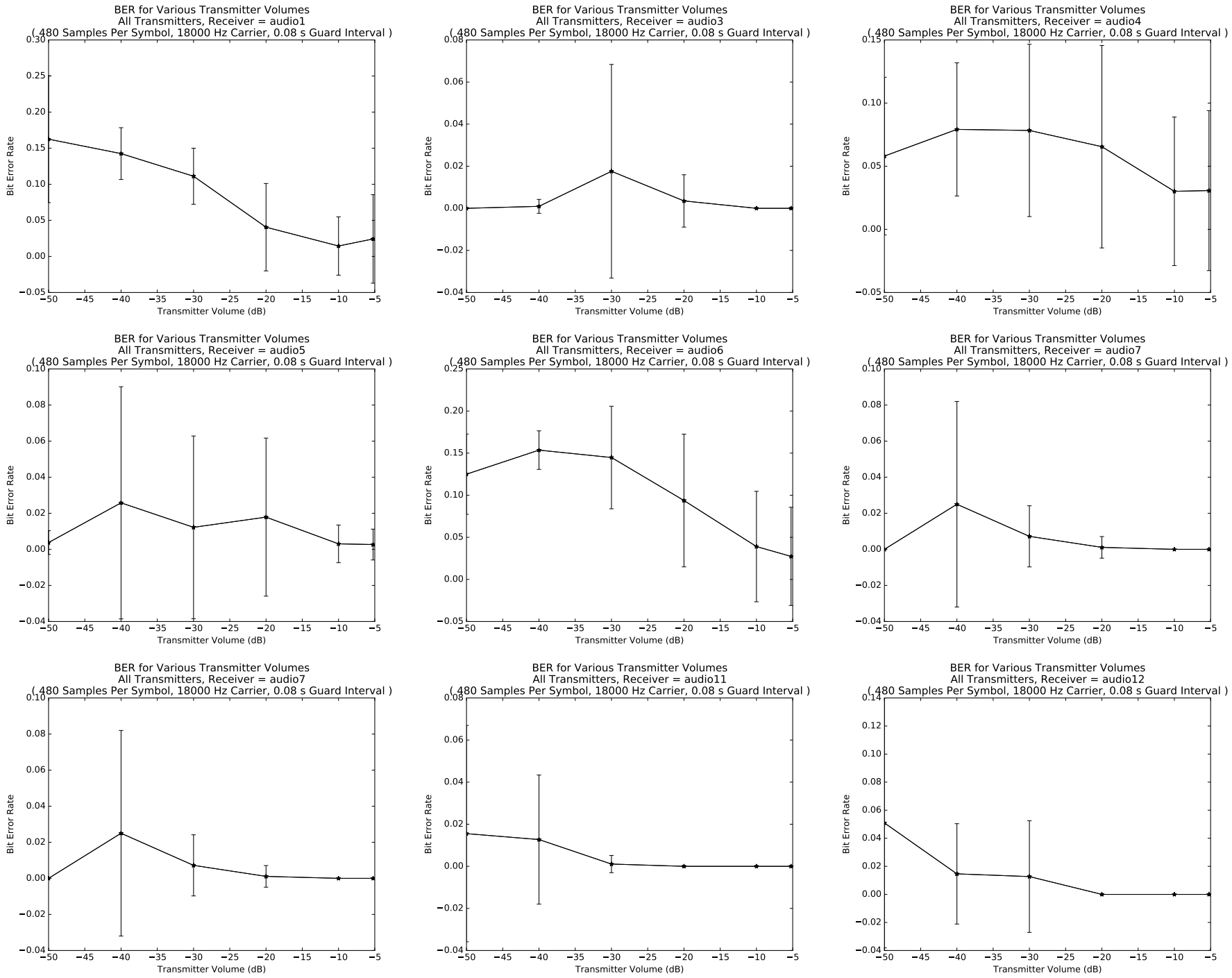



Figure D.18: Bit Error Rate versus Volume for Each Device as Receiver (Part 1)

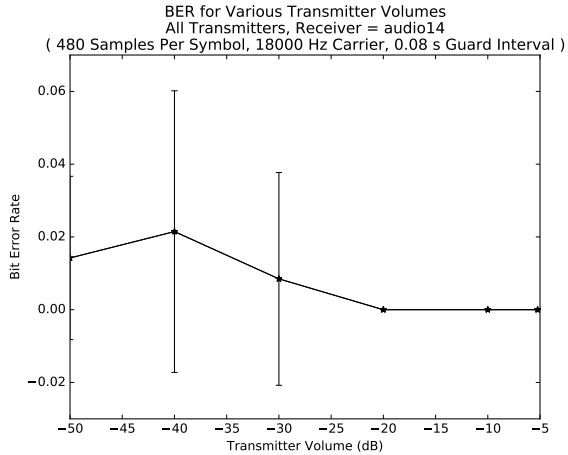



Figure D.19: Bit Error Rate versus Volume for Each Device as Receiver (Part 2)

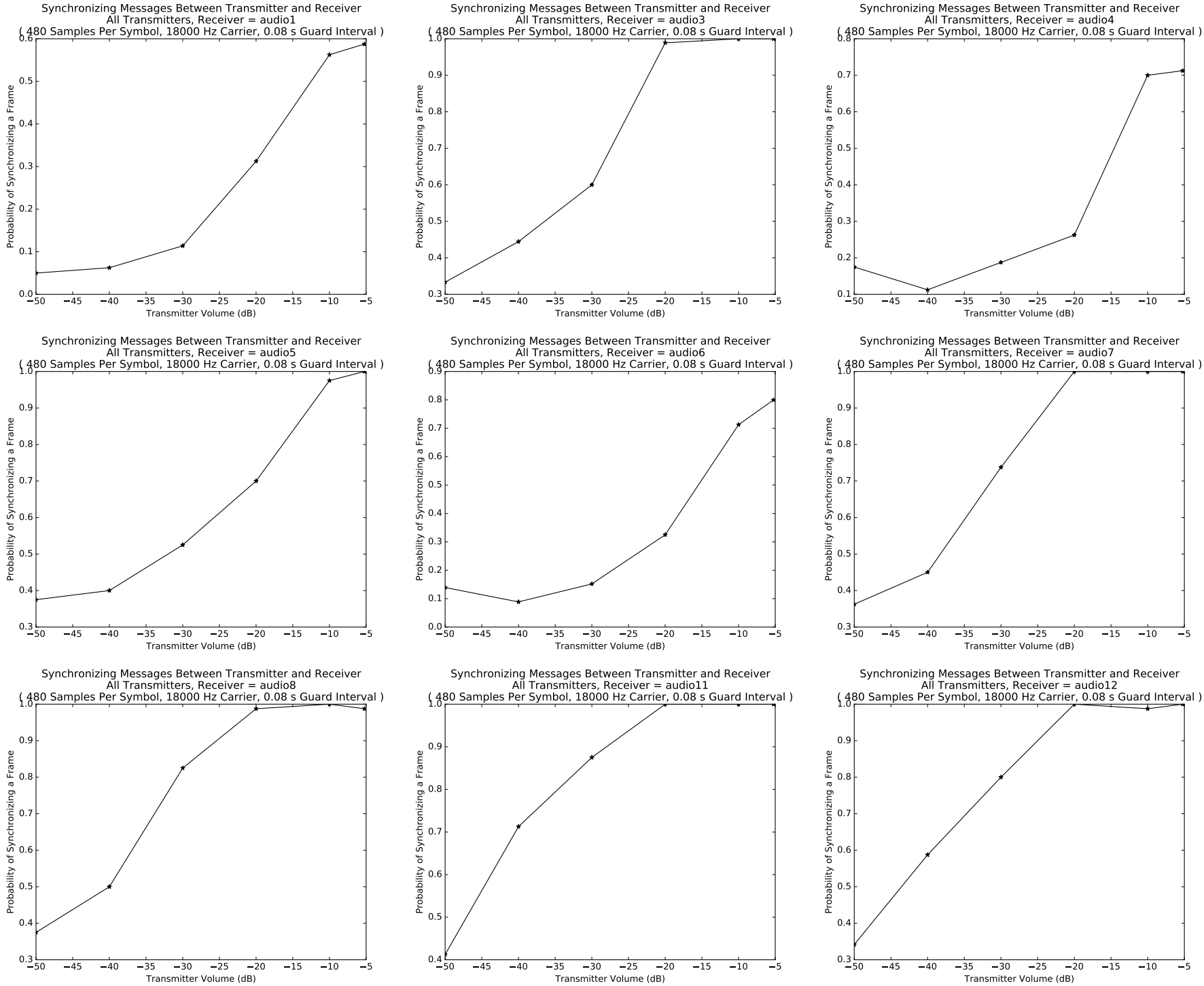



Figure D.20: Probability of Synchronization versus Volume for Each Device as Receiver (Part 1)

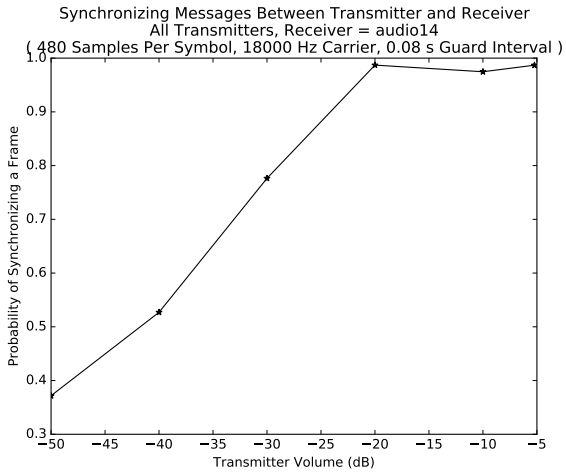



Figure D.21: Probability of Synchronization versus Volume for Each Device as Receiver (Part 2)

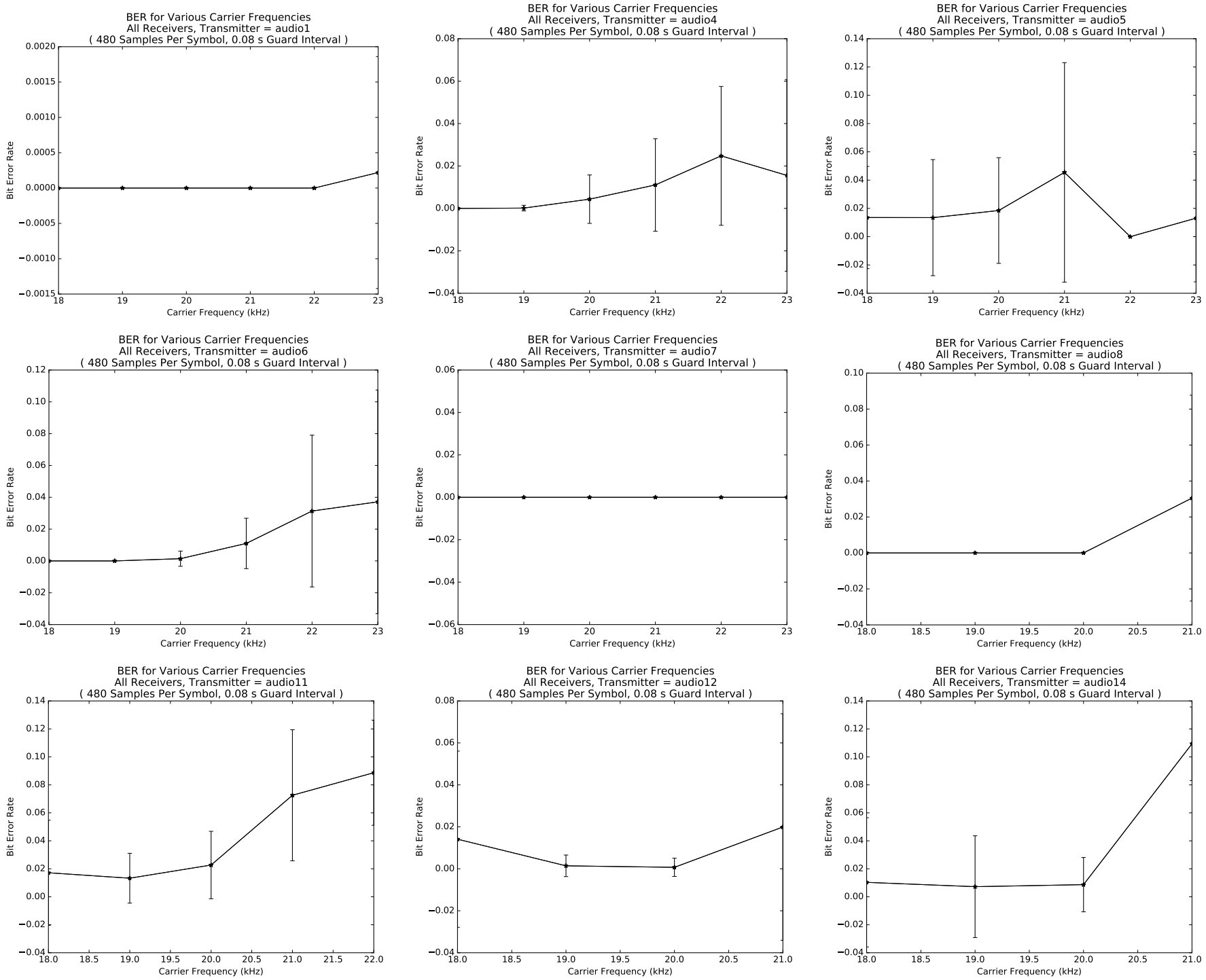



Figure D.22: Bit Error Rate versus Carrier Frequencies for Each Device as Transmitter

