Design of Efficient MAC Protocols for IEEE 802.15.4-based Wireless Sensor Networks

By

Mounib Khanafer

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 Electrical Engineering and Computer Science

Faculty of Engineering

University of Ottawa

Abstract

Wireless Sensor Networks (WSNs) have enticed a strong attention in the research community due to the broad range of applications and services they support. WSNs are composed of intelligent sensor nodes that have the capabilities to monitor different types of environmental phenomena or critical activities. Sensor nodes operate under stringent requirements of scarce power resources, limited storage capacities, limited processing capabilities, and hostile environmental surroundings. However, conserving sensor nodes' power resources is the top priority requirement in the design of a WSN as it has a direct impact on its lifetime. The IEEE 802.15.4 standard defines a set of specifications for both the PHY layer and the MAC sub-layer that abide by the distinguished requirements of WSNs. The standard's MAC protocol employs an intelligent backoff algorithm, called the Binary Exponent Backoff (BEB), that minimizes the drainage of power in these networks. In this thesis we present an in-depth study of the IEEE 802.15.4 MAC protocol to highlight both its strong and weak aspects. We show that we have enticing opportunities to improve the performance of this protocol in the context of WSNs. We propose three new backoff algorithms, namely, the Standby-BEB (SB-BEB), the Adaptive Backoff Algorithm (ABA), and the Priority-Based BEB (PB-BEB), to replace the standard BEB. The main contribution of the thesis is that it develops a new design concept that drives the design of efficient backoff algorithms for the IEEE 802.15.4-based WSNs. The concept dictates that controlling the algorithms parameters *probabilistically* has a direct impact on enhancing the backoff algorithm's performance. We provide detailed discrete-time Markov-based models (for AB-BEB and ABA) and extensive simulation studies (for the three algorithms) to prove the superiority of our new algorithms over the standard BEB.

Acknowledgements

I'm indebted to many people for the accomplishment of this thesis. Special thanks to my supervisor, Prof. Hussein T. Mouftah, for his strong support and care throughout the preparation for this thesis. Prof. Mouftah was always willing to encourage and engage in constructive discussions that contributed solely to the completeness of this thesis.

Warm thanks to Mr. Mouhcine Guennoun, my colleague at the School of Electrical Engineering and Computer Science, who made his strong and broad technical background ready for my utilization. Mr. Guennoun spent with me a considerable amount of his time in brainstorming ideas and approaches. His sharp critique and careful revisions of my work reflected in elegant and successful research achievements.

Dedication

I dedicate this thesis to my parents, Mohamad-Ali and Fawzie, who encouraged me to pursue my doctoral study. They have been the major driving force that led to my success.

I also dedicate this thesis to my brothers, Hassib, Adib, Nassib, Labib, and Ali, and sisters, Majida, Aida, Raeda, Khalida, and Sajida. Their existence beside me has been a valuable source of inspiration.

In particular, I dedicate this thesis to my wife, Maysaa, and beloved children, Mariam, Mira, and Mohamad. Their limitless patience and priceless support have been pivotal to the success I achieved. Maysaa has keenly watched every stage of my thesis and provided exceptional sacrifice without which this thesis would have never seen the light. A lot of time should have been spent with you and our children, and I'm indebted to all of you to get this work done.

Table of Contents

List of Tables

List of Figures

List of Acronyms

ABA	Adaptive Backoff Algorithm
ACK	Acknowledgement packet
BE	Backoff Exponent
BEB	Binary Exponent Backoff
BI	Beacon Interval
BS	Base Station
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CSMA-CA	Carrier Sense Multiple Access-Collision Avoidance
CV(RMSD)	Coefficient of variation of the root-mean-square deviation
CW	Contention Window
GTS	Guaranteed Time Slot
MAC	Medium Access Control
PB-BEB	Priority-Based BEB
SD	Superframe Duration
SB-BEB	Standby BEB
WSN	Wireless Sensor Network

List of Symbols

α	Probability of finding the channel busy during CCA1
$b_{i,j}$	Probability of being at state (i, j) in the Markov chain
β	Probability of finding the channel busy during CCA2
m	Maximum number of allowed backoffs before discarding a packet
n	Maximum number of allowed re-transmissions before discarding a packet
L	Length of the packet
L_{ACK}	Length of the ACK packet
L_c	Duration of packet collision
L_s	Duration of packet transmission
N	Number of nodes in the network
N_C	Eexpected number of nodes involved in a collision
π_{B_i}	Probability of experiencing the *i*th backoff
π_{C_i}	Probability of experiencing the *i*th collision
π_f	Probability of packet transmission failure
π_s	Probability of successful packet transmission
P_c	Probability of packet collision
τ	Probability of having a node attempt CCA1
T_{CC}	Time wasted while the channel observes a collision
T_{CI}	Time wasted while the channel is idle with no activities

Chapter 1

Introduction

1.1 Background

The unprecedented advances in hardware manufacturing technology and the advent of the Micro-Electro-Mechanical-Switches (MEMS) paved the way for building smart sensor nodes that are capable of performing three important functions: sensing, processing, and wireless communication. These wireless sensor nodes are characterized by being intelligent, small-sized, low in cost, battery-driven, and easy to install and repair. These characteristics opened wide doors for a broad range of applications attained by deploying wireless sensor nodes in a dense, distributed manner to form specialized Wireless Sensor Networks (WSNs). The main objective of WSNs is to monitor physical or environmental phenomena like temperature, sound, vibration, relative humidity, pollutants … etc. The data collected by sensor nodes is reported to a central processing unit that analyses the gathered data and takes certain measures depending on the implemented application. Starting with critical military applications like battlefield surveillance, WSNs eventually entered enormous number of civil applications such as motion tracking, traffic monitoring, fire detection, seismic sensing, home automation, to mention only a few (see [BAK07], [SIM04], [YAP05], and [ZHA04] for more examples). The different aspects of WSNs attracted extensive research activities and a huge body of studies is now available in the literature [YIC08] [AKY02]. The development of WSN's architectures highly benefited from the wide experience in designing architectures for self-organizing, mobile, ad hoc networks [KAR05]. The

latter show emphasis on the need for decentralized, distributed form of organization and this is a shared characteristic with WSNs. WSN's design also benefit from the evolutions in real-time computing, peer-to-peer computing, active networks and mobile agents/swarm intelligence. Besides the networking and computing concepts just mentioned, many other factors play a significant role when devising architectures for a WSN. In the following, we list the critical factors that distinguish the design of WSNs' protocols/architectures from other types of wireless networks:

1. Power Consumption: this is a primary design factor for any WSN. Sensor nodes are battery-operated and they should utilize algorithms or protocols that are conservative in their power requirements. Minimizing power consumption rates can effectively prolong the lifetime of the network. In fact, *power conservation* is a distinguishing design factor for WSNs. Other wireless networks, depending on the nature of services they deliver, may consider QoS parameters (like, delay, throughput, fairness, etc.) as key design requirements. However, the nature of the tasks handled by the sensor nodes and the design of their platforms make it highly important to preserve nodes' power resources as much as possible. Therefore, prolonging the lifetime of WSNs becomes an essential design factor for these networks. Based on this observation, research activities target the development of power-aware protocols for WSNs. These protocols should carefully design the duty cycle of nodes (that is, when the nodes should be active or inactive). In fact, power-awareness should be incorporated in every stage of designing a WSN, which imposes constraints on the size and complexity of a sensor node platform.
2. Deployment Environment: the harsh conditions in some deployment environments (like battlefields and forests) make sensor nodes prone to frequent failures. These failures may lead

to network partitioning, and WSNs should self-adapt to these events and mange to operate as expected. These environments make it impractical to replace or recharge the nodes that fail or completely deplete their power resources. Introducing efficient protocols for WSNs under such tight requirements is a challenging problem. This necessitates the need for lightweight algorithms that are conservative in their power, memory, and processing requirements.

3. Fault Tolerance: WSNs are mainly used for monitoring critical phenomena. Therefore, it is essential for a WSN to sustain its functionality without disruptions, even if some nodes malfunction or die. Usually, WSNs are deployed in hostile environments where nodes may be damaged, due to environmental interference, or eventually die due to the impracticality of recharging or replacing their batteries. As mentioned above, frequent failure of nodes may result in severe situations like partitioning the network. The design of a WSN should guarantee that its functionality and services are never degraded by these failures.
4. Scalability: sensor nodes are deployed densely to form a WSN. This huge number of nodes has a direct impact on the design of schemes and protocols at different layers. For example, a MAC protocol (data-link layer) should be able to grant, in a fair fashion, each node access to the medium while minimizing or preventing collisions, which is very difficult given the huge number of available nodes. Also, a routing protocol (network layer) that depends on exchanging routing tables among nodes may not be efficient since there will be excessive control traffic that underutilizes the bandwidth of the medium. This motivates the use of distributed, rather than centralized, solutions for WSNs.
5. Production Cost: the cost of a single sensor node should be minimized since it determines the overall cost of the whole network under design.
6. Network Topology: the fact that WSNs are constituted by a huge number of nodes raises the

challenge of network topology maintenance and modification. The challenge occurs starting at the early stage of nodes deployment. Sensor nodes can be either thrown in a mass (e.g., from a plane) or manually placed one by one (e.g., by a human or a robot) in the field. Also, after nodes deployment, topology may change due to failures in some nodes, changes in nodes locations, lack of reachability (due to jamming for instance), and huge reductions in power resources at some nodes (which affect their transmission power levels to the limit that they vanish from the vicinity of neighboring nodes). The WSN should be able to adapt to these sudden changes to avoid any degradations in its functionality.

7. Security: in the environment of deployment, sensor nodes are either deployed very close to the phenomenon of interest or directly inside it. As a result, we can see that WSNs are usually not supervised (especially in remote geographic areas). This means that WSNs may be an enticing target for intruders.
8. QoS Support: WSNs support a very limited bandwidth (far less than 1 Mbps). This factor affects the time-sensitive applications (especially in military) that require support for real-time communication with guarantees on maximum delay, minimum bandwidth, and other QoS parameters.

With all these facts in mind, a huge number of architectures have been proposed for WSNs in the literature (the interested reader is referred to [KAR05] where the authors provide a comprehensive list of publications dedicated to explore WSN architectures). In general, nodes of a WSN are scattered in a field. These nodes collaborate in gathering data and disseminating them to a *sink* node. Usually, the sink node is a base station (BS), which is a single powerful station that connects the WSN to a wired network. A BS is usually supported with more power resources and far more communication and processing capabilities than a wireless sensor node.

We can identify two basic WSN architectures, and most of the other architectures can be derived from, or understood based on, them:

1. The Layered Architecture: Sensor nodes in this architecture are arranged in layers around the BS with each layer containing nodes that have the same hop-count to the BS. Nodes that are one-hop away from the BS are included in the first layer (1-hop layer); nodes that are two-hops away from the BS are included in the second layer (2-hop layer); and so on. The main advantage of this architecture is that nodes in a layer are involved in a short-distance communication with their neighboring layers. This leads to efficient power conservation.
2. The Clustered Architecture: Sensor nodes in this architecture are arranged in clusters, each governed by an elected cluster-head. In this architecture, nodes in a cluster exchange packets with their respective cluster-head. Only the cluster-heads communicate with the BS. In each cluster, the cluster-head aggregates the data it receives from the cluster members and eliminates any occurring redundancy. The latter feature significantly reduces the volume of communication traffic received by the BS.

The IEEE 802.15.4 standard emerges as the de facto set of specifications recommended for implementation in WSNs. IEEE 802.15.4 defines the specifications of the PHY layer and the MAC sub-layer in wireless devices that utilize low data rates, low-power, and short-range radio frequency transmissions in a wireless personal area network (WPAN) [RED-09]. This standard is quite suitable for implementation in WSNs as it conforms to their requirements and constraints

(see Appendix A for a detailed description of IEEE 802.15.4)[1]. In fact, the IEEE 802.15.4 MAC protocol is of major interest for us in this thesis. This is because it orchestrates the sensor nodes' access to the communication medium, and therefore, it plays a significant role in consuming nodes' power resources. Due to the diverse domain of WSN-based applications, IEEE 802.15.4 MAC has enticed considerable research activities to unveil its capabilities and improve its performance. In general, these activities have focused on two dimensions:

1. Mathematical modeling of IEEE 802.15.4 MAC: Extensive reports have worked on developing accurate analytical models that can predict the theoretical behavior of IEEE 802.15.4 MAC. A considerable portion of these reports used Markov-based analysis to develop their models. The objective of these models is to identify opportunities to enhance the performance of IEEE 802.15.4 MAC and mitigate any source of deterioration in it (see Chapter 2 for more details).
2. Enhancing IEEE 802.15.4 MAC: Modifying IEEE 802.15.4 MAC such that it achieves a superior functionality has received a strong attention in the research community. These modifications are mainly based on the available mathematical models or simulation studies that demonstrated the need to take IEEE 802.15.4 MAC's performance to the next level (see Chapter 2 for more details).

1.2 Motivation

The IEEE 802.15.4 MAC protocol manages sensor nodes' access to the wireless medium by utilizing both slotted and unslotted Carrier Sense Multiple Access-Collision Avoidance

[1] The reader is encouraged to review Appendix A to be familiar with several terminologies and concepts that we mention in the rest of this thesis.

(CSMA-CA) mechanisms. The latter mechanisms are employed as a means to reduce the level of collisions over the wireless medium. The slotted CSMA-CA mechanism adopts the Binary Exponent Backoff (BEB) approach to control the states a sensor node goes through while attempting to gain access to the medium. BEB is an ingenious backoff algorithm that has been originally employed in the IEEE 802.11 standard. This algorithm is distinguished by several strong aspects that are beneficial to WSNs. In particular, the employment of a backoff mechanism is an ingenious approach to conserve sensor nodes' power resources while reducing the likelihood of collisions over the communication medium. Nodes can conserve power because they remain in a sleep mode while waiting for an opportunity to contend for the medium. Having some nodes in the sleep state reduces the number of nodes that are about to conduct their CCAs, which reduces the probability of packet collisions. Also, the incorporation of two CCA periods is used as a means to protect the ACK packet against collisions. In other words, if a node is performing its CCA1 at the same instant that another node has finished its packet transmission; the first node will sense the medium free. Therefore, in order to give the second node a chance to receive its ACK packet, the first node is required to perform another CCA. This way, IEEE 802.15.4 MAC has implicitly employed a priority-based approach in which the ACK packet is favored over other data packets. Furthermore, the idea behind incrementing BE is to find its appropriate value that better adapts the duration of backoff to the level of activity over the communication medium. With that, nodes gradually adapt their duty cycles in a fashion that reduces the possibility of suffering from a collision. On the long-term, nodes will find themselves treated equally in terms of the chance to access the medium (long-term fairness).

However, we can identify several weaknesses in the IEEE 802.15.4 MAC protocol that can lead to deterioration in the performance. The selection of BE is quite random and does not take

into consideration the number of nodes available in the network, the level of communication activity over the medium (at the time of selecting BE), and the likelihood of packet collisions. A node with a packet to send *always* increases BE gradually in the same manner (that is with steps of 1). This is done regardless of how long the node has been trying to access the medium, what traffic intensity is currently available over the medium, or how urgent the node's traffic is. Also, BE is reset to its minimum after a successful transmission, discarding a packet, or exhausting the maximum number of transmission retries. This reset is done blindly without considering the reasons behind the failed (or the failed trials of) transmissions. In other words, the employed BEB is "memory-less" [ALB09] as it keeps no information about the network status or conditions. Besides, we may encounter situations where nodes are sleeping more than needed (because the selection of BE is random), and this may lead to having the medium idle for unnecessary extended periods of time. This has a direct impact on the throughput of the system.

