uOttawa

L'Université canadienne
Canada's university

t

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTOCTORALES

uOttawa

L'Université canadienne
Canada's university

FACULTY OF GRADUATE AND POSDOCTORAL STUDIES

Ilker Onat
AUTEUR DE LA THÈSE / AUTHOR OF THESIS

M.A.Sc. (Electrical and Computer Engineering)
GRADE / DEGREE

School of Information Technology and Engineering
FACULTÉ, ÉCOLE, DÉPARTEMENT / FACULTY, SCHOOL, DEPARTMENT

Secure and Efficient Cross-Layer Techniques for Low-Power Wireless Embedded Systems
TITRE DE LA THÈSE / TITLE OF THESIS

Ali Miri
DIRECTEUR (DIRECTRICE) DE LA THÈSE / THESIS SUPERVISOR

CO-DIRECTEUR (CO-DIRECTRICE) DE LA THÈSE / THESIS CO-SUPERVISOR

ChangCheng Huang

Ahmed Karmouch

Shervin Shirmohammadi

Amr Youssef
Concordia University

Gary W. Slater
Le Doyen de la Faculté des études supérieures et postdoctorales / Dean of the Faculty of Graduate and Postdoctoral Studies

Secure and Efficient Cross-Layer Techniques For Low-Power Wireless Embedded Systems

by

Ilker Onat

A thesis submitted to the

Faculty of Graduate and Postdoctoral Studies

in partial fulfillment of the requirements

for the Ph.D. degree in

Electrical and Computer Engineering

School of Information Technology and Engineering

Faculty of Engineering

University of Ottawa

Your file Votre référence
ISBN: 978-0-494-79677-1
Our file Notre référence
ISBN: 978-0-494-79677-1

Abstract

Energy efficiency is playing a major role in the proliferation of low-power wireless sensing and identification systems. Hardware, firmware and communication protocol design processes of such systems are becoming increasingly adapt to low-power techniques enhancing the device lifetime, range, and efficiency. This thesis focuses on the cross-layer security and medium access techniques for low-power wireless embedded devices. Layer interactions in these systems are pointed out and algorithms taking advantage of these interactions are proposed.

To improve the security of stationary systems, anomaly detection based algorithms can be used with various parameters at different layers. We introduce two distributed anomaly detection based security algorithms for wireless sensor networks, using the physical layer signal characteristics and network layer arrival patterns. By analyzing the received packet features at different layers, a node can effectively identify an intruder impersonating a legitimate neighbor.

In a wireless sensor node, the radio is the main energy spending component. To limit energy consumption, wireless sensor nodes are periodically waken up and put to sleep. This duty-cycling operation still constitutes the major energy drain for battery powered wireless sensor architectures. Duty-cycling also imposes major constraints on the medium access and network layer operations of sensor nodes. We propose a hardware based solution in which an RFID wakeup system eliminates the duty-cycling completely from sensor operations using a boosting circuit and a low-threshold rectifier. This solution

removes the burden of duty-cycling on the upper layers with a physical layer approach.

Efficiency of RFID systems can be improved with smart slot selection algorithms in MAC layer for slotted ALOHA based MAC protocols. We introduce a MAC scheme where tags select their transmission slot based on their distance from the reader which is deduced by the received power levels. Slotted ALOHA based RFID MAC algorithms achieve smallest total reading time when, at each reading round, the frame length is set equal to the actual number of remaining unread tags. We present an a posteriori tag count estimation algorithm for these RFID MAC protocols from the collision statistics of the previous reading round.

Acknowledgements

I am grateful to my supervisor Professor Ali Miri for his guidance and support. I would like to thank the other members of my committee for their valuable comments. I would also like to thank my wife Furuzan for her continuous support. Thanks to my parents, my sister, and my parents-in-law for their love and support.

Füruzan'a

Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Explanation
ACK	Acknowledgement
AES	Advanced Encryption Standard
CMOS	Complementary Metal Oxide Semiconductor
DiSEL	Distance Based Slot Selection
DPA	Differential Power Analysis
ECC	Elliptic Curve Cryptography
ECN	Explicit Congestion Notification
EIRP	Effective Isotropically Radiated Power
EMA	Electromagnetic Analysis
HDR	High Data Rate
IC	Integrated Circuit
ID	Intrusion Detection
IP	Intellectual Property
LAN	Local Area Network
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MCU	Microcontroller

QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
SNR	Signal-to-Noise Ratio
SPA	Simple Power Analysis
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UHF	Ultra High Frequency
WPAN	Wireless Personal Area Networks
WSN	Wireless Sensor Network

Chapter 1

Introduction

1.1 Research Motivation

Low-power wireless electronics is on its way to revolutionize environment monitoring and industrial instrumentation. The use of embedded systems is a ubiquitous part of our daily life, from simple devices such as alarm clocks to more complex gadgets like cell phones. In the near future, these systems will be enhanced to create intelligent environments responding to ambient conditions. The number of networked embedded systems is growing in environment monitoring, health care systems and smart spaces. Such networks usually consist of large number of nodes organizing themselves into multihop wireless networks. Although labeled with a general title, embedded systems vary greatly in complexity, resources, connectivity and security requirements. They can be designed to perform only a few tasks occasionally during their whole lifetime with small batteries or they can be

real-time systems with intense computational tasks controlling very important tools and processes that require high levels of speed and security. In this thesis, we concentrate on the cross-layer design aspects of very low-power and short-range embedded wireless systems, namely, passive and active radio-frequency identification (RFID) devices and wireless sensor network (WSN) nodes. The differences between wireless sensor nodes and RFID tags are getting less and less visible. In addition, there are now many implementations that use both technologies complementary to each other. Given the growing concerns of security and dependability, embedded system designers must pay greater attention to security in system design. Generally for the wireless embedded systems, specifically for the RFID systems, security and energy efficiency are the major obstacles to the proliferation of the application areas. Wireless communications is inherently more open to abuse and security flaws compared to wireline systems. Networked or not, security challenges for these low-power wireless devices are more serious because of their resource constraints.

In traditional layered design paradigm, each layer provides interfaces to neighboring layers and acts alone to perform its own tasks. This increases modularity, helps standardization and provides a framework for new designs and algorithms. Layers can independently choose their encapsulation schemes, packet lengths, headers and if necessary, error control and retransmission schemes. Protocols at different layers can be modified without affecting other layers as long as the interfaces are kept intact. Independency of each layer assumes that whatever happens at other layers, a specific layer has to

try its best to accomplish given tasks. Each layer has to be designed with built-in mechanisms to detect and act on the specific conditions, without receiving actual signals. On the other hand, layered design paradigm might sometimes end up in non-optimal designs because of the restricted functions of each layer that do not allow a joint optimum for the whole system. The independent operation of layers may also cause different sort of layer interactions which may have adverse effects on the performance. Such interactions are generally given the name *cross-layer interference.* An algorithm operating at a specific layer, or using the services of a specific layer may not function due to cross-layer interference. Layered design paradigm has other shortcomings as well. Diverse applications with different QoS needs may not be supported using the provisions of layered design paradigm alone.

Cross-layer design is a general term used for the design solutions seeking optimum solutions through different sorts of layer cooperation. Cross-layer design solutions include the coupling adjacent layers, joint optimization of layers and other sorts of cooperative resource management techniques. In most cases, cross-layer design solutions require exchange of information such as measurements or statistics not provisioned in the layered design paradigm.

Layered design paradigm needs modifications especially in the face of growing wireless communications area. In general, wireless applications has to work in the capacity-limited broadcast communications medium with fast time-varying channels and high error rates. There are also growing number of heterogeneous applications in wireless networks with

strict constraints which change the design principles across all layers. Strictly layered design methods can be especially limiting for low-power wireless embedded systems because of their limited resources dedicated to each layer.

1.2 Research Contributions and Thesis Outline

In Chapter-2 we give an overview of cross-layer design techniques and a background study on the specific needs of wireless low-power embedded systems that can benefit from them. We analyze general properties and system design parameters of the wireless sensor and RFID systems from the medium access and security perspective.

1.2.1 Anomaly Detection Using Physical Layer Signal Characteristics

Traditional symmetric and asymmetric key based cryptographic security solutions are difficult to apply to large scale and low-power wireless systems where key management is a challenge. Anomaly detection based security algorithms are designed with the goal of detecting unusual data or behavior patterns that do not conform the established system normals. Compared to the cryptographic solutions, anomaly detection based cross-layer security algorithms can be more easily implemented in resource constrained environments. They can be applied using various parameters at different layers in stationary systems. In Chapter-3 we present such a security scheme [54] for wireless sensor net-

works, using the physical layer signal characteristics. We introduce a novel dynamic, distributed and learning algorithm to detect anomalies in received signal characteristics. We show that by looking at the received packet features at different layers, a node can effectively identify an intruder impersonating a legitimate neighbor. The introduced detection algorithm is distributed and immune to instantaneous measurement spikes since it raises alarm flags if the deviations of short term statistics from the long term statistics are persistent over the event log.

1.2.2 Network Layer Traffic Anomaly Detection

Sensor network traffic models, especially the variations experienced by a single node is a new area of research since there are not many practical and widely used sensor network deployments yet. Another reason for difficulty is the dynamic and unpredictable nature of sensor network traffic even if they have low packet rates. In Chapter-3 we also present a security algorithm [55] to detect packet arrival rate anomalies. We first introduce a new arrival model for the traffic that can be received by a sensor node and devise a scheme to detect anomalous changes in this arrival process. Our detection algorithm keeps short-term dynamic statistics using a multi-level, sliding window event storage scheme. In this algorithm, arrival processes at different time scales are compared using node resourcewise computable, low-complexity, aggregate features.

1.2.3 Elimination of Duty-Cycling for Embedded Wireless Radios

Battery powered low-power wireless radios used in sensor nodes must mostly be in sleep mode and periodically waken up to detect wireless transmissions. This operation is called the *duty-cycling* of the sensor radio. In Chapter-4 we detail an RFID wakeup system to eliminate the energy draining duty-cycling operation. We aim at collecting enough energy from the RF signal emitted from the regular low-power sensor radios capable of occasional high power burst transfers. We introduce a boosting circuit and a low-threshold Schottky diode based rectifier for this goal. We demonstrate that a passive resonant voltage boosting circuit and the rectifier system can wake up a sensor radio thereby eliminating the need for the duty-cycling process for wireless sensor nodes. The cross-layer aspect of this work is the elimination of the constraints imposed by duty-cycling on medium access and networking layers by a physical layer solution.

1.2.4 Distance Based Slot Selection for RFID MAC Protocols

One of the major design problems in RFID systems is an efficient tag reading scheme minimizing both the number of collisions and the total reading time of all the tags in range. In Chapter-5 we first summarize the challenges of medium access control in passive RFID systems. We then introduce a new MAC protocol for passive RFID systems [57]. The protocol is designed as an enhancement to framed slotted ALOHA MAC protocols in which tags randomly select a slot number on a given frame size. We show

that the completely random slot selection in framed slotted ALOHA systems is not the optimum approach to the slot selection problem. To minimize the collision probability, our protocol, uses a cross-layer approach for tags to select the most appropriate time slot in a given frame. Tags use the maximum and minimum received power levels of the reader-tag communications to choose a slot number. We test our algorithm under various tag deployment and density scenarios and show that it decreases the tag collision probability in both random uniform and evenly spaced dense tag deployments.

1.2.5 Tag Count Estimation in RFID MAC Protocols

The performance of RFID MAC algorithms is expressed in terms of the total time it takes by a reader to read all the tags in the reading range. It is proven that this class of algorithms achieve smallest total reading time when, at each reading round, the frame length is set equal to the actual number of remaining unread tags. An important design challenge to increase the performance of this class of algorithms is to estimate the remaining tag count before each reading round. In Chapter-6 we introduce an a posteriori tag count estimation algorithm [53] for these RFID MAC protocols from the collision statistics of the previous reading round. We compare the algorithm with the optimum, lower bound and other a posteriori estimation algorithms and demonstrate its efficiency. The introduced algorithm also achieves a much smaller computational overhead compared to the other schemes in the literature.

Chapter-7 concludes the thesis with a summary and a discussion of possible future

work directions.

1.2.6 List of Publications

- Ilker Onat and Ali Miri, A tag count estimation algorithm for dynamic framed ALOHA based RFID MAC protocols, submitted to Pervasive and Mobile Computing Journal, Elsevier

- Ilker Onat and Ali Miri, RFID Standards, to appear in Advanced Security and Privacy for RFID Technologies, 2010

- Ilker Onat and Ali Miri, RFID Wireless Link Threats, to appear in Advanced Security and Privacy for RFID Technologies, 2010

- Ilker Onat and Ali Miri, Designing Secure Wireless Embedded Systems, Security in RFID and Sensor Networks, Auerbach Publications, Taylor & Francis Group, 2008

- Ilker Onat and Ali Miri, DiSEL: A Distance Based Slot Selection Protocol for Framed Slotted ALOHA RFID Systems, in the Proceedings of IEEE Wireless Communications and Networking Conference, WCNC 2009

- Ilker Onat and Ali Miri, A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks, in the Proceedings of IEEE International Conference on Sensor Networks, SENET 2005.

- Ilker Onat and Ali Miri, An Intrusion Detection System for Wireless Sensor Networks, in the Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2005.

- Ilker Onat and Ali Miri, Securing Sensor Networks Using Anomaly Detection, in the Proceeding of Workshop on Critical Infrastructure Protection and Emergency Preparedness, Ottawa, Canada, December 2004

Chapter 2

Background

Small, low-power wireless devices are now an important part of our daily lives. Intelligent algorithms using system resources efficiently through information sharing and communication among system components can increase the capabilities of these devices for important system tasks such as networking, medium access control and security. Connectivity, especially in the wireless form, exposes embedded systems to attacks. The advances in microelectronics and integrated circuit (IC) technology increases the potential for incorporating elaborate protection algorithms while at the same time opening doors to new vulnerabilities. In this chapter we will first overview the vulnerabilities of wireless embedded systems and defense methods. We will then analyze the cross-layer design techniques to increase the system performance at different layers and for different system goals.

2.1 RFID and Wireless Sensor Systems

RFID and sensor technologies are getting integrated at two different contexts: At the application layer, sensing and identification applications are becoming increasingly interrelated and unified. At the hardware technology and architecture level, passive RFID methods of powering low-power radios are starting to be utilized to overcome the energy bottleneck of the ad-hoc wireless sensor network deployments. From many aspects, the individual sensor node and the RFID tag can be treated under the main title of *low-power wireless embedded device.* Security and energy efficiency are two essential pillars of design principles of these systems. Although design and operation principles are very simple, widespread use of embedded wireless technology comes with complex security and privacy issues. Sensitive health-monitoring tasks and biometric data use is growing in low-power wireless applications, hence the demand for dependable secure operation is increasing. New generation of RFID tags often include built-in sensing capabilities. Sensor network deployments for environmental monitoring and home applications are also starting to include RFID based unique identification means for data origin determination for sensory reportings where a global addressing structure is not in place. Integration of sensor networks to the global RFID database opens a wide area of applications. For example, any object to be identified with RFID technology can also transmit and relay context related information thereby changing the landscape for information gathering. With sensory additions, RFID systems bring context aware computation means to the logistics systems. However, as expected, the merge of these two technologies brings

new security and privacy challenges. With the improvements in complementary metal–oxide–semiconductor (CMOS) and other semiconductor technologies, main low-power sensor ICs, the radio and the microcontroller require a decreasing amount of power for the same distance communication and the same number of computations. This fact, combined with more efficient communication protocol stack and security schemes, makes the active and passive technologies increasingly similar.

2.1.1 Security of Wireless Sensor Networks

IEEE 802.15.4 [1] is the standard for low-rate, low-power Wireless Personal Area Networks (WPAN) that defines the physical and the medium access control layers. It supports 900 MHz and 2.4 GHz bands with data rates up to 250kb/s. ZigBee specification which is developed by the ZigBee industry alliance builds network and application layers on top of the 802.15.4 specified lower layers. 802.15.4 uses the Advanced Encryption Standard (AES) [21] in different modes to provide confidentiality and integrity. The AES has a very high theoretical security and is proven to be a good overall design for various architectures. In [45], software implementation of various block-ciphers are tested for their performance on an ultra low-power microcontroller. This study reveals that the overhead induced by AES may be high compared to other block ciphers in some microcontroller architectures. However, as the hardware implementation of AES is gaining popularity and it is a standard requirement for 802.15.4 compatible transceivers, AES will remain as the dominant security mechanism for WSN nodes for years to come. In

an AES enabled WSN, attacks often exploit the vulnerabilities in the embedded implementation of the algorithm.

2.1.2 Security of RFID Systems

An RFID system consists of two components: a transponder, or tag and a reader, or interrogator. The tag carries the actual data and is attached to the object to be identified. Tags can be passive or active. A passive tag obtains all of its energy for communications and data processing from the electric or magnetic field of the reader. An active tag on the other hand includes a battery. The general operation of a passive tag is given in Figure-2.1.

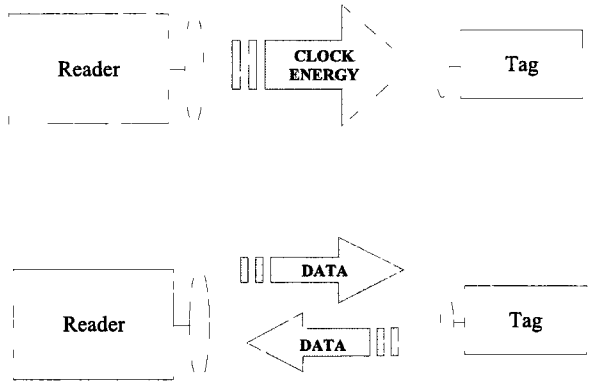

Figure 2.1: Passive tag communications

RFID systems are categorized according to fundamental operating principles, tag complexity, operating frequency, range and powering methods. According to hardware

complexity, RFID tags can be low-end, mid-range and high-end systems. Low-end systems are mostly low-cost, low-power one-bit transponders with no medium access control. Mid-range tags allow reading and writing on their memory. They can be addressed and they can support cryptographic security primitives. High-end tags such as smartcards allow complex authentication algorithms. Top-end smartcards carry cryptographic co-processors allowing complex calculations. There are three main physical operation types for RFID tags: inductive coupling, electromagnetic backscatter and close coupling.

Inductively coupled transponders receive energy from the reader generated strong electromagnetic field which passes through the transponder's coil area. This electromagnetic field induces a current proportional to its strength (decreasing with distance), the coil area and the number of windings, providing energy to the transponder. Majority of inductively coupled systems use either 30-300 kHz low frequency or 3-30 MHz high frequency ranges. They constitute about 90% of today's RFID systems [28]. Their range is less than 1 m. Inductively coupled systems use *load modulation* to transfer data from the transponder to the reader. A resonant transponder is a transponder with a self-resonant frequency same as the transmission frequency of the reader [28]. In load modulation, a resistor on a resonant transponder switched on and off according to data which effects the voltage across the reader and transmits data.

Electromagnetic backscatter transponders reflect back the electromagnetic waves created by the reader. The radiation power of the waves decreases with the square of the distance from the source, therefore a much weaker signal is returned to the reader by

the passive backscatter transponder. Increasing frequency increases reflectivity hence these transponders use ultra high frequency (UHF) range at 900 MHz or 2.4 GHz. Short wavelengths at these frequencies enable the construction of smaller antennas than the inductively coupled system coils. The UHF backscatter systems are also called long-range systems since they can transmit at up to 5 m apart from the reader.

Close coupling systems are powered through the magnetic field generated on the transponder coil when it is placed between the two windings of the reader carrying high frequency alternating current. The transponder can be coupled up to 1 cm away from the reader. The frequency used is usually less than 30 MHz. Close coupling is used in contactless smart cards which are common in secure identification systems.

Because of the very limited useful energy that can be converted and used at the passive transponders, they can send information only to very limited distances. *Active transponders* on the other hand, are very similar to WSN nodes with their activation methods being the only functional difference. A WSN node generally uses duty-cycling (put to sleep and waken up periodically to check for the incoming message) whereas an active RFID tag is activated the same way as passive tags. Since there is no duty-cycling, active tags have longer lifetimes compared to wireless sensor nodes. Active backscatter transponders have significantly higher ranges but their use is limited because of the maintenance and cost issues associated with battery use. The other transponder type is the *semi-passive transponders* which use battery to retain memory contents or to do data processing; their radio functions supplied power through the reader as in passive

readers.

In any system, security is a function of available system resources. Providing security in the light of very limited system resources is the main design challenge for low-power wireless embedded devices which is the topic of this study.

Security and privacy breaches such as unauthorized reading and writing of the RFID tags can cause a wide range of problems from small monetary losses for the retailers to major disruptions in the supply chain [58]. In many cases, the data contained in an RFID tag should be protected against unauthorized reading. This privacy problem is especially important for the RFID systems storing biometric data for authentication such as RFID enabled passports. With the growing number of such sensitive fields, security issues surrounding the RFID technology have become a major concern. RFID systems' security also depend on the bigger picture. Other components of the system such as the database management system and middleware also have to be designed securely. The information derived from the tags has to be safely processed and transferred to processing centers. However, in this thesis we concentrate only on the embedded device level security issues.

Different RFID technologies come with different problems and require different solutions. Device capabilities and available energy determines the use of security algorithms. In general, when security is concerned, the generalizations should clearly specify the target sub-area. As a general rule, short range systems can provide more power to transponders hence complicated security algorithms can be implemented. Low power usage at

the transponder increases the range of passive RFID systems. Higher transmit power, increased antenna gain are the other factors effecting the range of an RFID system. If an RFID system has a higher range, it can be powered from far, thus can be read from far. The problem is also partly due to the fact that in long range backscatter systems the power at the tag is very limited and it is a challenge to use full-scale cryptographic primitives on a general-purpose microcontroller powered by RF energy. Authentication and encryption operations, even in their simplest versions, require the capabilities of a microcontroller, hence when such algorithms are implemented at a tag, enough energy has to be transmitted to power the microcontroller running these algorithms.

It is not possible to talk about an operating system or a security software in RFID systems. Both devices merely contain communications and encryption units. However, even bare bone cryptography can be a challenge for RFID devices. Mainly because of the technology oriented power limitation and application oriented cost constraints, RFID tags usually contain a few thousand logic gates as computation elements. Especially in the case of UHF backscatter tags, until recently, it was not possible to equip them even with very low-power microcontrollers that will perform cryptographic operations. Many lightweight and minimalist protocols are proposed for this resource constrained environment [6, 17, 62, 63]. Recent studies such as [11] demonstrated the use of conventional strong cryptographic algorithms on a UHF RFID tag. Ultimately, the use of microcontrollers in the UHF tags is an efficient rectifier design problem, that is able to collect and supply enough power to tag's microelectronic circuit and the ultra low-power micro-

controller. All RFID devices contain non-volatile memory in various forms. The unique identifiers of RFID tags are stored using non-volatile memory. In addition, all the embedded code, including network stack and security algorithms also have to be stored in the non-volatile memory. Therefore, elaborate security algorithms increase the size of non-volatile memory. Security solutions also require volatile memory tied to processor usage.

In [70] authors explain and demonstrate the possibility of application layer malware for RFID systems that was thought to threaten only more capable higher level systems. RFID viruses and worms, and other attacks such as sniffing, tracking, spoofing, replay and denial of service create important vulnerabilities for RFID systems.