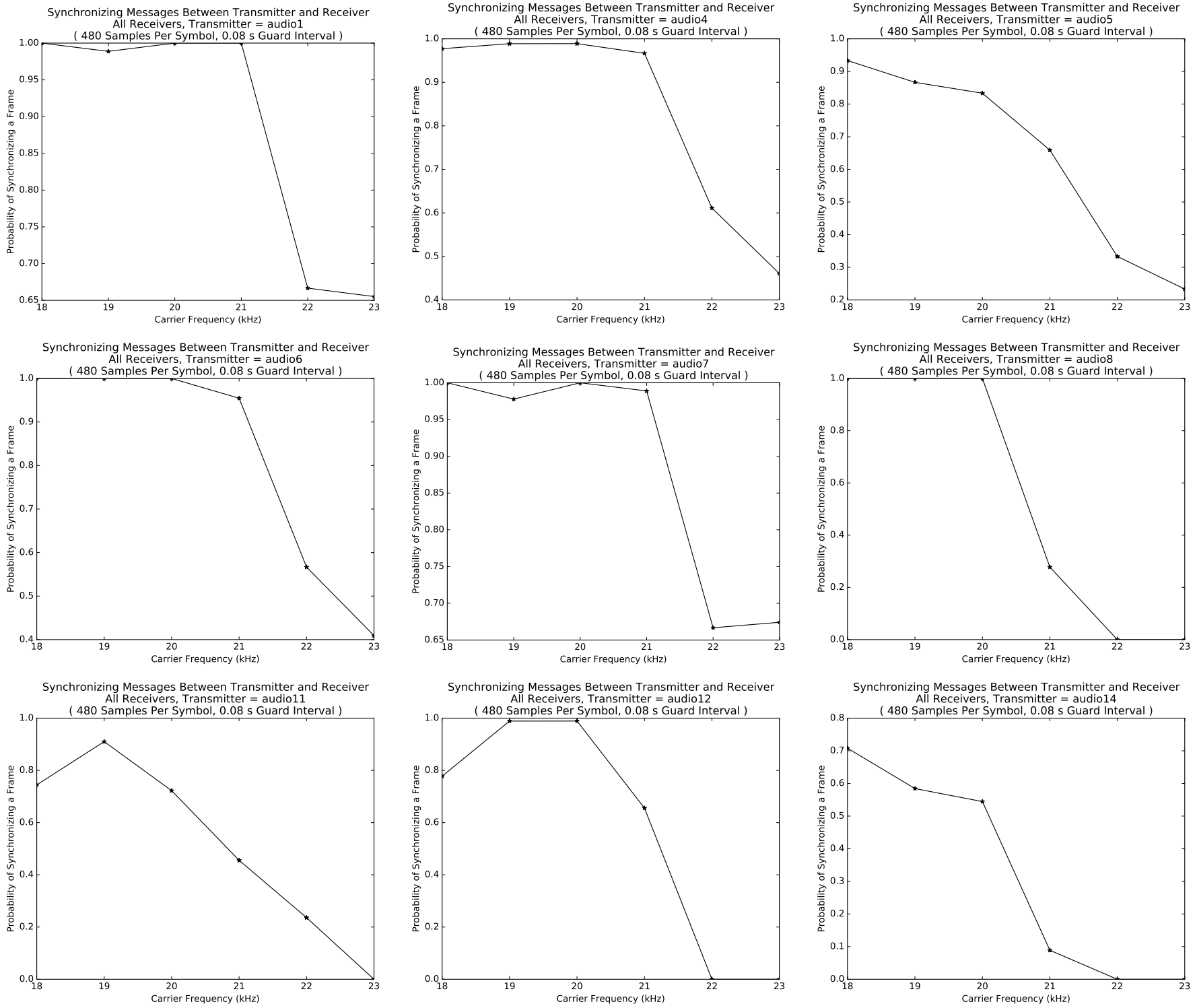



Figure D.23: Probability of Synchronization versus Carrier Frequencies Each Device as Transmitter

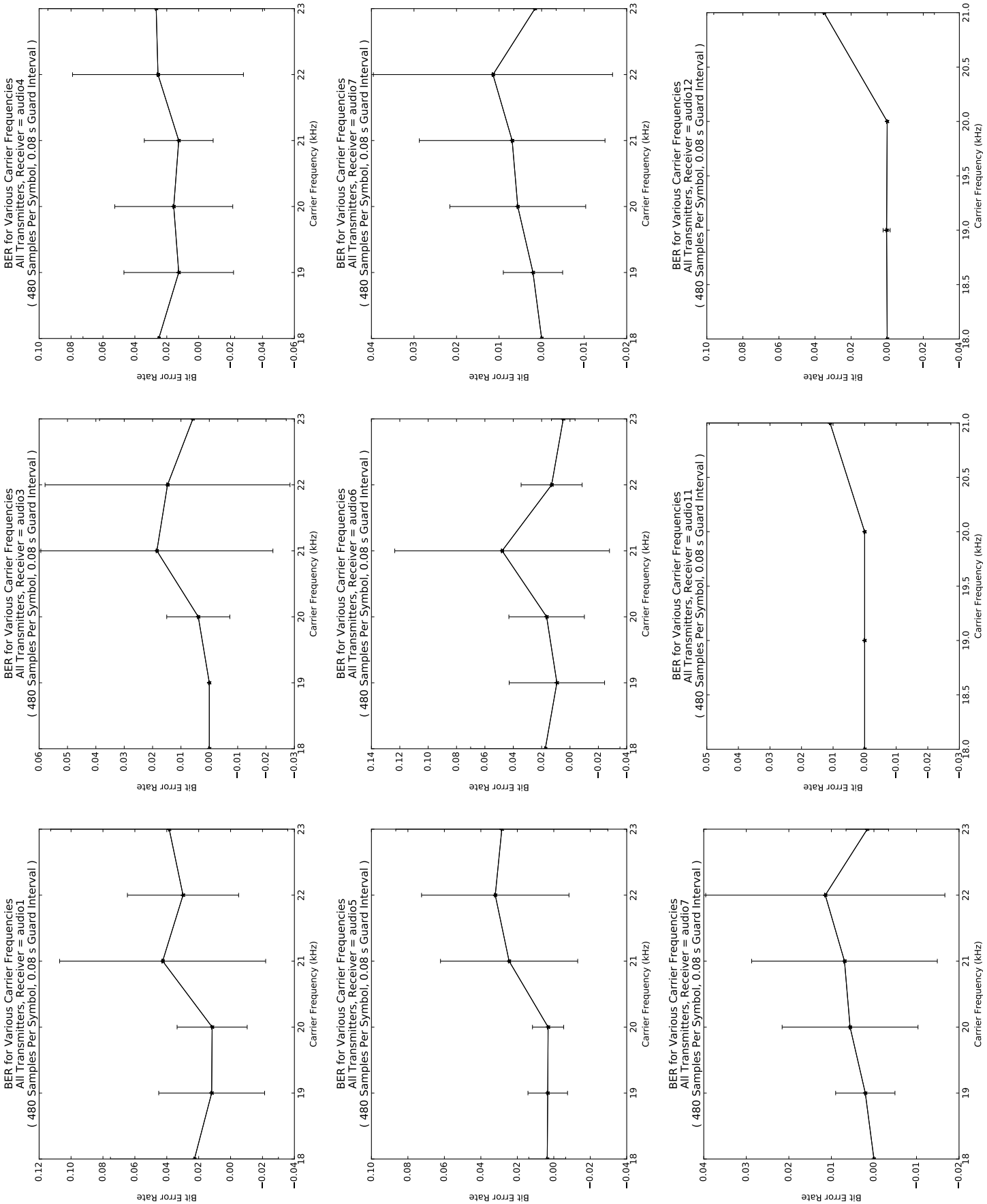



Figure D.24: Bit Error Rate versus Carrier Frequencies for Each Device as Receiver (Part 1)

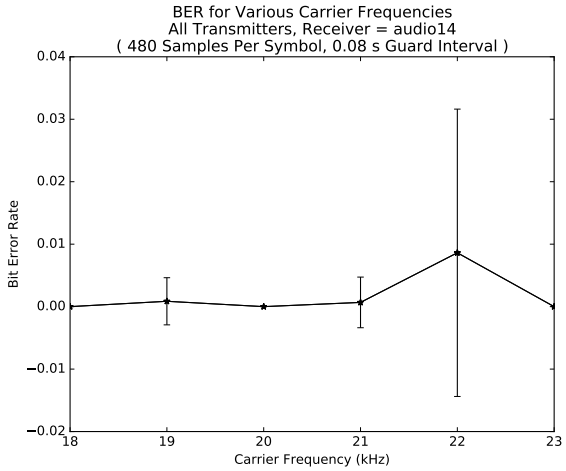



Figure D.25: Bit Error Rate versus Carrier Frequencies for Each Device as Receiver (Part 2)

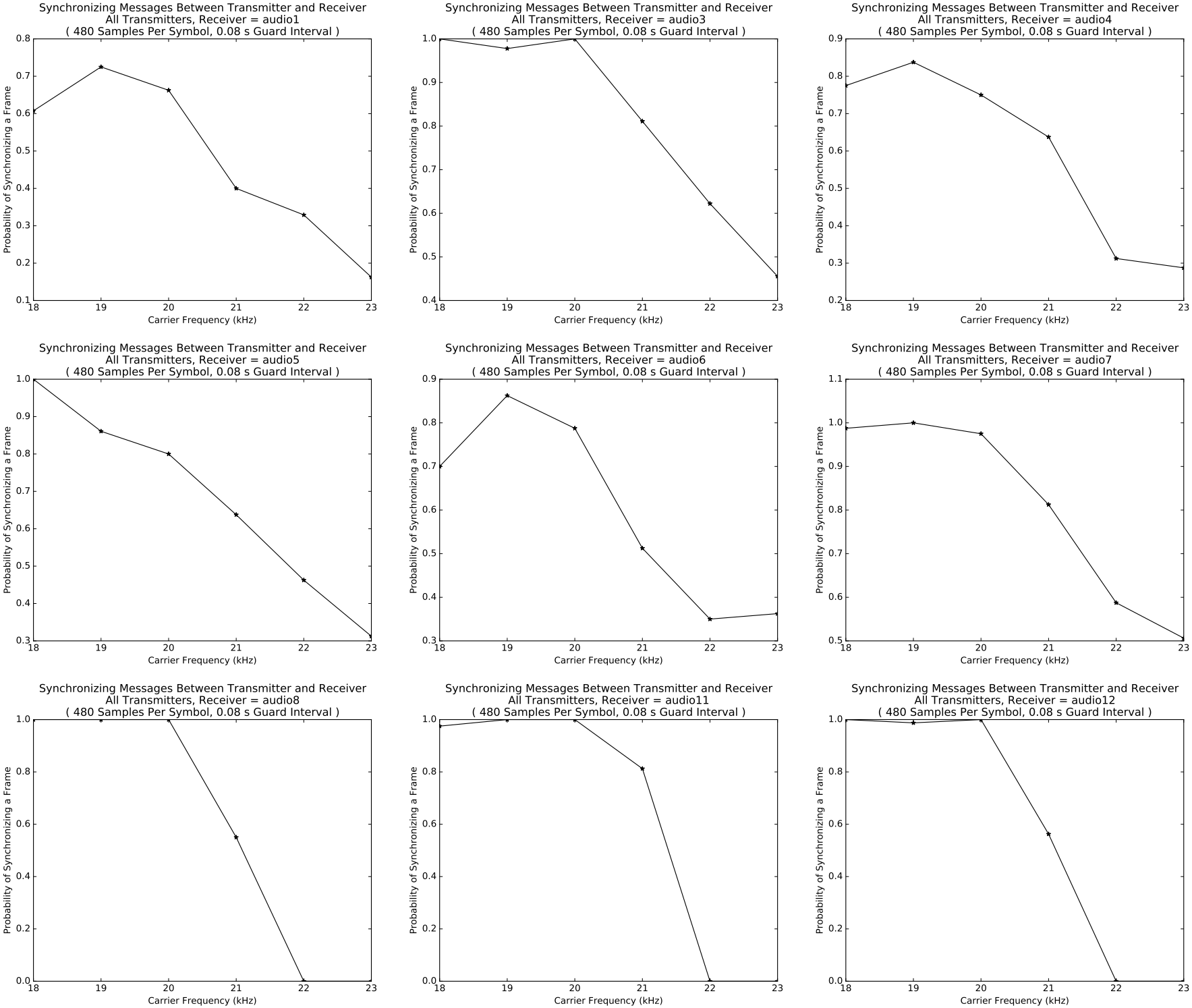



Figure D.26: Probability of Synchronization versus Carrier Frequencies for Each Device as Receiver (Part 1)