Also, the functionality of BEB is mainly deterministic and responds slowly to the changes in the network (in terms of the size of the network, the intensity of the traffic load…etc). The algorithm lacks dynamic, adaptive capabilities that can optimize the duty cycle of the sensor nodes such that minimal power expenditure is experienced.

Moreover, nodes that cannot complete their transaction during the current CAP are required to postpone their transmission to the beginning of the next CAP. The problem with this approach is that at the beginning of the next superframe we may have multiple simultaneous transmissions that are about to contend for the medium [KOU06]. This situation leads to high probabilities of collisions that can degrade the throughput of the overall network.

IEEE 802.15.4 MAC may also behave unfairly, on the short-term, under saturation conditions (that is, when nodes have always packets to send) [KAM08]. This can be seen from

noticing that a node that fails to access the medium tends to backoff for longer periods (because BE keeps increasing as mentioned earlier), reducing its opportunity of sending its packets. However, a node that has just finished its successful transmission will reset its BE to its minimum, which results in shorter backoff periods and thus higher chances of accessing the medium. That is, the last successful node is favored on the account of other nodes [XU01]. Clearly, under saturation conditions we will face a high rate of packet collisions, which leads to excessive power consumption and degraded throughput [LEE08]. Furthermore, this behavior raises serious security concerns. A selfish node may deliberately tune its BE such that it always achieves the minimum backoff period among the nodes. That way, the selfish node will access the medium much more frequently than the other nodes in the network (for more details on this misbehavior and how to mitigate it, see [SER10], [GUA06], [GUA08], and [RAY06]). On the other hand, a node may act maliciously by tuning BE to be at its maximum. This way, the node refrains from accessing the medium, which discourages other nodes from using this node as their next hop while forwarding packets.

IEEE 802.15.4 MAC suffers also from the lack of any measures for prioritizing traffics or nodes. The only *implicit* prioritization considered by the standard is associated with the ACK packet, which is assigned a higher priority over other packets. No special rules are employed to classify traffics based on their urgency, or to classify nodes based on their persistency to access the medium. This behaviour can burden nodes' power resources as certain nodes, which may be persistent in their access attempts, may deplete their batteries at a higher pace than other nodes.

These functionality issues in IEEE 802.15.4 MAC are far from being acceptable in WSN. Therefore, new strategies and algorithms are needed to mitigate many of these pitfalls such that a more efficient performance is achieved.

1.3 Objectives

The objective of this thesis is to conduct a thorough study of the IEEE 802.15.4 MAC protocol and develop efficient enhancements to its backoff algorithm. This study considers both theoretical analysis and simulations to provide a stronger understanding of the standard, and therefore, pave the way for new enhancements. The latter form a foundation for new backoff algorithms that can achieve promising performance in WSNs. It is a pivotal target in our work to support IEEE 802.15.4 MAC with adaptive, distributed, power-conservative backoff algorithms that can operate in WSNs more efficiently.

1.4 Contributions

The main research contributions of this thesis are as follows:

1. We develop a new concept, named the collision-aware concept, that drives the development of efficient backoff algorithms for the IEEE 802.15.4 MAC protocol.
2. We introduce three novel backoff algorithms that enhance the performance of the IEEE 802.15.4 MAC protocol in WSNs.
3. We develop a simplified, yet accurate, Markov-based model that can capture the core functionality of the backoff algorithm in IEEE 802.15.4 MAC. This model can provide the basis for further extensions to this MAC protocol. The model avoids the complexity that accompanied most of the available contributions in the literature and can be easily modified to reflect the functionality of other backoff algorithms.
4. We develop a user-defined, C-based simulator that implements the functionality of the IEEE 802.15.4 MAC protocol. The simulator can be easily extended/modified to capture the functionality of various MAC protocols proposed in the literature for the IEEE 802.15.4 standard.

5. We provide a new categorization of the available research proposals to improve the IEEE 802.15.4 MAC protocol. This categorization helps in identifying the key factors that should be considered when designing new MAC protocols for WSNs.

1.5 Thesis Outline

The remainder of this thesis is organized as follows. Chapter 2 surveys the available research contributions to enhance the IEEE 802.15.4 MAC protocol. Chapter 3 introduces our first new backoff algorithm, the Standby-BEB, that targets enhancing the savings in power in WSNSs. Chapter 4 describes our second new backoff algorithm, the Adaptive Backoff Algorithm that aims at enhancing the performance in terms of channel utilization. Chapter 5 presents our third new backoff algorithm, the Priority-Based BEB, that supports the prioritization among sensor nodes. Finally, Chapter 6 concludes this thesis and envisions future research directions.

1.6 List of Publications

1.6.1 Journal Papers

1. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "A Probabilistic, Collision-Aware MAC Protocol for Wireless Sensor Networks," submitted.
2. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "Priority-Based CCA Periods for Efficient and Reliable Communications in Wireless Sensor Networks," Wireless Sensor Network, vol. 4, no. 2, pp. 45-51, Feb. 2012.

1.6.2 Conference Papers

3. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "An Efficient Adaptive Backoff Algorithm for Wireless Sensor Networks," Proceedings of IEEE Global Communications Conference (GLOBECOM '11), Houston, Texas, USA, Dec. 2011.
4. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "Adaptive Sleeping Periods in Slotted IEEE 802.15.4 for Efficient Energy Savings: Markov-Based Theoretical Analysis," Proceedings of IEEE International Conference on Communications (ICC '11), Kyoto, Japan, Jun. 2011.
5. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "Extending Beacon-Enabled IEEE 802.15.4 to achieve Efficient Energy Savings: Simulation-Based Performance Analysis," Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security Program (NTMS '11), Paris, France, Feb. 2011.
6. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "Intrusion Detection System for WSN-based Intelligent Transportation Systems," Proceedings of IEEE Global Communications Conference (GLOBECOM '10), Miami, Florida, USA, Dec. 2010.
7. Mounib Khanafer, Mouhcine Guennoun, Hussein T. Mouftah, "WSN Architectures for Intelligent Transportation Systems," Proceedings of the 3rd IFIP International Conference on New Technologies, Mobility, and Security (NTMS '09), Cairo, Egypt, Dec. 2009.
8. Mounib Khanafer, Mouhcine Guennoun and Hussein T. Mouftah, "An Efficient Adaptive Backoff Algorithm for Wireless Sensor Networks," a poster presented at 2011 WiSense Workshop, University of Ottawa, Ottawa, September 2011 ***(First Best Poster Award)*.**

9. Mounib Khanafer, Mouhcine Guennoun and Hussein T. Mouftah, “Intrusion Detection in WSN-based Intelligent Transportation Systems,” a poster presented at 2011 NSERC-DIVA Workshop, University of Ottawa, Ottawa, September 2011.
10. Mounib Khanafer and Hussein T. Mouftah, “WSN Architectures for Intelligent Transportation Systems,” a poster presented at 2009 WiSense Workshop, University of Ottawa, Ottawa, July 2009.

Chapter 2

Survey of Related Work

2.1 Introduction

The IEEE 802.15.4 standard is the de facto set of specifications recommended to operate WSNs. The broad range of applications inspired by the advent of WSNs, along with the different performance requirements of these applications, have enticed the research community to focus on enhancing IEEE 802.15.4 MAC to mitigate its shortcomings. IEEE 802.15.4 MAC has been under the scope of research interest for more than a decade, with different objectives motivating the different research groups. These objectives include mainly reducing power consumption, improving channel utilization/throughput, improving packet delivery ratio/reliability, reducing the probability of collision, and reducing end-to-end delays. In achieving these targets, different approaches have been adopted and we review and discuss these approaches in this chapter. In the rest of this chapter we firstly review the works that targeted improving IEEE 802.15.4 MAC (Section 2.2), and then highlight the conclusions we draw from this review (Section 2.3).

2.2 Approaches to Improve IEEE 802.15.4 MAC

We can categorize the available literature to improve the IEEE 802.15.4 MAC protocol as follows:

– *Parameter Tuning-Based approaches*: These approaches are in favour of minimizing the modifications made to the standard in order to benefit from its strengths in terms of supporting the distinguishing characteristics of WSNs. Therefore, they argue that superior

performance can be achieved with the standard provided that its parameters are tuned properly. The benefit of these approaches is that they attempt to avoid introducing new overheads that may burden the sensor nodes' platforms with additional power expenditures. The drawback of these approaches, however, is that they tend to be application-specific and may require the sensor nodes to solve optimization problems in order to find the best tuning of their parameters, which may lead to extra power consumptions. Examples of these approaches include [ANA11], [PAR10], [ZHA10], and [POL08].

- *Cross Layer-Based approaches*: These approaches advocate the collaboration and exchange of information among the different layers of the protocol stack such that a better tuning of the MAC layer parameters is achieved. While these approaches may not necessarily change the standard itself, they base its parameters' configuration on the information provided by other layers, and thus excessive latency may be incurred. This is besides the overhead of changing the architecture of the protocol stack such that a new control channel or layer is used to convey the configuration data from a layer to another. However, the benefit of these approaches is that they work on having a comprehensive solution that optimizes the performance of the sensor node. Examples of these approaches include [FRA11] and [MAR10].
- *IEEE 802.11-Based approaches*: These approaches exploit the fact that BEB has been originally deployed in IEEE 802.11. Therefore, they migrate some solutions that have been proposed for IEEE 802.11 for deployment in the context of IEEE 802.15.4. These approaches anticipate that the solutions that have proven efficient in IEEE 802.11 should work properly in IEEE 802.15.4 networks. However, the main drawback of these approaches is that IEEE 802.11-based algorithms have not been designed considering the conservation of power as a

primary requirement. The latter is a pivotal requirement for IEEE 802.15.4-based WSNs. An example of these approaches is [MIN07].

- *Protection-Based approaches*: These are security-motivated approaches that focus on modifying the BEB algorithm to prevent some nodes from exploiting its vulnerabilities. These nodes tend to tune BEB's parameters such that they gain a more frequent access to the medium (selfish misbehaviour). The main challenge against these approaches is how to define strong security algorithms that are power-efficient. This is because of that strong security algorithms are usually complex and power-hungry and any simplification to their design may result in weak protection to the sensor nodes. Examples of these approaches include [SER10], [GUA06], and [RAY06].
- *Priority-Based approaches*: These approaches work on improving IEEE 802.15.4 MAC by recognizing the need to prioritize nodes' access to the medium. These approaches highlight the fact that the standard does not have special measures to categorize nodes, based on the urgency of their traffics for example, such that nodes are treated equally and fairly. Examples of these approaches include [SHI11], [SEV10], [JAR10], [TAK10], [KIM10], [NDI09], and [HUA08].
- *Duty Cycle-Based approaches*: These approaches work on managing nodes' access to the medium during the active and inactive periods, of the superframe, such that it becomes more power-efficient. The advantage of these approaches is that they reveal additional opportunities to conserve more power in the WSN without compromising other important performance metrics. Examples of these approaches include [DEP11], [LI11], [GIL11], [VAL10], [GAD10], [BHA08], [RAM07], [KOU08], and [MUT09].

– *Backoff-Based approaches*: These approaches focus on improving the performance of IEEE 802.15.4 MAC through devising new backoff algorithms that can control the nodes' medium access in a more efficient manner. Many of these approaches manage to make the backoff process more adaptive and dynamic. Examples of these approaches include [WAN11], [MOR11], [ZHU11a], [JIN11], [KHA10], [WON10a], [ROY10], [YED08], [WOO08], and [HA07].

It should be mentioned that some of the approaches cited above can fall under more than one category, but we use the classification that better reflects the methodology followed by the approach. In the following subsections we review all of the above cited research works.

2.2.1 Parameter Tuning-Based Approaches

Anastasi et al. in [ANA11] present a comprehensive analysis of the IEEE 802.15.4 MAC's performance in terms of reliability. The authors argue that this MAC protocol suffers from what they call the *802.15.4 MAC unreliability problem*. With this problem MAC performs poorly in terms of the proportion of packets that can successfully reach their destination. Basically, the authors blame the power management mechanism (attained by the utilization of CAP and CFP in the superframe), applied by IEEE 802.15.4 MAC to conserve the power resources of the sensor nodes, for this degradation in performance. This is confirmed through simulations that studied the packet delivery ratio while power management is enabled or disabled. To overcome this pitfall, the authors conduct additional simulations to understand the impact of the IEEE 802.15.4 MAC default attributes (that is, macMinBE, macMaxBE, macMaxCSMABACKoffs, and macMaxFrameRetries) on the observed performance degradation. In particular, the authors define three sets of CSMA-CA parameters in their simulations, namely, the Default Parameters Set (DPS), the Standard Parameter Set (SPS), and the Nonstandard Parameters Set (NPS). DPS

adopts the default parameter values as defined by IEEE 802.15.4 MAC. SPS uses the maximum values allowed by the standard. Finally, NPS depends on values that are beyond the standard's allowed maximums. The conducted simulations show that NPS achieves a superior performance in terms delivery ratio and per packet energy consumption, although these come at the expense of increased latency. The main conclusion of this study is that improving the performance of the standard's MAC can be achieved through proper tuning of its parameters; which requires a new set of allowed values. The benefit of this proposal is that it avoids any modifications to the core of the IEEE 802.15.4 standard and presents recommendations to enhance its overall behaviour.

Park et al. in [PAR10] propose an adaptive MAC sub-layer to minimize power consumptions, while achieving reliable and timely communications. They formulate an optimization problem with an objective function to minimize the total power consumption, subject to constraints on reliability and packet delivery delay. The decision variables are chosen to be the MAC parameters, namely, macMinBE, macMaxCSMABACKoffs, and macMaxFrameRetries. After presenting a generalized Markov chain model for the slotted CSMA-CA mechanism, under saturated traffic conditions, the authors provide numerical results that show how to properly tune the decision variables in order to prolong the lifetime of the network. The overall outcome is an adaptive MAC sub-layer protocol that conforms to the constraints of WSNs.

Zhao et al. in [ZHA10] propose the Power-efficient MAC (PeMAC) and the Bandwidth-efficient MAC (BeMAC) protocols to optimize IEEE 802.15.4 MAC's performance. Each node runs these protocols to adjust its local contention parameters in accordance to the number of nodes in the network. The objective of PeMAC and BeMAC is to improve power-efficiency (the number of successfully transmitted bits-per-second-per-Watt) and bandwidth efficiency (the

number of successfully transmitted bits-per-second), respectively. The authors derive mathematical expressions that relate each of these efficiencies to the transmission probability (which is a function of the network size). These expressions are beneficial in determining, given a network size, the optimal transmission probability at which maximum power and bandwidth efficiencies can be achieved. The size of the network, however, is not a directly controlled variable, and therefore, the nodes should estimate this size. This means that there is a need use adaptive techniques that can tune the contention parameters such that the optimal performance is achieved. These facts lead the authors to implement a look-up table at each node to compute its contention parameters based on the estimated size of the network, and therefore, achieve the targeted optimal performance. The overall performance of PeMAC and BeMAC is evaluated against IEEE 802.15.4 MAC through simulations. The collected results show that proposed protocols manage to improve both power and bandwidth efficiencies especially for large network sizes.