2.1.3 Component Selection for Secure Wireless Embedded Systems

The security of an embedded system as a whole is strongly dependent upon its subcomponents, hence it is important to select proper building blocks. Main building blocks of an embedded system are various generic or Intellectual Property (IP) based IC subsystems, mostly designed by other companies. The hardware and software security vulnerabilities of these components have direct effects on the whole embedded system security. Here we give a general characteristics of the components that are vital for the security of low-power wireless embedded systems.

Secure Embedded Microcontrollers

Other than very simple RFID systems that operate with a few thousand logic gates, most wireless embedded systems contain a general purpose microcontroller as the main computational element.

Many protection schemes such as voltage sensors, clock speed sensors, light sensors, metal layers, bus encryption and password protection are used in high-end processors [2]. For secure computation in general purpose processors operating at resource constrained environments, dedicated hardware is the preferred solution since it can achieve better performance with lower energy consumption. Hence, at the low-end market, cryptoprocessors are generally implemented as crypto co-processors in microcontrollers. Crypto co-processors and pseudo-random number generators decrease the power consumption and increase the speed of cryptographic operations. An embedded crypto co-processor is a tamper resistant processor that performs requested cryptographic operations using protected secrets. They are used in various applications requiring different levels of security. They can also support on-board key generation. Unlike smart cards which are specifically designed to protect against most known attacks, the majority of low-cost, low-power microcontrollers offer only weak protection [36] [7]. However, low-cost microcontroller designs are increasingly adopting secure design features from high-end secure microcontrollers.

Low-end crypto co-processor are increasingly becoming a part of our everyday lives through low-power wireless devices and smart cards. AES crypto co-processors are now

implemented in all IEEE 802.15.4 compatible low-power sensor transceivers [24, 50, 80], various RFID devices and smart cards [27, 32, 52]. These co-processors are also used for digital signature and identification and can implement complex authentication and encryption schemes such as RSA and Elliptic Curve Cryptography (ECC) [4]. A processor for low-power application should have low energy consumption and should fit in small chip area. It should be low cost and at the same time be robust against attacks. Such a processor also needs flexibility for changing program size in terms of volatile and non-volatile memory capacity.

Microcontroller selection for WSN nodes and active RFID tags

The microcontrollers used in active wireless devices should also have additional enhanced features. Since long device life-time is the most important design goal, consuming low-power and providing various power-down modes are the most important features of a processor designed for such applications. There should also be enough memory space for network stack and security algorithms. The processor should also be low-cost, fast enough to execute time-critical tasks with a wide operating voltage range.

Duty-cycling operation In order to save energy, the low-power transceiver and processor of a battery powered sensor node have to be put into sleep (power-down) mode. The nodes wake up periodically and check the air for preamble. The periodic wakeup of the radio is the task of the processor. The periodic duty-cycling may be enforced synchronously in the subnet, in which case precise timing of the wakeups are necessary. To

provide such timing, a sleeping processor will need to keep its low-frequency clock (oscillator) running continuously. Therefore, low-jitter, low-frequency internal clock feature of a processor is essential. When a preamble is detected during the wakeup, a node wakes up with all peripherals and prepares to process the incoming packet stream. One of the main design decision in sensor network deployments is to build an efficient duty-cycling mechanism, that will provide maximum system lifetime while maintaining application requirements. In this context, the proper use of low-power modes and the programming API is also critical.

External Interrupts If there is no duty-cycling, external interrupts are used to wake up the node from the sleep state. The powered-down processor in this case is waken up with a general purpose pin interrupt. Low voltage level interrupt capability and fast wakeup from the power-down modes is an important feature for microcontrollers that will be used in WSN nodes. Fast wakeups also decrease current consumption [81].

Radio selection

Passive RFID circuits are simple transceivers that operate at short ranges. Depending on the applications, cost, frequency band, size and form should be decided. Some applications may require higher reliability and faster response. The design should be modified according to application requirements and the budget. Unlike the rather simple transceiver circuitry of the passive tags, active tags and sensor nodes use full-featured low-power radios. These transceivers have to satisfy following criteria:

Power consumption A transceiver operates in four major states: sleeping, listening, receiving and transmitting. In low-power WSN or active RFID transceivers, listening, receiving and transmitting modes consume similar amount of power, on the order of $10-15$ mA. In the IEEE 802.15.4 standard, transceivers spend most of their operational life in a sleep state; each device periodically wakes up and listens to the RF channel to determine whether a message is pending. This is done through the detection of a preamble. Since listening mode is as power consuming as transmitting and receiving, and it occurs periodically according to duty-cycle, it is the major energy drain for duty-cycled embedded designs. This is also referred to as idle listening.

Fast wakeup Whether duty-cycled or not, transceivers should leave sleep state as fast as possible to listening state so as not to miss further from the preamble.

Output power High output power improves connectivity, decreases error rate but also drains the batteries faster and may expose the network to outside. High output power also increases interference to other close frequency devices. According to application needs a suitable output power should be selected. *Programmable output power* feature of a transceiver can be used to adapt the radio to different network and connectivity setups either statically before the deployment or dynamically during the operations.

Protocol stack and standards A protocol stack consists of layers of abstraction. Each layer provides well-defined interfaces to neighboring layers and uses interfaces pro-

vided by them. Basically, a network protocol stack consists of four main layers: Physical, medium access control (MAC), network layer and application. If an IEEE 802.15.4 compliant radio is selected, physical and MAC layers embedded in the radio firmware can be readily used instead of developing, for example, an in house collision avoidance scheme. Configuration options can be use for creating different, standard topologies. In general, the abstraction IEEE 802.15.4 provides in addressing, framing, channel access, acknowledgements and security is valuable for flexible designs. Standards also enforce specific data rates, frequency and modulation schemes that increases interoperability of devices from different vendors.

2.2 Cross-Layer Design Approach

The protocols at different network layers designed to function independently may interfere constructively or destructively with each other. Joint dependency of the system performance on more than one variable may be different from the single dependencies and it may be unpredictable. A system can also be effected by the interacting algorithms at different layers [34, 74, 78, 79]. Cross-layer system design goals can be achieved by

- **Joint Design:** It can be defined as jointly designing multiple protocol layers. It can also be defined as smaller scale coupling of adjacent layers to increase performance. This definition suggests a layer synergy and a joint optimization for managing same resources cooperatively.

- **Information Exchange:** Cross-layer design can also be defined as the exchange of information between layers. This information is not the part of the interface provisioned in the layered design paradigm. Examples are the measurements (e.g., signal strength of the links), statistics (e.g., retransmission count of the MAC layer) or any other information that might help other layer operations.

In order not to complicate maintenance and incrementally improved future designs, cross-layer algorithm design should preserve the basic functional divisions of the protocol layers.

2.2.1 Cross-Layer Design Parameters in Low-Power Wireless Systems

General resource allocation solutions for multihop wireless networks naturally target multiple layers. At the application layer, increasing number of heterogeneous applications with different QoS constraints effect the design principles across all layers. Limitations imposed by the layered design rules have important effects on the capacity and performance of wireless networks. Hence, various cross-layer network optimization techniques are proposed for wireless networks. Wireless applications use capacity-limited broadcast communication medium with fast time-varying, high error rate and fading channels. Wireless links are unstable and have very high error rates compared to the wireline links. Wireless systems are also effected by high contention at the MAC layer. Optimal use of the broadcast channel by the MAC layer can be very complex and may require distributed solutions [47]. Optimization based approaches to the resource allo-

cation problems is studied in the context of TCP congestion control algorithms. These approaches are difficult to apply to wireless networks because of the time-varying links, user mobility, multi-path, shadowing effects. Wireless links have varying propagation delays and connection-level instabilities. Cross-layer network optimization solutions are also challenged by the increasing adaptation of heterogeneous networks where wireline and wireless devices co-exist. In general, cross-layer design solutions for wireless networks target a better adaptation of upper layers to varying link and network conditions. Designing algorithms with guaranteed minimum throughput under these conditions may be challenging in most cases. Various parameters that can be jointly used to improve the system performance in these challenging conditions are summarized as follows:

- Physical layer: transmit and receive power levels, modulation scheme, transient characteristics of the RF signals,
- MAC layer: Persistence and delay parameters, sleep-awake schedules,
- Network and upper layers: Packet types and reception rates, application dependent packet statistics.

2.2.2 Examples of Cross-Layer Techniques

Channel state dependent techniques

Channel state dependent techniques make use of the instantaneous channel state of users while making scheduling decisions. In these techniques, fast changes in channel

state are exploited to give users with good channel state higher priority. From the cross-layer design point of view, channel state, which is a parameter of physical layer, is propagated to upper layers. One main example of such a scheme is CDMA/High Data Rate (HDR) [5]. In CDMA/HDR the channel state is periodically measured by the user and sent to the basestation. By constantly reporting to the base station their instantaneous channel capacity, users in an HDR system help the smart scheduler at the basestation take advantage of channel variations by giving priority to users with instantaneously better channels.

Transmit power control

Transmit power has implications across almost all protocol layers. It effects error rate at physical layer. At the MAC layer, interference characteristics are heavily dependent on power level of the transmission. Transmit power also changes the topology for the network layer. Many energy efficiency techniques developed recently make use of the transmit power control for longer network lifetime. Joint decision making about the transmit power level is therefore a must for an optimum protocol stack design.

MAC and network layer communication

QoS improvements to the IEEE 802.11 wireless LAN protocol necessitates the communication between the MAC and network layers. The MAC protocol checks the type of the packet it received from the network layer and gives different priorities to data and control packets. The joint design of MAC and network layers is now a part of IEEE

802.11e standard where MAC layer treats the network layer packet according to preset priorities using queuing, scheduling and back-off mechanisms.

Routing based on different parameters other than topology

Traditionally, routing is a network layer task that is done using only topology information. New routing strategies taking into account node parameters such as remaining node energy, node transmission and processing capabilities, channel parameters and transmission energy efficiency considerations are examples of cross-layer design methods.

Wireless TCP and ECN

Wireless channels are much more lossy compared to wireline links. Since TCP is originally designed for wireline networks, the packet losses in wireless environment significantly degrades TCP throughput. In TCP, routers indicate congestion by dropping packets which forces sources to decrease their transmission rate. TCP cannot differentiate between congestion related losses and wireless channel related losses. Even the temporary bad channel states causes sharp congestion window reductions. Explicit Congestion Notification (ECN) is a method proposed to differentiate between congestion related losses and other losses [75]. If congestion is explicitly notified, senders will not mistakenly lower their transmission rate because of the temporary bad channel state or transmission errors. In this case drop reason is propagated to transport layer for different actions.

Side-Channel Attacks and Defenses

The increased capabilities of wireless embedded devices also facilitated the implementation of powerful embedded security algorithms. At the same time, a new class of attacks called side channel attacks are developed using the device level information leakage. Independent from the theoretical strength of the security algorithm, various type of side-channel information, not traditionally considered during algorithm design are now becoming weak links in the system design processes. A survey of side channel attacks against smart cards is given in [33]. Various studies [48,60,73] pointed out the vulnerabilities of AES against side-channel attacks. Sensor radios equipped with AES co-processors are therefore vulnerable to side channel attacks. Side channel attacks against low-power, low-cost devices are in general much more effective since the constraints prohibit the implementation of strong countermeasures [56].

Timing [9, 42, 72], Simple Power Analysis (SPA) [41], Differential Power Analysis (DPA) [13,43] and Electromagnetic Analysis (EMA) [68] attacks have the common feature of using information leaked at the physical device level to attack the application level security schemes. Recent successful power attacks revealed the vulnerabilities of various RFID system types. The study in [59] targets passive UHF backscatter tags and details a method of measuring the power consumed by a tag during computations. The implications of this vulnerability is the requirement to build tags with cryptographic properties resistant to such power analysis attacks, which increases their cost. The attack described in [36] targets UHF RFID devices equipped with AES co-processors. The countermea-

sures against these attacks also use the cross-layer information protection techniques like blinding of the emitted signals or the redundant operations at the upper layers.

2.3 Chapter Conclusions

Designing secure embedded systems is a challenge in resource constrained environments. Still it is possible to design dependable secure embedded systems if the various aspects of the design are in line with the secure design principles for embedded systems. In this chapter, we discussed the adaptation of the general design rules to resource constrained environments. We concentrated our discussion on the low-power, low-rate, short-range embedded systems. We also analyzed various techniques and algorithms that are developed against powerful attacks.

We overviewed the secure system design from both hardware and software perspective. Secure design today requires more than ever a holistic approach combining all abstraction layers around the same goal: energy-efficient system and communication security. Because of this, both software and hardware designs are increasingly becoming interrelated and dependent on each other. Ultimately, secure system design is a tradeoff between capital resources to be invested for security and the actual value of the systems being protected. With the widespread use of low-power wireless embedded systems in critical applications, security vulnerabilities are no longer trivial secondary concerns but major design challenges for both hardware and firmware designers.

Chapter 3

Cross-Layer Design for Network Security

A sensor node is a tiny and simple device with limited computational capability and broadcast power. Wireless sensor networks are generally provisioned to consist of a large number of inexpensive nodes reporting their data to a central, more capable sink node using multihop transmission. In general, it is assumed that sensors will be equipped with non-rechargeable batteries and will be left unattended after deployment. However, current and foreseeable future technology have put severe restraints on energy resources of sensor devices. Because long term operation of nodes with limited battery energy is the main design bottleneck of sensor networks, sensor network protocols have to be designed to operate with minimum resource utilization. Security solutions for sensor networks also have to be designed with the limited computational power, limited memory and limited

battery life of sensor nodes in mind.

In general, network security solutions can be grouped into two main categories: *prevention* based techniques and *detection* based techniques. Prevention techniques, such as encryption and authentication, are often the first line of defense against attacks. Detection based techniques aim at identifying and excluding the attacker after prevention based techniques fail. Detection techniques are divided into two major categories: *signature* detection and *anomaly* detection. Signature detection techniques match the known attack profiles with the current changes, whereas anomaly detection uses established normal profiles and detects unusual deviations from this *normal behavior*.

Prevention based techniques are vulnerable to wireless networking challenges. Shared broadcast medium, the possibility of passive listening and resource-limited network elements decrease the effectiveness of prevention mechanisms. The multihop nature of a network also necessitates additional trust requirements among the nodes and increases the vulnerabilities. Although wireless sensor networks have less complex routing requirements when compared to Mobile Ad Hoc Networks (MANETs), securing a sensor network as a whole with prevention based techniques is difficult because of the scalability problems and the computation, communication and storage overhead associated with these methods. There are numerous prevention based solutions for MANETs and wireless sensor networks. There are also a few recently proposed detection based mechanisms for MANETs that we will summarize in the related work subsection. Neither prevention and nor detection solutions of MANETs can be directly applied to wireless

sensor networks. We give more detail about the differences between MANETs and sensor networks affecting the security requirements next.

3.1 Anomaly Detection Using Physical Layer Signal Characteristics

In this work, we introduce a novel anomaly based intrusion detection method for wireless sensor networks suited to their simple and resource-limited nature. In many attacks against sensor networks, the first step for an attacker is to establish itself as a legitimate node within the network. Although sensor nodes have low computation and communication capabilities, they have specific properties such as their stable neighborhood information that allows for detection of anomalies for various variables. To make a sensor node capable of detecting an intruder a simple dynamic statistical model of the neighboring nodes is built in conjunction with a low-complexity detection algorithm by monitoring received packet power levels and arrival rates. We show that such characteristics can be exploited to provide security to large scale sensor networks. The anomalies may present themselves at many different network layers. As long as the implementation is resource-aware, any layer may determine the normals of layer variables and trigger the intrusion alarms for abnormal deviations.

3.1.1 Motivation

Although wireless sensor networks belong to the general family of wireless ad hoc networks, they have their own distinctive features. The main differences between the MANETs and sensor networks from the security viewpoint can be summarized under the following titles:

- **Simpler device characteristics:** Sensor nodes are small and inexpensive devices with restricted transmit power (short range) and energy supplies. Due to low computation and communication capabilities authentication and encryption based security solutions are difficult to implement in a large scale sensor network. Unlike typical mobile devices, sensor nodes spend a considerable amount of energy not only while sending and receiving data but also in the listening mode [26]. Thus, sensor networks are more vulnerable to resource depletion attacks.

- **Lack of mobility:** In most applications, sensor nodes are stationary. They stay put wherever they are deployed. This decreases routing overhead. Most important, in sensor networks, route request broadcasts of reactive routing protocols and periodic updates of proactive routing protocols either do not occur or occur much less frequently.

- **Large network size:** Sensor networks consist of large numbers of nodes. Security architectures developed for small scale ad hoc networks are infeasible for resource-limited large-scale sensor networks.

- **Stable communication pattern:** In MANETs, nodes are assumed to communicate among themselves (point-to-point). Most MANET applications require transport layer connection mechanisms both for the construction and restoration of flows. However, in sensor networks most of the traffic created as many-to-one sporadic transmissions, as nodes reporting sensor readings to a central, more capable node. In sensor networks, data flow is directional. Each node presumably has a single destination, a next-hop either toward a central node or a clusterhead. This simple forwarding structure is immune to many elaborate routing attacks.

Routing in Sensor Networks

If a sensor network uses an elaborate routing protocol like a MANET, all the attacks against this routing structure will apply to the sensor network as well. A review of such routing attacks and counter measures are given in [38]. The attacks include changed routing information, hello flooding, selective forwarding, sinkholes, wormholes and sybil attacks.

However, since there are no mobility and no point-to-point links, we assume that most large-scale sensor network communications will be in the form of *many-to-one* transmissions as ordinary sensor nodes reporting to single or fixed destinations in a multi-hop fashion with relatively stable paths (similar to rooted trees). There will be no specific communication between the nodes requiring network-wide route request floods. Indeed, in a large scale sensor network, arbitrary point-to-point communication is neither

feasible, nor necessary. Instead, a particular sensor node will most likely use only the *next-hop* information to send its own packets and to forward its neighbors' packets for which it is the next-hop. There will also be no mobility and no irregular new node deployments that frequently invalidate this simple forwarding structure.

3.1.2 Related Work

Prevention Based Techniques

Authentication and encryption based security schemes for sensor networks are adaptations of security algorithms developed for MANETs. These adaptations aim to decrease the computation and communication overhead of these methods which were originally designed for more capable and less resource constrained MANET nodes. An initial overview of security constraints and a variety of approaches for key agreement and key distribution for sensor networks were presented by Carman et al. in [10]. In [65], Perrig et al. introduce a symmetric key cryptography technique adapted to resource limited sensor networks. The architecture in [65] consists of two main building blocks. The first block, SNEP, provides confidentiality, authentication and freshness between source and destination. The second block, μTESLA, provides authentication for broadcasts. In [25], Eschenauer et al. detail a random key distribution scheme for sensor networks. In the key pre-distribution phase, a random key pool is selected from the key space. Each sensor node is randomly assigned a subset of keys from the key pool. The shared key discovery phase occurs after network deployment. A link between two nodes exists only

if they are within communication range and they share a key. At the end, if the graph is connected, and if two neighbors do not share a key, a one-hop link between the neighbors can be formed by transferring a path-key over the already existing longer, secure path. Three other random key distribution mechanisms for sensor networks are introduced by Chan et al. [12]. The security analysis of major routing protocols and energy conserving and topology maintenance schemes for sensor networks are explained in Karlof et al. [38] together with major attacks and countermeasures.

Prevention based security schemes are difficult to implement especially over large scale sensor networks. It is not feasible to implement a dynamic public key cryptography scheme and to provide key exchanges with a trusted central authority. On the other hand, symmetric key cryptography can be used to authenticate neighbors. In any case, powerful encryption schemes will not be available because of the computational capacity of the nodes. Thus, security provided to sensor networks with prevention-only techniques is not always sufficient, or practical.

Detection Based Techniques

The first Intrusion Detection (ID) based security scheme for MANETs was introduced in [88] along with a general overview of requirements and architectural differences between ID systems for wireline networks and MANETs. In [34], Huang et al. detail an anomaly detection technique that explores the correlations among the features of a MANET node. The work in [35] is a simulation based study of the detection idea introduced in [34].

In [89], some of the MANET routing protocols are used in simulations to detect intrusions where a relatively small number of routing specific features are analyzed using well-known classifiers as anomaly detectors. Authors in [84] present a more coarse-grained intrusion detection technique based on the analysis of packet streams (both data and routing) in an AODV [64] based MANET. Received packets are matched against a number of state-transition attack scenarios describing different attacks.

In [31], the authors propose an intrusion detection system for 802.11 based MANETs using radio frequency fingerprinting. In this work, the idea is that there are unique hardware characteristics of tranceivers that cannot be forged. The nodes in the network are identified by their signals' transient portion. This enables a basestation to easily identify an intruder using the identity of a legitimate node. The algorithm introduced consists of steps such as calculating the variance of the phase, discrete wavelet transforms, statistical classifiers and Bayesian filter. Although this method is appealing for sensor nodes to identify their neighbors, the very limited computational resources of a sensor node do not allow such a code to be executed efficiently.

Compared to the sensor nodes, dynamic nature of the MANETs necessitates more complex routing protocols. This increases the number of both topology and routing variables. Higher numbers of variables increases the chances of variable interactions which may lead to the detection of even subtle deviations from the normal interactions as shown in [35]. However such complex data mining schemes are beyond the capabilities of the restricted sensor nodes. It is highly unlikely that a sensor node will have the storage

and analysis capabilities required by such schemes even with low number of variables. The ID systems designed for MANETs are therefore not suitable for sensor networks.

3.1.3 Securing Sensor Networks Using Detection Techniques

In order to prevent powerful intruders disrupting network operations, one has to look at the specific properties of sensor networks. In this context, node cooperation relying on the detection of deviations from expected neighbor behavior may be a feasible methodology. Here, a cooperative solution refers to the attack confirmation and collective action of neighboring nodes against intruders. The following are the key elements required for such a solution:

- Nodes know what to expect from other nodes, particularly from their neighbors. They detect and report anomalies to each other. The essential property of sensor networks that allows for intelligent node decisions is the long term operation of the network with relatively stable neighborhood information for each node.

- Nodes share the unexpected behavior of their neighbors with other nodes. This provides confirmation and common action against the attacker(s).

Next, we illustrate the detection and containment of an intruder using node cooperation. In Figure-3.1, node B is an attacker impersonating a legitimate node. It can be assumed that the legitimate node is destroyed, otherwise a node can easily detect a node using its own id. When the suspicious actions of node B are detected by node A,

it shares this with its relevant neighbors, nodes F and E. If the overall picture reveals an anomaly, meaning if a node learns that more than a fixed number[1] of other nodes confirm the unusual patterns, it declares the node as an intruder. After hearing the *intruder detected* broadcast, other nodes detecting but not confirming (due to smaller numbers of confirmations) the intruder immediately conclude that *node B* is the intruder. With the overall action of neighbors, the attacker is contained. Detecting nodes may also propagate this information to neighbors that are not yet aware of the intruder.