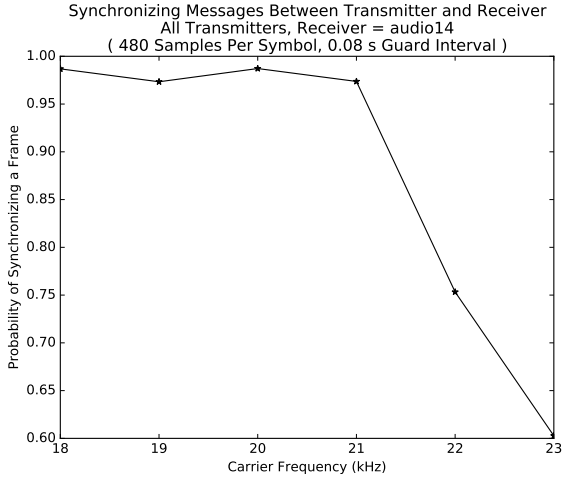



Figure D.27: Probability of Synchronization versus Carrier Frequencies for Each Device as Receiver (Part 2)

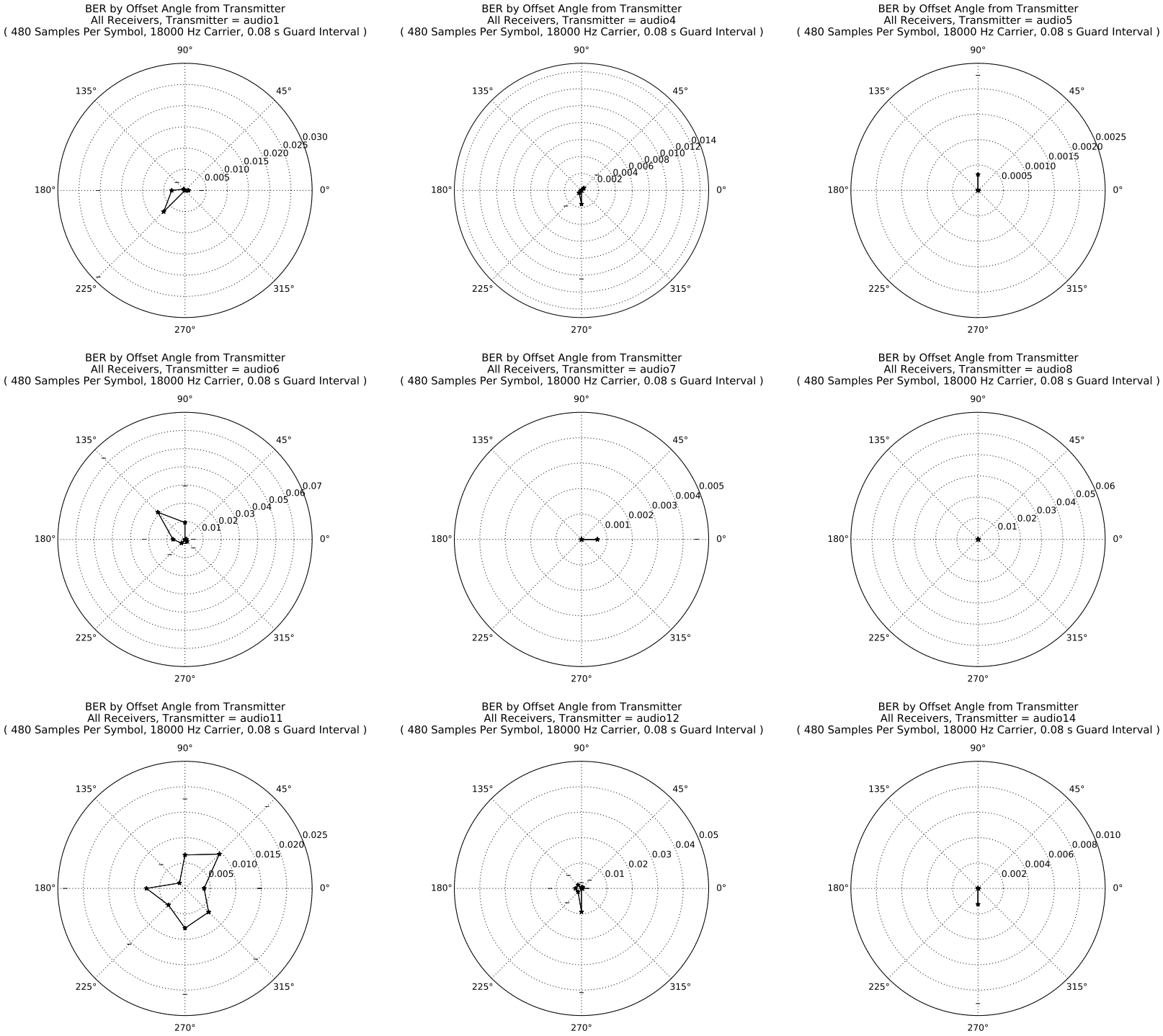



Figure D.28: Bit Error Rate versus Receiver Offset Angle for Each Device as Transmitter

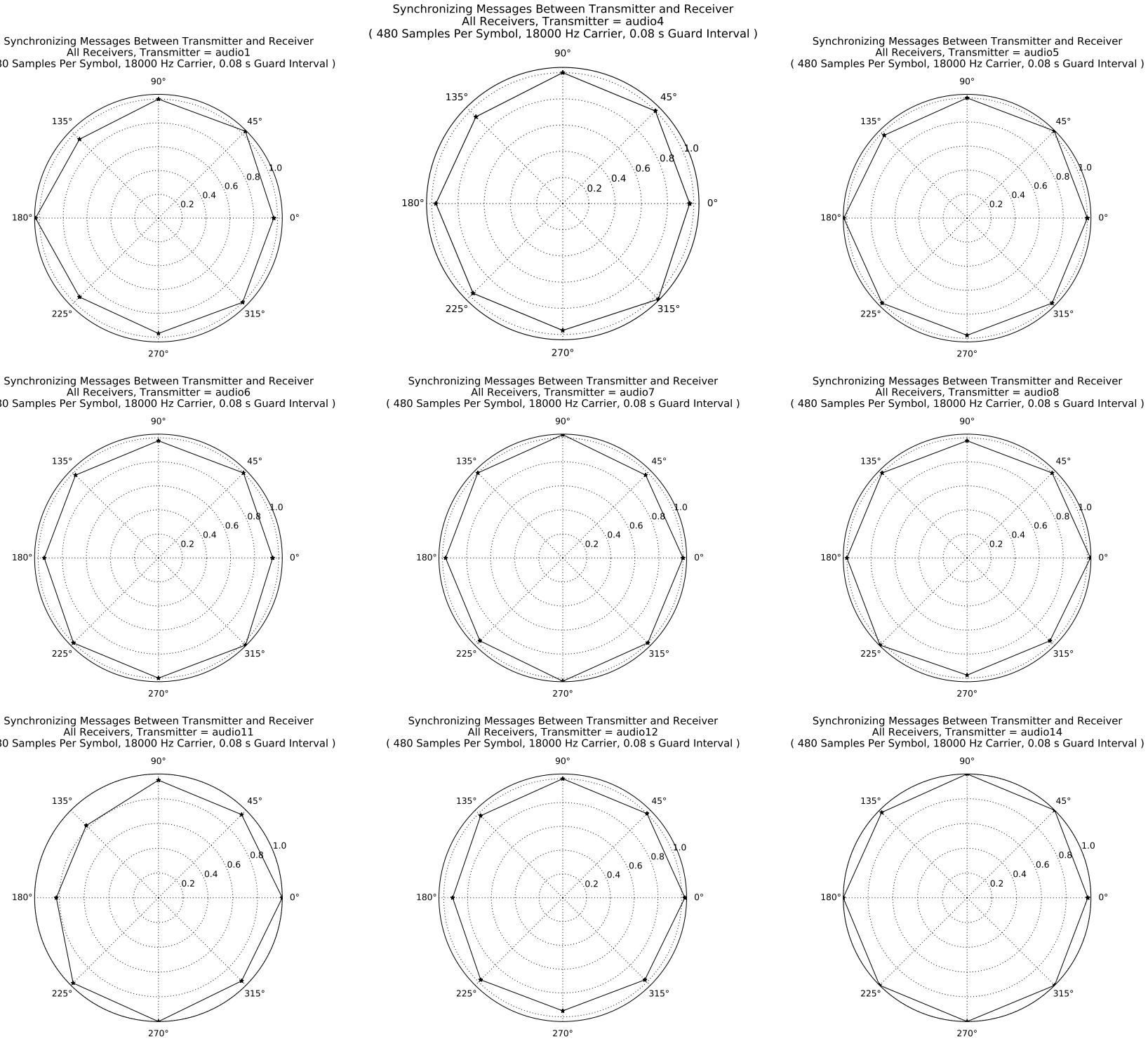



Figure D.29: Probability of Synchronization versus Receiver Offset Angle for Each Device as Transmitter

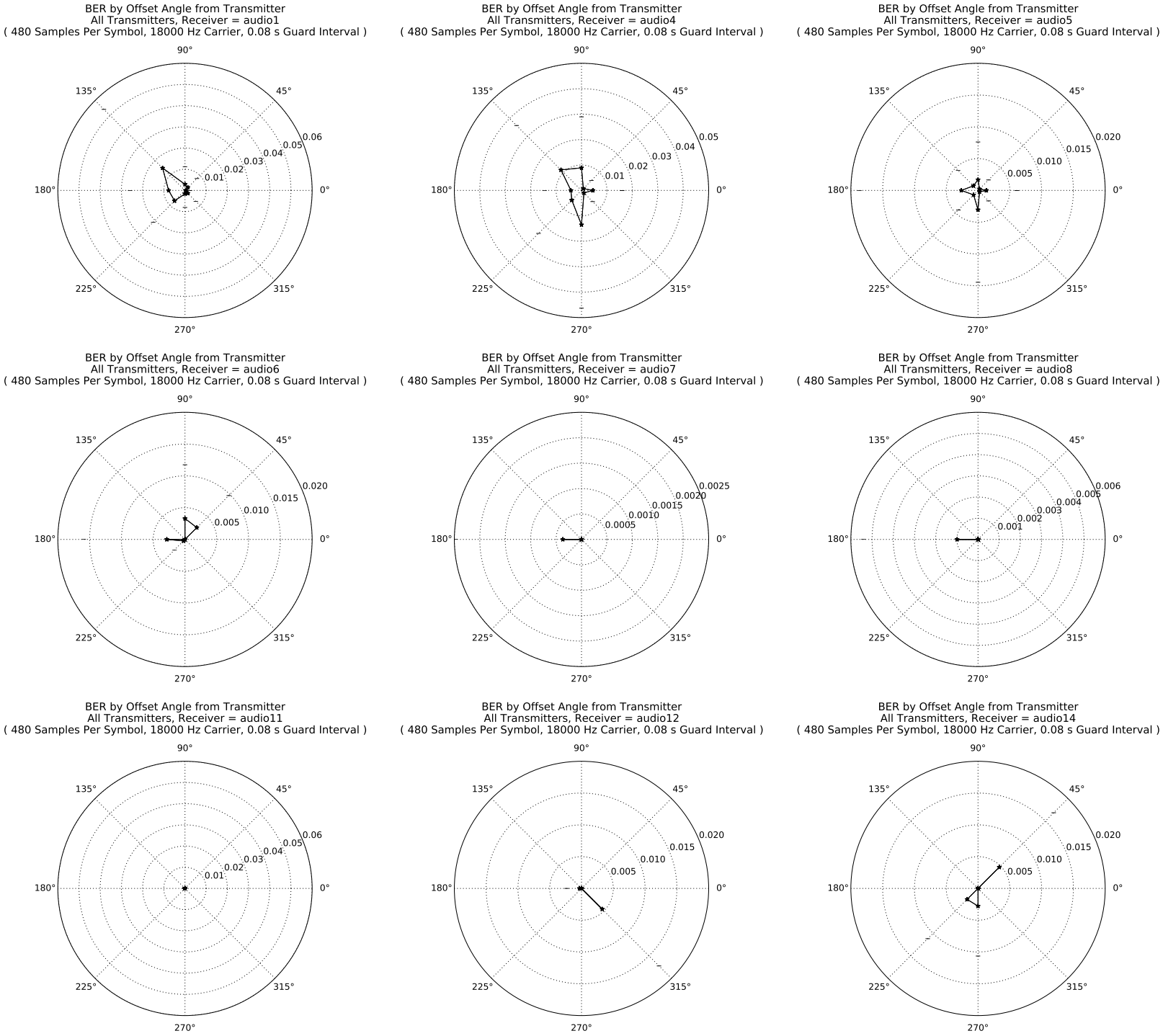



Figure D.30: Bit Error Rate versus Receiver Offset Angle for Each Device as Receiver