Pollin et al. in [POL08] provide a comprehensive, analytical evaluation for the slotted CSMA-CA algorithm in the presence of acknowledged and unacknowledged uplink data transmissions, under both saturated and unsaturated conditions. A Markov-based model is developed and the performance of the standard in terms of power consumption and throughput is analyzed. They describe guidelines to tune the MAC parameters to increase throughput and power savings.

2.2.2 Cross Layer-Based Approaches

Francesco et al. in [FRA11] propose the ADaptive Access Parameters Tuning (ADAPT) algorithm, a cross-layer distributed framework for WSNs that implement the IEEE 802.15.4/ZigBee standards. The objective of ADAPT is to achieve a reliable and energy-efficient

data communications in WSNs. Basically, the authors observe that different applications require different reliability levels, and therefore, they target improving the IEEE 802.15.4 MAC to obey that fact. Energy consumption, on the other hand, depends solely on the operating conditions of the network, which are very dynamic in nature. Therefore, conserving nodes' energy requires a system that can adapt its parameters such that the lifetime of the network is prolonged. ADAPT employs an *adaptation module* that directly interacts with all the layers of the ZigBee stack. To facilitate the interaction, this module is realized as a vertical component that has direct access with each layer of the protocol stack. This architecture gives the adaptation module the ability to collect information from each layer and optimize the overall functionality of the node. Therefore, when the application layer specifies a targeted reliability, the adaptation module interacts with the MAC layer to tune its parameters in a way that makes the desired reliability possible. The authors also address the main factors that affect the level of the reliability, namely, contention and channel errors, and incorporate two control schemes in ADAPT to mitigate their impact. Both control schemes tune the MAC parameters such that the reliability is confined to a certain predefined range. ADAPT is mathematically modelled and simulated for both single-hop and multiple-hop networks. The simulations show that ADAPT manages to outperform the standard in terms of delivery ratio and energy consumption per message.

Marco et al. in [MAR10] introduce the Timely, Reliable, Energy-efficient and Dynamic (TREnD) cross-layer protocol for WSN-based control applications in industrial environments. The authors argue that concentrating on cross-layer approaches is more efficient in capturing and exploiting the complex interactions among the different protocol layers, which achieves a superior functionality. TREnD enables collaboration between the routing algorithm, MAC layer, and power control such that the desired reliability and latency are achieved. This is attained

through an optimization process that is run with an objective to minimize the energy consumption. In TREnD, the routing mechanism is divided into static routing, to handle inter-cluster communications, and dynamic routing, to handle inter-node communications. The static routing is supported by a novel MAC protocol that follows a hybrid TDMA/CSMA approach. According to this MAC protocol, nodes wake up to transmit/receive only during the TDMA-slot associated to their cluster for transmitting/receiving, which reflects in more energy savings. The TDMA-cycle is organized in a way such that the different traffic patterns, for different cluster locations, are considered. Packets are exchanged between clusters. Nodes, within a transmitting cluster, with packets to send enter in the listening state. At the receiving cluster, each node multicasts a beacon message to all of the nodes in the transmitting cluster. A node that receives the beacon senses the channel and, once it finds the channel clear, unicasts its packet to the beacon's sender. If no beacons are received, nodes at the transmitting cluster either keep on listening in the next CSMA-slot or enter the sleep mode. The sink node is the one responsible of setting the optimal parameters of operation, based on the available traffic and cluster topology, and communicating these parameters to the nodes in the network. Simulations show that TREnD performs effectively in terms of reliability, latency, duty cycling, and load balancing.

2.2.3 IEEE 802.11-Based Approaches

Minooei and Nojumi in [MIN07] study the improvement of BEB in the context of IEEE 802.11. Lee et al. investigated the performance of that algorithm, which they call the Non-Overlapping BEB (NO-BEB), in the context of IEEE 802.15.4 networks [LEE09]. NO-BEB modifies the way BEB selects the length of the contention window after an access failure. Basically, in order to reduce the level of contention over the medium, the contention window (W) is randomly selected from the range $[W_{i-1}, W_i]$ rather than $[0, W_i]$, where W_i is the

contention window of the ith backoff stage [MIN07]. This change guarantees that no overlapping with the previous range (that is, $[0, W_i]$) occurs. As a result, nodes experiencing different number of medium access failures have better chances of acquiring different contention windows from the non-overlapped regions. NO-BEB is modeled using Markov chain in [LEE09] and shown to outperform BEB in terms of throughput, probability of collisions and average access delay.

2.2.4 Protection-Based Approaches

Serrano et al. in [SER10] proposes a scheme to detect selfish configurations of IEEE 802.11e-compliant devices[1]. The main focus in this proposal is on selfish manipulations of the minimum contention window (W_{min}), as selfish nodes tend to keep this window very small to gain more access to the communication channel. The scheme is based on the fact that IEEE 802.11 avoids duplicates using a retry bit to mark the retransmitted frames. This retry bit is set to 0 when firstly transmitting the frame and then set to 1 on every retransmission. With that, given a node that always has packets to send, the time periods between every two successfully received frames is uniformly distributed between 0 and W_{min} if the retry bit of the second frame is set to 0 [SER10]. This behaviour of IEEE 802.11 is benefitted from as follows. A controller node keeps monitoring all the successful transmissions originating from a node. On a periodical basis, the time slots between these transmissions are examined to check if they conform to a uniform distribution between 0 and W_{min}. This proposal requires no estimation of any WLAN and imposes no assumptions on the radio conditions. It should be mentioned that the access point (AP) is the entity responsible for the monitoring process and the calculations associated with it. This is very useful in networks like WSNs as we can assign these tasks to a BS or cluster-heads,

[1] IEEE 802.11e is an extension to IEEE802.11 to support QoS applications.

without imposing further tasks on regular sensor nodes. The authors further quantify the gain attained by the selfish node due to its misbehaviour. This gain is expressed as the ratio between the throughput of the selfish node and the throughput of a well-behaved one. Migrating this proposal to WSNs requires special attention to the power requirements when assigning the BS or cluster-heads the monitoring task.

Guang and Assi in [GUA06] propose the Predictable Random Backoff (PRB) algorithm to mitigate the selfish MAC misbehaviour of intruders in ad hoc networks. The PRB algorithm introduces a minor modification to the Binary Exponential Backoff (BEB) algorithm that is standard in the IEEE 802.11 MAC layer. The main target of PRB is to deal with selfish attempts to adaptively manipulate the contention window such that better throughput or better power conservation is achieved. PRB is designed such that if the selfish node abides by it, the negative impact of the node's attacks will be mitigated. Otherwise, if the selfish node does not follow PRB, the node's misbehaviour will be detected easily by the receiver it is communicating with. The basic idea of PRB is that after a node successfully transmits a packet, it should choose its next backoff interval, for its next transmission, from an interval that has a lower bound greater than zero (according to certain calculations). In other words, in the original BEB, the backoff is chosen between 0 and W_{min}. In PRB, the interval will be bounded by W_{lb} and W_{min}. The lower bound (W_{lb}) is defined based on a predefined threshold window size (W_{thresh}). This modification aims at preventing the selfish node from choosing smaller window sizes on a frequent basis, which results in unfairness in the network and higher throughput for the selfish node. The detection of selfish nodes is a role assigned to receiver nodes. Upon detecting such nodes, a receiver can punish the selfish sender by denying its traffic.

Raya et al. in [RAY06] introduce the pioneering DOMINO (Detection Of greedy behaviour in the MAC layer of IEEE 802.11 public NetwOrks) software that is installed at the Access Point (i.e., adopts centralized approach for intrusion detection). DOMINO requires no modifications to the 802.11 MAC protocol and works on detecting greedy nodes in the network. DOMINO periodically monitors active nodes to collect traffic traces. These traces are fed into a series of different tests, each of which targets the detection of a specific intrusion scenario. Basically, the tests target the capturing of misbehaviours that include scrambled frames, transmitting before DIFS passes, oversized NAV, and backoff manipulation strategies. The outputs of these tests are directed to a decision maker that issues the final conclusion on whether a node is misbehaving or not. Once nodes are dubbed as cheaters, operators are informed to perform appropriate actions. It is worth noticing that DOMINO adopts a modular architecture that allows for the addition of new tests that can capture previously unknown attacks. DOMINO is one of the pioneering contributions in the area of detecting greedy nodes that has been cited and benefited from extensively in the literature.

2.2.5 Priority-Based Approaches

Shi et al. in [SHI11] tackle the problem of real-time abnormal events monitoring and the need to distinguish between alarm signals and ordinary signals. They propose an improved CSMA-CA protocol based on Weighted-Fair-Queue (FQ-CSMA/CA) algorithm. This algorithm works on balancing the transmission quality among different signals based on their urgency, which is lacking in the IEEE 802.15.4 standard. Basically, FQ-CSMA/CA aims at guaranteeing reduced transmission delays for alarm signals, without compromising the transmission quality of ordinary signals. Towards that end, FQ-CSMA/CA uses weighted-fair-queuing to divide the nodes' packets according to their priority. This means that weights are used to mark the different

packets available in the queues of a node. A weight is the proportion of bandwidth assigned for a specific queue. This weight is explicitly specified within the data frame in the field priority-label. This weight is used by a classifier at each node to organize the nodes in the queues according to their priority. A packet scheduler will then select the packets with highest priority to service them first. The authors define five categories of signals, namely, sensor collected data, control command, ACK frame, system setting, and alarm signals, and state that alarm signals are given the largest weight (or priority), while the ACK frame is given the smallest one. The rest of the data are assigned equal weights. This categorization of data aims at achieving a level of fairness with which each type of data, except for the ACK frame, is given an equal opportunity of being transmitted provided that the alarm signals are sent first if they occur. Simulations show that FQ-CSMA/CA outperforms the IEEE 802.15.4 standard in term of the frame success probability. In particular, except for the ACK frames, FQ-CSMA/CA manages to deliver all the frames with probabilities better than IEEE 802.15.4. A similar observation can be seen with the average queue delay experienced by the different packets. With FQ-CSMA/CA, except for the ACK frames, all the frames have to wait for a period shorter than IEEE 802.15.4 before being serviced.

Severino et al. in [SEV10] work in differentiating traffic classes within the CAP such that differentiated services are offered to time-critical messages. Their approach is based on the proper tuning of the IEEE 802.15.4 MAC parameters macMinBE, macMaxBE, and W_{init} (the initial size of the contention window). The tuning depends on whether the frame is identified as a high-priority or not. Data frames are considered of low priority while command frames, like alarm reports and GTS requests, are considered of high priority. Therefore, nodes use different parameter settings depending on their traffic type. Similar to [NDI09], the settings are chosen such that the backoff periods of high-priority frames are made shorter than those for the low-

priority frames. Furthermore, while a queue of different frames is building up, a Priority Queuing is used such that higher-priority frames are selected first for transmission.

Jardosh et al. in [JAR10] propose an explicit priority scheme for IEEE 802.15.4 MAC. According to this scheme, nodes are categorized into critical nodes and normal nodes. Critical nodes are the ones that have important information to send to the coordinator while normal nodes that send routine information, which can tolerate some delay. Critical nodes are considered of high-priority while normal nodes are considered of low-priority. The coordinator can learn about this categorization using a secondary beacon. Basically, critical nodes send the coordinator this beacon to indicate their high priority traffic. With that information, the coordinator restricts the contention during the CAP to only those critical nodes. That is, the coordinator includes the priority information in the primary beacon that it periodically broadcasts to all the nodes. Once notified, the normal nodes will refrain from attempting to access the medium during the CAP. This way traffic priority is preserved and critical information is given preference over regular information.

Takaffoli et al. in [TAK10] propose the GTS-TDMA algorithm which targets the improvement of GTS scheduling to recognize the nodes' different priority classes. Under GTS-TDMA, nodes do not request GTSs, GTSs are rather allocated to them using a GTS allocation scheme. The network is viewed as a multi-level tree and a TDMA schedule is constructed for it. The schedule is constructed such that maximum data rate is achieved for each node in the network. In other words, the TDMA-GTS algorithm seeks the optimal allocation of GTSs such that each node is provided with the maximum data rate it requires. Simulation results show that TDMA-GTS is capable of achieving almost twice the throughput of CSMA-CA. However,

similar to AGA above, this algorithm exploits the GTS capability of IEEE 802.15.4 MAC and does not consider solving the priority problem during the CAP.

Kim and Kang in [KIM10] tackle the problem of service differentiation in IEEE 802.15.4-based WSNs operating under non-saturation conditions. The authors propose two mechanisms, namely, the Contention Window Differentiation (CWD) mechanism and the Backoff Exponent Differentiation (BED) mechanism, with the objective of supporting a priority-based service differentiation scheme for WSNs. Under these mechanisms, nodes are grouped into different priority classes. Priorities are recognized according to the importance of the packets to be transmitted. For example, nodes that need high bandwidths and generate emergency data must have higher priorities than other nodes. Service differentiation is realized through the variation of the size of the contention window (with CWD) and the binary exponent (with BED). With CWD, nodes with different priorities are assigned different contention windows such that high-priority nodes experience short contention windows and vice versa. In the same manner, BED assigns different binary exponents to the different nodes' priorities. Both BED and CWD apply a scheme known as the Backoff Counter Selection (BCS) that selects the next backoff period, after finding the medium busy during any CCA, from a shortened range (smaller than the range used in the IEEE 802.15.4 standard). The shortened range gives different nodes better chances of choosing different backoff periods. The benefits of that are the preservation of nodes' priorities and the reduction in the probability of collision. The inclusion of the BCS scheme assists in accelerating the process of service differentiation. The authors develop Markov-based analytical models their new mechanisms. Simulations show that both CWD and BED are capable of prioritizing nodes according to the importance of their packets. However, it is shown that CWD

and BED perform differently in terms of different performance metrics. Therefore, a guideline is presented to recommend the usage of CWD or BED depending on the desired performance.

Ndih et al. in [NDI09] observe that IEEE 802.15.4 offers a priority-independent functionality. This is resulting from having the nodes use the same contention access parameters. Therefore, the authors in develop a Markov-based analytical model for the CAP in which different sets of access parameters are permitted for the nodes with different priority classes. Two priority classes are recognized: high-priority (class 1) and low-priority (class 2). A node-state Markov-chain is developed for each priority class, beside a Markov-chain for the channel state. The priorities or service differentiation is based on assigning a contention window of 1 for class 1 nodes and 2 for class 2 nodes. Using these settings of the contention window, while maintaining the other backoff parameters at their standard-defined defaults, gives high-priority nodes higher opportunity to access the medium. This is because their small contention window size reduces the duration of their idle channel sensing.

Huang et al. in [HUA08] propose the Adaptive GTS Allocation (AGA) scheme to support low latency and fairness. The idea of AGA is to provide an estimate of future GTS needs of the nodes. With that estimate, the coordinator gives higher priority of GTS allocation to needy nodes. AGA operates in a two-phase manner. In the first phase, nodes are classified according to their recent usage of GTSs and then assigned priority numbers (priority decreases as the priority number increases). In the second phase, GTSs are allocated with reference to the priority numbers such that nodes with low priority numbers are considered first. Although AGA shows promising results, over IEEE 802.15.4, in terms of fairness and low latency, the scheme concentrates on improving medium access during the CFP without considering the CAP.