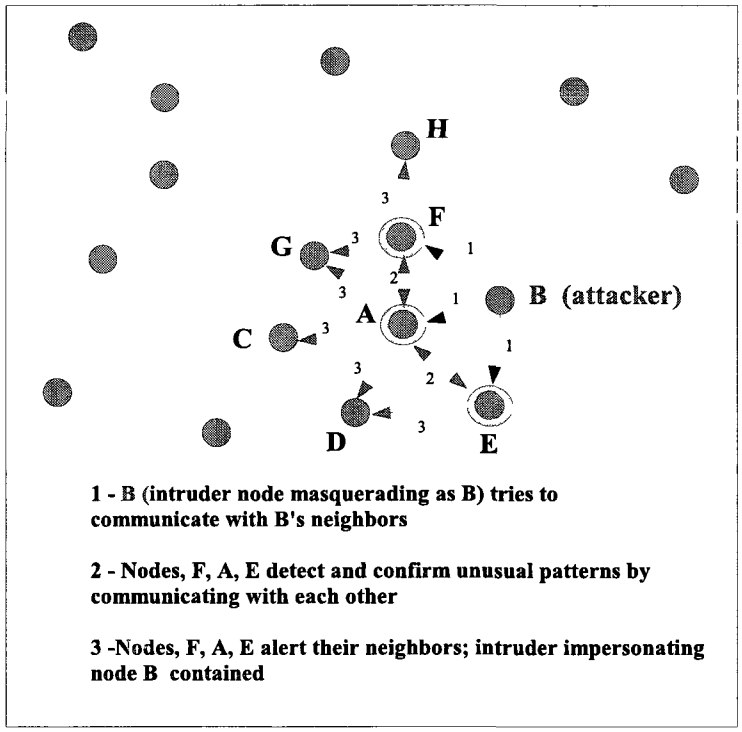

Figure 3.1: An intruder containment example

[1]A number selected based on the deployment density

The first step in designing such cooperative containment solutions[2] is the implementation of a node-based statistics gathering and analyzing algorithm. In the remainder of this section, we address this part of the problem.

3.1.4 Attack Models for Wireless Sensor Networks

In this chapter, we consider the following types of attacks:

- *Node Impersonation*: In order to use or disrupt a sensor network, an intruder has to establish itself as a legitimate node, most likely by spoofing the id of another node. An attacker may then start to deplete the resources of the network or propagate false alarms.

- *Resource Depletion*: This attack can also be seen as the next step of a successful node impersonation attack. Because of the large-scale, multihop and cooperative nature of sensor networks, an intruder can create a high volume of data and control packets that can quickly deplete the batteries of many nodes and disrupt the network.

Nodes keep statistics about their neighbors. The attacks listed above reveal themselves by deviations from the *normal* transceiver and traffic behaviors.

[2]The detection algorithm implemented does not have to be cooperative. Each detecting node may take independent action without getting confirmation from its neighbors. This may well be enough for containment. However, low-complexity cooperative solutions may greatly reduce false alarms and increase detection capability.

Assumptions

We make the following assumptions:

- The neighbors of a specific node do not change during the course of the analysis. This means three things:
  - Nodes are stationary
  - A node transmits with the same power
  - No new node is deployed
- Each node can uniquely identify its neighbors (using, for example, a manufacturer assigned id). Nodes do not need to have unique network id's.
- Data and control packet flows are directional and nodes use a tree based forwarding structure as the routing protocol.
- All nodes are peer entities. They use the same hardware with constant transmission power and run the same protocol stack.
- Each node has a clock that does not have to be synchronized with other nodes.

Features

The initial step in detection based security systems is the selection of *system features* that will be utilized. Since large scale sensor networks have a rather simple routing structure, stable topology and a low number of control messages, sensor nodes have relatively small

numbers of features. We have selected the average receive power (in dBm) and average[3] packet arrival rate (in $packets/unitTime$) as representatives of neighbor activities.

3.1.5 Detection Algorithm

Next important step is the selection of a *detection algorithm* which detects intrusion patterns based on the rules. The complexity of a detection algorithm depends on the number and characteristics of system features. A small number of noninteracting features decreases the complexity of the detection algorithm.

We use the following distributed method which is in compliance with the storage and computation capacity of a sensor node. The algorithm has a packet count based *sliding window* approach. At every node, only the last B packets received from each neighbor are used to calculate the statistics for that neighbor and each arriving packet is compared against these values. We call B the *main packet buffer length.* If the packet conforms to the statistics of the neighbor, it is accepted as *normal* and is used for new calculations. The oldest packet's values are removed from the list. We record the *arrival time* and *receive power* of each incoming packet.

To monitor receive powers for anomalies, *min* and *max* values of packet receive power are updated with each *regular* packet reception. An anomalous packet is a packet whose receive power is *below the min* or *above the max* of receive powers currently kept in the

[3]Here the term *average* is used to refer to the *sample* arrival rate of the packet buffer, not the average rate of the packet generating Poisson process which is represented by λ.

main packet buffer of length B. Depending on the sensor network deployment environment and the application, intrusion alarms may be raised with each anomalous packet or after *a predefined number of consecutive packets* show anomalous patterns. In the latter case, anomalous packets have to be kept separate from the regular arrivals until a decision is made. We call the buffer used for this the *intrusion buffer* and represent its length as B_1. This system is shown in Figure-3.2.

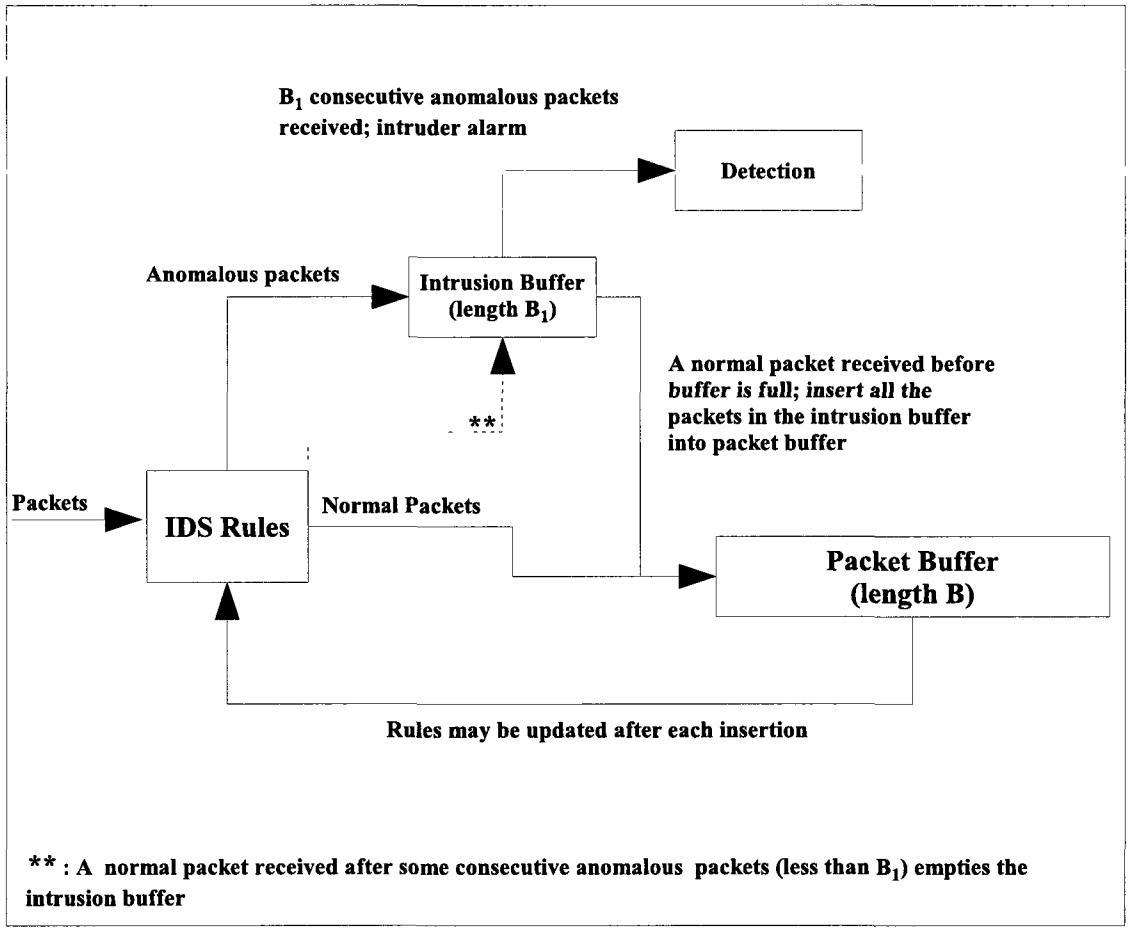

Figure 3.2: Receive power anomaly detection

To check packet reception rate anomalies, another packet count is utilized and represented by B_2. We keep two rates: the rate at which the last B_2 packets are received (including the last packet), $rate_{B_2}$ and the rate at which the last B packets are received, $rate_B$. If the ratio of these two rates is above a *comparison rate threshold* called K ($(rate_{B_2}/rate_B) \geq K$) an intrusion alarm is triggered. This method is illustrated in Figure-3.3.

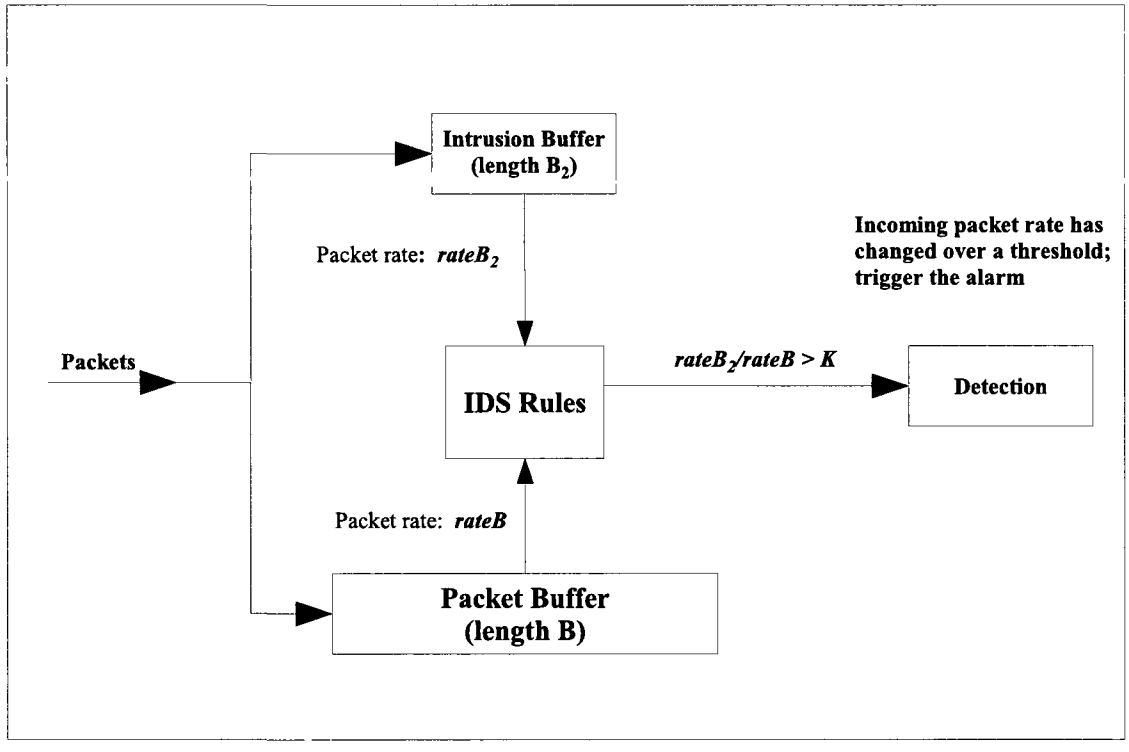

Figure 3.3: Packet arrival rate anomaly detection

We also change the value of K to see the effects of changing rules. Our sliding window based approach is suitable for the nodal and operational characteristics of sensor networks. Keeping long term averages with long buffers, using sampling, or using averages

updated starting from the beginning of the deployment may lead to false alarms. The slowly decreasing battery power of nodes may raise false alarms due to drops they cause in the transmit powers. The physical changes in the environment may also cause deviations that may seem abrupt when long term statistics are considered. For this reason, in our scheme, we propose keeping an amount of arrival statistics necessary to detect the anomalies but immune to channel fluctuations. The number of packets after which we conclude that the detection has failed is called the *miss threshold* and its length is represented with $B_{missThr}$. If the anomalies go undetected for B packets, they will change the characteristic of the main packet buffer and will never be detected. Therefore, $B_{missThr}$ has to be smaller than B.

Selection of proper B, B_1, B_2, K and $B_{missThr}$ values depending on security vulnerabilities has crucial influence as these values strongly affect both the probability of detection and the detection time as shown in the next section.

With our proposed power anomaly detection scheme, for a successful attack, the attacker has to keep its relative distance to each node previously hearing from the impersonated node close to the previous distances. If the location of the intruder is significantly different, the possibility of detection due to receive power anomalies increases. To break into the network, the attacker also has to have either the same transceiver circuitry or power control capabilities to perfectly emulate the transceiver of the impersonated node(s). Our arrival rate anomaly detection algorithm forces the intruder to learn the regular packet forwarding patterns of the impersonated node(s).

3.1.6 Experimental Results

Propagation Model

We assume that the wireless channel does not change during the transmission of a whole packet, however, it is random and independent from packet to packet. We use the log-normal shadowing path loss model [69] to calculate receive power variations at different packet receptions. We assume that the average received power decreases with distance d as $(1/d)^{\beta}$. Random fluctuations around this average are represented by a zero-mean Gaussian random variable called X_{σ} (in dB) with standard deviation σ (also in dB). The general formula for this model is the following:

$$PL(d)[dB] = PL(d_0) + 10\beta log(\frac{d}{d_0}) + X_{\sigma} \tag{3.1}$$

In the equation above, $PL(d)$ is the path loss from a distance d. It is calculated using a close-in reference distance d_0. The variable β is called the *path loss exponent* and standard deviation σ is called the *shadowing deviation*. The received signal power, P_r from a distance d is then calculated using

$$P_r(d)[dBm] = P_{tr}[dBm] - PL(d)[dB] \tag{3.2}$$

where P_{tr} is the output power of the transmitter. In addition, a packet is received only if its receive power is above a threshold value. In our experiments, in accordance with the results of recent low-power sensor transceiver circuitry and link characteristics research presented in [14] and [90], we used the values listed in Table-3.1.

Table 3.1: Shadowing and transceiver parameters

Parameters	Values
β	2.5
σ	$5dB$
d_0	$1m$
Transmit power P_{tr}	$5dBm$
Receive power threshold	$-90dBm$

Intrusion Detection Using Receive Power Anomalies

In this section, we present the results of receive power level anomaly detection capabilities of our algorithm with the simulation parameters given in Table-3.2.

Table 3.2: Simulation parameters-1

Parameters	Values
Initial transmit power (training power) P_{tr}	$5dBm$
Distance between nodes, d	$25m$
Receive buffer length, B	100
Miss threshold, $B_{missThr}$	25

The Figure-3.4 represents the probability of false alarm with changing intrusion buffer lengths, B_1 values. In this context, a false alarm means that the algorithm marks the sender as an intruder although the power level variations are only due to the channel variations as modeled by the shadowing model (at constant P_{tr} of $5dBm$).

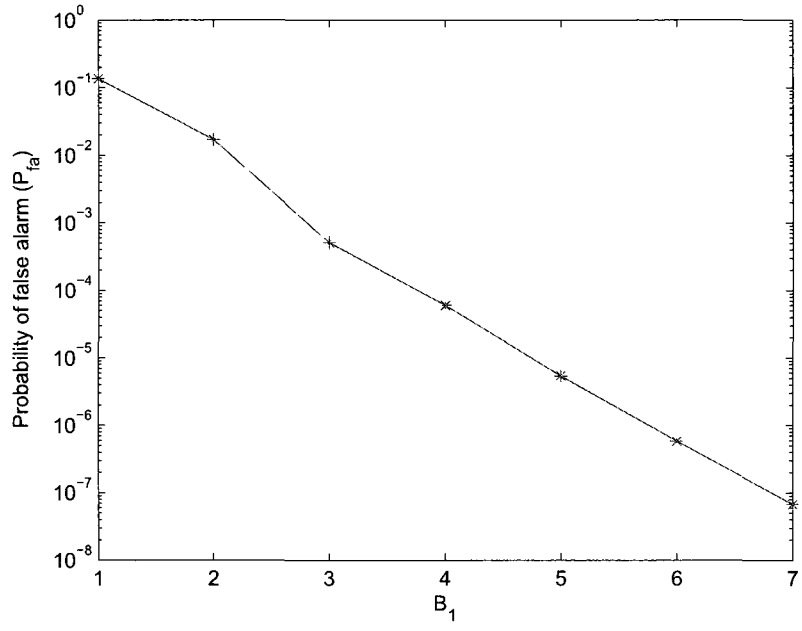

Figure 3.4: Intrusion buffer length B_1 vs probability of false alarm

In Figure-3.5 and Figure-3.6 we test the performance of the detection algorithm against the sender's actual transmission power changes and for different intrusion buffer lengths (B_1). This experiment requires an initial training period that teaches the detecting node the normal receive power levels of its neighbor. For the first B packets, we keep the transmitter's initial power level of $5dBm$ unchanged. Then the power level of the transmitter is increased and the detection probabilities and detection times are recorded. The number of undetected anomalous transmissions after which we conclude that the detection has failed ($B_{missThr}$) is kept constant at 25.

As expected, when the degree of anomaly increases, it is detected with higher probability and in a shorter period of time. In addition, smaller intrusion buffer lengths (B_1)

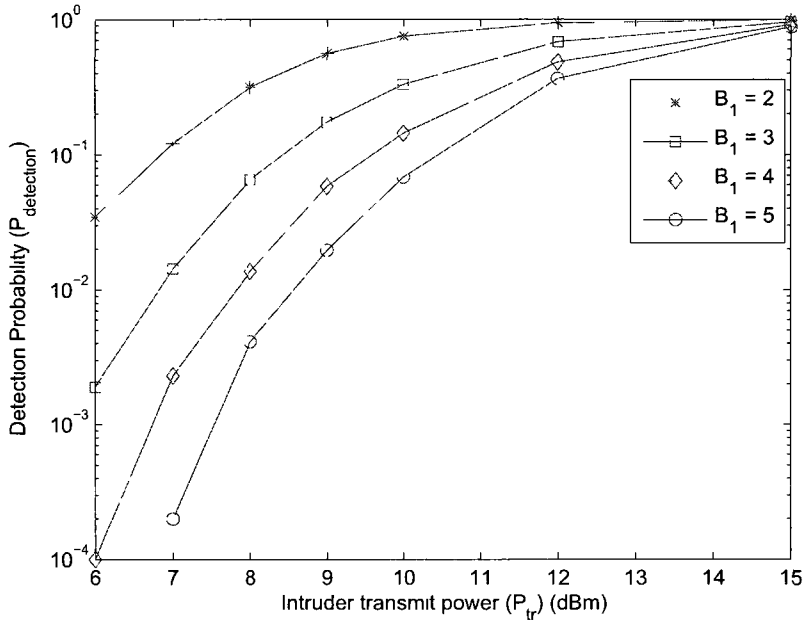

Figure 3.5: Intruder power vs detection probability

give better detection probability and detection delays, however they also increase the false alarm rate. In actual deployments, this trade-off has to be judged according to application security requirements.

Intrusion Detection Using Packet Arrival Rate Anomalies

We consider the following traffic model: during a fixed time slot, each node may sense a phenomenon to report with probability p. This means, during that time slot, each node may generate a packet with that probability, independent from other nodes. Therefore, we approximate each node's packet generation as a Poisson process with average rate parameter λ $(packets/unitTime)$. We assume a lightly loaded network where there is no

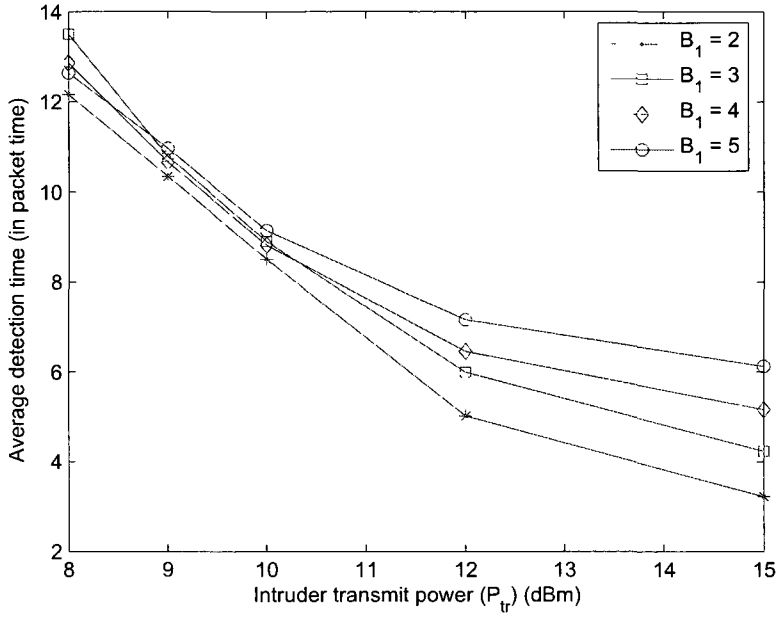

Figure 3.6: Intruder power vs detection time

queuing delay or other traffic interactions. Thus, the total number of packets received by each node is a sum of independent Poisson processes which is another Poisson process.

To model the arrival rate anomalies we increase the average packet generation rate of the neighbor to λ_n. The ratio of the two packet reception rates at two buffers $(rate_{B_2}/rate_B)$ is checked against the rate threshold K. If the rate is greater than K, an intrusion alarm is triggered.

Simulation parameters used for arrival rate anomaly detection are given in Table-3.3. Intrusion detection based on packet arrival rate analysis requires a higher number of previously received packet information, corresponding to higher B, B_2 and $B_{missThr}$ values.

Table 3.3: Simulation parameters-2

Parameters	**Values**
Transmit power P_{tr}	$5dBm$
Initial average Poisson rate (training rate)	$\lambda = 1$
New average Poisson rate	λ_n
Intrusion buffer length, B	1000
Miss threshold, $B_{missThr}$	1000

We first check the false alarm probability. Figure-3.7 represents the probability of a false alarm with changing intrusion buffer lengths (B_2). Here, a false alarm is an alarm raised because of the receive rate variations without an actual Poisson average sending rate change (average rate is constant at $\lambda = 1$ $packet/unitTime$).

We train the receiver with 1000 transmissions of average Poisson rate $\lambda = 1$. The intrusion buffer length B_2 is selected as 100 and the detection capability and performance is evaluated as a function of λ_n/λ and with different K values. $B_{missThr}$ is kept constant at 1000. Figure-3.8 and Figure-3.9 show detection probability and detection times, respectively.

For the chosen magnitude increases in average Poisson rate, the detection probability and time do not change significantly. On the other hand, as the rate threshold K decreases, performance of the detection algorithm gets better. However, this also increases the false alarm rate. Again, the selection of K in actual sensor networks is a design decision that relies on traffic and network properties.