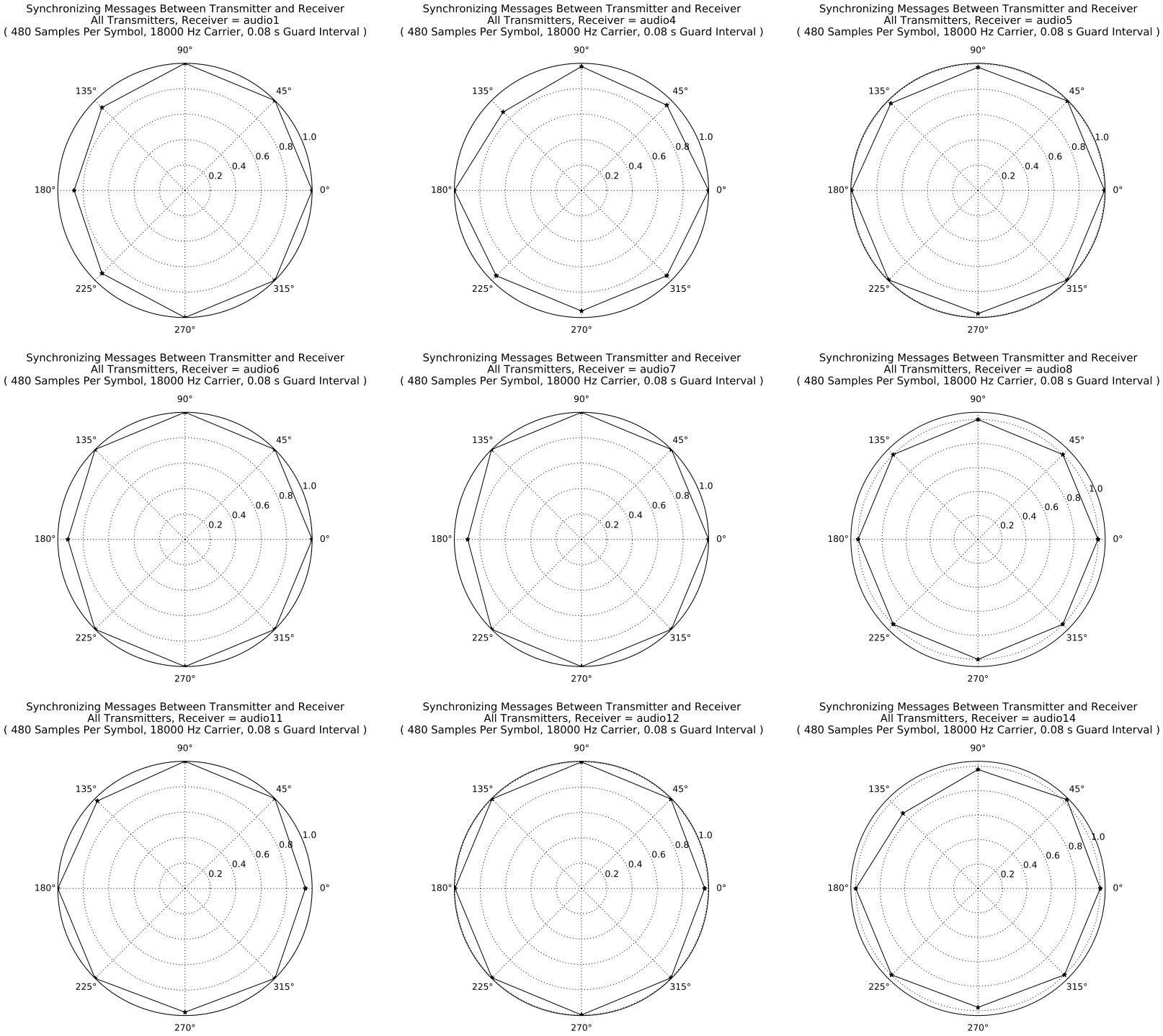



Figure D.31: Probability of Synchronization versus Receiver Offset Angle for Each Device as Receiver

Table D.1: OFDM Results for All Receivers, by Transmitter (Table 1)

| $f_1$ **(Hz)** | $f_2$ **(Hz)** | $N$ | $T_{guard}(s)$ | $P_{sync}$ | $\mu_{errors}$ | $\sigma_{errors}$ | $R$ $(\frac{\textbf{bits}}{\textbf{sec}})$ | **Transmitter** |
|---|---|---|---|---|---|---|---|---|
| 18000 | 19600 | 4 | 0.08 | 0.9815 | 0.0116 | 0.0382 | 44.4444 | audio1 |
| 18000 | 19600 | 8 | 0.04 | 0.9417 | 0.0655 | 0.0681 | 160.0000 | audio1 |
| 18000 | 20500 | 6 | 0.08 | 0.9815 | 0.0213 | 0.0420 | 66.6667 | audio1 |
| 18000 | 20500 | 12 | 0.04 | 0.8208 | 0.0750 | 0.0682 | 240.0000 | audio1 |
| 20000 | 21000 | 2 | 0.08 | 0.9333 | 0.0078 | 0.0350 | 22.2222 | audio1 |
| 20000 | 21000 | 5 | 0.04 | 0.9717 | 0.0322 | 0.0588 | 100.0000 | audio1 |
| 18000 | 19600 | 4 | 0.08 | 0.6389 | 0.0310 | 0.0544 | 44.4444 | audio11 |
| 18000 | 19600 | 8 | 0.04 | 0.5577 | 0.0647 | 0.0607 | 160.0000 | audio11 |
| 18000 | 20500 | 6 | 0.08 | 0.5981 | 0.0333 | 0.0543 | 66.6667 | audio11 |
| 18000 | 20500 | 12 | 0.04 | 0.5140 | 0.0772 | 0.0604 | 240.0000 | audio11 |
| 20000 | 21000 | 2 | 0.08 | 0.5962 | 0.0363 | 0.0522 | 22.2222 | audio11 |
| 20000 | 21000 | 5 | 0.04 | 0.5607 | 0.1093 | 0.0725 | 100.0000 | audio11 |
| 18000 | 19600 | 4 | 0.08 | 0.7037 | 0.0375 | 0.0600 | 44.4444 | audio12 |
| 18000 | 19600 | 8 | 0.04 | 0.5962 | 0.0517 | 0.0787 | 160.0000 | audio12 |
| 18000 | 20500 | 6 | 0.08 | 0.5926 | 0.0224 | 0.0593 | 66.6667 | audio12 |
| 18000 | 20500 | 12 | 0.04 | 0.5283 | 0.0312 | 0.0554 | 240.0000 | audio12 |
| 20000 | 21000 | 2 | 0.08 | 0.7850 | 0.0142 | 0.0298 | 22.2222 | audio12 |
| 20000 | 21000 | 5 | 0.04 | 0.6250 | 0.0697 | 0.0876 | 100.0000 | audio12 |
| 18000 | 19600 | 4 | 0.08 | 0.5688 | 0.0526 | 0.0732 | 44.4444 | audio14 |
| 18000 | 19600 | 8 | 0.04 | 0.3704 | 0.1094 | 0.0834 | 160.0000 | audio14 |
| 18000 | 20500 | 6 | 0.08 | 0.4771 | 0.1127 | 0.0766 | 66.6667 | audio14 |
| 18000 | 20500 | 12 | 0.04 | 0.1743 | 0.1657 | 0.0566 | 240.0000 | audio14 |
| 20000 | 21000 | 2 | 0.08 | 0.3056 | 0.1284 | 0.0935 | 22.2222 | audio14 |
| 20000 | 21000 | 5 | 0.04 | 0.0275 | 0.2042 | 0.0029 | 100.0000 | audio14 |
| 18000 | 19600 | 4 | 0.08 | 0.9815 | 0.0208 | 0.0503 | 44.4444 | audio4 |
| 18000 | 19600 | 8 | 0.04 | 0.9434 | 0.0734 | 0.0704 | 160.0000 | audio4 |
| 18000 | 20500 | 6 | 0.08 | 0.9630 | 0.0353 | 0.0618 | 66.6667 | audio4 |
| 18000 | 20500 | 12 | 0.04 | 0.7264 | 0.0707 | 0.0676 | 240.0000 | audio4 |
| 20000 | 21000 | 2 | 0.08 | 0.8713 | 0.0116 | 0.0450 | 22.2222 | audio4 |
| 20000 | 21000 | 5 | 0.04 | 0.7767 | 0.0673 | 0.0783 | 100.0000 | audio4 |
| 18000 | 19600 | 4 | 0.08 | 0.6759 | 0.0489 | 0.0703 | 44.4444 | audio5 |
| 18000 | 19600 | 8 | 0.04 | 0.6075 | 0.1192 | 0.0638 | 160.0000 | audio5 |
| 18000 | 20500 | 6 | 0.08 | 0.6852 | 0.0726 | 0.0625 | 66.6667 | audio5 |
| 18000 | 20500 | 12 | 0.04 | 0.3333 | 0.1012 | 0.0726 | 240.0000 | audio5 |
| 20000 | 21000 | 2 | 0.08 | 0.6190 | 0.0243 | 0.0536 | 22.2222 | audio5 |
| 20000 | 21000 | 5 | 0.04 | 0.5143 | 0.0900 | 0.0699 | 100.0000 | audio5 |
| 18000 | 19600 | 4 | 0.08 | 0.8611 | 0.0379 | 0.0686 | 44.4444 | audio6 |
| 18000 | 19600 | 8 | 0.04 | 0.6729 | 0.0470 | 0.0372 | 160.0000 | audio6 |
| 18000 | 20500 | 6 | 0.08 | 0.7290 | 0.0399 | 0.0757 | 66.6667 | audio6 |
| 18000 | 20500 | 12 | 0.04 | 0.6190 | 0.0619 | 0.0592 | 240.0000 | audio6 |
| 20000 | 21000 | 2 | 0.08 | 0.7358 | 0.0191 | 0.0508 | 22.2222 | audio6 |

Table D.2: OFDM Results for All Receivers, by Transmitter (Table 2)

| $f_1$ **(Hz)** | $f_2$ **(Hz)** | $N$ | $T_{guard}(s)$ | $P_{sync}$ | $\mu_{errors}$ | $\sigma_{errors}$ | $R$ ($\frac{\textbf{bits}}{\textbf{sec}}$) | **Transmitter** |
|---|---|---|---|---|---|---|---|---|
| 20000 | 21000 | 5 | 0.04 | 0.6154 | 0.0536 | 0.0750 | 100.0000 | audio6 |
| 18000 | 19600 | 4 | 0.08 | 1.0000 | 0.0066 | 0.0313 | 44.4444 | audio7 |
| 18000 | 19600 | 8 | 0.04 | 1.0000 | 0.0363 | 0.0324 | 160.0000 | audio7 |
| 18000 | 20500 | 6 | 0.08 | 1.0000 | 0.0046 | 0.0249 | 66.6667 | audio7 |
| 18000 | 20500 | 12 | 0.04 | 0.9810 | 0.0530 | 0.0569 | 240.0000 | audio7 |
| 20000 | 21000 | 2 | 0.08 | 1.0000 | 0.0045 | 0.0325 | 22.2222 | audio7 |
| 20000 | 21000 | 5 | 0.04 | 1.0000 | 0.0269 | 0.0614 | 100.0000 | audio7 |
| 18000 | 19600 | 4 | 0.08 | 0.9537 | 0.0025 | 0.0179 | 44.4444 | audio8 |
| 18000 | 19600 | 8 | 0.04 | 1.0000 | 0.0165 | 0.0393 | 160.0000 | audio8 |
| 18000 | 20500 | 6 | 0.08 | 0.9722 | 0.0366 | 0.0479 | 66.6667 | audio8 |
| 18000 | 20500 | 12 | 0.04 | 0.9906 | 0.0721 | 0.0740 | 240.0000 | audio8 |
| 20000 | 21000 | 2 | 0.08 | 0.7500 | 0.0674 | 0.0960 | 22.2222 | audio8 |
| 20000 | 21000 | 5 | 0.04 | 0.4571 | 0.1241 | 0.0606 | 100.0000 | audio8 |