2.2.6 Duty Cycle-Based Approaches

De Paz Alberola and Pesch in [DEP11] propose the Duty Cycle Learning Algorithm (DCLA) to define how the nodes should be configured to achieve the optimal network performance under different traffic conditions. DCLA alleviates the need for human intervention and adapts the nodes' duty cycles in a way to minimise power consumption while achieving superior performance in terms of successful data delivery. By running on the coordinator nodes, DCLA firstly gathers statistics from different nodes to estimate the incoming traffic load. Based on the gathered information, the Reinforcement Learning (RL) framework (see [SUT98]) is used to decide on the duty cycle to use. Basically, RL depends on repetitive interactions, with the nodes, through which the selected duty cycle is updated iteratively till the best one, that achieves the targeted optimal performance, is hit. This way DCLA can achieve a fully adaptive system that can self-correct its parameters based on the traffic conditions, without the need for any manual configurations that conform to specific requirements of different applications. This gives DCLA the credit of reducing time and cost of installation, operation and management. DCLA runs as a software on the coordinator nodes and requires low memory and processing capacities. Simulations show that DCLA, compared to other duty cycle adaptation schemes, is capable of achieving a superior performance in terms of energy efficiency, end-to-end delay, and probability of success.

Li et al. in [LI11] propose enhancements for the beacon-enabled mode in IEEE 802.15.4 MAC. The enhanced version of the standard, referred to as the Enhanced Beacon-Enabled Mode, aim at improving network performance and conserving more power for low data rate applications. The new mode is realized by two optional functions, namely, the Synchronized Low Power Listening (S-LPL) function and the Periodic Wakeup (PW) function. S-LPL helps in

reducing the overhead of synchronization for low data rate applications, while PW, which is implemented during the inactive portion of the superframe, helps in reducing both transmission delays and packet loss rate. These two function scan be implemented in tandem or individually. The target of S-LPL is to improve the ability of nodes to save more power. Basically, the authors in [LI11] note that the IEEE 802.15.4 standard supports a BO of between 0 and 14. This is a relatively small range that constraints the ability of saving more power in low duty cycle applications. The standard does not support larger BOs for two reasons. First, with large BOs a node experiences synchronization overhead. That is, the node will spend more time to associate itself with a PAN coordinator. This extra time is accompanied with more depletion of the node's power resources and the standard aims at avoiding that. Second, large BOs may cause synchronization difficulties because of the clock drift between nodes (see [LI11] for more details). With S-LPL longer synchronization periods are permitted for a portion of the nodes. These nodes receive the beacon less frequently (once every K beacons sent to the rest of the nodes). This means that these nodes will have to listen for extended periods of time before receiving the next beacon from the coordinator. Although this may lead to faster depletion of their power resources, S-LPL mitigates that by mandating that the coordinator should send a series of Virtual Preambles (VPs) to these nodes. The latter operate in a Low Power Listening (LPL) mode, which enables them to detect the VPs and synchronize their clocks with the coordinator. Under LPL, the nodes' listening is on for a period of two VPs and off for a period of one VP. In this manner, nodes are able to conserve more power; and this reduces the effect of using longer synchronization periods. The authors show that the effect of sending the VPs on the power resources of the coordinator are minimal, provided that S-LPL is implemented for low data rate applications. PW, on the other hand, is introduced to handle the problem of delaying the

data generated during the inactive period of the superframe. With PW, nodes with queued as well as newly generated data are permitted to send their data to the coordinator, which turns on its listening, during the inactive period. This behaviour guarantees lower latency for these data. The coordinator, however, does not need to stay awake for the whole inactive duration; periodic sleeps, to compensate for the situations when the nodes are not sending anything, can still be implemented to reduce the coordinator's loss of power. By coupling the PW capability with the aforementioned capability of enlarging BO, the anticipated transmission latency can be comparable to that achieved with the IEEE 802.15.4 standard. The Enhanced Beacon-Enabled Mode's performance is studied through extensive simulations. These simulations show that the new mode can outperform the IEEE 802.15.4 standard in terms of the mean power consumption, the mean duty cycle, and the packet loss rate.

Gilani et al. in [GIL11] introduce an adaptive CSMA/TDMA hybrid MAC protocol to improve the throughput and the energy consumption of the IEEE 802.15.4 MAC. The authors are motivated by the observation that CSMA-CA does not perform well under high traffic loads. Therefore, they propose to incorporate the concept of time division multiple access (TDMA) in the CAP of the superframe. In other words, a dynamic TDMA period is incorporated into the CAP. The coordinator node is assigned the task of adaptively dividing the CAP into CSMA-CA slots and TDMA slots. The division is based on the state of the nodes' queues and the level of collisions over the wireless medium. The state of the data queues can be known through reserved bits in the transmitted frames. Having the coordinator assign TDMA slots resolves the latter's challenging problem of synchronization; the beacon frames that are sent periodically help in this direction. Also, since the targeted scenario in [GIL11] is WSNs operating under heavy traffic loads, the use of a greedy algorithm to allocate TDMA slots can resolve the known issue with

TDMA networks, namely, the underutilization of the communication channel. The main advantage of including TDMA slots in the CAP is that the number of nodes that take part in the contention is constrained. Therefore, lower collisions are anticipated, which reflects in improved throughput. Also, as nodes obey the TDMA concept, they refrain from contending for the medium and therefore their RF transmitters should be turned off. This is beneficial in reducing the energy expenditure of these nodes. These anticipations are confirmed through the simulations conducted by the authors. The simulations, however, show that the CSMA/TDMA hybrid protocol leads to increased end-to-end delays, compared to the IEEE 802.15.4 MAC, except when the superframe duration is set carefully. In other words, when long superframes are used, TDMA nodes have to wait longer before being able to send their packets, which contributes to increased delays.

Valero et al. in [VAL10] propose DEEP, a MAC protocol for beacon-enabled IEEE 802.15.4 that optimizes the distribution of the guaranteed time slots (GTSs) such that better energy conservation is achieved. In particular, instead of having a GTS descriptor (that defines the node's address as well as the GTS slot and direct) available in all subsequent beacons till the node requests its de-allocation, DEEP removes the GTS descriptor from the beacon once the associated node acknowledges its reception. Indeed, nodes that do not support DEEP can still follow the IEEE 802.15.4 standard in keeping the unacknowledged GTS descriptor in all beacons. This makes DEEP backward compatible. DEEP can effectively reduce the size of the communicated beacons and thus the power consumed to process them at the receiving nodes is significantly reduced.

Gadallah and Jaafari in [GAD10] propose enhancements for the non-beaconed IEEE 802.15.4. Their enhancements target energy-efficiency as well as reliable delivery of critical

traffic. Basically, during network initialization, the duty cycle of the nodes is divided into active and inactive periods. During the active periods, nodes contend to access the medium according to the unslotted CSMA scheme. However, nodes sleep during the inactive periods. Nodes remain in the active mode while delivering critical data traffics. This behavior achieves higher reliability. However, inactive nodes allow nodes to conserve more power than the case is in the original non-beaconed IEEE 802.15.4, in which nodes are always awake and contending to access the medium. While this proposal outperforms the IEEE 802.15.4 standard as per the aforementioned parameters, it requires the employment of a synchronization scheme in the non-beaconed mode of IEEE 802.15.4. The overhead associated with that is not addressed in [GAD10].

Bhatti et al. in [BHA08] propose modifications to beacon-enabled IEEE 802.15.4 to improve its performance in terms of latency and reliability, and therefore, make it conform to the requirements of industrial applications. Towards that, the authors propose three schemes 1) swap the positions of CAP and CFP in the superframe and allow failed GTS frames to be retransmitted in during the CAP, 2) in the original IEEE 802.15.4 MAC, allow the retransmission of GTS frames in the CAP of the following superframe, and 3) in the original IEEE 802.15.4 MAC, allow the retransmission of GTS frames in the CAP of the current frame. Through a simulation study, the authors point out the gains they can achieve with their modifications over the original IEEE 802.15.4 MAC.

Ram et al. in [RAM07] present a thorough study and modelling of IEEE 802.15.4 MAC based on Markov chain. Their aim is to examine the performance in terms of throughput and energy consumption. The developed Markov-based model observes some approximations, In particular, the CSMA algorithm is assumed to be non-persistent. Also, in computing the probability of finding the channel busy during a specific time slot or the probability of sending a

packet in a specific time slot, the *steady-state* probabilities are used to simplify the calculations. Finally, instead of selecting the next backoff period, after sensing the channel busy, based on a uniform distribution, it is assumed that a *geometric* distribution is used. The objective of this study is to understand the effect of shutting nodes down while no packets are available for transmission. After that, a modification to the specification of IEEE 802.15.4 MAC, in terms of the initialization of the contention window, is proposed to improve the performance.

Koubâa et al. in [KOU08] propose the Time Division Beacon Scheduling (TDBS) mechanism to mitigate the beacon frame collision problem in cluster-tree WSNs. With this problem, beacon frames collide due to having two or more coordinators either in the transmission range of each other, or communicating with overlapping transmission ranges. To resolve this situation, which is directly related to the synchronization problem, the authors present the TDBS mechanism in which the superframe duration scheduling (SDS) algorithm employed. In SDS, avoiding beacons collision depends on finding a cyclic schedule for the SDs such that at least one SD is accommodated in each BI. Also, the distance between any two consecutive SDs must be equal to BI. These rules guarantee that no overlapping can occur among beacon transmissions. SDS is also coupled with an efficient duty cycle management mechanism that distributes the bandwidth resources in a fair manner. This mechanism allocates bandwidth to the coordinators, based on their traffic needs, using an optimization formulation. This formulation defines a set of linear equations that describe the network constraints associated with the duty cycle of each coordinator and its relation to other coordinators' duty cycles. These constraints, like having the sum of all duty-cycles to be one at most, depend on the metric being optimized (duty cycle in our case) and can be easily modified to optimize other metrics (like

delay, buffer size...etc). Finally, the feasibility of the TDBS mechanism is demonstrated through implementation in an experimental test-bed.

Muthukumaran et al. in [MUT09] propose MeshMAC, a distributed beacon scheduling mechanism that enables the IEEE 802.15.4 standard to support peer-to-peer WSNs in the low-power, beacon-enabled mode. Basically, MeshMAC assumes that the whole network operates on the same BI and SD (the values of which are defined by the standard). To allocate a schedule for a node, the sum of the duty cycles of its 2-hop neighbours should be one at most. MeshMAC reserves one active SD exclusively for broadcast communication. Each node educates itself with the time slots that are already occupied by all other nodes in its 2-hop transmission range.
Based on that knowledge, a node selects the first empty time slot it encounters and then broadcasts its selection to the other nodes. Two types of data transmission are supported by MeshMAC, namely, broadcast and unicast. Broadcast happens during the aforementioned reserved time slot. This slot is used for synchronizing the nodes. The unicast transmission happens during the active period of a destination node. The major benefit of MeshMAC is that nodes prepare their schedules in a distributed manner (that is, each node uses its local information about its 2-hop neighbours) that requires no intervention from a coordinator node. The evaluation of MeshMAC shows that it can perform in an energy-efficient, scalable fashion compared to the IEEE 802.15.4 MAC.

2.2.7 Backoff-Based Approaches

Wang et al. in [WAN11] provide a comprehensive performance analysis of the CAP in the IEEE 802.15.4 MAC protocol. Both node states and channel states models are developed based on Markov chain. The authors demonstrate that these models can accurately match the functionality of IEEE 802.15.4 MAC during the CAP. Based on these models, it is proven that

the standard performs poorly in terms of the achieved throughput. The authors discuss that this degradation in the performance is due to the inappropriate length of the backoff slot, which is set to aUnitBackoffPeriod in the standard. This length is relatively big and reduces the points at which nodes are allowed to compete for medium access, and therefore, this reflects into higher probabilities of collisions. Motivated by this discussion, the authors propose a modification to the superframe CAP. In this modification, the standard duration of the backoff slot is divided evenly into multiple smaller slots. This means that the number of the starting points at which the nodes contend to access the medium are increased; this provides better opportunities for accessing the medium. This change in the CAP requires is not accompanied with any no modifications to the CSMA-CA algorithm itself. New node/channel states models are developed to capture the new changes to and a performance comparison is held with the original CSMA-CA algorithm. Simulations show that the changes are showing significant improvement in the achieved throughput (which is a result of reducing packet collisions). To more enhance the performance of the CSMA-CA algorithm, a new backoff mechanism is proposed in which a new time unit is used along with a relatively large range to randomly select the backoff periods from. The definition of the new time unit is inspired by the aforementioned division of aUnitBackoffPeriod into smaller slots. On the other hand, the wider range to select the backoff periods from is introduced to guarantee that the number of nodes contending to access the medium is reduced, which reflects in a reduced probability of collisions. Finally, the study in [WAN11] is supported with additional simulations to examine the performance of these modifications. The results show that the proposed enhancements to CSMA-CA can significantly improve the throughput, reduce the end-to-end delay, and increase the rate of packet delivery success.

Mori et al. in [MOR11] propose a distributed backoff mechanism to enhance the transmission performance of IEEE 802.15.4 MAC in cluster-based WSNs. The authors highlight the problem of channel access congestion that appears among the nodes that did not have enough time to send their packets during the last CAP. These nodes will commence their packet transmission, concurrently, at the beginning of the next CAP. This leads to higher incidents of collisions, and therefore, degrades the transmission performance. To mitigate this consequence, the authors propose that the nodes are required, at the beginning of the next CAP, to start their backoff periods at different time instants within the range of CAP. This is coupled with the fact that nodes should use a constant BE, set to the default macMinBE. The distinct starting points of the backoffs are *randomly* selected by each node from a Distribution Window (DW). The length of DW can be either constant (CDW) or adaptive (ADW). ADW is adapted in accordance to the traffic load experienced in the cluster. That is, DW shrinks with light traffic loads and expands otherwise. The coordinator of the cluster is responsible of informing the nodes about the heaviness of the traffic load. The authors provide a simulation study to examine the performance of this new backoff mechanism in terms of throughput and transmission delay. It is shown that the throughput of the new mechanism is directly affected by the lengths of the DW. The proper setting of DW can guarantee a throughput that is comparable to the conventional IEEE 802.15.4 MAC. However, the effectiveness of the new mechanism appears in its ability to outperform the IEEE 802.15.4 MAC protocol in terms of the reduction in the transmission delay under heavy traffic load. Again, the setting of DW greatly affects the latter performance.

Zhu et al. in [ZHU11a] introduce the Linear Increase Backoff (LIB), a modified CSMA-CA mechanism to better serve time-critical applications. LIB targets enhancing the performance in terms of packet delay without affecting the energy efficiency and the throughput. The main

change introduced by LIB is that backoff counters increase linearly, instead of exponentially, when either of the two CCAs reveals that the channel is busy. This change is motivated by the fact that the exponential increase in the backoff counter may force certain nodes to wait for an extended period of time before being able to commence its CCAs. This allows other nodes, with relatively shorter backoff periods, to capture the medium more frequently. The linear increase in the backoff counter, however, can guarantee to keep the backoff periods at reasonable lengths that allow nodes to gain a fair access to the medium. LIB also requires other changes to the standard CSMA-CA algorithm. It mandates that if a packet cannot be sent within a superframe, it should be dropped and not deferred to the next superframe. Also, nodes should be in the *sleep* mode, rather than the *receiving-idle* mode, during the backoff states, at the end of a successful transmission, when crossing the retries limit, and when crossing the maximum number of backoff stages. Furthermore, LIB assumes that the redundancy in the deployed sensor nodes can obviate the need for using ACK packets. A comprehensive Markov-based model is developed for LIB to analyze its characteristics. Simulations show that LIB is effective in achieving a considerable reduction in the delay. Also, for large network sizes and high traffic intensity, LIB shows promising results in terms of improving the throughput and reducing the energy consumption.