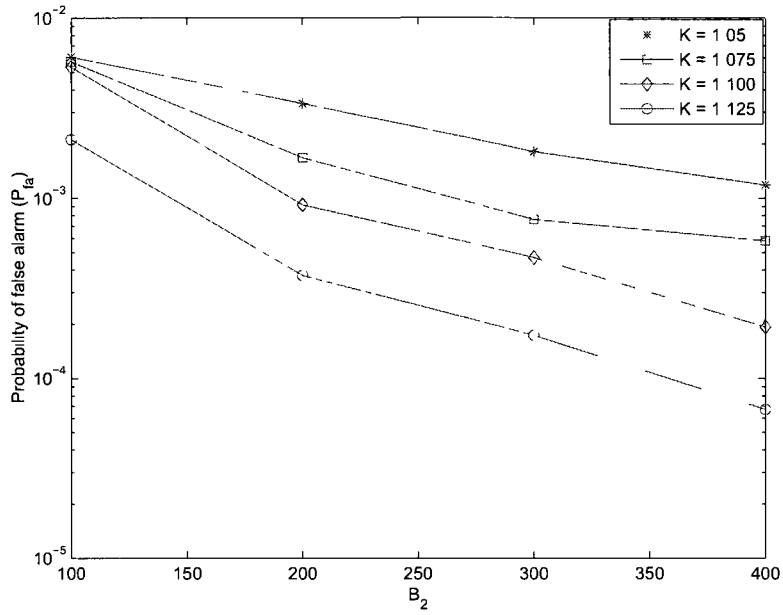

Figure 3.7: Intrusion buffer length B_2 vs probability of false alarm

3.2 Network Layer Traffic Anomaly Detection in Wireless Sensor Networks

In this section, we develop a new traffic model for a sensor node and devise a scheme to detect anomalous changes in this arrival process. Our detection algorithm keeps short-term dynamic statistics using a multi-level, sliding window event storage scheme. In this algorithm, arrival processes at different time scales are compared using node resourcewise computable, low-complexity, aggregate features. We introduce a real-time, host-based anomaly detection method that detects the deviations from the established, normal neighbor traffic profiles. Given a list of common operation environment assump-

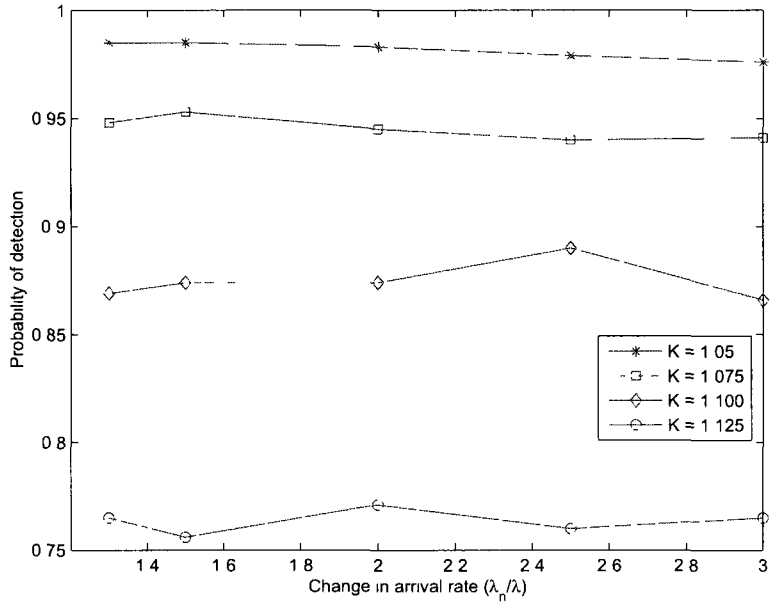

Figure 3.8: Arrival rate change (in λ_n/λ) vs detection probability

tions, we introduce an arrival process model using a Pareto distribution with long *OFF* and short *ON* periods. During the *ON* intervals, we create sub-processes. Each sensor builds a simple statistical model of the incoming traffic for each neighbor. Short and relatively longer term statistics are updated with each incoming packet and short term values are compared against longer term values which are accepted as temporary normals. The deviations from the normality criteria are deemed anomalous since nodes lack mobility and follow a predictable traffic generation behavior even if the multihop nature introduces traffic aggregations or event clouds activate more than one node and cause correlations.

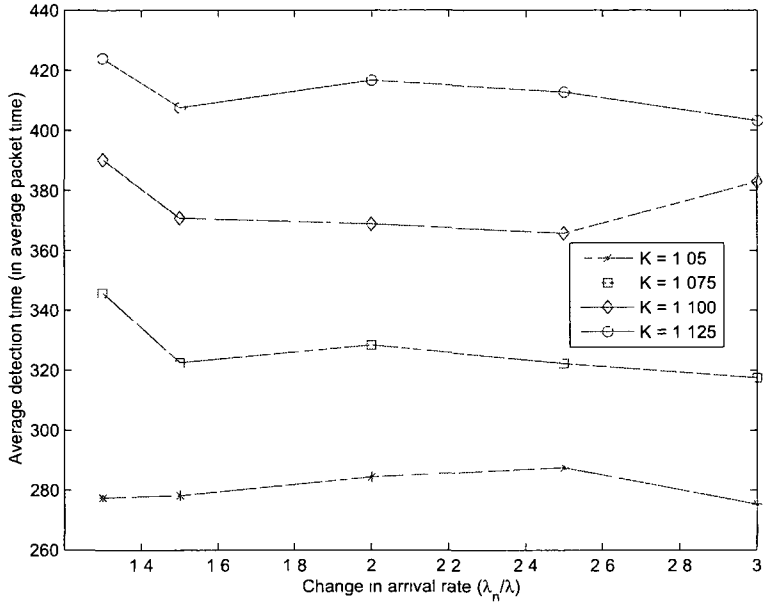

Figure 3.9: Arrival rate change (in λ_n/λ) vs detection time

3.2.1 Modeling Traffic in Sensor Networks

Although there is a rich literature about distributed control, routing and medium access protocols in sensor networks, there is so far no work on the traffic characterization in WSNs from a single node perspective and under different operation assumptions. Due to the multihop nature of the network, a sensor node will forward packets for other nodes along with its own packets. The arrival process experienced by a sensor node will be affected by the application, event reporting rules, the nature of distributed control mechanism (power cycles, data aggregation and clustering algorithms), network scale and the distribution of sink nodes. The following likely operating environment of a WSN

can help us build a model for the arrival process experienced by a sensor node. Assume that,

- sensors report event-based (in lieu of periodic reporting),
- when an event is detected, a sensor sends a fixed number of possibly identical messages (to guarantee delivery), with short intervals,
- events to be reported occur rarely and the ratio (transmit time)/(idle time) is large, on the order of a hundred,
- a sensor may forward other sensors' packets; due to the light loaded nature of the network, aggregate traffic also shows similar arrival patterns,
- an event cloud sensed by a single node is likely to affect more than one node; therefore events cause neighborhood activation and gateway-like nodes along with all other nodes on the path toward sink experience arrivals in bursts.

Based on the assumptions above, we create a general Pareto arrival process with short bursts of *ON* and long *OFF* intervals. For each *ON* burst, we create a Poisson sub-process. Figure-3.10 illustrates this compound process.

3.2.2 Intrusion Detection From Traffic Anomalies

In order to disrupt a sensor network, an attacker has to establish itself as a legitimate node, most likely by spoofing the id of another node. He can then create a large amount

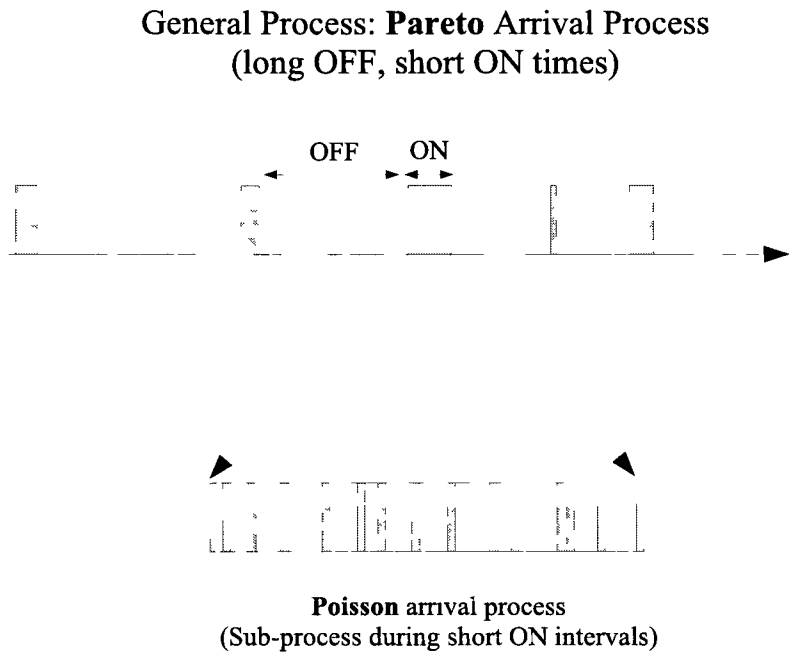

Figure 3.10: Arrival process model

of traffic and/or propagate false alarms. Because of the large-scale, multihop and cooperative nature of WSNs, high packet traffic can deplete the batteries of sensors quickly and interfere with the network operations.

In order to prevent intruders impersonating legitimate nodes, a node may observe its neighbors and can build an arrival process profile for each neighbor. Because of changing wireless channel conditions, normal traffic profiles must be calculated dynamically. In our algorithm presented next, normal profiles are updated with each received packet and significant deviations are used to detect the intruders acting as legitimate nodes.

Detection Algorithm

We assume that the neighbors of a node do not change during the course of analysis Each node can uniquely identify its neighbors and has a clock that does not have to be synchronized with other nodes It is also assumed that the network is lightly loaded and there is no queuing delay or other traffic interactions The detection algorithm has a packet based sliding window approach At every node, only last B packets received from each neighbor are used to calculate the statistics for that neighbor We call this buffer of length B as the *receive buffer* To detect anomalous deviations from the normality criteria created by the receive buffer, another buffer that gives us shorter term statistics is used This buffer of length B_3 is called the *intrusion buffer* When a packet arrives at a node, it enters into the intrusion buffer and the oldest packet in this buffer is dropped The statistics about the observed features are updated at the intrusion buffer and compared against the statics of the receive buffer If the comparison does not reveal an anomaly, the packet is marked as normal and transferred to the receive buffer as illustrated in Figure-3 11 Similarly, the oldest packet in this buffer is dropped and new statistics are calculated

We record the *arrival time* of each packet and check the *mean* and the *standard deviation* of interarrival times of the packets in these two buffers An arrival is considered anomalous if the following buffer feature comparison criteria holds

$$|mean(\text{recBuff}) - mean(\text{intBuff})| > K * std(\text{recBuff})$$

If with the new arrival, the mean of the interarrival times at the small intrusion buffer is K

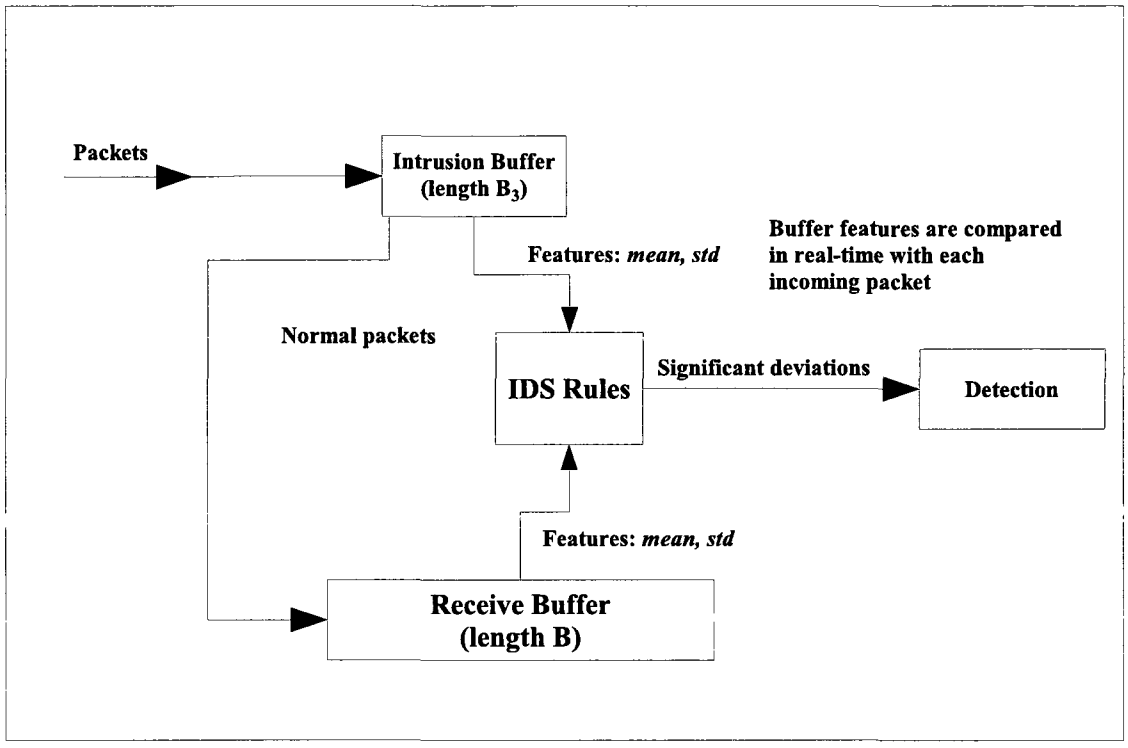

Figure 3.11: Interarrival time anomaly detection

standard deviation of the receive buffer times different than the mean of the interarrival times of the receive buffer, an intrusion alarm is set off. We also change the comparison threshold value K to see the effects of changing rules. The sliding window approach is suitable for the nodal and operational characteristics of sensor networks. Keeping long term averages may lead to false alarms. Higher packet drop rates due to physical changes in the environment may cause traffic changes that may seem abrupt when long term statistics are considered. Therefore this algorithm keeps a reasonable amount of arrival statistics necessary to detect the anomalies but immune to channel fluctuations. The number of packets after which it is concluded that the detection has failed is represented

by $B_{missThr}$. If the anomalies go undetected for a long period of time, they will change the characteristic of the main buffer and will never be detected. Therefore, $B_{missThr}$ has to be smaller than B. Selection of proper B, B_3, $B_{missThr}$ and K values depending on security vulnerabilities and available resources has crucial influence as these values strongly affect both the probability of detection and the detection time as shown with simulation results.

3.2.3 Experimental Results

We first create a general Pareto process with the Hurst exponent H. Given mean period length of m time units (m_{on} for ON and m_{off} for OFF periods), calculate α and Q where $Q = m(\alpha - 1)$ and $\alpha = 3 - 2H$. The length of a period is a random variable L where $L = Q(x^{-1/\alpha} - 1)$ and x is a uniform random variable between $0 \leq x < 1$. Each ON period has a Poisson subprocess with average rate λ. The new average rate used to simulate anomalies is represented by λ_n.

Traffic Anomalies and Their Detection

To model the anomalies, both the Poisson and Pareto process parameters are changed. The malicious behavior is modeled by assuming that an intruder will be changing interarrival times by either constantly transmitting or disregarding previous long waiting times between the bursts. During the learning process, we train the receiver with 1000 transmissions with the parameters in Table-3.4.

Table 3.4: Training parameters

Parameters	**Values**
Hurst exponent, H	0.9
m_{on} (in unitTime)	2
m_{off} (in unitTime)	$100.m_{\text{on}}$
Poisson average rate, λ (in packets/unitTime)	1
Receive buffer length, B	1000
Intrusion buffer length, B_3	100
Miss threshold, $B_{missThr}$	250

The system sets off an alarm if the absolute value of the difference between the mean interarrival times are greater than K standard deviations of the interarrival times in the longer buffer. For different K values, by varying Poisson sub-process average arrival rate λ we evaluate the performance of our detection algorithm observing the time it takes to detect and the probability of missing an anomaly.

Figure-3.12 and Figure-3.13 show the changing characteristic of detection with different arrival rate increments. Increasing the average Poisson rate, decreases the mean interarrival times, since the increase is more salient in the small intrusion buffer, a node can detect such changes in the incoming traffic. The detection times are shorter and the detection probabilities are higher for small K values.

Figure-3.14 gives the detection probability of anomalies created by perturbing the Pareto parameter which takes values between $0.5 < H < 0.85$ (new value, H_n).

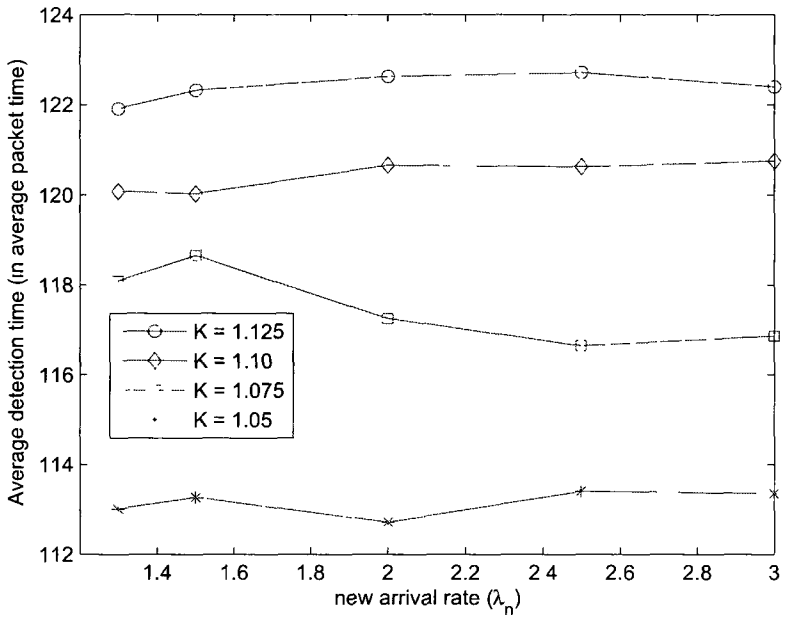

Figure 3.12: New arrival rate λ_n vs detection time

As H_n approaches the training parameter (0.9), detection probability decreases and the detection is easier with small K values.

Figure-3.15 shows the detection time of anomalies created by changing the mean burst length m_{on} (hence m_{off}) in the process. Detection is difficult when the new m_{on} is closer to the training value, 2 time units.

False Alarm Rates

The following parameters are used while checking the false alarm probability: $H = 0.9$, $m = 2$, Poisson rate $\lambda = 1$, $B = 1000$ and varying B_3 and K values. A *false alarm* is an alarm raised because of changes in the mean interarrival times of packets without an

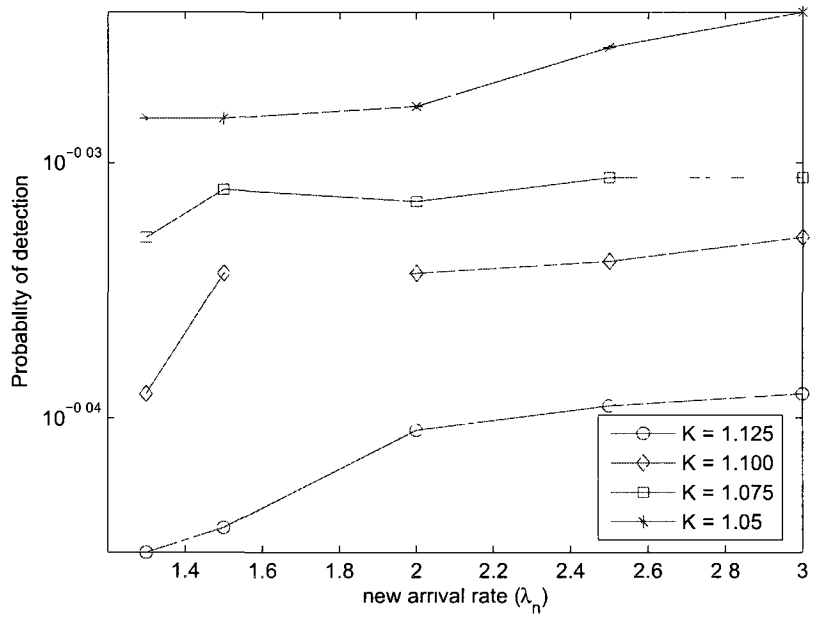

Figure 3.13: New arrival rate λ_n vs detection probability

actual process parameter change. Figure-3.16 represents the probability of false alarm with changing intrusion buffer lengths (B_3). As the intrusion buffer length increases, false alarm rate decreases. That is because longer intrusion buffer lengths are more resilient against the effects of normal system randomness.

3.3 Chapter Conclusions

While designing security algorithms for WSNs, it is essential to keep in mind sensor node capabilities. In this chapter, we have introduced novel anomaly detection based security algorithms for large scale sensor networks using their stable neighborhood infor-

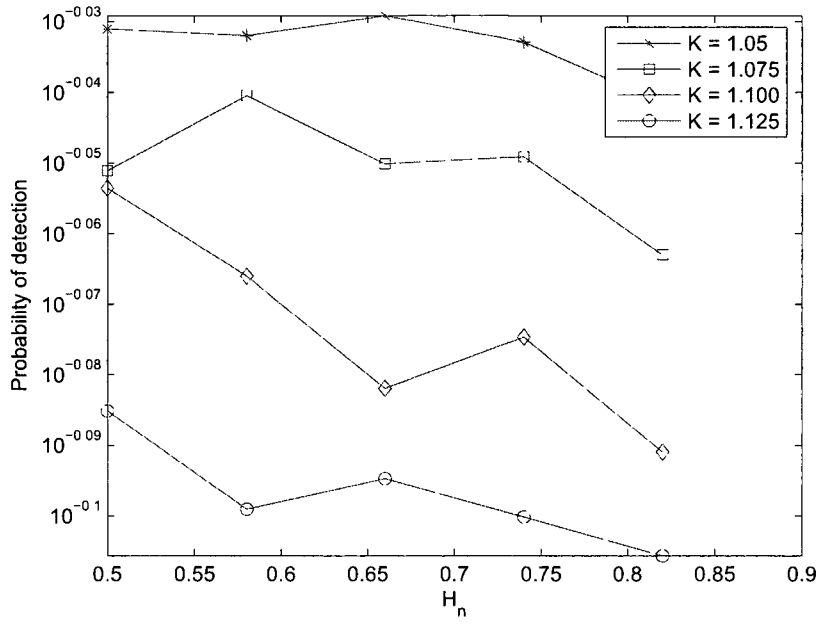

Figure 3.14: New Pareto parameter H_n vs detection probability

mation. If each node can build statistical models for its neighbor characteristics, these statistics can later be used to detect changes in them. We have shown that, by looking at a relatively small number of received packet features, a node can effectively identify an intruder impersonating a legitimate neighbor. In this chapter, we also introduced a new traffic model that can be experienced by a single node in a large scale WSN. Using a sliding window packet storage scheme, arrival-processes at different time scales are compared and anomalous changes are detected. Our implementation is distributed in nature, since the anomaly detection algorithm is executed at each node separately. Different routing, medium-access and distributed control algorithms will introduce different features. Further research can focus on examining other node features to address specific

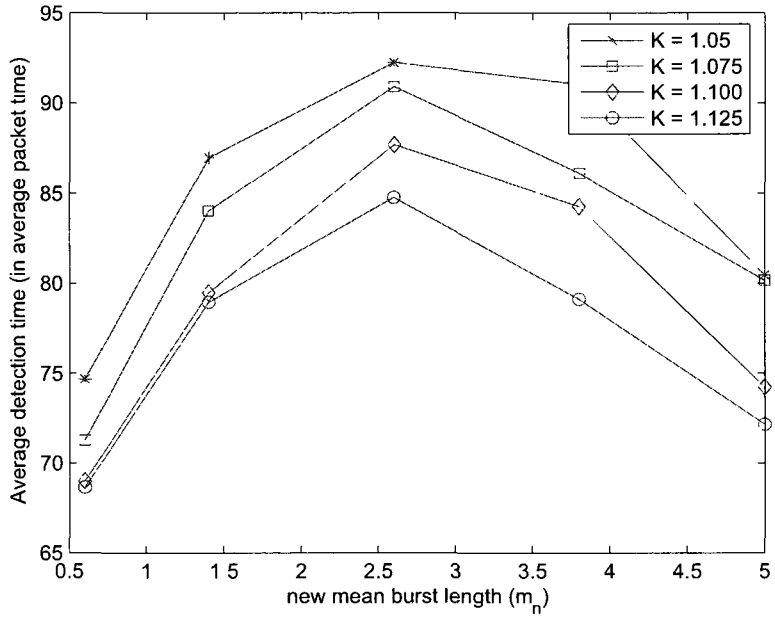

Figure 3.15: New mean burst length m_n vs detection time

vulnerabilities with limited sensor node capabilities in mind.