Table D.3: OFDM Results for All Transmitters, by Receiver (Table 1)

| $f_1$ **(Hz)** | $f_2$ **(Hz)** | $N$ | $T_{guard}(s)$ | $P_{sync}$ | $\mu_{errors}$ | $\sigma_{errors}$ | $R$ ($\frac{\textbf{bits}}{\textbf{sec}}$) | **Receiver** |
|---|---|---|---|---|---|---|---|---|
| 18000 | 19600 | 4 | 0.08 | 0.4062 | 0.0321 | 0.0602 | 44.4444 | audio1 |
| 18000 | 19600 | 8 | 0.04 | 0.3438 | 0.0749 | 0.0803 | 160.0000 | audio1 |
| 18000 | 20500 | 6 | 0.08 | 0.3958 | 0.1010 | 0.0792 | 66.6667 | audio1 |
| 18000 | 20500 | 12 | 0.04 | 0.2500 | 0.1223 | 0.0672 | 240.0000 | audio1 |
| 20000 | 21000 | 2 | 0.08 | 0.2211 | 0.0842 | 0.0996 | 22.2222 | audio1 |
| 20000 | 21000 | 5 | 0.04 | 0.1354 | 0.0413 | 0.0671 | 100.0000 | audio1 |
| 18000 | 19600 | 4 | 0.08 | 0.9688 | 0.0113 | 0.0423 | 44.4444 | audio11 |
| 18000 | 19600 | 8 | 0.04 | 1.0000 | 0.0317 | 0.0457 | 160.0000 | audio11 |
| 18000 | 20500 | 6 | 0.08 | 1.0000 | 0.0093 | 0.0344 | 66.6667 | audio11 |
| 18000 | 20500 | 12 | 0.04 | 0.9583 | 0.0514 | 0.0608 | 240.0000 | audio11 |
| 20000 | 21000 | 2 | 0.08 | 0.9896 | 0.0068 | 0.0377 | 22.2222 | audio11 |
| 20000 | 21000 | 5 | 0.04 | 0.8854 | 0.0346 | 0.0576 | 100.0000 | audio11 |
| 18000 | 19600 | 4 | 0.08 | 0.9688 | 0.0088 | 0.0323 | 44.4444 | audio12 |
| 18000 | 19600 | 8 | 0.04 | 1.0000 | 0.0501 | 0.0576 | 160.0000 | audio12 |
| 18000 | 20500 | 6 | 0.08 | 0.9896 | 0.0161 | 0.0379 | 66.6667 | audio12 |
| 18000 | 20500 | 12 | 0.04 | 0.9167 | 0.0621 | 0.0700 | 240.0000 | audio12 |
| 20000 | 21000 | 2 | 0.08 | 0.9062 | 0.0280 | 0.0687 | 22.2222 | audio12 |
| 20000 | 21000 | 5 | 0.04 | 0.7917 | 0.0859 | 0.0771 | 100.0000 | audio12 |
| 18000 | 19600 | 4 | 0.08 | 1.0000 | 0.0299 | 0.0461 | 44.4444 | audio14 |
| 18000 | 19600 | 8 | 0.04 | 1.0000 | 0.0630 | 0.0506 | 160.0000 | audio14 |
| 18000 | 20500 | 6 | 0.08 | 1.0000 | 0.0265 | 0.0446 | 66.6667 | audio14 |
| 18000 | 20500 | 12 | 0.04 | 0.9494 | 0.0604 | 0.0533 | 240.0000 | audio14 |
| 20000 | 21000 | 2 | 0.08 | 0.9571 | 0.0006 | 0.0026 | 22.2222 | audio14 |
| 20000 | 21000 | 5 | 0.04 | 0.9865 | 0.0402 | 0.0592 | 100.0000 | audio14 |
| 18000 | 19600 | 4 | 0.08 | 0.9815 | 0.0157 | 0.0471 | 44.4444 | audio3 |
| 18000 | 19600 | 8 | 0.04 | 0.9074 | 0.0623 | 0.0737 | 160.0000 | audio3 |
| 18000 | 20500 | 6 | 0.08 | 0.9815 | 0.0424 | 0.0699 | 66.6667 | audio3 |
| 18000 | 20500 | 12 | 0.04 | 0.7685 | 0.0447 | 0.0558 | 240.0000 | audio3 |
| 20000 | 21000 | 2 | 0.08 | 0.8426 | 0.0141 | 0.0455 | 22.2222 | audio3 |
| 20000 | 21000 | 5 | 0.04 | 0.8426 | 0.0526 | 0.0709 | 100.0000 | audio3 |
| 18000 | 19600 | 4 | 0.08 | 0.5625 | 0.0633 | 0.0780 | 44.4444 | audio4 |
| 18000 | 19600 | 8 | 0.04 | 0.3750 | 0.0842 | 0.0851 | 160.0000 | audio4 |
| 18000 | 20500 | 6 | 0.08 | 0.4271 | 0.0775 | 0.0580 | 66.6667 | audio4 |
| 18000 | 20500 | 12 | 0.04 | 0.2500 | 0.1177 | 0.0722 | 240.0000 | audio4 |
| 20000 | 21000 | 2 | 0.08 | 0.5104 | 0.0718 | 0.0849 | 22.2222 | audio4 |
| 20000 | 21000 | 5 | 0.04 | 0.2917 | 0.0975 | 0.0936 | 100.0000 | audio4 |
| 18000 | 19600 | 4 | 0.08 | 0.7708 | 0.0258 | 0.0403 | 44.4444 | audio5 |
| 18000 | 19600 | 8 | 0.04 | 0.5625 | 0.0633 | 0.0651 | 160.0000 | audio5 |
| 18000 | 20500 | 6 | 0.08 | 0.6562 | 0.0599 | 0.0759 | 66.6667 | audio5 |
| 18000 | 20500 | 12 | 0.04 | 0.4271 | 0.1232 | 0.0619 | 240.0000 | audio5 |
| 20000 | 21000 | 2 | 0.08 | 0.7604 | 0.0472 | 0.0681 | 22.2222 | audio5 |

Table D.4: OFDM Results for All Transmitters, by Receiver (Table 2)

| $f_1$ **(Hz)** | $f_2$ **(Hz)** | $N$ | $T_{guard}(s)$ | $P_{sync}$ | $\mu_{errors}$ | $\sigma_{errors}$ | $R$ ($\frac{\textbf{bits}}{\textbf{sec}}$) | **Receiver** |
|---|---|---|---|---|---|---|---|---|
| 20000 | 21000 | 5 | 0.04 | 0.4479 | 0.0940 | 0.0794 | 100.0000 | audio5 |
| 18000 | 19600 | 4 | 0.08 | 0.5729 | 0.0398 | 0.0783 | 44.4444 | audio6 |
| 18000 | 19600 | 8 | 0.04 | 0.4792 | 0.0831 | 0.0774 | 160.0000 | audio6 |
| 18000 | 20500 | 6 | 0.08 | 0.4583 | 0.0424 | 0.0496 | 66.6667 | audio6 |
| 18000 | 20500 | 12 | 0.04 | 0.3542 | 0.1112 | 0.0652 | 240.0000 | audio6 |
| 20000 | 21000 | 2 | 0.08 | 0.5417 | 0.0558 | 0.0815 | 22.2222 | audio6 |
| 20000 | 21000 | 5 | 0.04 | 0.3229 | 0.0669 | 0.0990 | 100.0000 | audio6 |
| 18000 | 19600 | 4 | 0.08 | 0.9583 | 0.0214 | 0.0528 | 44.4444 | audio7 |
| 18000 | 19600 | 8 | 0.04 | 0.8438 | 0.0600 | 0.0691 | 160.0000 | audio7 |
| 18000 | 20500 | 6 | 0.08 | 0.8958 | 0.0269 | 0.0508 | 66.6667 | audio7 |
| 18000 | 20500 | 12 | 0.04 | 0.7500 | 0.0592 | 0.0753 | 240.0000 | audio7 |
| 20000 | 21000 | 2 | 0.08 | 0.8542 | 0.0034 | 0.0269 | 22.2222 | audio7 |
| 20000 | 21000 | 5 | 0.04 | 0.8542 | 0.0436 | 0.0587 | 100.0000 | audio7 |
| 18000 | 19600 | 4 | 0.08 | 0.9688 | 0.0279 | 0.0622 | 44.4444 | audio8 |
| 18000 | 19600 | 8 | 0.04 | 0.9479 | 0.0599 | 0.0608 | 160.0000 | audio8 |
| 18000 | 20500 | 6 | 0.08 | 0.9479 | 0.0417 | 0.0719 | 66.6667 | audio8 |
| 18000 | 20500 | 12 | 0.04 | 0.7188 | 0.0639 | 0.0606 | 240.0000 | audio8 |
| 20000 | 21000 | 2 | 0.08 | 0.7708 | 0.0265 | 0.0548 | 22.2222 | audio8 |
| 20000 | 21000 | 5 | 0.04 | 0.6458 | 0.1192 | 0.0846 | 100.0000 | audio8 |

# References


[1] The NetBSD packages collection: security/stegtunnel. URL ftp://ftp.netbsd.org/pub/pkgsrc/current/pkgsrc/security/stegtunnel/README.html. (Date last accessed: September 23, 2015).

[2] Common Criteria: Part 1: Introduction and general model, August 1999. URL https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v21.pdf. (Date last accessed: September 23, 2015).

[3] Common Criteris: Part 3: Security assurance components, August 2005. URL https://www.commoncriteriaportal.org/files/ccfiles/ccpart3v2.3.pdf. (Date last accessed: September 22, 2015).

[4] NSA's ANT division catalog of exploits for nearly every major software/hardware/firmware, 2013. URL http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/. (Date last accessed: September 18, 2015).

[5] Audio capture, 2016. URL https://developer.android.com/guide/topics/media/audio-capture.html. (Date last accessed: March 1, 2016).

[6] AVAudioSession, 2016. URL https://developer.apple.com/library/prerelease/ios/documentation/AVFoundation/Reference/AVAudioSession_ClassReference/index.html#//apple_ref/c/tdef/AVAudioSessionRecordPermission. (Date last accessed: March 1, 2016).

[7] S. H. Abdel-Aty. Approximate formulae for the percentage points and the probability integral of the non-central chi-square distribution. *Biometrika*, 41(3/4):538–540, 1954.

[8] Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matthew Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter G Neumann, Susan Landau, et al. Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 2015.

[9] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The EM sidechannel(s). In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 29–45. Springer, 2003.

[10] Kamran Ahsan and Deepa Kundur. Practical data hiding in TCP/IP. *Proc. Workshop on Multimedia Security at ACM Multimedia*, 2(7), 2002.

[11] Ahmed Al-Haiqi, Mahamod Ismail, and Rosdiadee Nordin. A new sensors-based covert channel on Android. *The Scientific World Journal*, 2014.

[12] James P Anderson. Computer security technology planning study. volume 2. Technical report, DTIC Document, 1972.

[13] R.J. Anderson and Fabien A.P. Petitcolas. On the limits of steganography. *Selected Areas in Communications, IEEE Journal on*, 16(4):474–481, May 1998.

[14] Ross Anderson. *Security engineering*. John Wiley & Sons, 2008.

[15] Ross Anderson, Serge Vaudenay, Bart Preneel, and Kaisa Nyberg. The Newton channel. In Ross Anderson, editor, *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 151–156. Springer Berlin Heidelberg, 1996. ISBN 978-3-540-61996-3.

[16] Ross Anderson, Mike Bond, Jolyon Clulow, and Sergei Skorobogatov. Cryptographic processors-a survey. *Proceedings of the IEEE*, 94(2):357–369, 2006.

[17] Ross J Anderson and Markus G Kuhn. Soft tempest–an opportunity for NATO. *Protecting NATO Information Systems in the 21st Century*, 1999.

[18] Simurgh Aryan, Homa Aryan, and J. Alex Halderman. Internet censorship in Iran: A first look. In *Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet*, Washington, D.C., 2013. USENIX.

[19] M. Backes, M. Durmuth, and D. Unruh. Compromising reflections-or-how to read LCD monitors around the corner. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 158–169, May 2008.

[20] M. Backes, Tongbo Chen, M. Duermuth, H. Lensch, and M. Welk. Tempest in a teapot: Compromising reflections revisited. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 315–327, May 2009.

[21] Ronald J Baken and Robert F Orlikoff. *Clinical measurement of speech and voice*. Cengage Learning, 2000.

[22] Dirk Balfanz, Diana K Smetters, Paul Stewart, and H Chi Wong. Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium*, 2002.

[23] B.A. Bash, D. Goeckel, and D. Towsley. Square root law for communication with low probability of detection on AWGN channels. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 448–452, July 2012.

[24] B.A. Bash, D. Goeckel, and D. Towsley. Limits of reliable communication with low probability of detection on AWGN channels. *Selected Areas in Communications, IEEE Journal on*, 31(9):1921–1930, September 2013.

[25] Boulat A. Bash, Dennis Goeckel, and Don Towsley. LPD communication when the warden does not know when. *CoRR*, abs/1403.1013, 2014. URL `http://arxiv.org/abs/1403.1013`.

[26] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Mark Felegyhazi. The cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, 4(4):971–1003, 2012.

[27] Krista Bennett. Linguistic steganography: Survey, analysis, and robustness concerns for hiding information in text, 2004.

[28] Eric Byres. The air gap: SCADA's enduring security myth. *Commun. ACM*, 56(8): 29–31, August 2013. ISSN 0001-0782.

[29] Serdar Cabuk. *Network Covert Channels: Design, Analysis, Detection, and Elimination*. PhD thesis, Purdue University, West Lafayette, IN, USA, 2006. AAI3260014.

[30] Serdar Cabuk, Carla E. Brodley, and Clay Shields. IP covert timing channels: Design and detection. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, pages 178–187, New York, NY, USA, 2004. ACM. ISBN 1-58113-961-6.

[31] Serdar Cabuk, Carla E. Brodley, and Clay Shields. IP covert timing channels: Design and detection. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*, CCS '04, pages 178–187, New York, NY, USA, 2004. ACM.

[32] Serdar Cabuk, Carla E. Brodley, and Clay Shields. IP covert channel detection. *ACM Trans. Inf. Syst. Secur.*, 12(4):22:1–22:29, April 2009. ISSN 1094-9224.

[33] Christian Cachin. An information-theoretic model for steganography. In *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 306–318. Springer Berlin Heidelberg, 1998.

[34] Brent Carrara. pyCovertAudio, 2016. URL `https://github.com/bcarr092/pyCovertAudio`. (Date last accessed: April 6, 2016).

[35] Brent Carrara, 2016. URL `http://www.site.uottawa.ca/~bcarr092/thesis/chapter6.py`. (Date last accessed: March 24, 2016).

[36] Brent Carrara, 2016. URL `http://www.site.uottawa.ca/~bcarr092/thesis/chapter7.py`. (Date last accessed: March 24, 2016).

[37] Brent Carrara, 2016. URL `http://www.site.uottawa.ca/~bcarr092/thesis/chapter8.py`. (Date last accessed: March 24, 2016).

[38] Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon. Image steganography and steganalysis: Concepts and practice. In *Digital Watermarking*, pages 35–49. Springer, 2004.