Jing et al. in [JIN11] tackle the problem of maximizing the throughput of the IEEE 802.15.4 standard through a new adaptive backoff mechanism. The authors use nonlinear programming (NLP) to optimize the throughput in the network, considering a certain network size and the data payload. Based on the results of the optimization problem, the backoff mechanism is designed using an approximate Markov model. In this backoff mechanism, after finding the medium busy at a certain backoff stage, the node dos not choose its next backoff

period based on a uniform probability (as the case is with IEEE 802.15.4 MAC). Instead, the next backoff period is chosen based on a probability that controls the length of this period depending on the networks size. Therefore, as the network size increases, backoff periods are chosen large such that the contention to access the medium is reduced. Simulations have been conducted and showed that the new backoff mechanism outperforms IEEE 802.15.4 MAC in terms of throughput and the probability of successful transmission.

Khan et al. in [KHA10] introduce the Improved BEB (IBEB) algorithm. In IBEB each node, after specifying its BE, randomly selects an Interim Backoff (IB), which is restricted to be 10% to 40% of the specified backoff delay. The authors argue that this approach tends to reduce packet collisions since the probability of having two nodes randomly selecting the same BE and IB is quite low. The authors provided a simulation study to examine IBEB's performance in terms of latency, channel utilization, goodput, and average number of collisions. The results showed that IBEB outperforms BEB in terms of these parameters.

Wong and Hsu in [WON10a] introduce the Additional Carrier Sensing (ACS) algorithm to enhance the performance of CSMA-CA. ACS is designed specifically for WSNs operating under acknowledged traffic conditions. The authors highlight the fact that the wireless medium can be busy during the CCA2 due to two reasons. First, when a node's CCA1 coincides with another node's CCA2. In this case, the latter node commences its packet transmission during the former node's CCA2. Second, when a node initiates its CCA1 while another node waits for the ACK packet. In this case, the latter node receives its ACK during the former node's CCA2. The ACS algorithm exploits the latter situation by allowing the node with the failing CCA2 to conduct an additional CCA (referred to as CCA3). In this case, there is a chance that the medium becomes idle after the ACK packet has been delivered. Therefore, the node initiating CCA3 has an

opportunity to find the medium idle, which allows it to send its packet thereafter. This behaviour saves the node the need to experience another backoff period, which is anticipated to result in enhanced performance. ACS has been mathematically modelled, using Markov chain, and simulated to study its performance. The collected results show that ACS is superior to the standard CSMA-CA in terms of the achieved throughput and delay. Also, the number of CCAs used by a node before sending a packet is found to be less with ACS. This implies that ACS loses less power during CCAs.

Royo et al. in [ROY10] propose the 2-Cell with Sorted wait for WSNs (2CS-WSN) algorithm to resolve conflicts among nodes contending to access the medium. 2CS-WSN is a collision resolution mechanism by which nodes that suffered from a collision during a certain time slot will start a procedure to resolve their conflict in the next time slot. The procedure ends once all of the collided nodes manage to send their packets. With 2CS-WSN starts operating after the ordinary, standard two CCAs have been conducted. Once a collision occurs, nodes will be grouped into two cells, namely, the Transmission Cell (TC) and the Waiting Cell (WC). TC includes the nodes that *randomly* choose to retry their transmission attempts, while WC contains the nodes that *randomly* choose to defer their packet transmissions. Next, TC's nodes retry their transmissions at the same time, which results in another collision. This forces some of these nodes to form a new WC, called WC_1, while the old WC is renamed as WC_2. The TC keeps on shrinking, and WCs keep on forming, until one node remains in the TC. The latter node ends up successful in transmitting its packet. After that, WC_1's nodes move to TC and the nodes in any WC_{i+1} move to the next WC_i. This procedure is repeated until all of the nodes that experienced the aforementioned collision mange to send their packets. Simulations are run to study the performance of 2CS-WSN against the standard CSMA-CA. In terms of throughput, 2CS-WSN

manages to outperform CSMA-CA significantly. Furthermore, although the mean packet delay increases highly with 2CS-WSN, the algorithm tolerates that for the sake of reducing the rate of packet loss. In terms of the time as well as the number of retries needed to resolve a collision; it is found that 2CS-WSN reduces these metrics effectively when the number of colliding nodes increases.

Yedvalli and Krishnamachari in [YED08] propose enhancements to the IEEE 802.15.4 MAC protocol in dense sensor WSNs. The authors are motivated by the protocol's poor performance in terms of throughput and energy consumption as the number of transmitting nodes increase in the network. In their solution, they firstly model the IEEE 802.15.4 MAC protocol as a p-persistent CSMA with changing transmission probability. From this model they extract the optimal transmission probabilities with which throughput and energy conservation are maximized. It is noted that when the optimal probabilities are used, the ratio of the idle time between successful transmissions to the delay between them is constant. Furthermore, this ratio tends to increase as the transmission probability gets below the optimal probability and vice versa. Based on this observation, the authors develop an enhanced IEEE 802.15.4 MAC protocol that uses distributed channel feedback-based mechanism to tune the transmission probabilities dynamically towards the optimal values. Basically, the standard backoff mechanism is changed as follows. First, the update of the backoff window's size is made after successful transmissions, rather than collisions or busy CCAs. Second, under saturated traffic, the window sizes should be consistent with the size of the network. Third, under unsaturated traffic, the window sizes should decrease following every successful transmission as the optimal probability increases. In brief, the new enhanced protocol modifies the standard only in terms of when and how the backoff

window is updated. Simulations show that the enhanced protocol manages to outperform the standard in terms of the achieved throughput and the consumed energy.

Woo et al. in [WOO08] propose the Knowledge-based Exponential Backoff (KEB) algorithm. The main target of KEB is to improve the throughput depending on the channel state information as collected by each node. Each node uses the Exponential Weighted Moving Average (EWMA), with a smoothing factor β, to compute locally the collision rate after each successful transmission. Based on that computation, the value of BE is adjusted to achieve higher throughput. In other words, as the collision rate increases beyond a predefined collision threshold α, BE will be increased and thus nodes backoff for longer periods of time (in order to reduce the level of communications over the medium, which reduces the collisions). In contrast, as the collision rate remains below α, nodes backoff for shorter periods of time, which improves the utilization of the communication channel. KEB has been modeled using Markov chain and then simulated to validate the analytical model. The provided results show that KEB outperforms BEB in terms of throughput. The authors also provide a simulation study to find out the optimal values of the smoothing factor and the collision threshold that achieve the best throughput performance.

Ha et al. in [HA07] propose two mechanisms to improve the performance of CSMA-CA algorithm in IEEE 802.15.4 terms of throughput and energy efficiency. These mechanisms are the Enhanced Collision Resolution (ECR) and the Enhanced Backoff (EB) mechanisms. The ECR mechanism changes the standard's approach in updating the value of BE. The authors notice that a pair of CCAs is not enough to indicate the level of contention. Therefore, with ECR the value of BE is not increased until a *fixed number* of consecutive CCAs are found busy. This fixed number is set to mcMaxCSMABAckoffs. Also, rather than resetting BE to its minimum

value after a transmission (as in the standard), BE's value is adjusted based on the result of the packet transmission. If the transmission fails, it indicates high channel contention and thus BE is increased. If transmission succeeds, BE is decreased. This approach guarantees that BE is decreased slowly, and therefore, the information about the level of contention over the channel is preserved. Being aware of the status of the communication channel has a direct positive effect on the behavior of the CSMA-CA algorithm and it can enhance the overall performance of IEEE 802.15.4 MAC. On the other hand, the EB mechanism works on avoiding overlaps among different backoffs and CCAs, for different nodes, by shifting the range of backoff counters. The shift is based on an estimate of the expected number of busy backoff periods to follow (the details of how this estimate is computed can be found in [HA07]. Both ECR and EB mechanisms are evaluated in terms of throughput and energy efficiency (ratio of throughput and energy consumption). The provided simulations show that under saturated traffic conditions, ECR is superior to the IEEE 802.15.4 MAC protocol in terms of both performance metrics. Moreover, combining both ECR and EB can provide further improvements over IEEE 802.15.4 MAC. With unsaturated traffic conditions, the same improvements are observed only as the number of nodes increase in the network.

2.3 Conclusion

The research contributions that we have reviewed in this chapter reveal the criticality of the IEEE 802.15.4 standard and the importance of improving it to support a diverse field of applications. In devising new enhancements to this standard, we can clearly see that any new contributions should conform to the following specifications:

1. Distributed solutions: given the huge size of WSNs and the scarce power resources of the sensor nodes, distributed solutions are preferred over centralized ones. Distributed solutions can effectively support scalability and simplify the deployment/elimination of sensor nodes.
2. Adaptive solutions: given the self-organizing nature of WSNs, sensor nodes should have high ability to change their local parameters and adapt them to different conditions in the network. These conditions include the level of collisions over the wireless medium, traffic urgency, number of medium access failures, size of the network…etc.
3. Power-efficient solutions: conserving the power resources of sensor nodes is a stringent requirement that cannot be undermined. Complex solutions that burden the sensor's platform with additional power-consuming tasks are not favored in WSNs.
4. IEEE 802.15.4-centerd solutions: aside from the drawbacks of IEEE 802.15.4, its design abides by the general characteristics of WSNs and we need to build new solutions on top of it. That is, modifications to this standard should not change its core functionality. Rather, we need to focus on exploiting the strengths of this standard to mitigate its limitations (for example, how to benefit from the innovative idea of CCAs to achieve more power savings).

Chapter 3

Power-Efficient MAC protocol for IEEE 802.15.4-based WSNs

3.1 Introduction

Power conservation assumes the top priority requirement in the design of any algorithm or system for WSNs. In this chapter we introduce a new power-efficient backoff algorithm, called the Standby-BEB (SB-BEB) that aims at finding new opportunities to conserve more power for the sensor nodes operating according to the IEEE 802.15.4 standard. We develop an analytical model for SB-BEB based on discrete-time Markov chain[1]. Also, we conduct simulations to assert that the new algorithm does not degrade other important performance metrics, like channel utilization and reliability. The rest of this chapter is organized as follows. In Section 3.2 we describe the SB-BEB algorithm and develop a Markov-based analytical model for it. In Section 3.3 we validate our analytical model and conduct extensive simulations to study the performance of SB-BEB. Finally, Section 3.4 concludes the chapter.

[1] In the rest of this thesis, we refer to discrete-time Markov chain simply as Markov chain.

3.2 The Standby-BEB Algorithm

The known strategy of conserving power is to force nodes to sleep whenever possible. Nodes should not sleep for relatively short periods as this drains their power resources and reduces their lifetime. Also, nodes should avoid sleeping for extended periods of time since this may leave the communication channel underutilized. Instead, there should be a compromise between sleep periods and performance.

Based on the above discussion, we propose that a node enters the sleep mode after each successful transmission. That is, as the nodes compete to access the communication medium, once a node captures the medium and starts transmitting its packet, it should sleep for certain duration of time directly after finishing the transmission. This behaviour reduces the level of contention among the nodes to access the medium. That is, the probability of collision (which is usually associated with wasted power as the node needs to retransmit the collided packet again) is reduced. The usefulness of this new sleep state can be better observed if we notice that many nodes can be in the sleep mode at the same time, which reflects into a significant reduction in the probability of collisions. We call this new sleep state as the standby state. The BEB algorithm implementing the standby state is referred to as the Standby-BEB (SB-BEB). The flow diagram of the CSMA-CA mechanism implementing SB-BEB is shown in Figure 3-1 (this is a modified version of the chart found in [ZIG06]). The flow chart clearly reflects our extension to BEB, in which a node is forced to standby after a successful transmission and before commencing its next transmission. In the following subsections we describe our Markov-based model for SB-BEB.

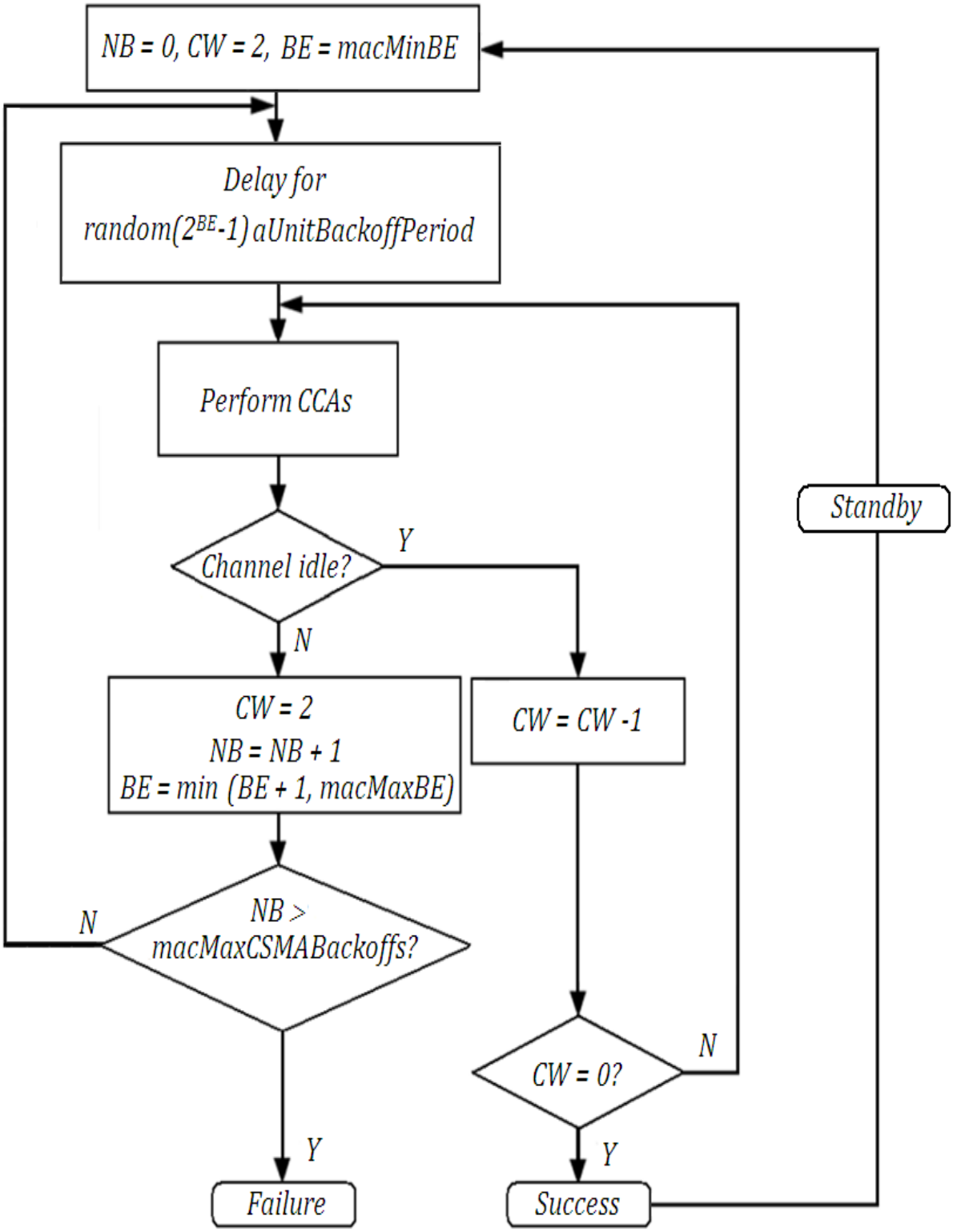

Figure 3-1: SB-BEB Algorithm.