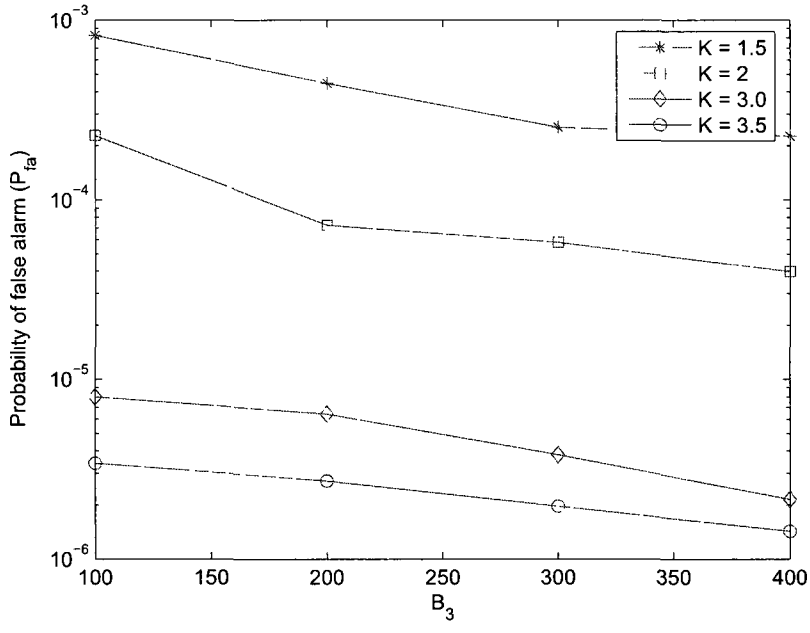

Figure 3.16: Intrusion buffer length B_3 vs probability of false alarm

Chapter 4

Elimination of Duty-Cycling For Embedded Wireless Radios

The radio is the main energy spending component in a wireless sensor node. In order to limit their energy consumption, wireless sensor nodes are periodically waken up and put to sleep. Even with this duty-cycling, energy spent at the radio while it is awake is the main resource bottleneck for the sensor node architecture. In this chapter we analyze solutions targeting the elimination of duty-cycling using RFID based methods. We introduce an RFID wakeup system that uses a boosting circuit and a low-threshold Schottky diode based rectifier. Our design targets the collection of enough energy from RF signal emitted from the regular low-power sensor radios capable of occasional high power burst transfers on the order of 20 dBm. The performance of different rectifier structures are compared for this wakeup system.

4.1 Introduction

With the increasingly efficient energy scavenging techniques, capturing the ambient low-power RF energy will be a mainstream technology in the near feature. Elimination of energy wasting bottlenecks with such methods will improve the lifetime of networked embedded devices and facilitate the deployment of ambient intelligence based applications. For this to occur, the energy harvested from the radio waves captured with efficient collectors should be high enough to power or activate very low-power microcontrollers.

A low-power sensor radio (transceiver) can be in four different modes: *Listen*, *receive*, *transmit* and *sleep*. In order to save energy, low-power radios used in battery powered sensor nodes have to be put into sleep mode. In sleep mode, a radio cannot hear the incoming transmission. *Duty-cycling* in this context, is the periodic wake up of a radio to check the air for preamble. When a preamble is detected in the listen mode, the radio enters into receive mode and duty-cycling is ceased. In the receive and transmit modes, a node wakes up with all peripherals, preparing to process or send data streams. One of the main design decision in sensor network deployments is building efficient duty-cycling mechanisms that provide maximum system lifetime while satisfying application requirements.

A wireless sensor network node is basically made up of two major IC elements: a low-power microcontroller (MCU) and a low-power radio. In current wireless sensor node architectures, duty-cycling firmware, along with the protocol stack resides in the MCU's flash memory. A low-frequency, low-power MCU clock is used to implement the timer

that will create the necessary periodic wakeup interrupt for the MCU in the sleep mode, which eventually wakes up the radio to the listen mode. When no preamble is detected during listen mode, both go back to sleep modes with MCU low-power clock running to fire the next wakeup interrupt. In general, low-power clock running mode power consumption is very low, on the order of 1 μA [81] and can be ignored when compared to radio power consumption. When duty-cycled around 1%, most commercial embedded low-power radio designs achieve lifetimes of around two to four years using two 800 mAh AA batteries. For example, a 1% duty-cycled, two AA type battery equipped system with a listening mode power consumption of 10 mA will last only 1.82 years.

$$\frac{2.800mA}{10mA}.100 = 16000hours \approx 1.82years \tag{4.1}$$

The 10 mA figure is the about the minimum of listening mode power consumption of many efficient low-power transceivers such as [24, 50, 80] and usually this figure is higher when the MCU and peripheral power consumptions are added. This figure does not include the data receive and transfer mode power consumptions, which are slightly higher than the listen mode power consumption. In moderate usage single or multihop network scenarios, packet transmissions and receptions will further add up to the *radio-on* time, and decrease the system lifetime. It is therefore clear that sensor network lifetime and performance will greatly benefit from the use of efficient schemes eliminating duty-cycling and hence idle listening.

Active and passive RFID technology has potential to greatly impact the low-power,

low-rate and short range communications. The ZigBee specification which is based on IEEE 802.15.4 greatly suffers from the energy wasted because of duty-cycling. There are many MAC layer schemes targeting low-power wireless sensor applications. The majority of these schemes incorporate duty-cycling assumptions in their design. In general, from the duty-cycling perspective, they can be categorized as *synchronous* or *asynchronous* periodic sleeping protocols. In synchronous schemes, members of the sensor subnet share a common clock and obey to a general schedule with very little allowed jitter. In asynchronous schemes, nodes sleep independent from their neighbors' schedules. Surveys of different MAC algorithms for wireless sensor networks can be found in [22] and [44].

In this work, our main challenge is to build a wakeup system capable of working at very low incident RF power levels, by those emitted from regular low-power short range embedded wireless radios. We detail system components, their design requirements and associated challenges. Collecting enough energy from RF signal emitted from the regular low-power sensor radios using passive methods is a big challenge yet it is the most efficient technique both from the cost and energy perspective. Efficient wakeup systems eliminating the duty-cycling will open the doors for energy efficient and longer life sensor networks.

The remainder of this chapter is organized as follows. In Section-4.2 we summarize previous solution proposals. We detail the wakeup system and related MCU and radio characteristics in Section-4.3. In Section-4.4 the voltage boosting circuit is described. An overview of the rectifier model and the performance comparison of two three-stage,

Schottky diode based passive RFID rectifiers are given in Section-4.5. In Section-4.6 the effects of the removal of the radio duty-cycling at various protocol layers and conclusions are presented.

4.2 Related Work

There is a rich literature about the wakeup schemes for wireless sensor radios with the goal of achieving longer system lifetime. Efficient wakeup schemes are primary important energy savers for most of the current sensor network deployments. Solutions targeting the elimination of energy wasting duty-cycling in low-power radios has been around since the beginning of the low-power sensor networking era. Authors in [20] proposed a much lower power PicoRadio as an add-on to wireless embedded node to watch the channel for wireless activity. In this scheme, a node with data to transmit first wakes up its own radio, and then sends a short wakeup beacon to the next node using the wakeup radio channel. A similar idea is proposed in the active RFID context in [51] using active RFID radios as additional transceivers. It also gives a usage scenario about the cooperation of the two radios, their functional differences, signal differentiation and communication protocol issues. In both [20] and [51], receiving nodes power up higher power radio if they are informed about the pending transmission through the channel of the low-power radio. In both studies, low-power radios are always on and in an addressable state. The target nodes then wake up the regular radio and get ready for the higher rate and higher power transmissions. Disadvantages of these schemes are their increased hardware

cost, complexity and additional energy use because of the secondary active radio. Albeit very low-power, these solutions are less optimal than the passive receiver solutions that eliminate the need for an always-on active radio, which we overview next.

Using passive RFID tags to wake up low-power sensor radios idea was mentioned in studies [30] and [77] around the same time independently. The work in [77] is a brief mention of the idea without much details on the relevant hardware design whereas in [30] authors present general design considerations with a basic SPICE simulation model. In the latter work the antenna is modeled as an AC source that feeds a step up transformer to increase the voltage level and charge a capacitor with the resulting signal. Authors in [71] give a general system overview of an RFID wakeup system using two antennas connected to the sensor radio. One antenna is used for regular data transfer and the other, which is called the *reader* in the paper, for the wakeup purpose. The use of a larger standard antenna connected to the low-power radio to act as a reader-like transmitter complicates the system design and requires special transceivers that have multiple RF output pins.

An active/passive UHF RFID tag design is presented in [67]. When used in the active mode, the battery powered tag design achieves a lifetime exceeding ten years even with a very small 100 mAh battery. When duty-cycling is eliminated, the lifetime of the sensor node will mostly depend on the energy use of the auxiliary RFID radio, especially in the light use scenarios where the sensing and communication occurs only occasionally. An active RFID wakeup circuit design that uses battery powered components to amplify, filter and generate the required wakeup signal is given in [83]. Authors in this work use a

separate MCU to perform the decoding and filtering of the signal amplified by an operational amplifier. In the analog domain, using diodes, the very small UHF wakeup signal is first converted down to the original on-off keying frequency. Then the baseband signal at 862 Hz is amplified with a factor of 10^5. In order to reduce the power consumption, instead of a single amplifier, four low-power, low gain amplifiers are used.

Efficient rectifier design is the most important task for wakeup applications. In general, RFID rectifiers are optimized for maximum output power delivered to the IC. In [39], an integrated passive CMOS transponder and rectifier combination with a reading range of around 10 meters is introduced. The study in [19] introduces a symmetrized full-wave rectifier design. The implementation of the model in the latter achieves high conversion efficiency at low power levels where the diodes are operating near their threshold voltages. In [18] a passive tag working at 2.4 GHz using the rectifier introduced in [19] is described. This tag can be powered from 12 m with a 4 W effective isotropically radiated power (EIRP).

4.3 Passive RFID wakeup system design

In our design, there is no battery and we need an efficient rectifier capable of shifting the signal to a high enough level and for a long enough time to create a pin interrupt on an embedded processor in the sleep mode. In order to overcome the diode turn on voltages, the RF signal should be boosted passively using a resonant booster circuit such as the one studied for UHF frequencies in [87]. The next stage is the rectifier capable

of producing the necessary DC voltage from the boosted output signal. Along with the efficiency of the passive rectifier chain, high transmit power of the sensor radio and high tag antenna gain are important factors to consider. From the perspective of efficient energy collection and use at the tag, the studies that provide the most insight are [39] and [18].

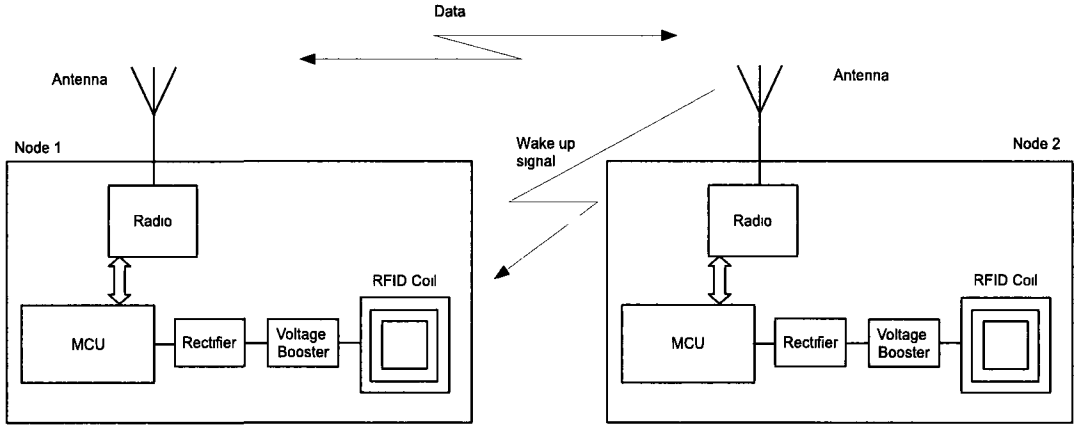

Figure 4.1: Passive tag wakeup system view

In RFID terminology, in the initial wakeup phase, a node transmitting will be acting as a reader and the receiving nodes will be acting as tags, but the communication is only one way since tags return no information. A general sketch of the system is given in Figure-4.1. All the power sent is rectified and used only for one purpose; to create a pin interrupt on one of the processor pins. As mentioned earlier, RFID rectifiers maximize the power delivered to the tag so that the IC can be powered and in the UHF case, there is enough energy for backscattering. Our application is different in that it requires much

less power to operate. There will be no IC to power up using RF energy and the tag will not return a signal. Since the rectifier is connected to a high impedance pin, the output of the rectifier can be assumed an open circuit with I_{out} equal to zero. MCUs with low-voltage interrupt capability are better suited for the wakeup applications due to limited voltage at the output of the rectifier.

In our design, all sensor nodes are identical and the components are as follows:

- A single send and receive antenna connected to the radio. This antenna will be used to transmit both the wakeup and data signals.
- A simple RFID coil collecting the RF energy from the reader and delivering it to rectifier.
- A resonant voltage boosting circuit providing high amplitude swing from the small RF signal.
- A rectifier between the boosting circuit and the MCU converting the UHF signal into a sufficient magnitude DC signal to create a pin interrupt.

The IEEE 802.15.4 standard specifies that a transmitter should be capable of transmitting at least 3 dBm and the maximum transmit power is limited only by local regulations. Hence, in most cases, low-power radios can transmit as high as the maximum allowed transmitter power level. [16] gives an overview of standard regulations and a ZigBee radio that can transmit at 20 dBm output power. Although will be used occasionally, the programmable high power transmit capability is important in RFID wakeup

applications. Europe limits the EIRP with 20 dBm [37]. Most ZigBee chipsets have a maximum RF power of 0 dBm. The 0 dBm maximum power is common because this level can be achieved without an additional RF power amplifier, whereas a 20 dBm output power requires such an amplifier. Depending on the traffic scenarios, occasional high power burst transfers required to wake up other nodes will already be compensated by the elimination of idle listening. In order to avoid waking up the whole neighborhood, addressed RFID wakeups [18] can be used. The wakeup of the nodes along the data path should occur with low latency to guarantee the required bandwidth and other upper layer requirements.

4.4 Boosting circuit

For the power levels considered, in order to overcome the dead zone occurring due to the diode threshold voltages, the input voltage has to be amplified. This can be done either with active methods using cascaded amplifiers [83] or using passive methods such as the voltage boosting circuit [87] shown in Figure-4.2. In this circuit, the resonant frequency is

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{4.2}$$

and the output voltage v_{out} is equal to

$$v_{out} = \frac{1}{R_{in}}\sqrt{\frac{L}{C}}v_{in} \tag{4.3}$$

Since the output voltage is directly proportional to the inductance and inversely proportional to capacitance, large inductance and appropriate capacitance values for the given resonant frequency should be selected.

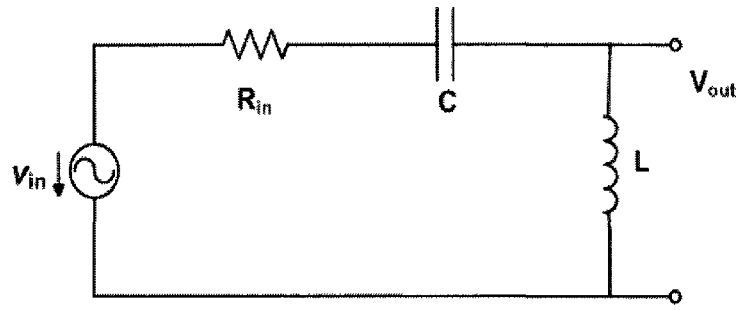

Figure 4.2: Voltage booster circuit

In Spice transient simulation analysis, we observed that the resonant circuit achieves the performance predicted by (4.3). A v_{in} of 900 MHz, with peak amplitude $\widehat{v_{in}}$ of 5 mV and 50 Ω source resistance, a 104.2 nH inductor and a 300 fF capacitor, the output peak settles to a 60 mV in 20 ns. In practice, losses in the inductor and capacitor, and the frequency fluctuations decrease the amplitude of the output voltage and the sharpness of the peak. With increasing source resistance R_{in}, the output voltage decreases. Increasing R_{in} also decreases the settling time. Overall, with careful component selection, optimized antenna design and frequency tuning, losses can be minimized and such a resonant circuit

can be used to boost the small voltage at the input of the rectifier.

4.5 Rectifier Design

As the distance between the tag and the reader increases, the tag receives less power from the reader. The maximum distance that can still provide the minimum power can be found using the Friis formula,

$$P_{RX} = P_{TX} G_{TX} G_{RX} (\frac{\lambda}{4\pi r})^2 \tag{4.4}$$

where P_{TX} is transmit power, G_{TX} is the transmit antenna gain, G_{RX} is the receive antenna gain. At 900 MHz the wavelength $\lambda = 0.33$ m. At the distance $r = 10$ m, with $P_{TX} = 20$ dBm, a voltage $v_{rms} = 59$ mV will be received by a 50 Ω antenna when unity transmit and receive antenna gains are assumed.

In our application, there will be no power transfer to the IC, therefore our goal is to maximize the voltage at the rectifier output. In our simulations we assumed that the high impedance pin state can be effectively represented as an open circuit. For example, TI MSP430 digital I/O pins have less than 50 nA leakage current. This significantly decreases the power requirements at the rectifier output.

The main challenge for the rectifiers in RFID applications is operating with very low-power incident electromagnetic radiation. Rectifiers should receive enough signal magnitudes to overcome the unresponsive dead zone at low input voltages. The dead

zone occurs because of the diode threshold voltages. For the wakeup application, the input voltage levels are very low even after the voltage boosting network, and therefore the power of the received signal should overcome threshold voltages. Schottky diodes are the most efficient diodes for this purpose because of their low turn-on voltage and low substrate leakage.

The most cost effective way of producing an RFID tag is building the whole system including the rectifier and IC in a standard CMOS process. However, since there is no RFID IC in the wakeup systems and Schottky diodes are not part of the standard CMOS processes we will concentrate on efficient external rectifier systems and analyze their output voltage performance using Spice transient simulations.

With increasing distance, the peak input voltage decreases at the input of the rectifier and at some point the voltage level cannot overcome diode thresholds. Various passive solutions exist to boost the RF signal amplitude. [82] and [76] present CMOS based optimized power harvester circuits. Similarly in [87] a voltage boosting network based on resonant tank is employed. Harvesting enough power with passive techniques is possible either through a dedicated antenna or using such a tank circuit.

The antenna connected to a rectifier input can can be modeled as Figure-4.3 where Z_{ant} and Z_{in} are the antenna and the load impedances. When Z_{in} goes to infinity, v_{in} reaches a maximum but the absorbed power by the rectifier decreases to zero.

For maximum power transfer optimized rectifiers the efficiency η, is defined as

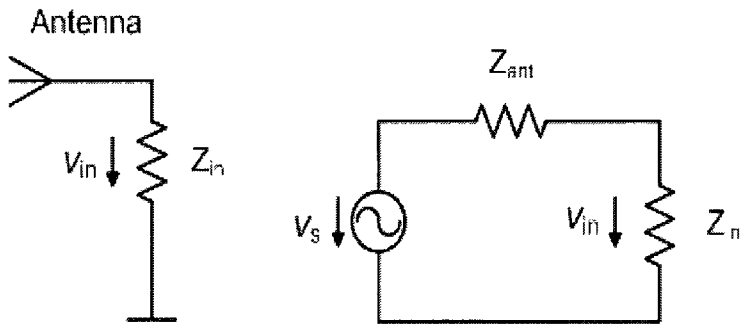

Figure 4.3: Antenna equivalent circuit

$$\eta = \frac{DC\ output\ power}{RF\ input\ power} \tag{4.5}$$

For maximum voltage transfer applications there is no need for impedance matching and the general rule is to maximize Z_{load} against the output impedance of the rectifier, Z_{rec} as illustrated in Figure-4.4.

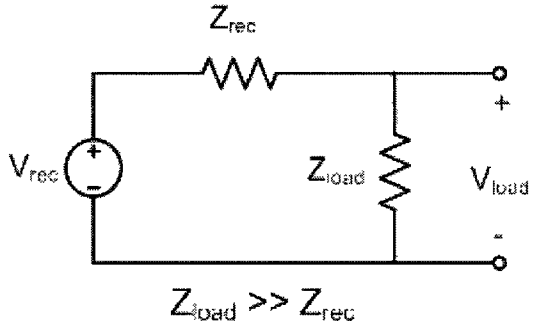

Figure 4.4: Rectifier equivalent circuit

Voltage rectification using cascaded diode-capacitor stages is a common technique in

various industrial applications. For small input voltages such as this wakeup application, Schottky diodes are particularly useful because of their low forward voltage that leads to increased efficiency; at any stage, for voltage conversion to occur, the input voltage of the stage should be higher than the Schottky forward voltage. To get good efficiency, diodes should have high saturation current (I_s), low junction capacitance (C_j), low series resistance (R_s) and low substrate capacitance (C_{sub}). For low C_j, a small diode size should be used. The output voltage does not heavily depend on the rectifier capacitance values. Larger capacitors only charge more slowly. For higher efficiency, coupling capacitors should have low R_s and low C_{sub}. More rectifier stages can be cascaded to achieve higher voltage. However, depending on the power levels, energy losses along the chain limit the number of stages.

4.5.1 Analysis of Rectifiers

In this section, two three-stage voltage multipliers built with Schottky diodes are analyzed. Both rectifiers are optimized for maximum voltage transfer for the wakeup application. Figure-4.5 is a conventional three-stage rectifier with identical 250pF capacitors and Schottky diodes with C_j of 12 fF, R_s of 50 Ω and I_s of 1 uA. Figure-4.6 is a three-stage symmetrized rectifier. The input for both rectifiers is a 900 MHz sinusoidal with a peak magnitude of 100mV.