[39] Suresh Chari, Josyula R Rao, and Pankaj Rohatgi. Template attacks. In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 13–28. Springer, 2003.

[40] Pak Hou Che, M. Bakshi, and S. Jaggi. Reliable deniable communication: Hiding messages in noise. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2945–2949, July 2013.

[41] Pak Hou Che, M. Bakshi, Chung Chan, and S. Jaggi. Reliable, deniable and hidable communication. In *Information Theory and Applications Workshop (ITA), 2014*, pages 1–10, Feb 2014.

[42] Pak Hou Che, Mayank Bakshi, Chung Chan, and Sidharth Jaggi. Reliable deniable communication with channel uncertainty. In *Information Theory Workshop (ITW), 2014 IEEE*, pages 30–34, Nov 2014.

[43] Pak Hou Che, S. Kadhe, M. Bakshi, Chung Chan, S. Jaggi, and A. Sprintson. Reliable, deniable and hidable communication: A quick survey. In *Information Theory Workshop (ITW), 2014 IEEE*, pages 227–231, Nov 2014.

[44] Richard Clayton, StevenJ. Murdoch, and RobertN.M. Watson. Ignoring the Great Firewall of China. In George Danezis and Philippe Golle, editors, *Privacy Enhancing Technologies*, volume 4258 of *Lecture Notes in Computer Science*, pages 20–35. Springer Berlin Heidelberg, 2006. ISBN 978-3-540-68790-0.

[45] Alexander J Cohen, Edward KY Jung, Royce A Levien, Robert W Lord, Mark A Malamud, and John D Rinaldo Jr. Device pairing via device to device contact, April 12 2011. US Patent 7,925,022.

[46] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[47] Scott Craver. On public-key steganography in the presence of an active warden. In *Information Hiding*, pages 355–368. Springer, 1998.

[48] Scott Craver, Enping Li, Jun Yu, and Idris Atakli. A supraliminal channel in a videoconferencing application. In Kaushal Solanki, Kenneth Sullivan, and Upamanyu Madhow, editors, *Information Hiding*, volume 5284 of *Lecture Notes in Computer Science*, pages 283–293. Springer Berlin Heidelberg, 2008. ISBN 978-3-540-88960-1.

[49] Joan Daemen and Vincent Rijmen. AES proposal: Rijndael, 1998.

[50] daemon9. Project Loki, August 1996. URL `http://phrack.org/issues/49/6.html#article`. (Date last accessed: September 23, 2015).

[51] R. deGraaf, J. Aycock, and M. Jacobson. Improved port knocking with strong authentication. In *Computer Security Applications Conference, 21st Annual*, pages 10 pp.–462, Dec 2005.

[52] Department of Electronics and Information Technology. Draft national encryption policy, 2015. URL `http://deity.gov.in/sites/upload_files/dit/files/draft%20Encryption%20Policyv1.pdf`. (Date last accessed: October 1, 2015).

[53] Luke Deshotels. Inaudible sound as a covert channel in mobile devices. In *Proceedings of the 8th USENIX Conference on Offensive Technologies*, WOOT'14, pages 16–16, Berkeley, CA, USA, 2014. USENIX Association.

[54] David Dittrich. The "stacheldraht" distributed denial of service attack tool, December 1999. URL `https://staff.washington.edu/dittrich/misc/stacheldraht.analysis`. (Date last accessed: September 23, 2015).

[55] Natacha Domingues, Joao Lacerda, Pedro M.Q. Aguiar, and Cristina V. Lopes. Aerial communications using piano, clarinet, and bells. In *Multimedia Signal Processing, 2002 IEEE Workshop on*, pages 460–463. IEEE, Dec 2002.

[56] Shiwei Dong, Xu Jiadong, Haobin Zhang, and Wu Changying. On compromising emanations from computer vdu and its interception. In *Electromagnetic Compatibility, 2002 3rd International Symposium on*, pages 692–695. IEEE, May 2002.

[57] Allen B Downey. *Think Complexity: Complexity Science and Computational Modeling*. O'Reilly Media, Inc., 2012.

[58] Margaret M. Hilferty Edwin B. Wilson. The distribution of chi-square. *Proceedings of the National Academy of Sciences of the United States of America*, 17:684–688, December 1931.

[59] Fürkan Elibol, Uğur Sarac, and Işın Erer. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European*, pages 1767–1771. IEEE, Aug 2012.

[60] Robert J Ellison, John B Goodenough, Charles B Weinstock, and Carol Woody. Evaluating and mitigating software supply chain security risks. Technical report, DTIC Document, 2010.

[61] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32.Stuxnet Dossier. *White paper, Symantec Corp., Security Response*, 5, 2011.

[62] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32.Stuxnet dossier, February 2011. URL `https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf`. (Date last accessed: January 22, 2016).

[63] FBI National Press Office. Update on Sony investigation, December 2014. URL `https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation`. (Date last accessed: January 22, 2016).

[64] David Ferraiolo, D Richard Kuhn, and Ramaswamy Chandramouli. *Role-based access control*. Artech House, 2003.

[65] T. Filler and J. Fridrich. Complete characterization of perfectly secure stego-systems with mutually independent embedding operation. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, pages 1429–1432, April 2009.

[66] Tom Filler and Jessica Fridrich. Fisher information determines capacity of ε-secure steganography. In *Information Hiding*, Lecture Notes in Computer Science, pages 31–47. Springer Berlin Heidelberg, 2009.

[67] Tom Filler, Andrew D. Ker, and Jessica Fridrich. The square root law of steganographic capacity for markov covers. In *Proc. SPIE*, volume 7254, pages 725408–725408–11, 2009.

[68] D.V. Forte, C. Maruti, M.R. Vetturi, and M. Zambelli. SecSyslog: An approach to secure logging based on covert channels. In *Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on*, pages 248–263, Nov 2005.

[69] Igor Furgel. Security domain separation and business flexibility. In *9th International CC Conferenc*, September 2008.

[70] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 251–261. Springer Berlin Heidelberg, 2001. ISBN 978-3-540-42521-2.

[71] Matthias Gauger, Olga Saukh, and Pedro J. Marron. Enlighten me! Secure key assignment in wireless sensor networks. In *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, pages 246–255. IEEE, Oct 2009.

[72] Daniel Genkin, Adi Shamir, and Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. *IACR Cryptology ePrint Archive*, 2013:857, 2013.

[73] Vadim Gerasimov and Walter Bender. Things that talk: using sound for device-to-device and device-to-human communication. *IBM Systems Journal*, 39(3.4):530–546, 2000.

[74] S. Gianvecchio and Haining Wang. An entropy-based approach to detecting covert timing channels. *Dependable and Secure Computing, IEEE Transactions on*, 8(6): 785–797, Nov 2011.

[75] Christophe Giraud and Hugues Thiebeauld. A survey on fault attacks. In *Smart Card Research and Advanced Applications VI*, pages 159–176. Springer, 2004.

[76] C. G. Girling. Covert channels in LAN's. *IEEE Trans. Softw. Eng.*, 13(2):292–296, 1987.

[77] Virgil D Gligor. *A guide to understanding covert channel analysis of trusted systems*. National Computer Security Center, 1994.

[78] Joseph A Goguen and José Meseguer. Security policies and security models. In *2012 IEEE Symposium on Security and Privacy*, pages 11–11. IEEE Computer Society, 1982.

[79] James W. III Gray. On introducing noise into the bus-contention channel. In *Research in Security and Privacy, 1993. Proceedings., 1993 IEEE Computer Society Symposium on*, pages 90–98. IEEE, May 1993.

[80] James W. III Gray. Countermeasures and tradeoffs for a class of covert timing channels. Technical report, The Hong Kong University of Science and Technology, 1994. URL `http://repository.ust.hk/ir/Record/1783.1-25`. (Date last accessed: October 6, 2015).

[81] David Jeffrey Griffiths and Reed College. *Introduction to electrodynamics*, volume 3. Prentice hall Upper Saddle River, NJ, 1999.

[82] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici. AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*, pages 58–67, Oct 2014.

[83] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. GSMem: Data exfiltration from air-gapped computers over GSM frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 849–864, Washington, D.C., August 2015. USENIX Association. ISBN 978-1-931971-232.

[84] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations. *CoRR*, abs/1503.07919, 2015. URL `http://arxiv.org/abs/1503.07919`.

[85] J. T. Haigh, R. A. Kemmerer, J. Mchugh, and W. D. Young. An experience using two covert channel analysis techniques on a real system design. *IEEE Transactions on Software Engineering*, SE-13(2):157–168, Feb 1987.

[86] Tzipora Halevi and Nitesh Saxena. On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, pages 97–108, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0245-6.

[87] Mark Handley, Vern Paxson, and Christian Kreibich. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics. In *USENIX Security Symposium*, pages 115–131, 2001.

[88] George S Hanna, Robert J Higgins, John B Preston, and Daniel A Tealdi. Method and system for near-field wireless device pairing, August 3 2009. US Patent App. 12/534,246.

[89] Michael Hanspach and Michael Goetz. On covert acoustical mesh networks in air. *CoRR*, abs/1406.1213, 2014. URL `http://arxiv.org/abs/1406.1213`.

[90] Michael Hanspach and Michael Goetz. Recent developments in covert acoustical communications. In *Sicherheit*, pages 243–254, 2014.

[91] Michael Hanspach and Jörg Keller. On the implications, the identification and the mitigation of covert physical channels. In *9th Future Security 2014*, pages 563–570, 2014.

[92] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating systems. *Commun. ACM*, 19(8):461–471, August 1976. ISSN 0001-0782.

[93] Ragib Hasan, Nitesh Saxena, Tzipora Haleviz, Shams Zawoad, and Dustin Rinehart. Sensing-enabled channels for hard-to-detect command and control of mobile devices. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 469–480, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-1767-2.

[94] J. He and V.D. Gligor. Information-flow analysis for covert-channel identification in multilevel secure operating systems. In *Computer Security Foundations Workshop III, 1990. Proceedings*, pages 139–148. IEEE, Jun 1990.

[95] Harold Joseph Highland. The tempest over leaking computers. *Abacus*, 5(2):10–18, 1988.

[96] Zhang Hongxin, Huang Yuewang, Wang Jianxin, Lu Yinghua, and Zhang Jinling. Recognition of electro-magnetic leakage information from computer radiation with svm. *Computers & Security*, 28(1):72–76, 2009.

[97] Maarten Van Horenbeeck. Entity tags as an HTTP covert channel. URL `http://www.daemon.be/maarten/etagtunnel.html`. (Date last accessed: September 23, 2015).

[98] Jie Hou and Gerhard Kramer. Effective secrecy: Reliability, confusion and stealth. *CoRR*, abs/1311.1411, 2013. URL `http://arxiv.org/abs/1311.1411`.

[99] W.-M. Hu. Reducing timing channels with fuzzy time. In *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*, pages 8–20, May 1991.

[100] Wei-Ming Hu. Reducing timing channels with fuzzy time. *Journal of computer security*, 1(3):233–254, 1992.

[101] J. C. Huskamp. *Covert communication channels in timesharing systems*. PhD thesis, California Univ., Berkeley, 1978.

[102] P Jayaram, HR Ranganatha, and HS Anupama. Information hiding using audio steganography–a survey. *The International Journal of Multimedia & Its Applications (IJMA) Vol*, 3:86–96, 2011.

[103] E. Jones, O. Le Moigne, and J.-M. Robert. IP traceback solutions based on time to live covert channel. In *Networks, 2004. (ICON 2004). Proceedings. 12th IEEE International Conference on*, volume 2, pages 451–457 vol.2, Nov 2004.

[104] Dan Kaminsky. Attacking distributed systems: The DNS case study, 2004. URL `https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Kaminsky.pdf`. (Date last accessed: September 23, 2015).

[105] Myong H. Kang and Ira S. Moskowitz. A pump for rapid, reliable, secure communication. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 119–129, New York, NY, USA, 1993. ACM. ISBN 0-89791-629-8.

[106] P.A. Karger and J.C. Wray. Storage channels in disk arm optimization. In *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*, pages 52–61. IEEE Computer Society, May 1991.

[107] Kaspersky Labs. Gauss: Abnormal distribution, August 2012. URL `https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-lab-gauss.pdf`. (Date last accessed: September 17, 2015).

[108] Kaspersky Labs. A Fanny Equation: I am your father, Stuxnet, February 2015. URL `https://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/`. (Date last accessed: September 17, 2015).

[109] Kaspersky Labs. Equation Group: Questions and answers, February 2015. URL `https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf`. (Date last accessed: September 17, 2015).

[110] Richard A Kemmerer. Shared resource matrix methodology: An approach to identifying storage and timing channels. *ACM Transactions on Computer Systems (TOCS)*, 1(3):256–277, 1983.

[111] Richard A. Kemmerer and Phillip A. Porras. Covert flow trees: A visual approach to analyzing covert storage channels. *Software Engineering, IEEE Transactions on*, 17(11):1166–1185, 1991.

[112] Andrew D Ker. A capacity result for batch steganography. *Signal Processing Letters, IEEE*, 14(8):525–528, 2007.

[113] Andrew D. Ker. Estimating steganographic Fisher information in real images. In *Information Hiding*, volume 5806 of *Lecture Notes in Computer Science*, pages 73–88. Springer Berlin Heidelberg, 2009.