3.2.1 System Model and Analysis

To simplify our work, we depend on incorporating our modifications to BEB in the Markov model proposed by Park et al. in [PAR10] (we refer to it as Park's model in the rest of this thesis). We choose this model due to its accuracy in capturing the main characteristics of the IEEE 802.15.4 MAC protocol. We firstly describe Park's system model and analysis and then we discuss our extensions to it. Park uses Markov chain to model the slotted CSMA-CA mechanism of the MAC protocol, with acknowledged, unsaturated traffic and retry limits. A star topology, with a PAN coordinator, is assumed with N nodes. The PAN coordinator is the data sink. Similar to the well-known Bianchi's model [BIA00], the developed Markov model is per node. Three stochastic processes are defined, namely, the backoff stage at time t (denoted as s(t)), the state of the backoff counter at time t (denoted as c(t)), and the state of the retransmission counter at time t (denoted as r(t)). These processes describe the states experienced by a node to transmit a packet. An essential assumption for the Markov chain to be applicable here is that each node has an independent probability to start sensing the medium. As a result, the stationary probability τ that a node attempts the first clear channel assessment (CCA1) at a random time slot is constant and independent of other nodes. Therefore, we end up with a 3-dimentional Markov chain described by the tuple (s(t), c(t), r(t)). In Figure 3-2 we show a simplified version of Park's Markov chain model in which only the first backoff stage is shown (refer to [PAR10] for the complete model).

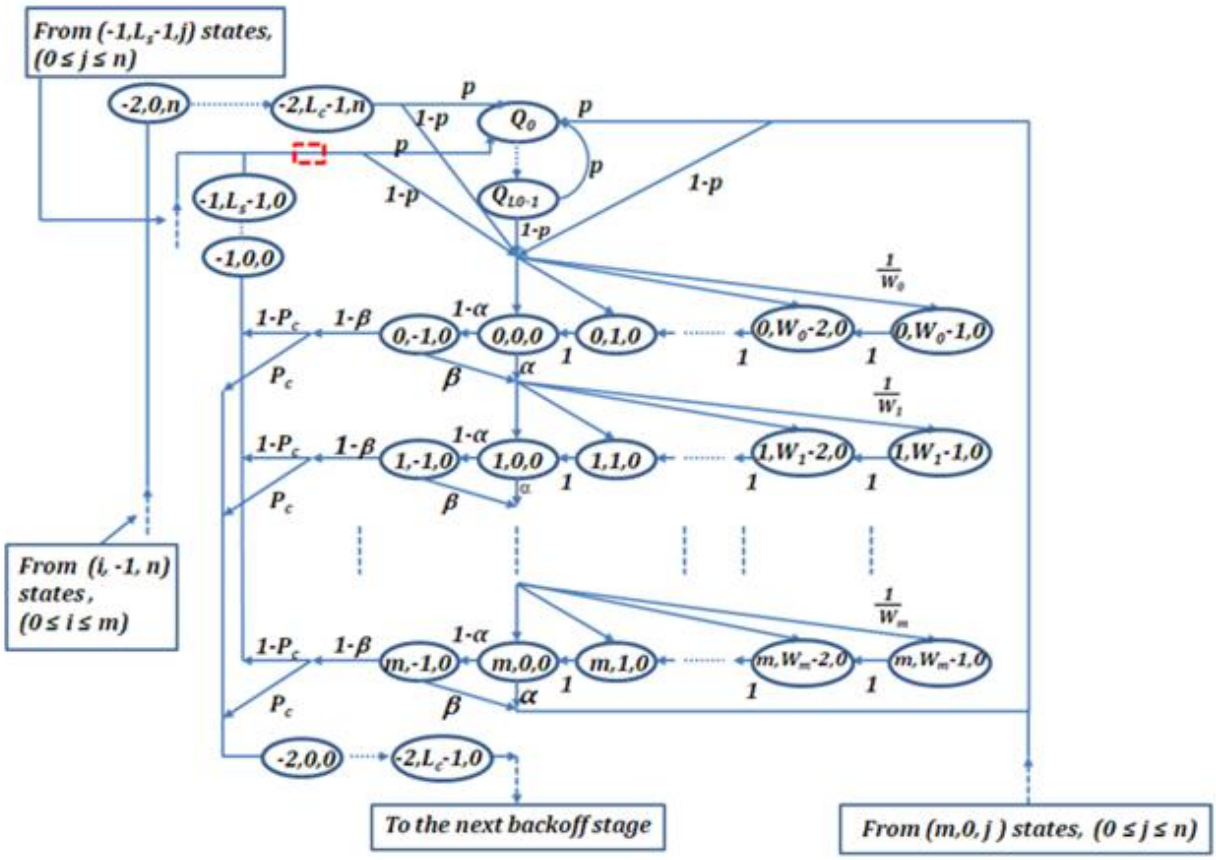

Figure 3-2: A simplified version of Park's Markov chain model.

Now, we describe each and every state of the Markov chain shown in this figure. The states (i,W_0-1,j) to (i,W_m-1, j) are the backoff states. W_0 is the smallest contention window size and is equal to $2^{macMinBE}$. The parameters m and n are set to the values macMaxCSMABackoffs and macMaxFrameRetries, respectively. The states Q_0 to Q_{L0-1} are the idle states in which the node has no packets to send. These states model the unsaturated traffic condition, since the node remains at these states as long as no packet arrival occurs. States (i, 0, j) and (i, -1, j) represent CCA1 and CCA2, respectively. States (-1, k, j) and (-2, k, j) represent the successful transmission and packet collision, respectively. The probabilities α, β, p, and P_c represent the probability of finding CCA1 busy, the probability of finding CCA2 busy, the probability of having no packet arrivals, and the probability of collision, respectively. The parameters L_0, L_s,

and L_c are the duration of the idle states, the duration of successful transmission, and the duration of packet collision, respectively. Assuming the stationary distribution of the Markov chain to be $b_{i,k,j} = lim_{t\to\infty} P(s(t) = i, c(t) = k, r(t) = j)$, where $i \in (-2, m)$, $k \in \left(-1, max(W_i - 1, L_s - 1, L_c - 1)\right)$, $j \in (0, n)$, we can now derive the closed form expressions for the distribution chain. The details of the derivations are tedious and the interested reader can refer to [PAR10]. Also, the authors approximate the formulas they derived in order to reduce their complexity and thus make them implementable on sensor nodes. In the following we provide the approximated formulas that are of interest to our work:

$\sum_{i=0}^{m}\sum_{k=0}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} + \sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,-1,j} +$

$$\sum_{j=0}^{n}\left(\sum_{k=0}^{L_s-1} b_{-1,k,j} + \sum_{k=0}^{L_c-1} b_{-2,k,j}\right) + \sum_{l=0}^{L_0-1} Q_l = 1 \quad (3.1)$$

$$\sum_{i=0}^{m}\sum_{k=0}^{W_i-1}\sum_{j=0}^{n} b_{i,k,j} \approx \frac{b_{0,0,0}}{2}[(1+2x)W_0 + 1 + x](1+y) \quad (3.2)$$

$$\sum_{i=0}^{m}\sum_{j=0}^{n} b_{i,-1,j} \approx b_{0,0,0}(1-\alpha)(1+x)(1+y) \quad (3.3)$$

$$\sum_{j=0}^{n}\left(\sum_{k=0}^{L_s-1} b_{-1,k,j} + \sum_{k=0}^{L_c-1} b_{-2,k,j}\right) \approx b_{0,0,0} L_s (1 - x^{m+1})(1+y) \quad (3.4)$$

$$\sum_{l=0}^{L_0-1} Q_l \approx b_{0,0,0} K_0 [1 + y + P_c(1 - x^{m+1})(y^n - y - 1)] \quad (3.5)$$

$$\tau \approx (1+x)(1+y) b_{0,0,0} \quad (3.6)$$

where,

$$x = \alpha + (1-\alpha)\beta \quad (3.7)$$

$$y = P_c(1 - x^{m+1}) \quad (3.8)$$

$$\alpha = LP_c(1-\alpha)(1-\beta) + L_{ack}\frac{N\tau(1-\tau)^{N-1}}{1-(1-\tau)^N} P_c(1-\alpha)(1-\beta) \quad (3.9)$$

$$\beta = \frac{P_c + N\tau(1-\tau)^{N-1}}{2-(1-\tau)^N + N\tau(1-\tau)^{N-1}} \quad (3.10)$$

$$P_c = 1 - (1-\tau)^{N-1} \quad (3.11)$$

where, L is the length of the packet and L_{ack} is the length of the ACK packet (all measured in terms of aUnitBackoffPeriod).

From Equations (3.2)-(3.5) we can derive a closed form expression for $b_{0,0,0}$. However, some additional approximations are applied (like approximating the term $1 - x^{m+1}$ as $1 - x^2$) and an approximation for $b_{0,0,0}$ is denoted as $\tilde{b}_{0,0,0}$ and formulated as follows:

$$\tilde{b}_{0,0,0} \approx \frac{2}{W_0 r_1 + 2r_2} \tag{3.12}$$

where, $r_1 = (1 + 2x)(1 + \hat{y})$, $r_2 = L_s(1 - x^2)(1 + \hat{y}) + \frac{p}{1-p} L_0(1 - \hat{y}^2 + \hat{y}^{n+1})$, and $\hat{y} = P_c(1 - x^2)$.

3.2.2 . Modeling SB-BEB

We abide by the assumptions of Park's model stated in the previous section. Our extension to Park's model is attained by introducing the standby state (SB state for simplicity) to model the fact that a node will sleep after each successful packet transmission. The SB state will be included in the dashed box that is shown directly following the state (-1, L_s-1, n) in Figure 3-1. The dashed box is better illustrated in the snapshot shown in Figure 3-3.

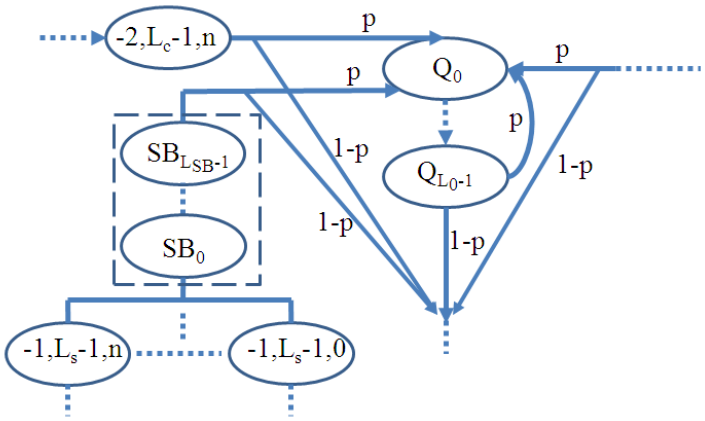

Figure 3-3: Introducing the SB state into Park's Markov chain model.

L_{SB} is the total period of time the node spends in the SB state. We denote the probability of being in any of the states $SB_0 \dots SB_{L_{SB}-1}$ by b_{SB}. Note that $b_{SB_0} = b_{SB_1} = \cdots = b_{SB_{L_{SB}-1}}$. Therefore, $\sum_{l=0}^{L_{SB}-1} b_{SB_l} = L_{SB} b_{SB_0} = L_{SB} b_{SB}$. From Figure 3-2, by applying the chain regularities, we can find the formula of b_{SB}:

$$b_{SB} = \sum_{j=0}^{n} b_{-1,L_s-1,j} = (1-P_c)(1-x^{m+1})\left(\frac{1-y^{n+1}}{1-y}\right) b_{0,0,0} \quad (3.13)$$

Using Equation (3.12) and by approximating $\frac{1-y^{n+1}}{1-y}$ as $1+y$ (because y << 1), Equation (3.13) can be further approximated as:

$$b_{SB} \approx (1-P_c)(1-x^2)(1+y)\tilde{b}_{0,0,0} \quad (3.14)$$

Therefore, the normalization condition in Equation (3.1) should be updated to include the probability of being in the SB state, that is, $\sum_{l=0}^{L_{SB}-1} b_{SB_l}$.

From Equation (3.11) we can see that the probability of packet collision takes into account the fact that all nodes except the sensing node itself (i.e., N-1 nodes) should refrain from sending packets for the collision to be avoided. Introducing the SB state results in that a lesser number of nodes will be sensing the medium to send their packets, because some nodes may be sleeping (i.e., in the SB state) and thus should not be counted. Therefore, Equation (3.11) should consider the nodes that are in the SB state. We denote the expected number of nodes that are in the SB state at any time by $E(n_{SB})$. The formula for $E(n_{SB})$ is:

$$E(n_{SB}) = L_{SB} b_{SB} (N-1) \quad (3.15)$$

As a result, Equations (3.9)-(3.11) should be updated such that "N" is replaced by "N-$E(n_{SB})$" and "N-1" is replaced by "N-1-$E(n_{SB})$"

Therefore, Equation (3.11) becomes:

$$P_c = 1-(1-\tau)^{N-1-E(n_{SB})} \quad (3.16)$$

Equation (3.16) indicates, when compared to (3.11), that a reduction in the packet collision is anticipated due to the inclusion of the SB state. Equations (3.6), (3.9), (3.10), (3.12) and (3.13) form a system of five nonlinear equations with five variables, namely, α, β, τ, b_{SB}, and $b_{0,0,0}$. Therefore, we can solve this system using numerical methods. In the following subsections we derive the formulas for some performance metrics that we will use later to evaluate the functionality of the SB-BEB algorithm.

3.2.2.1 Channel Utilization under SB-BEB

Channel Utilization (U) is an important performance metric to evaluate SB-BEB, because we need to see whether forcing nodes to sleep, after each successful packet transmission, is underutilizing the communication channel or not. We define the channel utilization by the ratio of the packet length (L) and the total time (D) spent starting from sensing the channel to send the packet till the ACK packet is received back. That is, $U = \frac{L}{D}$. In [PAR10], D is defined taking into account the time spent till the packet is successfully transmitted (L_s), the time wasted due to j packet collisions (jL_c), and the time wasted during the backoff stage (D_{BO}). By introducing the SB state, we also need to consider the time wasted due to being in the SB state. In other words, once all nodes succeed to successfully transmit their packets, assuming that L_{SB} is much longer than $L_s+jL_c+D_{BO}$, we will reach a stage where all nodes are in the SB state and the communication medium is idle. At that level, the medium is not being utilized and thus the SB will contribute to the underutilization of the medium. The time wasted while all nodes are in the SB state is $L_{SB} - D(N-1)$. The latter factor should be included in the computation of the total delay (D_T). Thus, the formula for U will be given by:

$$U = \frac{L}{D_T} = \frac{L}{X_{R+}\left(L_{SB}-D(N-1)\right)*\left(L_{SB}-D(N-1)\right)+D} \quad (3.17)$$

Where, X_{R+} is the indicator function. X_{R+}evaluates to 1 if the SB state is deployed (with L_{SB} bigger than D(N-1)). Otherwise, X_{R+}evaluates to zero, which reduces Equation 3.17 to Park's formula.