In order to increase the output voltage in both circuits, the number of stages can be increased. However, this also increases the output impedance. In general, the steady-

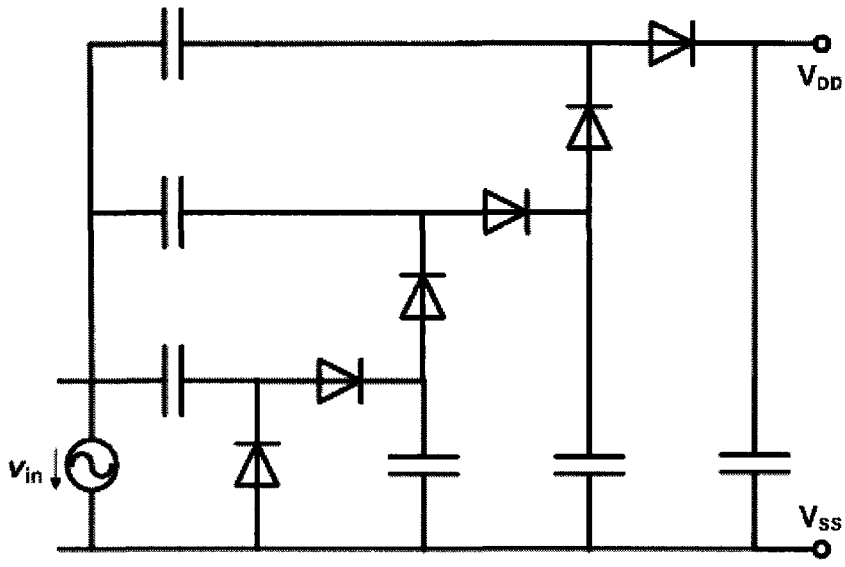

Figure 4.5: Three-stage conventional rectifier

state output voltage can be approximated using

$$V_{out} = 2N(\widehat{v_{in}} - V_{Diode}) \tag{4.6}$$

where N is to number of diodes, $\widehat{v_{in}}$ corresponds to peak incident voltage from the antenna, and V_{Diode} represents the turn-on voltage of the diodes. A similar conventional rectifier structure is analyzed in [39]. In general, for rectifiers built with Schottky diodes, the impedance is a function of diode parameters and substrate capacitances. Hence, in general, imaginary part of the impedance is higher compared to real part. For wakeup application however, since there is no output current other than the very small pin leakage, the output of the rectifier is essentially an open circuit and the real part of the impedance is much higher than the imaginary part.

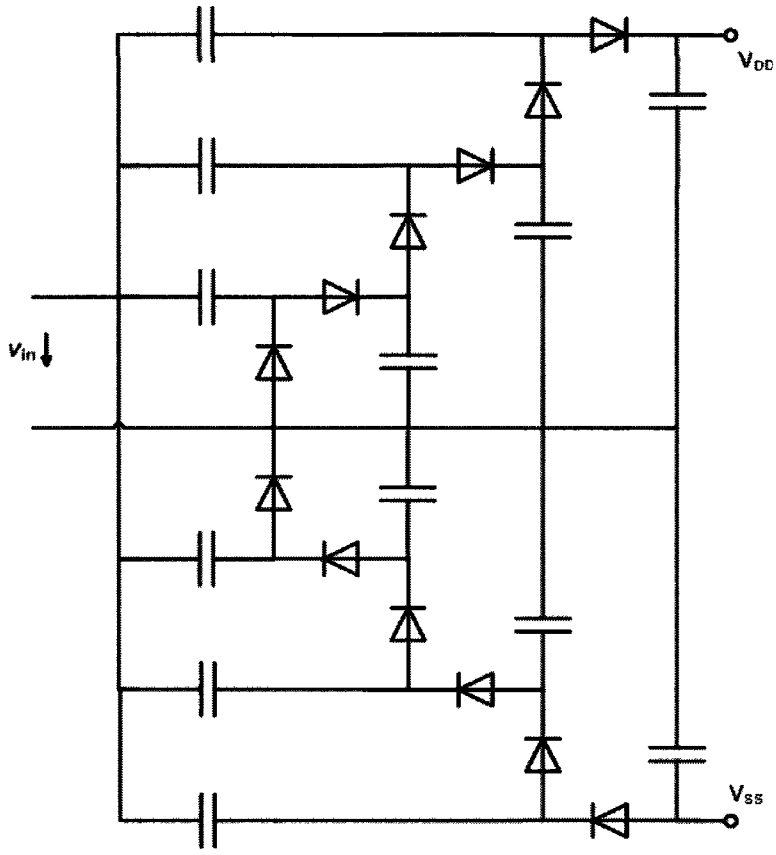

Figure 4.6: Three-stage symmetrized rectifier

As expected, the symmetrized structure doubles the output voltage which can be approximated using

$$V_{out} = 4N(\widehat{v_{in}} - V_{Diode}) \tag{4.7}$$

Figure-4.7 is the Spice transient simulation results of the two rectifier structures. For the UHF frequencies considered, the fluctuations in the input frequency does not have a

significant effect on the output voltage. The three-stage symmetrized rectifier achieves a better performance when compared to the three-stage conventional rectifier. The reason for this is its symmetrized structure with capacitor rearranged so that every diode is excited with the same signal level. A detailed discussion about the performance of a similar two-stage configuration can be found in [19].

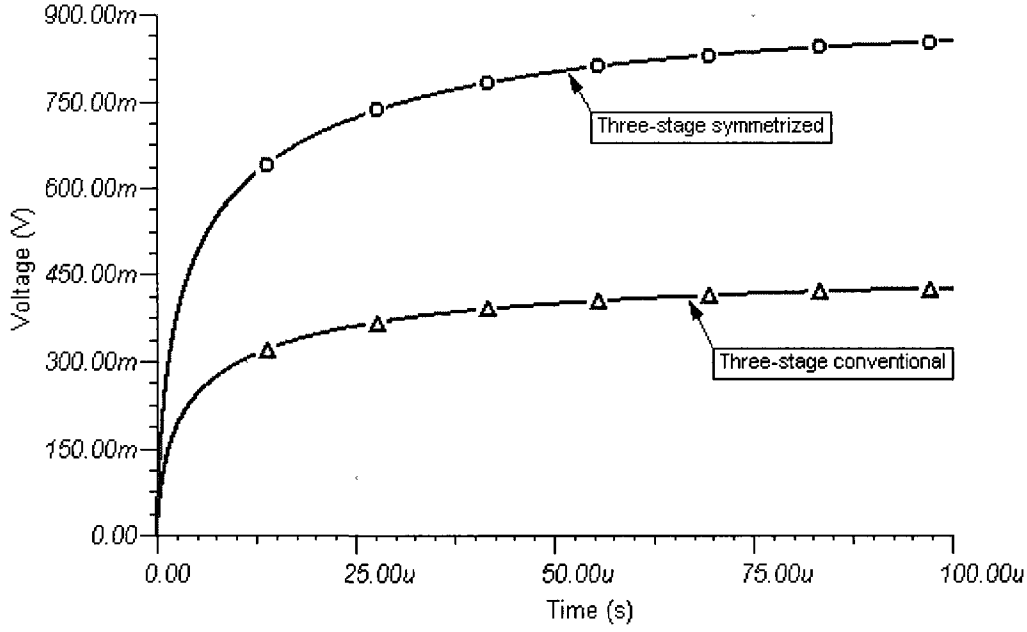

Figure 4.7: Spice transient simulation of the three-stage rectifiers

4.6 Chapter Conclusions

Duty-cycling of embedded radios constitutes the major energy bottleneck for WSNs. The elimination of duty-cycling has many direct benefits, most importantly at the medium access layer, which carries the heavy burden of the complex rules and requirements associated with duty-cycle based energy efficiency algorithms. Managing the sleep intervals according to application requirements is difficult to tune and the inherent latency problems usually constrain upper network layer designs. With the elimination of duty-cycling process, sensor networks will be more efficient in their operations by lasting longer and by not missing events they are programmed to detect, either because of a lost packet or a dead battery.

In this work, we introduced an RFID wakeup system model, and analyzed and simulated different rectifier candidates to be used in this system. We also summarized current state of the art in other important system components such as the boosting network. The performance of different rectifier structures are compared for this wakeup system. To create the necessary pin interrupt for the wakeup application the low-power radio should be capable of transmitting with 20 dBm output power for a short duration. With this transmit power, the frequency matched resonant boosting network and the rectifier system introduced can create the required pin interrupt on the embedded MCU from a distance of around 10 meters.

Chapter 5

Cross-Layer Design of RFID MAC Algorithms

Classical wireless multiple access techniques cannot be directly used in resource constrained RFID systems where MAC protocol design poses various challenges for designers. The vast majority of RFID tags are small in size, with limited memory and computation capabilities. In addition, these tags are passive with no built-in power source, for which regular radio operations such as listening the channel for activity is not possible. These constraints tie the protocol designers' hands and force rather simple channel access and collision-resolution protocols when compared to wireless systems with built-in power sources.

Since RF powered passive radios cannot listen the channel for activity, they cannot make intelligent and independent decisions to reduce the collision probability. The chan-

nel access schemes for passive RFID devices are therefore generally reader initiated and controlled. One of the major design problems in RFID systems is an efficient tag reading scheme minimizing both the collisions and total reading time of all the tags in range.

5.1 Introduction

There are two basic MAC approaches for RFID systems: *binary tree search methods* and *ALOHA-based channel access randomization* methods. In binary tree search based methods, the same length binary ID cloud of a tag group can be represented as a tree with ones and zeros representing diverging leaves. As a result, an inverted tree structure with each ID at the end of a unique path can be created. The simplest polling procedure in this structure is the exhaustive search of the every possible tag ID by examining each possible node in the tree. Starting from the first bits, by increasing the bit count at every query, all tags can be identified. Since each branch is queried only once, the performance of this procedure is determined by the reader side algorithm, depending on the rates of collision and error while singulating the tags. At the end of this process, each tag can be uniquely identified since no other tag will respond, other than the final fully identified tag. The time it takes to locate a tag is theoretically logarithmic in the number of nodes with the elimination of empty leaves, which are abundant in sparsely populated or highly concentrated tree structures where large number of leaves can be eliminated at the initial stages. Only in the uniformly distributed dense deployment case, most tree leaves have to be queried, which almost never occurs in practice due to the enormous length of the

possible key space. In general, binary tree search based algorithms are more wasteful in that they require a much bigger number of exchanges between the tags and the readers compared to ALOHA based schemes.

In the general ALOHA based wireless medium access control systems, an active station which is ready to transmit senses the medium, transmits and waits for an acknowledgement. No acknowledgment from the destination means the loss of the packet either by transmission errors or by a collision. After a random wait time the station retransmits and the process continues with random and increasing waiting (back-off) time. A more efficient variant of this procedure is called *slotted* ALOHA where time is divided into slots and a station can only transmit at specific time slots. In *framed slotted* ALOHA [86], time slots are further grouped into frames, with N time slots per frame. Each station in this protocol can transmit only once in a given frame, on a randomly selected time slot. A collision occurs when multiple transmissions start within the same slot.

For passive RFID tags, carrier sensing and relevant operations can only be performed at the readers and communicated to the tags through separate messages. ALOHA protocols are efficient when the channel utilization is low. ALOHA adapts to varying number of tags and requires a rather simple reader design. The only function the reader has to perform is to listen to the transmissions. The slotted ALOHA protocol doubles the utilization of ALOHA by limiting transmission to slot boundaries. However, it carries some synchronization overhead both at the reader and at the tags in the form of control packets informing the tags about the slot boundaries. The framed slotted ALOHA tags

talk only once during a frame. In addition to synchronization overhead, this scheme also requires tags to keep track of the current slot number and to know the frame size N, expressed as the total number of available slots on a given frame.

Various performance enhancement techniques are in use in practical ALOHA based systems. When a tag response is received, the acknowledgement from the reader can *mute* the tag to prevent the unnecessary responses, until the next activate command. A tag can be switched-off after being read, can be slowed-down with random back-off command or temporarily muted when another tag is transmitting. The same methods can be used more efficiently when slotted ALOHA is used. However, complicated timers cannot be implemented on the tags. For this reason, only simple counters to be incremented or decremented by the reader commands are available.

In slotted ALOHA based RFID MAC algorithms, tags must be synchronized and be informed about the slot boundaries. This synchronization requirement can be accomplished either by the beacons sent by the reader or by the internal timers of the tags. Another important design challenge is to adapt the frame size to the number of tags; if there are more tags than the available slots, tags will be constrained and there will be excessive number of collisions. When the frame size is unnecessarily larger than the tag count, many slots will be empty and system resources will be under-utilized. The maximum throughput for the framed slotted ALOHA systems with random slot selection is achieved when the number of tags is equal to the number of slots. One of the earliest and widely used commercial examples of protocols built on framed slotted ALOHA is Philips

I*Code [66]. In this system, the slot position for a tag is determined by AND'ing the hash value of offset ID with the slot mask. In [85] and [40] authors introduce algorithms to optimize the tag reading process by estimating number of tags using the previous round statistics.

5.2 Distance Based Slot Selection in RFID Systems

We introduce a new MAC protocol for RFID systems. The protocol is designed as an enhancement to framed slotted ALOHA MAC protocols in which tags randomly select a slot number on a given frame size. As shown in this work, the completely random slot selection in framed slotted ALOHA systems is not the optimum approach to the slot selection problem. To minimize the collision probability, our protocol, named Distance Based Slot Selection (DiSEL), uses a cross-layer approach for tags to select the most appropriate time slot in a given frame. A tag in DiSEL uses the maximum and minimum received power levels of the reader-tag communications to choose a slot number. We test DiSEL under various tag deployment and density scenarios and show that DiSEL decreases the tag collision probability in both random uniform and evenly spaced dense tag deployments.

The DiSEL protocol conveys a new notion for the slot selection process. It is designed as an enhancement to framed slotted ALOHA MAC protocols where tags select a slot number randomly, based on their random number generator outcome. When multiple tags select the same slot, a collision occurs and data from those tags selecting that

particular slot for transmission are lost. We argue and demonstrate that, instead of responding blindly and exposing their transmissions to collisions, tags may base their response timing and slot selection to the physical layer characteristics of the reader signal observed at the tags. We make use of the fact that, tags are located at different distances from the reader and the received power differences at the tags may provide enough granularity for the tags to make decisions about their relative distance to the reader, to be used in the slot selection on a given frame size.

We concentrate on 900 MHz UHF RFID systems. The DiSEL protocol uses a cross-layer approach for tags to select a time slot in a given frame, in a deterministic fashion. A tag in DiSEL uses the received power levels of reader-tag communications to choose the slot number. In general, for the propagation models for UHF RFID systems discussed in literature such as [8] and [3], the received signal power level at the receiver depends mainly on the distance between the transmitter and the receiver. DiSEL makes use of the fact that no two tags can be located at the same physical location, and their distance hence their receive power levels can be used to differentiate their slot selection, or their response time to the reader commands. DiSEL introduces one additional power level probing round to the traditional ALOHA based systems. Each tag delays the timing of the responses based on the previous round statistics sent by the reader. Tags select the slot to be used according to a deterministic *slot selection formula*. Before the start of the algorithm we assume that there is a tag count estimation and corresponding frame size setting algorithm in place, such as those introduced in [85] or [40]. Following are the

steps of a reading round in DiSEL:

(i) *Power_probe* message: Reader initially queries the tags for their receive power level of the current transmission with the initial frame size N:

Reader to tags: $\rightarrow (power\_probe, N)$

(ii) Each tag receiving *power_probe* message reports the received power level of this *power_probe* message, P_{power_probe}, as in general slotted ALOHA systems, choosing a slot randomly, according to N:

Tags to reader: $\rightarrow (P_{power\_probe})$

(iii) Reader determines the minimum (P_{min}) and maximum (P_{max}) received power levels, re-estimates N, and broadcasts them to tags:

Reader to tags: $\rightarrow (P_{min}, P_{max}, N)$

(iv) Each tag calculates its slot number n according to the slot selection formula:

$$n = int\left(\frac{P_{power\_probe} - P_{min}}{P_{max} - P_{min}} N\right) \tag{5.1}$$

where *int* is a function that rounds the number towards the nearest integer.

(v) Reader will reply with the *collision array* control message, informing tags about the success of their transmissions, such as zeros representing success and ones representing failure.

(vi) For tags with failed transmissions, the algorithm can be run again with reduced frame size.

5.3 Hardware Requirements of the System

The DiSEL protocol performs better when received power granularity is high at each tag. Therefore a passive voltage boosting network and an efficient rectifier system can increase the ability of the analog-to-digital converter at the tag in producing a sufficiently differentiating number for the received power level among the neighboring tags. The analog-to-digital converter is operated by the voltage diverted from the rectifier output which is also fed into its analog input.

5.4 Propagation Model

A radio signal may be reflected, diffracted, or scattered and different copies of the signal, called multipath components, may arrive to the destination along with the main line-of-sight signal. The multipath components, can be attenuated, delayed and shifted and, they often create distortions to the LOS signal at the receiver.

Signal propagation models for UHF RFID systems is a new topic in the propagation models and RFID literature. In [3] authors present the experimental results for the short range propagation effects of UHF RFID systems with varying distance between the reader and the tag, with different antenna and tag heights, at different UHF frequencies and

with varying clutter. They conclude that the simple breakpoint [61] and ray tracing models do not fully represent the propagation effects for UHF RFID systems.

Authors in [8] perform a simulation study of propagation effects of different UHF RFID systems with differing physical structures and surroundings. The paper points out that physical surroundings and the location of big reflecting objects have important effects on both the reader and the backreflected tag signals. Authors also state that ray tracing models can approximate the actual propagation effects if the modeling of the particular physical environment is done correctly. Their simulation setup includes variation of the angles and mounting heights, as well as different orientations of the tag antennas.

In ray tracing, reflection, diffraction, and scattering effects of a finite number of reflectors are approximated using simple geometric equations. Ray tracing model is most accurate when the receiver is many wavelengths away from the nearest scatterer, and all the scatterers are large [29]. If the system components are stationary, then the impact of the multipath components are fixed. As concluded in [8] and [3], ray tracing, specifically in non-cluttered depot or warehouse environments where the signal from the reader have only two components, one being the line-of-sight LOS and the other being the ground reflected signal, two-ray model is a good model that approximates the UHF RFID signal variations. In this chapter, we use a two-ray model to for the received signal power level variations. The received power, P_r in this model can be approximated with

$$P_r = P_t \left(\frac{\lambda}{4\pi}\right)^2 \left| \frac{\sqrt{G_l}}{l_1} + \frac{R\sqrt{G_r}e^{-\jmath\Delta\phi}}{l_2} \right|^2 \tag{5.2}$$

where

- G_l is the product of the transmit and receive antenna field radiation patterns in the LOS direction,
- G_r is the product of the transmit and receive antenna field radiation patterns corresponding to the reflected rays,
- $l_1 = \sqrt{d^2 + (h_t - h_r)^2}$ and $l_2 = \sqrt{d^2 + (h_t + h_r)^2}$
- d is the distance between transmitter and receiver,
- h_t and h_r are transmit and receive antenna heights,
- R is the ground reflection coefficient,
- $\Delta\phi = 2\pi(l_2 - l_1)/\lambda$ is the phase difference between the two received signal components.

5.5 Simulation Results

We used the following values for the constants: $G_l = 1$, $G_r = 1$, $R = 1$, the UHF frequency $f = 900MHz$, the reader height $h_r = 1m$ and the tag height $h_t = 1m$.

The performance of the algorithm is measured based on the number of collisions in a single round. We tested DiSEL at various tag densities, with different number of tags.

In all of our simulations, we kept *the frame size N the same as the number of tags* where random slot selection achieves its maximum throughput. Figure-5.1 shows the placement of the tags relative to the reader. Tags are distributed uniformly along the diameter line of the circle (shown as ellipse) with radius $r = 5m$. The center location of the circle is $d_c = 6m$. A single round tests the *throughput*, or *performance* p, measured with the number of slots with a single tag transmission (number of successful slots) S and frame size N ratio: $p = S/N$.

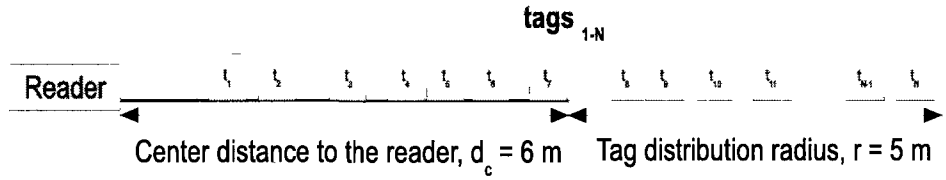

Figure 5.1: Reader and tags deployment

We compare our algorithm only with random slot selection method because, to the best of our knowledge, there is currently no other slot selection algorithm in the literature. Figure-5.2 shows the performance of DiSEL and random slot selection when tags are distributed randomly according to the uniform distribution along the diameter line. Figure-5.3 compares the performance of DiSEL against the random slot selection when tags are distributed along the diameter line as evenly spaced with distance among each other being equal to $d_t = diameter/number\ of\ tags$.

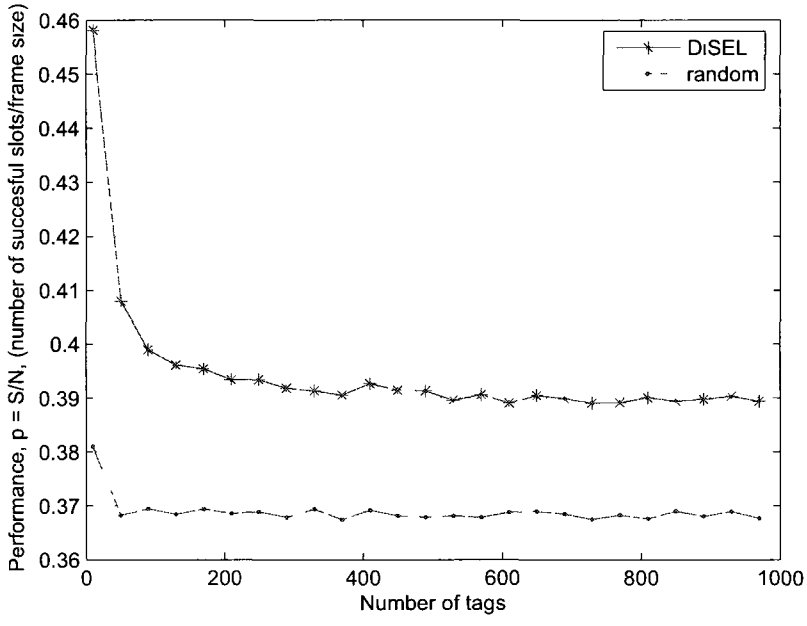

Figure 5.2: DiSEL vs random slot selection: random uniformly distributed tags

DiSEL achieves better performance when the tag deployment allows a sufficient power level granularity. This can be achieved with sensitive measurement or passive resonant boosting methods as explained in this chapter. The protocol performs well when the power level fluctuations are more of a function of the distance between the tags and the reader. The benefits of the DiSEL protocol are more pronounced when nodes are evenly spaced compared to the deployment scenarios where many tags end up very close to each other and received and digitized power level granularity cannot differentiate between those tags under the given slot selection formula.