[114] Andrew D. Ker. The square root law requires a linear key. In *Proceedings of the 11th ACM Workshop on Multimedia and Security*, MM&Sec '09, pages 85–92. ACM, 2009.

[115] Andrew D. Ker. The square root law in stegosystems with imperfect information. In *Information Hiding*, volume 6387 of *Lecture Notes in Computer Science*, pages 145–160. Springer Berlin Heidelberg, 2010.

[116] Andrew D. Ker. The square root law does not require a linear key. In *Proceedings of the 12th ACM Workshop on Multimedia and Security*, MM&Sec '10, pages 213–224. ACM, 2010.

[117] Andrew D. Ker, Tomáš Pevný, Jan Kodovský, and Jessica Fridrich. The square root law of steganographic capacity. In *Proceedings of the 10th ACM Workshop on Multimedia and Security*, pages 107–116, 2008.

[118] Auguste Kerckhoffs. *La cryptographie militaire*, volume 9. 1 1883.

[119] Fouad Kiamilev, Ryan Hoover, Ray Delvecchio, Nicholas Waite, Stephen Janansky, Rodney McGee, Corey Lange, and Michael Stamat. Demonstration of hardware trojans. *DEFCON*, 16, 2008.

[120] Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang. Serial hook-ups: A comparative usability study of secure device pairing methods. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 10:1–10:12, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-736-3.

[121] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology CRYPTO 99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer Berlin Heidelberg, 1999. ISBN 978-3-540-66347-8.

[122] NE Köksaldı, SS Şeker, and B Sankur. Information extraction from the radiation of VDUs by pattern recognition methods. In *EMC'98: Electromagnetic Compatibility Conference*, pages 678–683, September 1998.

[123] Markus G. Kuhn. Electromagnetic eavesdropping risks of flat-panel displays. In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, pages 88–107. Springer Berlin Heidelberg, 2005. ISBN 978-3-540-26203-9.

[124] Markus G Kuhn. Eavesdropping attacks on computer displays. *Information Security Summit*, 2006.

[125] Markus G. Kuhn and Ross J. Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In *Information Hiding*, volume 1525 of *Lecture Notes in Computer Science*, pages 124–142, 1998.

[126] M.G. Kuhn. Optical time-domain eavesdropping risks of CRT displays. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, pages 3–18, 2002.

[127] Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. Caveat eptor: A comparative study of secure device pairing methods. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, pages 1–10. IEEE, March 2009.

[128] Butler W Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973.

[129] Ulf Landström. Noise and fatigue in working environments. *Environment International*, 16(4):471–476, 1990.

[130] Donald C Latham. Department of Defense trusted computer system evaluation criteria. *Department of Defense*, 1986.

[131] Eunchong Lee, Hyunsoo Kim, and Ji Won Yoon. *Information Security Applications: 16th International Workshop, WISA 2015, Jeju Island, Korea, August 20-22, 2015, Revised Selected Papers*, chapter Various Threat Models to Circumvent Air-Gapped Systems for Preventing Network Attack, pages 187–199. Springer International Publishing, Cham, 2016.

[132] Ki-Seung Lee and Richard V Cox. A very low bit rate speech coder based on a recognition/synthesis paradigm. *Speech and Audio Processing, IEEE Transactions on*, 9(5):482–491, 2001.

[133] Erich L Lehmann and Joseph P Romano. *Testing statistical hypotheses*. Springer, 2006.

[134] Michael LeMay and Jack Tan. Acoustic surveillance of physically unmodified PCs. In *Security and Management*, pages 328–334, 2006.

[135] Geert Leus and Paul A van Walree. Multiband OFDM for covert acoustic communications. *Selected Areas in Communications, IEEE Journal on*, 26(9):1662–1673, 2008.

[136] Enping Li and Scott Craver. A supraliminal channel in a wireless phone application. In *Proceedings of the 11th ACM Workshop on Multimedia and Security*, MM Sec '09, pages 151–154, New York, NY, USA, 2009. ACM. ISBN 978-1-60558-492-8.

[137] Yang Li, Kazuo Ohta, and Kazuo Sakiyama. New fault-based side-channel attack using fault sensitivity. *Information Forensics and Security, IEEE Transactions on*, 7(1):88–97, 2012.

[138] Michael Libes. Method and system for communication between two wireless-enabled devices, February 2002. US Patent App. 10/087,536.

[139] Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson. Trojan side-channels: Lightweight hardware trojans through side-channel engineering. In *Cryptographic Hardware and Embedded Systems-CHES 2009*, pages 382–395. Springer, 2009.

[140] Ulf Lindqvist and Erland Jonsson. A map of security risks associated with using COTS. *Computer*, 31(6):60–66, 1998.

[141] Jun Ling, Hao He, Jian Li, William Roberts, and Petre Stoica. Covert underwater acoustic communications. *The Journal of the Acoustical Society of America*, 128(5): 2898–2909, 2010.

[142] Lu Ling, Nie Yan, and Zhang Hongjin. The electromagnetic leakage and protection for computer. In *Electromagnetic Compatibility Proceedings, 1997 International Symposium on*, pages 378–382. IEEE, May 1997.

[143] Steven B. Lipner. A comment on the confinement problem. *SIGOPS Oper. Syst. Rev.*, 9(5):192–196, November 1975. ISSN 0163-5980.

[144] Keith Loepere. Resolving covert channels within a B2 class secure system. *ACM SIGOPS Operating Systems Review*, 19(3):9–28, 1985.

[145] Cristina V. Lopes and Pedro M.Q. Aguiar. Aerial acoustic communications. In *Applications of Signal Processing to Audio and Acoustics, 2001 IEEE Workshop on the*, pages 219–222. IEEE, 2001.

[146] Cristina Videira Lopes and Pedro M. Q. Aguiar. Alternatives to speech in low bit rate communication systems. *Computing Research Repository*, abs/1010.3951, 2010. URL `http://arxiv.org/abs/1010.3951`.

[147] Cristina Videira Lopes and Pedro M.Q. Aguiar. Acoustic modems for ubiquitous computing. *IEEE Pervasive Computing*, 2(3):62–71, 2003. ISSN 1536-1268.

[148] Joe Loughry and David A Umphress. Information leakage from optical emanations. *ACM Transactions on Information and System Security (TISSEC)*, 5(3):262–289, 2002.

[149] A. Madhavapeddy, R. Sharp, D. Scott, and A. Tse. Audio networking: the forgotten wireless technology. *Pervasive Computing, IEEE*, 4(3):55–60, July 2005.

[150] Anil Madhavapeddy, David Scott, and Richard Sharp. Context-aware computing with sound. In AnindK. Dey, Albrecht Schmidt, and JosephF. McCarthy, editors, *UbiComp 2003: Ubiquitous Computing*, volume 2864 of *Lecture Notes in Computer Science*, pages 315–332. Springer Berlin Heidelberg, 2003. ISBN 978-3-540-20301-8.

[151] Steve Mansfield-Devine. Security through isolation. *Computer Fraud & Security*, 2010(5):8 – 11, 2010. ISSN 1361-3723.

[152] Claudio Marforio, Hubert Ritzdorf, Aurélien Francillon, and Srdjan Capkun. Analysis of the communication between colluding applications on modern smartphones. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, pages 51–60, New York, NY, USA, 2012. ACM. ISBN 978-1-4503-1312-4.

[153] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (Sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 551–562, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0948-6.

[154] Ramya Jayaram Masti, Devendra Rai, Aanjhan Ranganathan, Christian Müller, Lothar Thiele, and Srdjan Capkun. Thermal covert channels on multi-core platforms. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 865–880, Washington, D.C., August 2015. USENIX Association. ISBN 978-1-931971-232.

[155] Wojciech Mazurczyk and Zbigniew Kotulski. New security and control protocol for VoIP based on steganography and digital watermarking. *CoRR*, abs/cs/0602042, 2006. URL `http://arxiv.org/abs/cs/0602042`.

[156] Wojciech Mazurczyk and Zbigniew Kotulski. New VoIP traffic security scheme with digital watermarking. In Janusz Grski, editor, *Computer Safety, Reliability, and Security*, volume 4166 of *Lecture Notes in Computer Science*, pages 170–181. Springer Berlin Heidelberg, 2006. ISBN 978-3-540-45762-6.

[157] Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. Seeing-is-believing: using camera phones for human-verifiable authentication. In *Security and Privacy, 2005 IEEE Symposium on*, pages 110–124. IEEE, May 2005.

[158] J McDermott. The B2/C3 problem: how big buffers overcome covert channel cynicism in trusted database systems. Technical report, DTIC Document, 1994.

[159] John McHugh. Covert channel analysis. In *A chapter of the handbook for the computer security certification of trusted systems*. Citeseer, 1995.

[160] Catherine Meadows and Ira S. Moskowitz. Covert channelsa context-based view. In Ross Anderson, editor, *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 73–93. Springer Berlin Heidelberg, 1996. ISBN 978-3-540-61996-3.

[161] P.M. Melliar-Smith and L.E. Moser. Protection against covert storage and timing channels. In *Computer Security Foundations Workshop IV, 1991. Proceedings*, pages 209–214. IEEE, Jun 1991.

[162] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 1996. ISBN 9781439821916.

[163] J. Millen. 20 years of covert channel modeling and analysis. In *Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on*, pages 113–114. IEEE, 1999.

[164] J.K. Millen. Finite-state noiseless covert channels. In *Computer Security Foundations Workshop II, 1989., Proceedings of the*, pages 81–86, Jun 1989.

[165] Jonathan K Millen. Security kernel validation in practice. *Communications of the ACM*, 19(5):243–250, 1976.

[166] Yisroel Mirsky, Mordechai Guri, and Yuval Elovici. Hvacker: Bridging the air-gap by manipulating the environment temperature, 2015. URL `https://deepsec.net/docs/Slides/2015/Bridging_the_Air-Gap_Data_Exfiltration_from_Air-Gap_%20Networks_-_Yisroel_Mirsky.pdf`. (Date last accessed: January 27, 2016).

[167] Ira S. Moskowitz and Myong H. Kang. Discussion of a statistical channel. In *Proceedings IEEE-IMS Workshop on Information Theory and Statistics, p. 95*. Press, 1994.

[168] Ira S Moskowitz and Allen R Miller. The channel capacity of a certain noisy timing channel. *Information Theory, IEEE Transactions on*, 38(4):1339–1344, 1992.

[169] Ira S. Moskowitz, Li Wu Chang, and Richard E. Newman. Capacity is the wrong paradigm. In *Proceedings of the 2002 Workshop on New Security Paradigms*, NSPW '02, pages 114–126, New York, NY, USA, 2002. ACM. ISBN 1-58113-598-X.

[170] Ira S Moskowitz, Richard E Newman, and Paul F Syverson. Quasi-anonymous channels. Technical report, DTIC Document, 2003.

[171] I.S. Moskowitz and M.H. Kang. Covert channels-here to stay? In *Computer Assurance, 1994. COMPASS '94 Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security. Proceedings of the Ninth Annual Conference on*, pages 235–243. IEEE, Jun 1994.

[172] I.S. Moskowitz and A.R. Miller. Simple timing channels. In *Research in Security and Privacy, 1994. Proceedings., 1994 IEEE Computer Society Symposium on*, pages 56–64. IEEE, May 1994.

[173] P. Moulin and J.A. O'Sullivan. Information-theoretic analysis of information hiding. *Information Theory, IEEE Transactions on*, 49(3):563–593, Mar 2003.

[174] Luke Muehlhauser. Jonathan Millen on covert channel communication, April 2014. URL `https://intelligence.org/2014/04/12/jonathan-millen/`. (Date last accessed: September 23, 2015).

[175] Steven J. Murdoch. Hot or not: Revealing hidden services by their clock skew. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 27–36, 2006.

[176] Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkat Padmanabhan, and Ramarathnam Venkatesan. Dhwani: Secure peer-to-peer acoustic nfc. *SIGCOMM Comput. Commun. Rev.*, 43(4):63–74, August 2013. ISSN 0146-4833.

[177] NetDocuments. File sizes and types, January 2014. URL `https://support.netdocuments.com/hc/en-us/articles/205219000-File-Sizes-and-Types`. (Date last accessed: April 4, 2016).

[178] Ed Novak, Yutao Tang, Zijiang Hao, Qun Li, and Yifan Zhang. Physical media covert channels on smart mobile devices. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '15, pages 367–378, New York, NY, USA, 2015. ACM. ISBN 978-1-4503-3574-4.

[179] Office of Communications, OPM. OPM announces steps to protect federal workers and others from cyber threats, July 2015. URL `https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/`. (Date last accessed: January 22, 2016).

[180] H. Okhravi, S. Bak, and S.T. King. Design, implementation and evaluation of covert channel attacks. In *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, pages 481–487, Nov 2010.

[181] Samuel Joseph OMalley and Kim-Kwang Raymond Choo. Bridging the air gap: Inaudible data exfiltration by insiders. In *20th Americas Conference on Information Systems (AMCIS 2014)*, 2014. To appear.

[182] Pai Peng, Peng Ning, and D.S. Reeves. On the secrecy of timing-based active watermarking trace-back techniques. In *Security and Privacy, 2006 IEEE Symposium on*, pages 15 pp.–349, May 2006.

[183] Toni Perković, Ivo Stančić, Luka Mališa, and Mario Čagalj. Multichannel protocols for user-friendly and scalable initialization of sensor networks. In *Security and Privacy in Communication Networks*, pages 228–247. Springer, 2009.