3.2.2.2 Average Power Consumption under SB-BEB

In [PAR10], the author's state that the total average power consumed in the network (E_{tot}) is the sum of the average power consumed during backoff state (E_b), channel sensing state (E_{sc}), packet transmission state (E_t), idle state (E_q), and wake-up (E_w) state. We simply add a new term to reflect the average power consumed during the SB state (E_{SB}). Therefore, Park's formula to compute E_{tot} becomes as follows:

$$E_{tot} = E_b + E_{sc} + E_t + E_q + E_w + E_{SB} \quad (3.18)$$

In computing the average power consumed during each state, the power wasted at that state is multiplied by the probability of being at that state. For example, if the amount of power consumed during the SB state is P_{SB}, and we know that the probability of being in the SB state is $\sum_{l=0}^{L_{SB}-1} b_{SB_l}$, then the average power consumed during SB is $E_{SB} = P_b \sum_{l=0}^{L_{SB}-1} b_{SB_l}$. It should be noticed that the inclusion of the term $\sum_{l=0}^{L_{SB}-1} b_{SB_l}$in Equation (3.1) results in reducing the value of each of the other state probabilities in the same equation. This is directly reflected on the average power consumed at each of these states, since the value of the state probability is included in the power computation as stated above. Therefore, we anticipate that, compared to Park's model, the inclusion of the SB state will reduce the total average power consumed.

3.3 Simulations and Model Validation

In this section we conduct extensive simulations in order to validate the mathematical model developed for SB-BEB, and then compare its performance to the standard BEB. The comparison concentrates on four main performance metrics, namely, fairness, channel

utilization, reliability, and average power consumption. We use MATLAB 7.9.0 to solve the nonlinear system of equations we developed in subsection 3.2.2.

3.3.1 Model Validation

In validating our theoretical model we concentrate on both channel utilization and average power consumption. For each parameter studied, we compute the *coefficient of variation of the root-mean-square deviation RSMD* (*CV(RMSD)*), which is a measure of the accuracy of our mathematical model. In other words, *CV(RMSD)* measures the differences between the mathematical model and the simulations. *CV(RSMD)* is defined as follows:

$$CV(RSMD) = \frac{\sqrt{\frac{\sum_{i=1}^{n}(V_{theo} - V_{sim})^2}{n_{sample}}}}{\bar{V}}$$

where, V_{theo} is the predicted theoretical value, V_{sim} is the simulated value, $\bar{V}$ is the average of the sample values, and n_{sample} is the total number of the sample values used. An accurate theoretical model should achieve low values for $CV(RMSD)$.

Furthermore, we assume that L = L_s = L_c = 14 timeslots, L_0 = 1 timeslot, p = 0.1, m = 4, n = 3, and macMinBE = 3.

3.3.1.1 Channel Utilization

In Figure 3-4 we show the theoretical performance of SB-BEB in terms of channel utilization, as predicted by Equation 3.17, compared to the simulated performance. We show the performance behavior under different values of L_{SB} for different network sizes (from N = 10 to N = 50 nodes). We can clearly see that our model is accurate in predicting the values of the channel utilization under the SB-BEB algorithm. This is confirmed by noticing that for N =10,

20, 30, 40 and 50, the computed CV(RMSD) is 8.1%, 5.98%, 4.8%, 4.38%, and 5.79%, respectively.

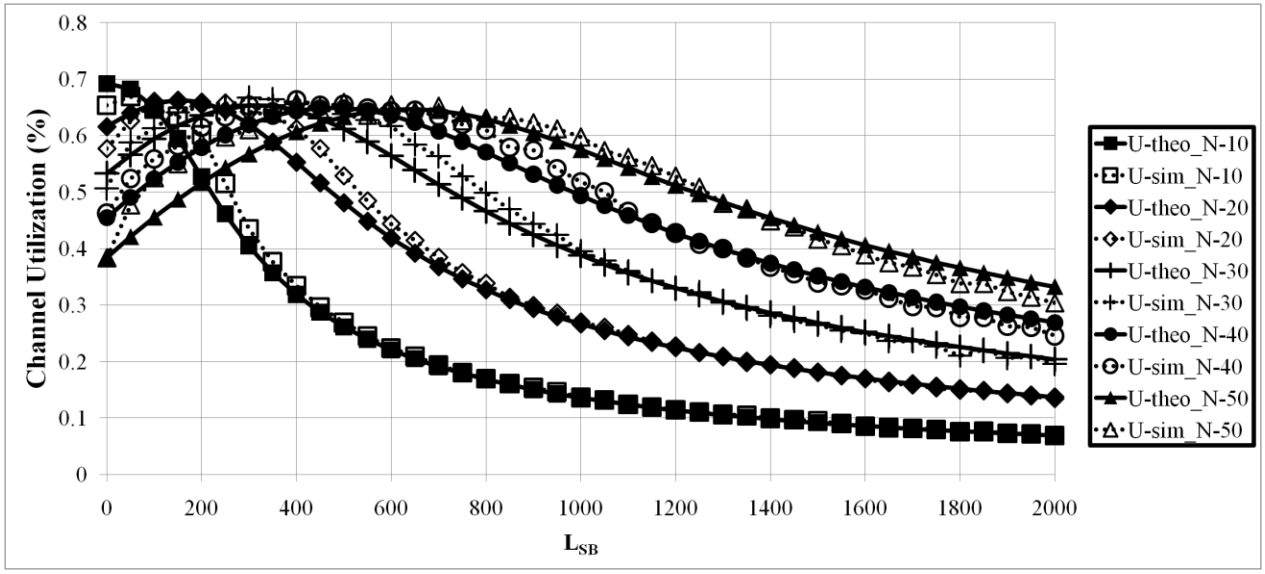

Figure 3-4: Channel Utilization (U) with respect to L_{SB} at different network sizes.

3.3.1.2 Average Power Consumption

In Figure 3-5 we show the theoretical performance of SB-BEB in terms of the average power consumed, as predicted by Equation 3.18, compared to the simulated performance. Again, we study the performance under different values of L_{SB} for different network sizes (from N = 10 to N = 50 nodes). The figure clearly shows that our model can accurately predict the average power consumed in the network when the SB-BEB algorithm is implemented. The computed CV(RMSD) for N =10, 20, 30, 40 and 50, 4.31%, 3.68%, 4.99%, 6.8%, and 2.78%, respectively. These values confirm the accuracy of our model.

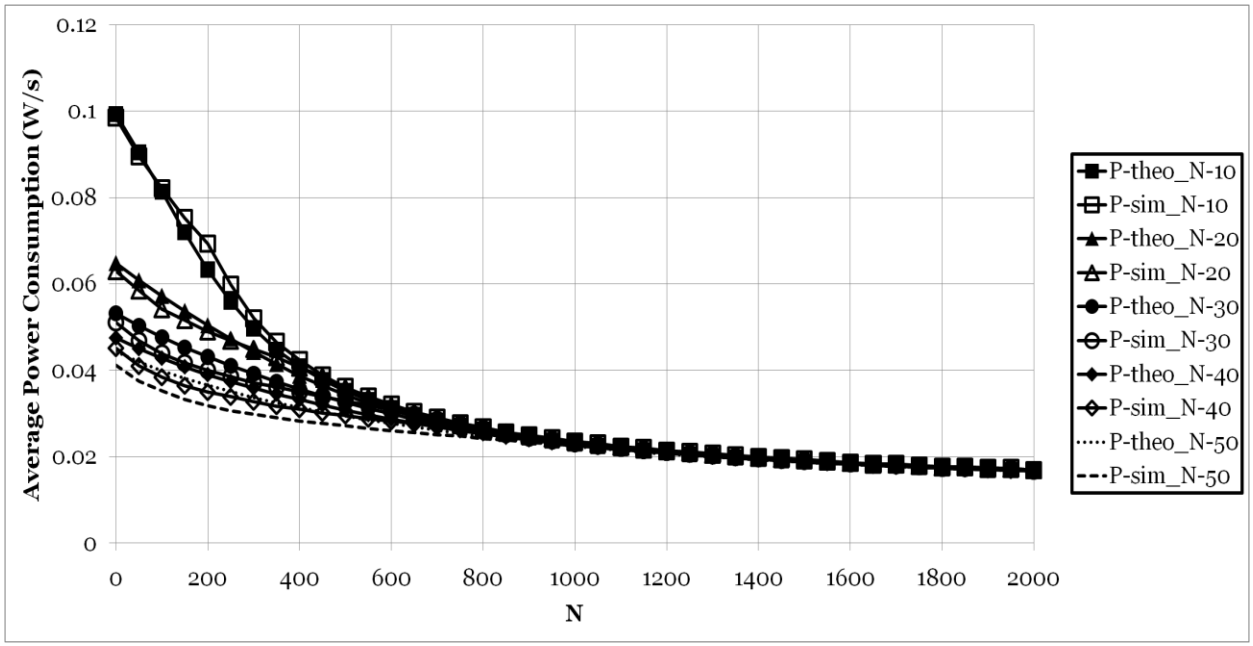

Figure 3-5: Average power consumed with respect to L_{SB} at different network sizes.

3.3.2 Comparing SB-BEB with the standard BEB

In this subsection we compare SB-BEB's performance to the standard BEB implemented in the IEEE 802.15.4 standard. We conduct simulations to study the performance in terms of fairness, channel utilization, reliability, and most importantly average power consumption. Our simulations are run on a C-based simulator that we have developed. The network under simulation is of a peer-to-peer topology. The simulation parameters are listed in Table 3-1 (we adopt some of the values defined in [POL08] for the same parameters). We assume that CFP and the inactive period are absent in the superframe. The data traffic is assumed to be saturated. That is, each node always has data to be transmitted. Also, the traffic is assumed to be acknowledged. In all of our simulation results a confidence interval (CI) of 95% is assumed. This CI is not shown in our graphs because it is too small to be observed (refer to Appendix B for more details). We now show and discuss the data collected to study each of the performance parameters mentioned earlier.

Table 3-1: SB-BEB Simulation Parameters

Average Power Consumed (mW.s)	Rx	40
	Tx	30
	CCA	40
	Sleep	0.8
Durations	1 timeslot	0.32 ms (80 bits)
	Packet Length (L)	14 timeslots
	ACK Packet Length (L_{ACK})	2 timeslots
	Simulation Time	320 s
IEEE 802.15.4 Parameter Settings	*macMaxCSMABackoffs*	5
	macMinBE	3
	macMaxBE	5

3.3.2.1 Fairness

It is essential to preserve *fairness* among nodes. That is, each node should have an equal probability of accessing the communication medium. We compute the fairness index using Jain's formula [JAI84]:

$$fairness\ index = \frac{(\sum x_i)^2}{N \sum {x_i}^2}$$

where, N is the number of contending nodes, and x_i is the medium share of the ith node. A fairness index of 1 implies that the protocol used is allowing each node in the network an equal

share of medium access. However, as the fairness index decreases towards zero, it implies that only a portion of the nodes is getting more opportunities to access the medium than other nodes. In Figure 3-6, for network sizes ranging from 10 to 50 nodes, we show the performance in terms of fairness under different values of L_{SB}. The figure clearly shows that we are almost always at a fairness index of 1 (only the curve for N = 10 is apparent because the curves have almost the same behavior and they overlap perfectly), indicating that our SB-BEB algorithm is achieving a fair treatment of the nodes in the network.

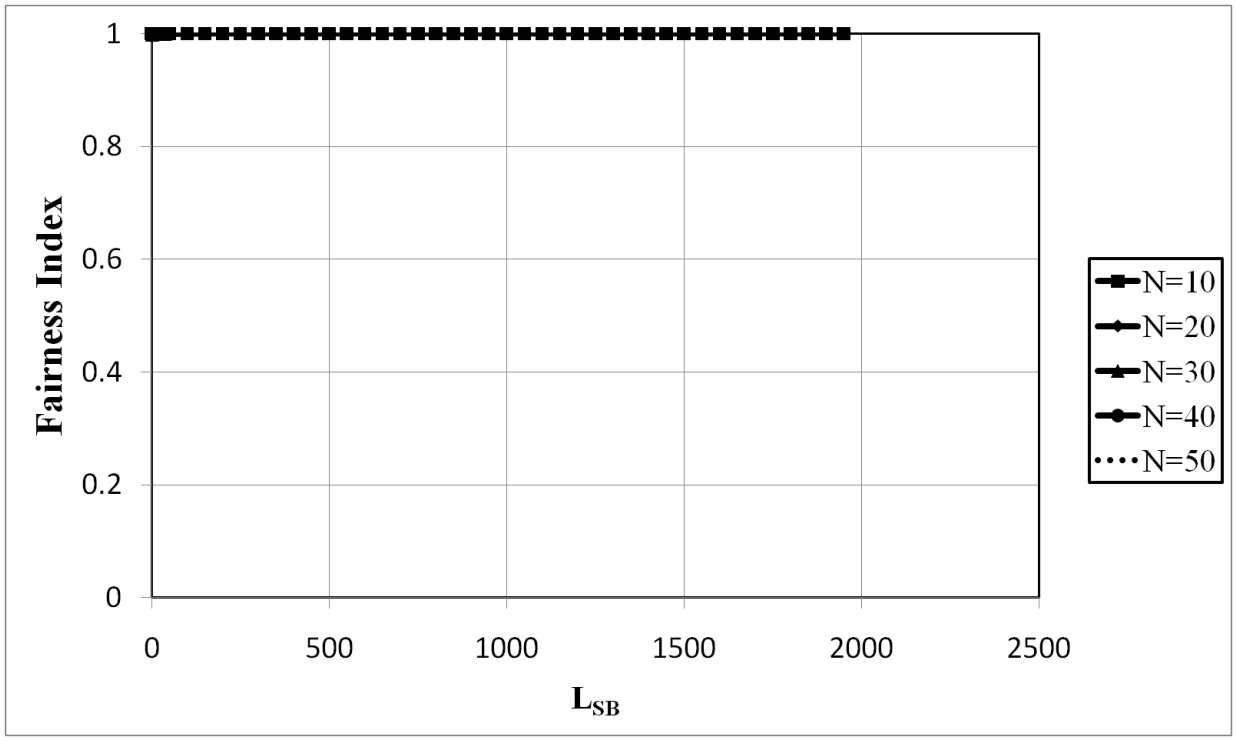

Figure 3-6: Fairness under different values of LSB for different network sizes.

3.3.2.2 Channel Utilization

It is essential to examine the behavior of SB-BEB in terms of wireless channel usage. We need to make sure that the proposed algorithm can achieve at least the same level of channel utilization (U) as the standard BEB does.

In Figure 3-7, for network sizes ranging from 10 to 50 nodes, we show the performance in terms of U under different values of L_{SB}. Interestingly enough, we observe that U shows an increasing trend till it reaches a maximum value (for example, for N = 30, U reaches a value of 66.75% at an L_{SB} of 150 timeslots) before declining as we increase the value of L_{SB}. The reason behind the increasing trend is that forcing nodes to go to the SB state is playing a significant role in reducing the number of contending nodes, and therefore, reducing the probability of packet collisions. Therefore, while L_{SB} is small, nodes are getting better opportunities of using the medium in order to successfully transmit their data. However, as we keep increasing L_{SB} we are actually forcing nodes to sleep for extended periods of time after each successful transmission. Once all nodes are in the SB state, the medium may remain idle for a long duration before any node starts the channel sensing again. This results in the underutilization of the communictaion channel.