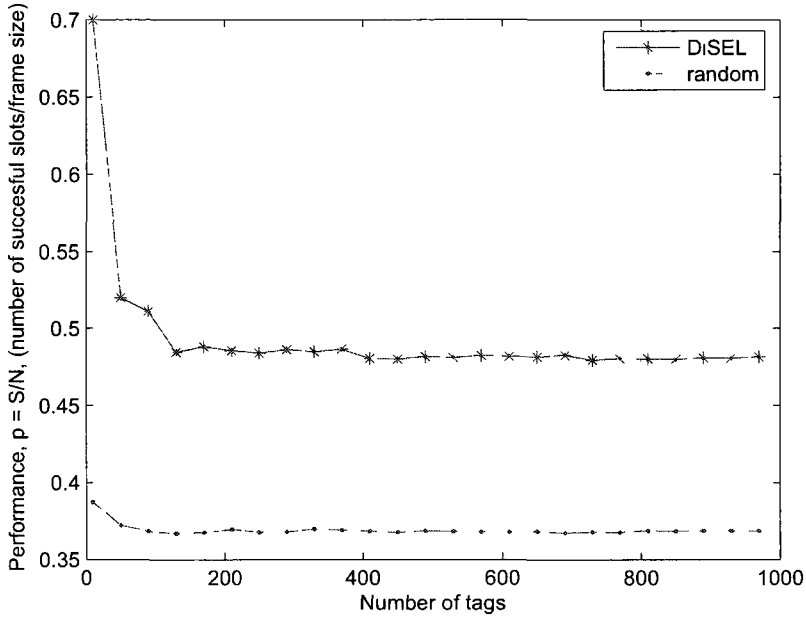

Figure 5.3: DiSEL vs random slot selection: evenly spaced tags

5.6 Chapter Conclusions

In this chapter, we introduced a new MAC scheme for passive UHF RFID systems using cross-layer design principles. The DiSEL protocol is an enhancement to framed slotted ALOHA MAC protocols where tags randomly select a slot number for a given frame size. In DiSEL, to minimize the collisions, tags in the first round report their received power levels to the reader. The reader then broadcasts the previous round's maximum and minimum received power levels to tags, to let them make informed decisions while selecting a slot number. Simulation results demonstrating the efficiency of DiSEL over the random method are given for different tag density and deployment scenarios.

Chapter 6

Tag Count Estimation for RFID MAC Protocols

The performance of RFID MAC algorithms is expressed in terms of the total time it takes by a reader to read all the tags in the reading range. One of the major MAC approaches for RFID systems is the framed slotted ALOHA based approach. An important design challenge to increase the performance of this class of algorithms is to estimate the remaining tag count before each reading round. It is proven that this class of algorithms achieve smallest total reading time when, at each reading round, the frame length is set equal to the actual number of remaining unread tags. Therefore for optimum performance, framed slotted ALOHA algorithms must adapt the frame size to the number of remaining tags at each reading round. Since a reader has no knowledge of actual remaining tag count before reading rounds, practical estimation algorithms must be available on the

reader side. In this chapter, we address the tag count estimation problem for such RFID systems. The introduced algorithm is an a posteriori tag count estimation scheme from the collision statistics of the previous reading round. We compare the algorithm with the optimum, lower bound and other a posteriori estimation algorithms and demonstrate its efficiency. The performance of the algorithm is better than the current a posteriori tag count estimation algorithms. The introduced algorithm also achieves a much smaller computational overhead compared to the other schemes in the literature.

6.1 A posteriori Remaining Tag Count Estimation Algorithms

A posteriori tag count estimation algorithms introduced in [15,40,46,85] make use of the collision statistics in estimating the remaining tag count for the next round. Problem is formulated as follows: assume there are n tags to be read, and let the frame length be L time slots. The probability of finding k tags on a given slot is a binomial distribution with n Bernouilli experiments and $1/L$ occupation probability.

$$B(k) = \binom{n}{k} \left(\frac{1}{L}\right)^k \left(1 - \frac{1}{L}\right)^{n-k} \tag{6.1}$$

Then the empty (p_e), success (p_s) and collision (p_c) probabilities for a given slot are obtained as

$$p_e = B(0) = (1 - \frac{1}{L})^n \tag{6.2}$$

$$p_s = B(1) = \frac{n}{L}(1 - \frac{1}{L})^{n-1} \tag{6.3}$$

$$p_c = 1 - p_e - p_s \tag{6.4}$$

since $p_e + p_s + p_c = 1$.

With n tags to be read, the probability of finding a single tag on a given slot is given by p_s. With L slots, the expected value of number of singly occupied slots is

$$E[S] = L.p_s = n(1 - \frac{1}{L})^{n-1} \tag{6.5}$$

Channel usage efficiency is defined as the ratio of expected value of successful slots count to the number of total slots.

$$U = \frac{E[S]}{L} = \frac{n}{L}(1 - \frac{1}{L})^{n-1} \tag{6.6}$$

To maximize the channel usage efficiency, the first derivative is taken with respect to L and its roots are found.

$$\frac{dU}{dL} = \frac{n(n-L)(L-1)^{n-2}}{L^{n+1}} \tag{6.7}$$

The maximum U is then obtained with $n = L$, which means that the number of slots should be set equal to the actual number of tags for maximum channel utilization, or throughput.

6.1.1 Chen's Method

In Chen's method [15], the probability that among L slots, there are C slots with collisions, E slots without transmission and S slots with single transmission, is modeled as a multinomial distribution with L independent trials.

$$P(E,S,C) = \frac{L!}{E!S!C!} p_e^E p_s^S p_c^C \tag{6.8}$$

For a read cycle with L slots, the a posteriori probability for the number of tags n, with given E, S, and C.

$$\begin{aligned} P(n|E,S,C) &= \frac{L!}{E!S!C!} \\ &\times \left[\left(1-\frac{1}{L}\right)^n\right]^E \left[\frac{n}{L}\left(1-\frac{1}{L}\right)^{n-1}\right]^S \\ &\times \left[1-\left(1-\frac{1}{L}\right)^n - \frac{n}{L}\left(1-\frac{1}{L}\right)^{n-1}\right]^C \end{aligned} \tag{6.9}$$

The decision rule proposed by Chen is to set the number of tags estimate equal to n that maximizes this probability, $P(n|E,S,C)$.

However, Chen's formulation does not take into account the fact that the outcomes of the L trials are not independent. The binomial distribution is the probability distribution of the number of successes in n independent Bernoulli trials, with the same probability of success in each trial. In the framed slotted ALOHA reading process, while performing L trials on a given round, the outcome of each trial, i.e., the placement of a tag on a slot randomly, effects the subsequent trials by changing the outcome probabilities.

6.1.2 Vogt's Method

Vogt's method [85] makes use of Chebyshevs inequality. Chebyshevs inequality states that the outcome of a random experiment involving a random variable is most likely somewhere near the expected value of it. Hence Vogt's method uses the n that minimizes the distance between read results and the expected values.

$$\varepsilon_{vd}(L,E,S,C) = min_n \left| \begin{pmatrix} a_0 \\ a_1 \\ a_m \end{pmatrix} - \begin{pmatrix} E \\ S \\ C \end{pmatrix} \right| \tag{6.10}$$

where a_0, a_1 and a_m are expected values of the number of empty, singly occupied and collision slots. They are defined as,

$$a_0 = LB(0) = L(1-\frac{1}{L})^n, \quad a_1 = LB(1) = n(1-\frac{1}{L})^{n-1}, \quad \text{and} \quad a_m = L - a_0 - a_1 \tag{6.11}$$

Note that for any algorithm, if the initial starting frame length is brought closer to the actual tag count, the performance of the algorithm will improve. However this knowledge is not available to the reader. Therefore the reader has to start from some appropriate initial slot count.

6.2 Proposed Algorithm

By checking the results of a reading round, we already know that there are at least $2C$ colliding tags that are waiting to be read over the next rounds. In order to approximate the actual number of unread tags we use this number as the lower bound. For a given

reading round, let C_n represent the expected number of collision slots where n tags are involved. Then,

- The expected value of collision slots count, $E(C) = (C_2 + C_3 + ... + C_n)$
- The expected value of number of remaining tags after a reading round, $E(N_{remaining}) = (2C_2 + 3C_3 + ... + nC_n)$
- The expected value of the lower bound for remaining tags count is $2E(C) = (2C_2 + 2C_3 + ... + 2C_n)$
- The expected value of the unknown parameter in our experiment is the value of $E(N_{remaining}) - 2E(C) = (C_3 + 2C_4 + 3C_5 + ... + (n-2)C_n)$

Let's define this unknown parameter as A. We know that, the expected value of $C_n = L.B(n)$. Then the expected value of A is equal to

$$E(A) = (C_3 + 2C_4 + 3C_5 + ... + (n-2)C_n) \quad = \sum_{i=1}^{n-2} L.i.\frac{n!}{(n-i-2)!(i+2)!}\left(\frac{1}{L}\right)^{i+2}\left(1-\frac{1}{L}\right)^{n-2-i} \tag{6.12}$$

For the optimum estimation case, i.e., when the number of tags is equal to number of slots ($n = L$), we plot the expected value of A in Figure-6.1. We observe that, $E(A)$ increases almost linearly with increasing L. In the same figure, we also plot the expected number of successful slots $E(S)$ and we observe a linear dependency between $E(S)$ and $E(A)$.

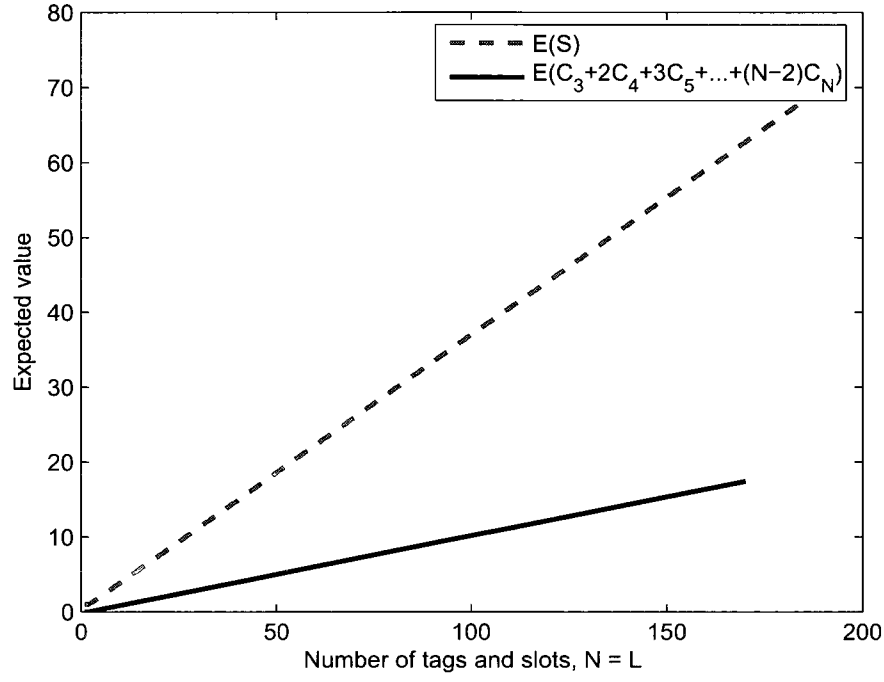

Figure 6.1: Expected values of S and A

Therefore we propose to approximate $E(A)$ as a linear function of $E(S)$ using

$$E(A) \cong \frac{1}{3.5} E(S) \tag{6.13}$$

where the constant 1/3.5 obtained numerically. When we set the remaining tag count to $N_{actual} = 2C + S/3.5$, we obtain very close performance results as the optimum oracle estimation, which sets the number of slots as equal to the actual number of remaining tags, as can be seen in Figure-6.2 and Figure-6.3. Since we now know this linear dependence on S, using trial an error, we balance the number of rounds and the number of slots required. We set the frame length L, as the remaining tag count estimate

$N_{estimate} = 2C + S$, where S represents the successful slots count and C represents the collision slots count of the current round[1]. Our estimation algorithm results in lower estimation error, lower number of total slots and lower number of rounds when compared to Vogt's and Chen's methods without requiring complex minimization or maximization routines on the reader side.

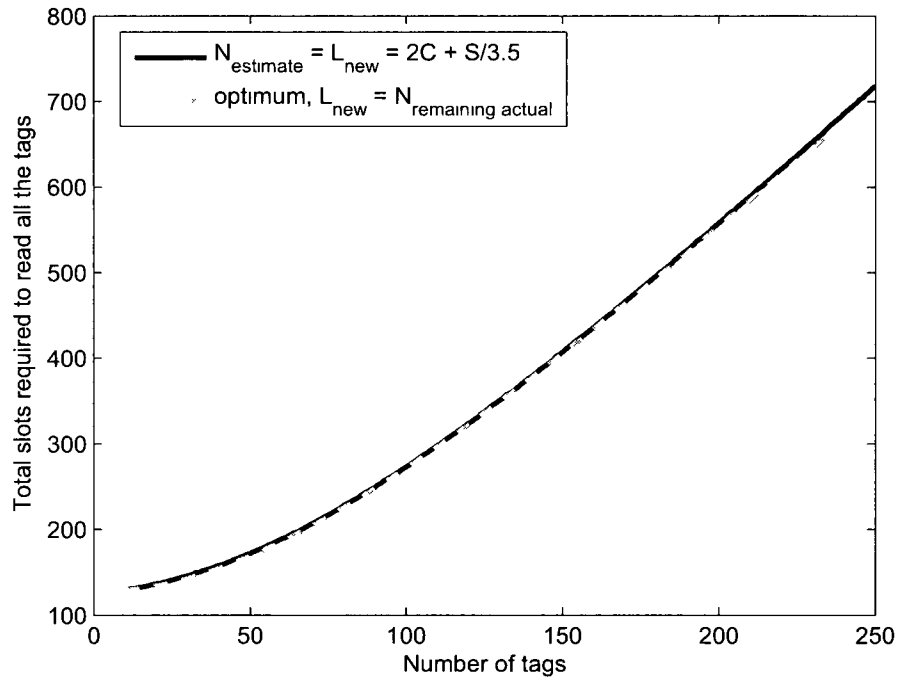

Figure 6.2: Total slots required, $L_{new} = 2C + S/3.5$ vs optimum

The simulations are performed according to Algorithm 1.

[1]Here we should emphasize that, if our tag count formulation was to be expressed as the current round's tag count estimation, it would be $N_{estimate} = 2C + 2S$. For the next round, since S tags are successful, the remaining tag count estimate will be $2C + S$.

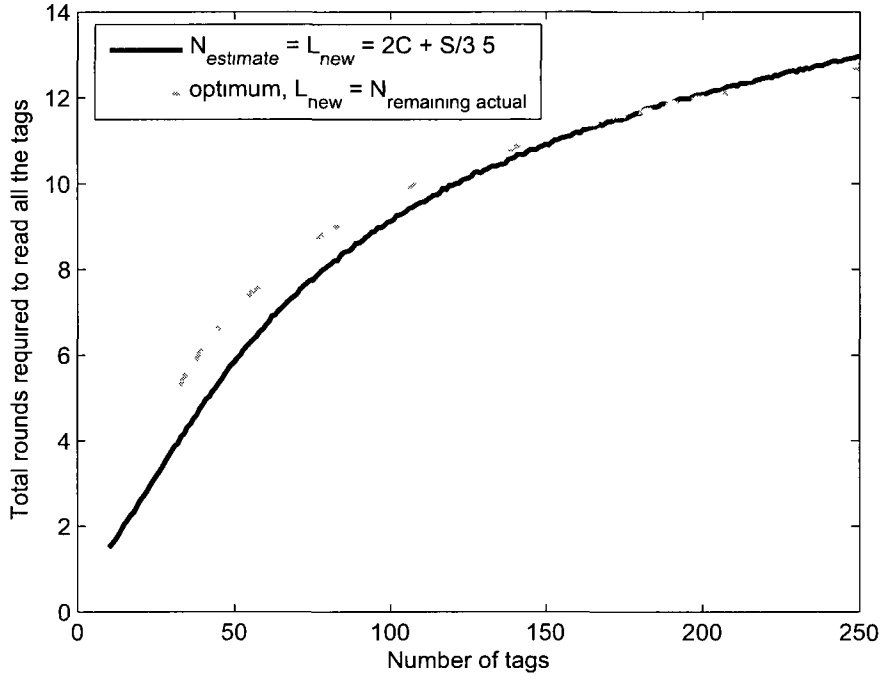

Figure 6.3: Total rounds required, $L_{new} = 2C + S/3.5$ vs optimum

6.3 Simulation Results

We compare the following remaining tag count estimation algorithms where $N_{estimate}$ represents the remaining tag count estimate :

- Optimum, $N_{estimate} = N_{actual}$
- Lower bound, $N_{estimate} = 2C$
- Vogt's algorithm
- Chen's algorithm

Algorithm 1 Remaining tag count estimate

Initial frame size, L_{init};

Current frame size, $L_{current} = L_{init}$;

$totalRoundsCount = 0$;

$totalSlotsCount = 0$;

while (there are unread tags) **do**

$totalRoundsCount++$;

$totalSlotsCount = totalSlotsCount + L_{current}$;

Initiate read cycle with the current frame size, $L_{current}$;

//Every remaining tag randomly selects a slot

Count empty (E), successful (S) and collision (C) slots

// Remaining tag count estimate is then

$N_{estimate} = L_{new} = 2C + S$;

$L_{current} = L_{new}$;

// repeat the cycle while there are unread tags

end while

- Our algorithm, $N_{estimate} = 2C + S$

6.3.1 Estimation Error

In this section we analyze the estimation error metric and the related tradeoffs. The normalized total number of errors in reading all the tags for a given number of actual

tags is the sum of single read cycle errors. In certain cases, this error function can be used to judge the quality of the tag count estimator. Error in a single read cycle is defined as

$$error = \frac{|n - \hat{n}|}{n} \tag{6.14}$$

where $\hat{n}$ is the tag count estimation The cumulative average estimation error for different number of actual slot counts is defined in Figure-6.4.

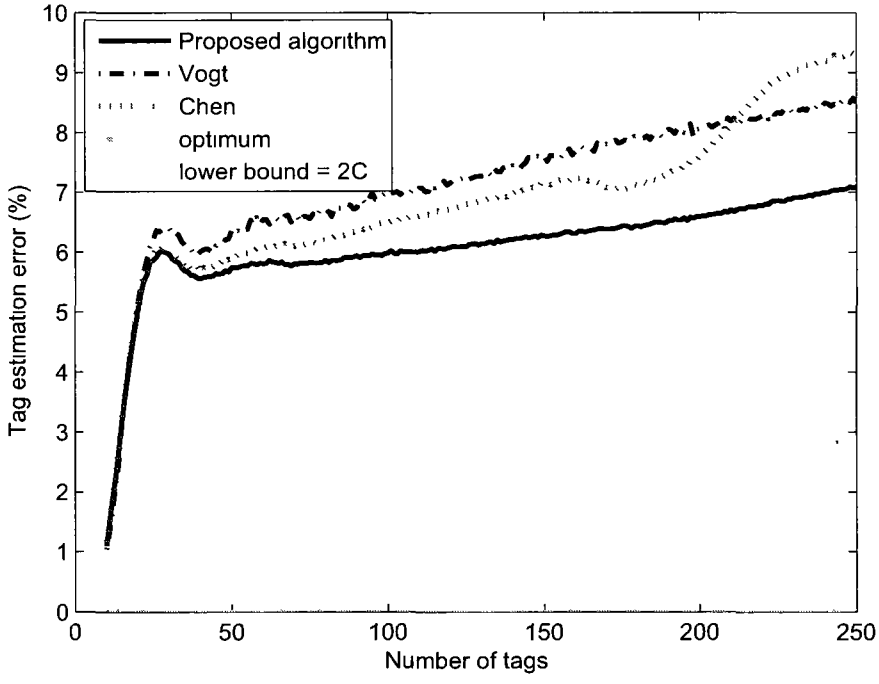

Figure 6.4: Tag estimation error

When the results related to estimation error metric are analyzed, we can see that a smaller average estimation error does not always result in smaller reading rounds count

For example, the *lower bound* algorithm gives a small cumulative average estimation error, however it has a high total number of required rounds. The downside of large number of rounds even if the total reading time is small, is the signalling and processing overhead which is difficult to predict and model in simulations. In practice, this overhead can be high and algorithms that have small total slots count while keeping the total number rounds under control are preferable.

6.3.2 Total reading time and total reading rounds

The total reading time is defined as the total number of slots multiplied with the slot duration. Initial slot count does not change the relative performance of the algorithms. In our simulations we selected the initial slot count, L_{init} as 128. Optimum and lower bound algorithms have the minimum total slots required. However they have very high number of required rounds, close to three times the number required by other algorithms. Figure-6.5 shows the performance of our algorithm in terms of the total time slots required. Another important metric measuring the performance of tag count estimation algorithms is the total rounds required to read all the tags. Figure-6.6 compares the performance of our scheme with the previous algorithms. Again, the number of total rounds metric is important because each reading round carries a handshaking and control messaging overhead, whose severity depends on the underlying communications system design. In any case, small number of rounds is an important design goal for estimation algorithms.