[184] Roger L Peterson, Rodger E Ziemer, and David E Borth. *Introduction to spread-spectrum communications*, volume 995. Prentice Hall New Jersey, 1995.

[185] Fabien AP Petitcolas, Ross J Anderson, and Markus G Kuhn. Information hiding-a survey. *Proceedings of the IEEE*, 87(7):1062–1078, 1999.

[186] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, August 2010. URL `http://dud.inf.tu-`

dresden.de/literatur/Anon_Terminology_v0.34.pdf. (Date last accessed: October 1, 2015).

[187] B. Pfitzmann. Information hiding terminology - results of an informal plenary meeting and additional proposals. In *Proceedings of the First International Workshop on Information Hiding*, pages 347–350, London, UK, UK, 1996. Springer-Verlag. ISBN 3-540-61996-8.

[188] J.G. Proakis and M. Salehi. *Fundamentals of Communication Systems*. Pearson Prentice Hall, 2005.

[189] John G Proakis. *Digital communications*. McGraw-Hill, New York, 2008.

[190] Huyu Qu, Qiang Cheng, and Ece Yaprak. Using covert channel to resist DoS attacks in WLAN. In *ICWN*, pages 38–44, 2005.

[191] Rahul Raguram, Andrew M. White, Dibyendusekhar Goswami, Fabian Monrose, and Jan-Michael Frahm. ispy: Automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 527–536, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0948-6.

[192] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial & Applied Mathematics*, 8(2):300–304, 1960.

[193] F. Rezaei, M. Hempel, P.L. Shrestha, S.M. Rakshit, and H. Sharif. Detecting covert timing channels using non-parametric statistical approaches. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*, pages 102–107, Aug 2015.

[194] Christopher Richardson. *Bridging the air gap: An information assurance perspective*. PhD thesis, University of Southampton, August 2012. URL http://eprints.soton.ac.uk/355926/.

[195] John Rinaldo, Royce Levien, Robert Lord, Alexander Cohen, Mark Malamud, Edward Jung, et al. Device pairing via human initiated contact, May 24 2005. US Patent App. 11/137,859.

[196] Rodrigo Roman and Javier Lopez. KeyLED - transmitting sensitive data over out-of-band channels in wireless sensor networks. In *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*, pages 796–801. IEEE, Sept 2008.

[197] Craig H. Rowland. Covert_tcp 1.0 - covert channel file transfer for linux, 1996. URL http://www-scf.usc.edu/~csci530l/downloads/covert_tcp.c. (Date last accessed: September 23, 2015).

[198] David Samyde, Sergei Skorobogatov, Ross Anderson, and Jean-Jacques Quisquater. On a new way to read data from memory. In *Security in Storage Workshop, 2002. Proceedings. First International IEEE*, pages 65–69. IEEE, Dec 2002.

[199] David E Sanger. Obama order sped up wave of cyberattacks against Iran, 2012. URL `http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html`. (Date last accessed: April 4, 2016).

[200] Nitesh Saxena, Md. Borhan Uddin, and Jonathan Voris. Universal device pairing using an auxiliary device. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, SOUPS '08, pages 56–67, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-276-4.

[201] Nitesh Saxena, Md Borhan Uddin, and Jonathan Voris. Treat'em like other devices: user authentication of multiple personal RFID tags. In *SOUPS*, volume 9, pages 1–1. Citeseer, 2009.

[202] Nitesh Saxena, J-E Ekberg, Kari Kostiainen, and N Asokan. Secure device pairing based on a visual channel: Design and usability study. *Information Forensics and Security, IEEE Transactions on*, 6(1):28–38, 2011.

[203] Marvin Schaefer, Barry Gold, Richard Linde, and John Scheid. Program confinement in KVM/370. In *Proceedings of the 1977 Annual Conference*, ACM '77, pages 404–410, New York, NY, USA, 1977. ACM. ISBN 978-1-4503-2308-6.

[204] Bruce Schneier. Air Gaps, 2013. URL `http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software://www.schneier.com/blog/archives/2013/10/air_gaps.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+feedburner%2FbDnSB+(Schneier+on+Security)`.

[205] Hidenori Sekiguchi. Measurement of radiated computer RGB signals. *Progress In Electromagnetics Research C*, 7:1–12, 2009.

[206] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, July 1948. ISSN 0005-8580. doi: 10.1002/j.1538-7305.1948.tb01338.x.

[207] Shiuh-Pyng Shieh and Arbee LP Chen. Estimating and measuring covert channel bandwidth in multilevel secure operating systems. *J. Inf. Sci. Eng.*, 15(1):91–106, 1999.

[208] R. Shirey. Internet security glossary, version 2. RFC 4949, RFC Editor, August 2007. URL `http://www.rfc-editor.org/rfc/rfc4949.txt`. `http://www.rfc-editor.org/rfc/rfc4949.txt`.

[209] Gustavus J. Simmons. The prisoners problem and the subliminal channel. In David Chaum, editor, *Advances in Cryptology*, pages 51–67. Springer US, 1984. ISBN 978-1-4684-4732-3.

[210] Gustavus J. Simmons. The subliminal channel and digital signatures. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology*, volume 209 of *Lecture Notes in Computer Science*, pages 364–378. Springer Berlin Heidelberg, 1985. ISBN 978-3-540-16076-2.

[211] Gustavus J. Simmons. Subliminal communication is easy using the DSA. In Tor Helleseth, editor, *Advances in Cryptology EUROCRYPT 93*, volume 765 of *Lecture Notes in Computer Science*, pages 218–232. Springer Berlin Heidelberg, 1994. ISBN 978-3-540-57600-6.

[212] Hitesh Singh, Pradeep Kumar Singh, and Kriti Saroha. A survey on text based steganography. In *Proceedings of the 3rd National Conference*, pages 3–9, 2009.

[213] Ronald William Smith. *On the Design of Network-based Covert Communication Systems*. PhD thesis, Royal Military College of Canada, 2007. AAINR29831.

[214] R.W. Smith and S.G. Knight. Predictable three-parameter design of network covert communication systems. *Information Forensics and Security, IEEE Transactions on*, 6(1):1–13, March 2011.

[215] R.W. Smith and G. Scott Knight. Predictable design of network-based covert communication systems. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 311–321, May 2008.

[216] Peter Smulders. The threat of information theft by reception of electromagnetic radiation from rs-232 cables. *Computers & Security*, 9(1):53–58, 1990.

[217] Taeshik Sohn, Jongsub Moon, Sangjin Lee, DongHoon Lee, and Jongin Lim. Covert channel detection in the ICMP payload using support vector machine. In Adnan Yazc and Cevat ener, editors, *Computer and Information Sciences - ISCIS 2003*, volume 2869 of *Lecture Notes in Computer Science*, pages 828–835. Springer Berlin Heidelberg, 2003. ISBN 978-3-540-20409-1.

[218] Taeshik Sohn, J Seo, and Jongsub Moon. A study on the covert channel detection of TCP/IP header using support vector machine. In *ICICS*, pages 313–324. Springer, 2003.

[219] Sang Hyuk Son, Ravi Mukkamala, and Rasikan David. Integrating security and real-time requirements using covert channel capacity. *Knowledge and Data Engineering, IEEE Transactions on*, 12(6):865–879, 2000.

[220] William Stallings. *Network security essentials: applications and standards*. Pearson Education India, 2007.

[221] Daniel Stødle. Ping tunnel, September 2011. URL `http://www.cs.uit.no/~daniels/PingTunnel/`. (Date last accessed: September 23, 2015).

[222] Ahren Studer, Timothy Passaro, and Lujo Bauer. Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11, pages 333–342, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0672-0.

[223] V. Subramanian, S. Uluagac, H. Cam, and R. Beyah. Examining the characteristics and implications of sensor side channels. In *Communications (ICC), 2013 IEEE International Conference on*, pages 2205–2210, June 2013.

[224] Symantec Corporation. PrettyPark.Worm, February 2007. URL `https://www.symantec.com/security_response/writeup.jsp?docid=2000-121508-3334-99`. (Date last accessed: September 23, 2015).

[225] Symantec Corporation. Internet security threat report, 2014, April 2014. URL `https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf`. (Date last accessed: January 22, 2016).

[226] Peter Szor. *The art of computer virus research and defense*. Pearson Education, 2005.

[227] Hidema Tanaka. Information leakage via electromagnetic emanations and evaluation of tempest countermeasures. In *Information Systems Security*, pages 167–179. Springer, 2007.

[228] Hidema Tanaka, Osamu Takizawa, and Akihiro Yamamura. Evaluation and improvement of the tempest fonts. In *Information security applications*, pages 457–469. Springer, 2005.

[229] Target Corporation. Target confirms unauthorized access to payment card data in US stores, December 2013. URL `https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car`. (Date last accessed: January 22, 2016).

[230] David W. Tempest. *The noise handbook*. Academic Pr, November 1985.

[231] Don Torrieri. *Principles of spread-spectrum communication systems*. Springer, 2015.

[232] Eran Tromer. Acoustic cryptanalysis: on nosy people and noisy machines. *Eurocrypt2004 Rump Session, May*, 2004.

[233] Eran Tromer. *Hardware-based cryptanalysis*. PhD thesis, Weizmann Institute of Science, Tese de Doutorado, 2007. URL `http://www.tau.ac.il/~tromer/papers/tromer-phd.pdf`. (Date last accessed: October 20, 2015).

[234] Jonathan T Trostle. Modelling a fuzzy time system. *Journal of Computer Security*, 2(4):291–309, 1993.

[235] C.-R. Tsai and V.D. Gligor. A bandwidth computation model for covert storage channels and its applications. In *Security and Privacy, 1988. Proceedings., 1988 IEEE Symposium on*, pages 108–121, Apr 1988.

[236] C-R Tsai, Virgil D. Gligor, and C. Sekar Chandersekaran. On the identification of covert storage channels in secure systems. *Software Engineering, IEEE Transactions on*, 16(6):569–580, 1990.

[237] Harry Urkowitz. Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55(4):523–531, April 1967.

[238] Wim Van Eck. Electromagnetic radiation from video display units: an eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

[239] Paul A van Walree, Thorsten Ludwig, Connie Solberg, Erland Sangfelt, Arto Laine, Giacomo Bertolotto, and Anders Ishøy. UUV covert acoustic communications. In *Proceedings of the 3rd conference on Underwater Acoustic Measurements: Technologies and Results*, 2009.

[240] Serge Vaudenay. Secure communications over insecure channels based on short authenticated strings. In Victor Shoup, editor, *Advances in Cryptology CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 309–326. Springer Berlin Heidelberg, 2005. ISBN 978-3-540-28114-6.

[241] Ligong Wang, Gregory W. Wornell, and Lizhong Zheng. Fundamental limits of communication with low probability of detection. *CoRR*, abs/1506.03236, 2015.

[242] Ying Wang and P. Moulin. Perfectly secure steganography: Capacity, error exponents, and code constructions. *Information Theory, IEEE Transactions on*, 54(6): 2706–2722, June 2008.

[243] Zhenghong Wang and RubyB. Lee. New constructive approach to covert channel modeling and channel capacity estimation. In Jianying Zhou, Javier Lopez, RobertH. Deng, and Feng Bao, editors, *Information Security*, volume 3650 of *Lecture Notes in Computer Science*, pages 498–505. Springer Berlin Heidelberg, 2005. ISBN 978-3-540-29001-8.

[244] Steffen Wendzel, Sebastian Zander, Bernhard Fechner, and Christian Herdin. A pattern-based survey and categorization of network covert channel techniques. *CoRR*, abs/1406.2901, 2014. URL `http://arxiv.org/abs/1406.2901`.

[245] Wikipedia. Bump (application), 2014. URL `https://en.wikipedia.org/wiki/Bump_(application)`.

[246] John C Wray. An analysis of covert timing channels. *Journal of Computer Security*, 1(3):219–232, 1992.

[247] Zhenyu Wu, Zhang Xu, and Haining Wang. Whispers in the hyper-space: High-speed covert channel attacks in the cloud. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*, pages 159–173, Bellevue, WA, 2012. USENIX. ISBN 978-931971-95-9.

[248] A.D. Wyner. The wire-tap channel. *Bell System Technical Journal, The*, 54(8): 1355–1387, Oct 1975.

[249] Sebastian Zander. *Performance of selected noisy covert channels and their countermeasures in IP networks*. PhD thesis, Swinburne University of Technology Melbourne, 2010.

[250] Sebastian Zander, Grenville J Armitage, and Philip Branch. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys and Tutorials*, 9(1-4):44–57, 2007.

[251] Sebastian Zander, Philip Branch, and Grenville Armitage. Capacity of temperature-based covert channels. *Communications Letters, IEEE*, 15(1):82–84, 2011.

[252] Kim Zetter. FAA: Boeings new 787 may be vulnerable to hacker attack, 2008. URL `http://www.wired.com/2008/01/dreamliner-security/`. (Date last accessed: April 4, 2016).

[253] Kim Zetter. NSA hacker chief explains how to keep him out of your system, January 2016. URL `http://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/`. (Date last accessed: February 5, 2016).

[254] Yong Bin Zhou and Deng Guo Feng. Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing. *IACR Cryptology ePrint Archive*, 2005:388, 2005.