Our algorithm achieves better results for every comparison parameter. It has a smaller

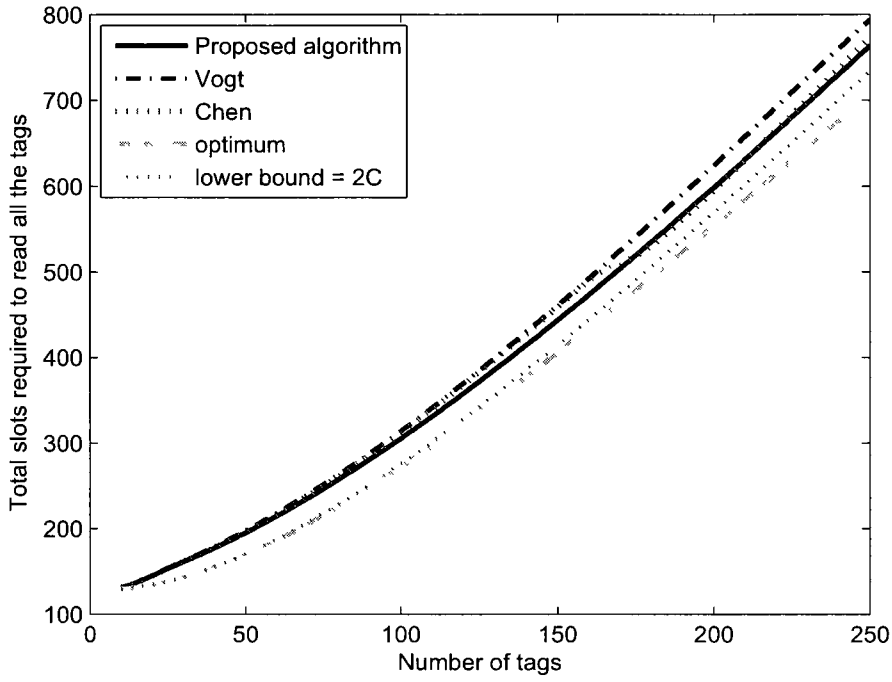

Figure 6.5: Total slots required

tag estimation error. It finishes in a smaller number of total slots and a smaller number of total rounds compared to the other algorithms. The benefits of our algorithm are more pronounced when the computational overhead is considered. Both [85] and [15] have comparatively higher computation time on the reader side. In order to come up with an estimate, Chen's algorithm finds the tag count that maximizes a nonlinear function. This requires the evaluation of that function which includes four factorials, and six exponentiations, for every tag count candidate in the entire scope of the candidates. Likewise, Vogt's algorithm finds the tag count that minimizes a nonlinear function by evaluating that function for the entire scope. Vogt's function contains six exponentiation,

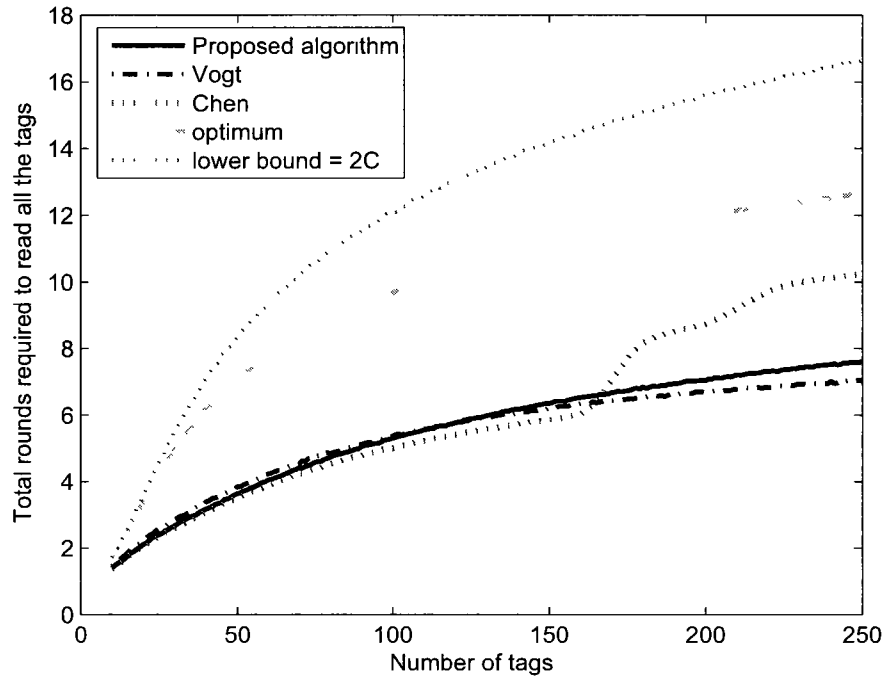

Figure 6.6: Total rounds required

while our algorithm requires a single multiplication and addition for an estimation.

6.4 Chapter Conclusions

In this chapter, we introduced a new tag number estimation scheme. Our algorithm performs better than the existing a posteriori tag count estimation algorithms. Current major RFID standard parts that deal with the collision avoidance problem such as ISO 18000-6 and ISO 14443-3 does not specify frame length estimation method for framed slotted ALOHA based algorithms. Our algorithm can be efficiently used in practice.

Another improvement brought by our algorithm is the elimination of complex reader side minimization and maximization calculations performed between reading rounds in the previous algorithms.

Chapter 7

Conclusions and Future Work Directions

Hardware and energy limitations of the low-power wireless embedded devices severely restrict the firmware size and complexity of the algorithms that are built for them. In order to deal with these limitations efficient cross-layer design methods jointly specifying hardware, protocol stack and applications can be used. Sensor and RFID systems are application specific, therefore cross-layering of physical, MAC and application layers is natural. In this thesis, we first gave a general overview of the cross-layer design approach and then introduced examples of this system level design methodology to enhance the security, medium access and networking performance and energy efficiency. We explained layer interactions and the importance of collaborative designs in seeking optimum performance for these system goals.

Chapter-3 presented two anomaly detection based security algorithms [54, 55] for wireless sensor networks, using the physical layer signal characteristics and network layer arrival patterns. Anomaly detection based security algorithms can be used with various parameters at different layers in stationary systems, especially our targets, sensor and RFID systems. We have shown that by analyzing the received packet features at different layers, a node can effectively identify an intruder impersonating a legitimate neighbor. The introduced detection algorithms are distributed since they run at each node independently from other nodes. Another important characteristic of the algorithms is their dynamic and learning nature. They are immune to instantaneous measurement results since they raise alarm flags if the deviations of short term statistics from the long term statistics are persistent over the event log.

The work presented in Chapter-3 can be extended in several ways:

- Information sharing among neighbor nodes for cooperative intrusion detection can be implemented to enhance detection probability.
- Deployment specific vulnerabilities and features of the network can be identified and new intrusion detection algorithms can be developed.
- Formal analysis of these algorithms can be performed to determine and eliminate the weak points of the algorithms against counter coercion attacks.

The duty-cycling operation has many constraints on the MAC and networking layers, and on the energy budget of wireless sensor nodes. In Chapter-4 we detailed an RFID

wakeup system to eliminate the duty-cycling process with physical layer signals. We proposed a boosting circuit and a low-threshold Schottky diode based rectifier for this goal. We demonstrated that, by collecting energy from the RF signal emitted from low-power sensor radios during their occasional high power burst transfers, a passive resonant voltage boosting circuit and the rectifier system can wake up a sensor radio and eliminate the need for the duty-cycling process.

An important future work of this study would be the hardware implementation of the boosting circuit and the rectifier.

In Chapter-5 we summarized the challenges of medium access control in passive RFID systems. We introduced the DiSEL algorithm [57], a MAC scheme for passive UHF RFID systems based on cross-layer design techniques. The protocol is an enhancement to framed slotted ALOHA based MAC protocols where tags randomly select a slot number over a given frame size. In DiSEL, tags select their transmission slot based on their distance from the reader which is deduced by the received power levels. The increased performance over the random slot selection method are demonstrated through simulations.

Further studies proposed to extend this line of research are as follows:

- Detailed and site-specific indoor UHF propagation models [23, 49] can be used to model the received power. The performance of DiSEL under these models can be re-assessed.

- Number of collisions on a given slot can be estimated using the total received power

in the collision slot divided by the closest successful slot's receive power. From this, new reading round's slot count can be estimated. This way total tag reading time will further be reduced.

- New cross-layer slot selection algorithms can be designed exploiting power-delay profiles of the received signal on a given slot at the reader.

Tag count estimation before each reading round is an important problem for RFID MAC algorithms based on framed slotted ALOHA. This class of MAC algorithms achieve smallest total reading time when, at each reading round, the frame length is set equal to the actual number of remaining unread tags. Current major RFID standard parts that deal with the collision avoidance problem do not specify frame length estimation method for framed slotted ALOHA based algorithms. In Chapter-6 we introduced an a posteriori tag count estimation algorithm for these RFID MAC protocols from the collision statistics of the previous reading round. We compared our algorithm with the optimum, lower bound and other a posteriori estimation algorithms and demonstrated its efficiency with extensive simulations. The introduced algorithm also achieves a much smaller computational overhead compared to the other schemes in the literature.

An interesting future work on this topic is the estimation of the tag count with the joint use of collision statistics and the physical layer measurements of the collision slots.

Bibliography

[1] IEEE std. 802.15.4 - 2003: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs). *available at http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.*

[2] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov. Cryptographic processors - A survey. *the Proceedings of the IEEE*, 94(2):357–369, Feb. 2006.

[3] S.R. Banerjee, R. Jesme, and R.A. Sainati. Performance analysis of short range UHF propagation as applicable to passive RFID. In *the Proceedings of the IEEE International Conference on RFID*, pages 30–36, 2007.

[4] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-key cryptography for RFID-tags. In *the Proceedings of the International Workshop on Pervasive Computing and Communication Security, PerSec'07*, pages 217–222, 2007.

[5] WP. Bender, P. Black, M. Grob, R. Padovani, N. Sindhushayana, and A. Viterbi. CDMA/HDR: A bandwidth efficient high speed wireless data service for nomadic users. pages 70–77, 2000.

[6] Calmels Benoit, Sbastien Canard, Marc Girault, and Herv Sibert. Low-cost cryptography for privacy in RFID systems. In *the Proceedings of the International Conference on Smart Card Research and Advanced Applications, CARDIS'06*, 2006.

[7] Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled RFID device. In *the Proceedings of the 14th conference on USENIX Security Symposium, SSYM'05*, 2005.

[8] Patrick Bosselmann and Bernhard Rembold. Investigations on UHF RFID wave propagation using a ray tracing simulator. *FREQUENZ: Journal of RF-Engineering and Telecommunications*, (60):38–45, 2006.

[9] David Brumley and Dan Boneh. Remote timing attacks are practical. In *the Proceedings of the 12th conference on USENIX Security Symposium, SSYM'03*, 2003.

[10] D.W. Carman, P.S. Kruus, and B.J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, 2002.

[11] H. Chae, D. Yeager, J. Smith, and K. Fu. Maximalist cryptography and computation on the WISP UHF RFID tag. In *the Proceedings of the Conference on RFID Security*, 2007.

[12] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *the Proceedings of the IEEE Symposium on Security and Privacy*, pages 197–215, 2003.

[13] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In *the Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO'99*, pages 398–412, 1999.

[14] Y.H. Chee, J. Rabaey, and A.M. Niknejad. A class A/B low power amplifier for wireless sensor networks. In *the Proceedings of the 2004 International Symposium on Circuits and Systems*, volume 4, pages 409–412, 2004.

[15] Wen-Tzu Chen. An accurate tag estimate method for improving the performance of an RFID anticollision algorithm based on dynamic frame length ALOHA. *IEEE Transactions on Automation Science and Engineering*, 6(1):9–15, 2009.

[16] Cirronet, Inc. *RF Power Options in ZigBee Solutions.* available at http://www.cirronet.com/pdf/wp_ZigBeePowerOptions.pdf.

[17] Yang Cui, Kazukuni Kobara, Kanta Matsuura, and Hideki Imai. Lightweight asymmetric privacy-preserving authentication protocols secure against active attack. In *the Proceedings of the International Workshop on Pervasive Computing and Communication Security, PerSec'07*, pages 223–228, 2007.

[18] J.-P. Curty, N. Joehl, C. Dehollain, and M.J. Declercq. Remotely powered addressable UHF RFID integrated system. *IEEE Journal of Solid-State Circuits*, 40(11):2193–2202, Nov. 2005.

[19] J.-P. Curty, N. Joehl, F. Krummenacher, C. Dehollain, and M.J. Declercq. A model for μ-power rectifier analysis and design. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications Circuits and Systems*, 52(12):2771–2779, Dec. 2005.

[20] J.L. da Silva, J. Shamberger, M.J. Ammer, C. Guo, S. Li, R. Shah, T. Tuan, M. Sheets, J.M. Rabaey, B. Nikolic, A. Sangiovanni-Vincentelli, and P. Wright. Design methodology for picoradio networks. In *the Proceedings of the Design, Automation and Test in Europe*, pages 314–323, 2001.

[21] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* 2002.

[22] I. Demirkol, C. Ersoy, and F. Alagoz. MAC protocols for wireless sensor networks: a survey. *IEEE Communications Magazine*, 44(4):115–121, 2006.

[23] T. Deyle, C.C. Kemp, and M.S. Reynolds. Probabilistic UHF RFID tag pose estimation with multiple antennas and a multipath RF propagation model. In *the Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS'08*, pages 1379–1384, 2008.

[24] Ember. *EM260: ZigBee/802.15.4 Network Processor.* available at http://www.ember.com/pdf/EM260/EM260_Datasheet.pdf.

[25] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *the Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41–47, 2002.

[26] Deborah Estrin, Akbar Sayeed, and Mani Srivastava. Wireless sensor networks. *Mobicom Tutorial, available at http://nesl.ee ucla.edu/tutorials/mobicom02/*, 2002.

[27] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong authentication for RFID systems using the AES algorithm. In *the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES'04*, volume 3156, pages 357–370, 2004.

[28] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.* John Wiley & Sons, Inc., 2003.

[29] Andrea Goldsmith. *Wireless Communications.* Cambridge University Press, 2005.

[30] Lin Gu and J.A. Stankovic. Radio-triggered wake-up capability for sensor networks. In *the Proceedings of the 10th IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS'04*, pages 27–36.

[31] J. Hall, M. Barbeau, and E. Kranakis. Detection of transient in radio frequency fingerprinting using phase characteristics of signals. In *the Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications, WOC*, pages 13–18, 2003.

[32] Panu Hamalainen, Timo Alho, Marko Hannikainen, and Timo D. Hamalainen. Design and implementation of low-area and low-power AES encryption hardware core. In *the Proceedings of the 9th EUROMICRO Conference on Digital System Design, DSD'06*, pages 577–583, 2006.

[33] E. Hess, N. Janssen, B. Meyer, and T. Schuetze. Information leakage attacks against smart card implementations of cryptographic algorithms and countermeasures - a survey. In *the Proceedings of the Eurosmart Security Conference*, pages 55–64, 2000.

[34] Yi-an Huang, Wei Fan, Wenke Lee, and Philip S. Yu. Cross-feature analysis for detecting ad-hoc routing anomalies. In *the Proceedings of the 23rd International Conference on Distributed Computing Systems, ICDCS'03*, pages 478–487, 2003.

[35] Yi-an Huang and Wenke Lee. A cooperative intrusion detection system for ad hoc networks. In *the Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks*, pages 135–147, 2003.

[36] Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and EM attacks on passive 13.56 MHz RFID devices. In *the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES'07*, volume 4727, pages 320–333, 2007.

[37] IEEE. *802.15.4 Regulatory Issues.* available at http://www.ieee802.org/15/pub/TG4.html.

[38] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *the Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, 2003.

[39] U. Karthaus and M. Fischer. Fully integrated passive UHF RFID transponder IC with 16.7-μW minimum RF input power. *IEEE Journal of Solid-State Circuits*, 38(10):1602–1608, Oct. 2003.

[40] G. Khandelwal, A. Yener, Kyounghwan Lee, and S. Serbetli. ASAP : A MAC protocol for dense and time constrained RFID systems. In *the Proceedings of the IEEE International Conference on Communications, ICC'06*, volume 9, pages 4028–4033.

[41] P. Kocher, J. Jaffe, and B. Jun. Introduction to differential power analysis and related attacks. Technical report, Cryptography Research Inc., 1998.

[42] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *the Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO'96*, pages 104–113, 1996.

[43] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *the Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO'99*, pages 388–397, 1999.

[44] K. Langendoen. *Medium Access Control in Wireless Sensor Networks, in book Medium Access Control in Wireless Networks, Volume II: Practice and Standards.* Nova Science Publishers, 2007.

[45] Yee Wei Law, Jeroen Doumen, and Pieter Hartel. Survey and benchmark of block ciphers for wireless sensor networks. *ACM Transactions on Sensor Networks*, 2(1):65–93, 2006.

[46] Su-Ryun Lee, Sung-Don Joo, and Chae-Woo Lee. An enhanced dynamic framed slotted ALOHA algorithm for RFID tag identification. In *the Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous'05*, pages 166–172, 2005.

[47] Xiaojun Lin, N.B. Shroff, and R. Srikant. A tutorial on cross-layer optimization in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(8):1452 –1463, 2006.

[48] S. Mangard and K. Schramm. Pinpointing the side-channel leakage of masked AES hardware implementations. In *the Proceedings of the CHES'06*, pages 76–90, 2006.

[49] G. Marrocco, E. Di Giampaolo, and R. Aliberti. Estimation of UHF RFID reading regions in real environments. *IEEE Antennas and Propagation Magazine*, 51(6):44–57, 2009.

[50] Nordic Semiconductor. *nRF24LU1:Single Chip 2.4GHz Transceiver.* available at http://www.nordicsemi.com/files/Prod_brief_RFSilicon_nRF24LU1.pdf.

[51] W. Nosovic and T.D. Todd. Scheduled rendezvous and RFID wakeup in embedded wireless networks. In *the Proceedings of the IEEE International Conference on Communications, ICC'02*, volume 5, pages 3325–3329.

[52] NXP Semiconductors. *Secure Smart Card Controller Platform.* available at http://www.nxp.com/documents/short_data_sheet/P5Cx009_P5Cx072_FAM_SDS.pdf.

[53] Ilker Onat and Ali Miri. A tag count estimation algorithm for dynamic framed ALOHA based RFID MAC protocols. *submitted to Pervasive and Mobile Computing Journal, Elsevier.*

[54] Ilker Onat and Ali Miri. An intrusion detection system for wireless sensor networks. In *the Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2005.

[55] Ilker Onat and Ali Miri. A real-time node-based traffic anomaly detection algorithm for wireless sensor networks. In *the Proceedings of the International Conference on Sensor Networks (SENET)*, 2005.

[56] Ilker Onat and Ali Miri. *Security in RFID and Sensor Networks*, chapter Designing Secure Wireless Embedded Systems, pages 510–522. Taylor & Francis Group, 2008.

[57] Ilker Onat and Ali Miri. DiSEL: A distance based slot selection protocol for framed slotted ALOHA RFID systems. In *the Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC'09*, 2009.

[58] Ilker Onat and Ali Miri. *to appear in Advanced Security and Privacy for RFID Technologies*, chapter RFID Wireless Link Threats. 2010.

[59] Yossef Oren and Adi Shamir. Remote password extraction from RFID tags. *IEEE Transactions on Computers*, 56(9):1292–1296, 2007.

[60] Siddika Berna Örs, Frank Gürkaynak, Elisabeth Oswald, and Bart Preneel. Power-analysis attack on an ASIC AES implementation. In *the Proceedings of the International Conference on Information Technology, ITCC'04*, volume 2, page 546, 2004.

[61] S.C.M. Perera, A.G. Williamson, and G.B. Rowe. Prediction of breakpoint distance in microcellular environments. *Electronics Letters*, 35(14):1135–1136, 1999.

[62] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In *the Proceedings of the International Conference on Ubiquitous Intelligence and Computing, UIC'06*, volume 4159, pages 912–923, 2006.

[63] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. EMAP: An efficient mutual authentication protocol for low-cost RFID tags. In *the Proceedings of the OTM Federated Conferences and Workshop: IS Workshop, IS'06*, volume 4277, pages 352–361, 2006.

[64] Charles E. Perkins and Elizabeth M. Royer. Ad hoc on-demand distance vector routing. In *the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1999.

[65] Adrian Perrig, Robert Szewczyk, Victor Wen, David E. Culler, and J. D. Tygar. SPINS: security protocols for sensor networks. *Mobile Computing and Networking*, pages 189–199, 2001.

[66] Philips Semiconductors. *Philips I*Code1 System Design, AN00025.* available at www.nxp.com/acrobat_download2/other/identification/SL048611.pdf.

[67] V. Pillai, H. Heinrich, D. Dieska, P.V. Nikitin, R. Martinez, and K.V.S. Rao. An ultra-low-power long range battery/passive RFID tag for UHF and microwave bands with a current consumption of 700 nA at 1.5 V. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 54(7):1500–1512, 2007.

[68] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and counter-measures for smart cards. In *the Proceedings of the International Conference on Research in Smart Cards, E-SMART'01*, pages 200–210, 2001.

[69] Theodore Rappaport. *Wireless Communications: Principles and Practice.* Prentice Hall, 2001.

[70] M.R. Rieback, B. Crispo P.N.D. Simpson, and A.S. Tanenbaum. RFID malware: Design principles and examples. *Pervasive and Mobile Computing (PMC) Journal*, 2, 405–426.

[71] Antonio G. Ruzzelli, Raja Jurdak, and Gregory M.P. O'Hare. The RFID wake-up impulse for multi-hop sensor networks. In *the Proceedings of the 1st ACM Workshop on Convergence of RFID and Wireless Sensor Networks and their Applications, SenseID'07*, 2007.

[72] Werner Schindler. A timing attack against RSA with the Chinese Remainder Theorem. In *the Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems, CHES'00*, pages 109–124, 2000.

[73] Kai Schramm, Gregor Leander, Patrick Felke, and Christof Paar. A collision-attack on AES combining side channel- and differential-attack. In *the Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, CHES'04*, pages 163–175, 2004.

[74] E. Setton, Taesang Yoo, Xiaoqing Zhu, A. Goldsmith, and B. Girod. Cross-layer design of ad hoc networks for real-time video streaming. *IEEE Wireless Communications*, 12(4):59 - 65, 2005.

[75] Sanjay Shakkottai, Theodore S. Rappaport, and Peter C. Karlsson. Cross-layer design for wireless networks. *IEEE Communications Magazine*, 41(10):74–80, 2003.

[76] A. Shameli, A. Safarian, A. Rofougaran, M. Rofougaran, and F. De Flaviis. Power harvester design for passive UHF RFID tag using a voltage boosting technique. *IEEE Transactions on Microwave Theory and Techniques*, 55(6):1089–1097, June 2007.

[77] Primoz Skraba, Hamid Aghajan, and Ahmad Bahai. RFID wakeup in event driven sensor networks. *SIGCOMM 2004 Poster Session.*

[78] I. Stojmenovic, A. Nayak, J. Kuruvila, F. Ovalle-Martinez, and E. Villanueva-Pena. Physical layer impact on the design and performance of routing and broadcasting protocols in ad hoc and sensor networks. *Computer Communications*, 28(10), 2005.

[79] V. R. Syrotiuk and A. Bikki. *Ad Hoc Networking*, chapter Modeling Cross Layer Interaction using Inverse Optimization, pages 411–426. John Wiley & Sons, 2004.

[80] Texas Instruments. *CC2420: Single-Chip 2.4 GHz IEEE 802.15.4 Compliant and ZigBee Ready RF Transceiver.* available at http://focus.ti.com/docs/prod/folders/print/cc2420.html.

[81] Texas Instruments. *Choosing An Ultralow-Power MCU.* available at http://focus.ti.com/lit/an/slaa207/slaa207.pdf.

[82] T. Umeda, H. Yoshida, S. Sekine, Y. Fujita, T. Suzuki, and S. Otaka. A 950-MHz rectifier circuit for sensor network tags with 10-m distance. *IEEE Journal of Solid-State Circuits*, 41(1):35–41, 2006.

[83] B. van der Doorn, W. Kavelaars, and K. Langendoen. A prototype low-cost wakeup radio for the 868 MHz band. *International Journal of Sensor Networks, IJSNet*, 2008.

[84] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer, and Richard A. Kemmerer. An intrusion detection tool for AODV-based ad hoc wireless networks. In *the Proceedings of the 20th Annual Computer Security Applications Conference*, pages 16–27, 2004.

[85] H. Vogt. Multiple object identification with passive RFID tags. In *the Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, volume 3, 2002.

[86] J.E. Wieselthier, A. Ephremides, and L.A. Michaels. An exact analysis and performance evaluation of framed ALOHA with capture. *IEEE Transactions on Communications*, 37(2):125–137, 1989.

[87] H. Yan, J.G. Macias Montero, A. Akhnoukh, L.C.N. de Vreede, and J.N. Burghartz. An integration scheme for RF power harvesting. In *the Proceedings of the STW Annual Workshop on Semiconductor Advances for Future Electronics and Sensors, SAFE'05*, June 2005.

[88] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. *Mobile Computing and Networking*, pages 275–283, 2000.

[89] Yongguang Zhang, Wenke Lee, and Yi-An Huang. Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 9(5):545–556, 2003.

[90] Marco Zuniga and Bhaskar Krishnamachari. Analyzing the transitional region in low power wireless links. In *the Proceedings of the IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON)*, 2004.