The interesting conclusion we gain from Figure 3-7 is that we are able to tune L_{SB}, once we know N, in order to achieve the highest U desired. For example, a network of 20 nodes can achieve its highest U by setting L_{SB} to almost 100 slots. From this conclusion, we can use Figure 3-7 to draw the relationship between N and L_{SB} that corresponds to the highest (optimal) U. This is shown in Figure 3-8. This figure is very helpful as it guides us on how to tune L_{SB} by just knowing the size of the network under study. Similar to [ZHA10], a look-up table, populated with the optimal L_{SB} values that correspond to different networks sizes, can be stored at each node. With that, each node can tune its L_{SB} as soon as it learns its network size, and the optimal channel utilization can be achieved.

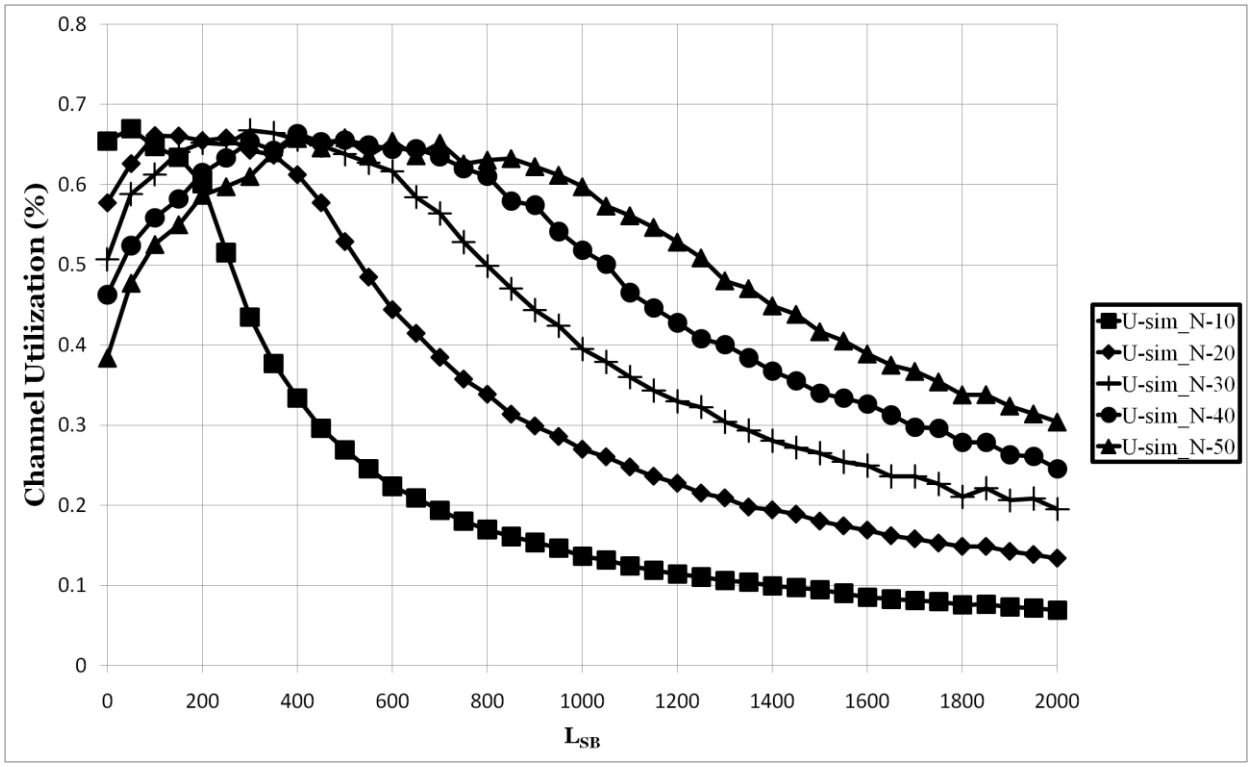

Figure 3-7: Channel Utilization under different values of L_{SB} for different network sizes.

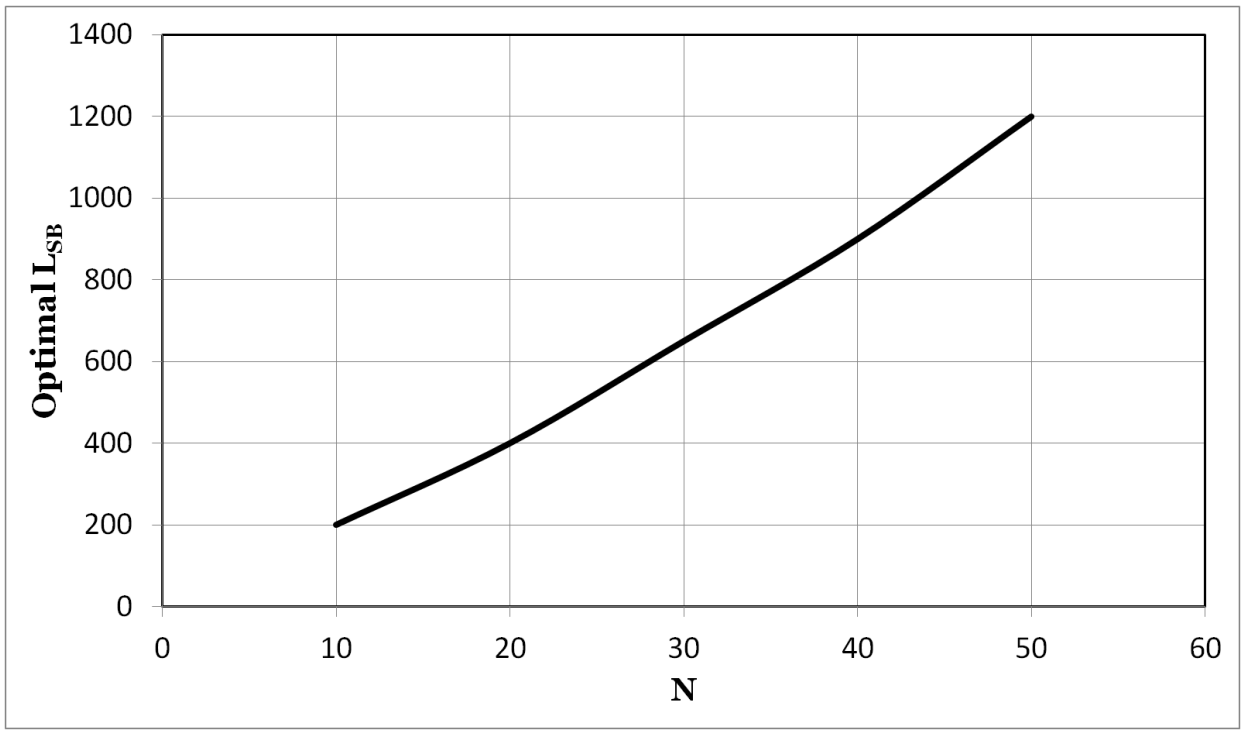

Figure 3-8: Optimal values of LSB to achieve maximum U, given the network sizes.

3.3.2.3 Reliability

As in [PAR10], we define *reliability* (R) as the probability of receiving a packet successfully. In Figure 3-9 we show the behavior of R under different L_{SB} values and for different network sizes. Apparently, as L_{SB} increases, R tends to reach, and remain at, the value of 1. This is due to that as nodes standby for longer periods, they actually contribute to excessive reduction in the probability of collision and thus more packets are reaching their destinations successfully. Figure 3-9 also shows that as the size of the network gets bigger, R remains at a lower value before it starts its rise towards the value of 1. This is due to that as the number of nodes increases in the network, packet collisions increase and we will need to force nodes to standby for longer periods of time, giving better chances of successful transmission for the awaken nodes. In Figure 3-10 we draw the values of R achieved at the optimum L_{SB} values found in subsection 3.3.2.2. In this figure, we compare these values of R with the reliability achieved under the standard BEB. Both curves are shown at different network sizes. We can clearly see that with the SB state we are able to outperform the original standard significantly.

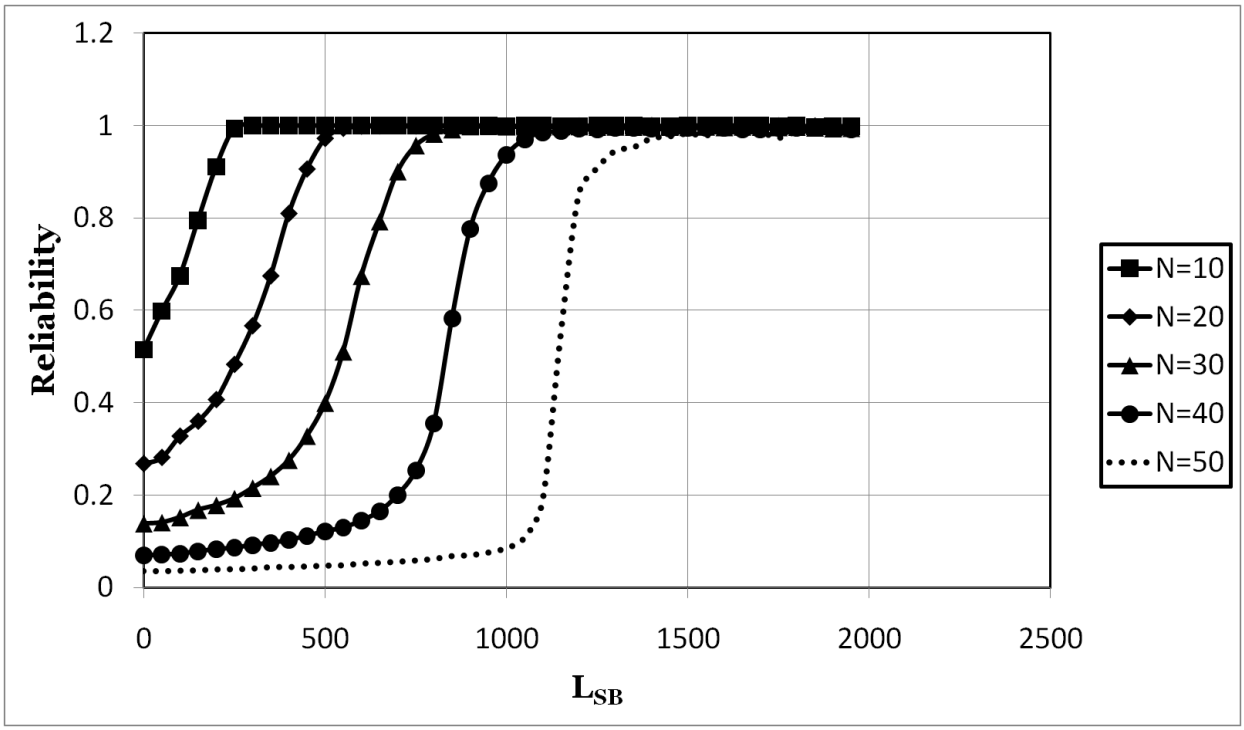

Figure 3-9: Reliability under different values of L_{SB} for different network sizes.

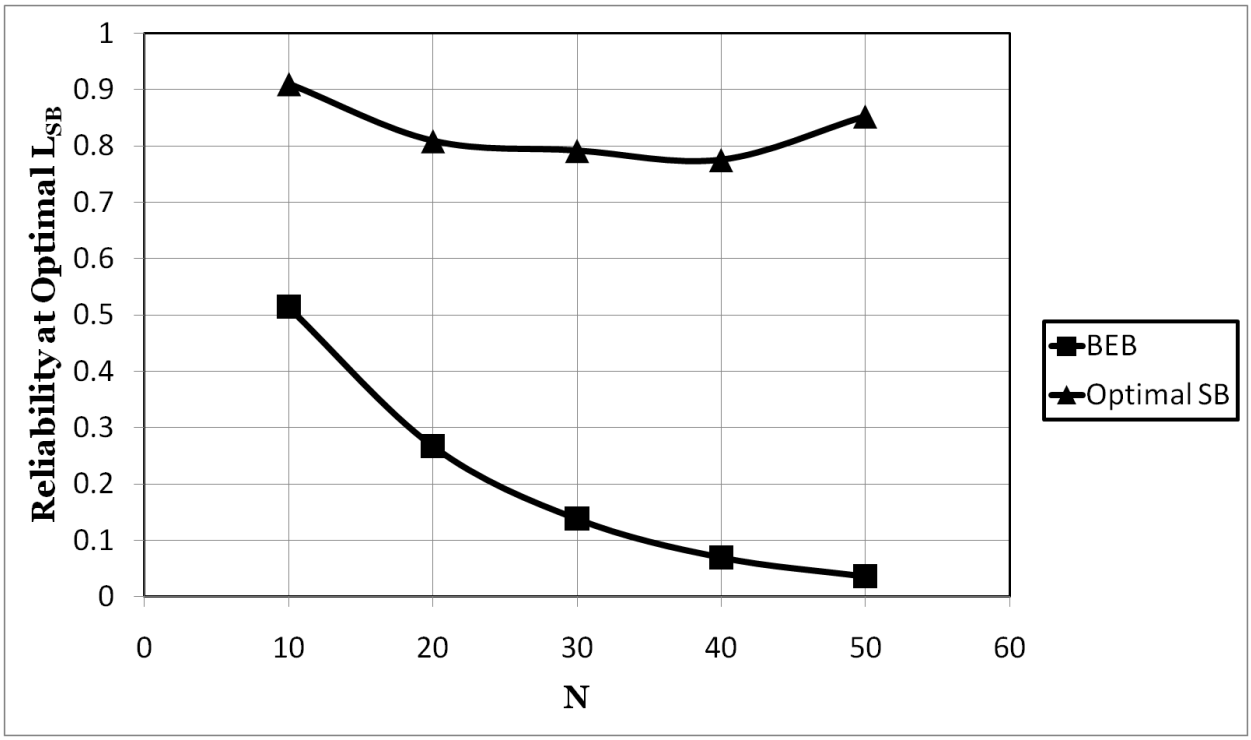

Figure 3-10: Reliability achieved at the optimal L_{SB} values, for different network sizes.

3.3.2.4 Average Power Consumption

In Figure 3-11 we illustrate the effect of introducing the SB state on the average power consumption (P) (which is the sum of the average power consumed during transmission, reception, sleep, CCA, and collisions). For different network sizes, we show P as the value of L_{SB} increases. This figure clearly shows the expected behavior of achieving more power savings as we force nodes to standby for longer periods. Also apparent in the same figure that networks constituted by 10 nodes suffer from relatively high P at lower values of L_{SB}. This can be understood if we notice that as we decrease N, nodes get better chances of successfully transmitting their packets (i.e., packet collisions are low). Therefore, since L_{SB} is low, nodes will be actively involved in accessing the communication channel to send packets and this contributes to higher P. In Figure 3-12, we use the optimum values of L_{SB} (from subsection 3.3.2.2) to find the average power consumption experienced with them. Compared to the average power consumed under the standard BEB, Figure 3.12 clearly shows the savings we can achieve by introducing the SB state in the IEEE 802.15.4 standard.

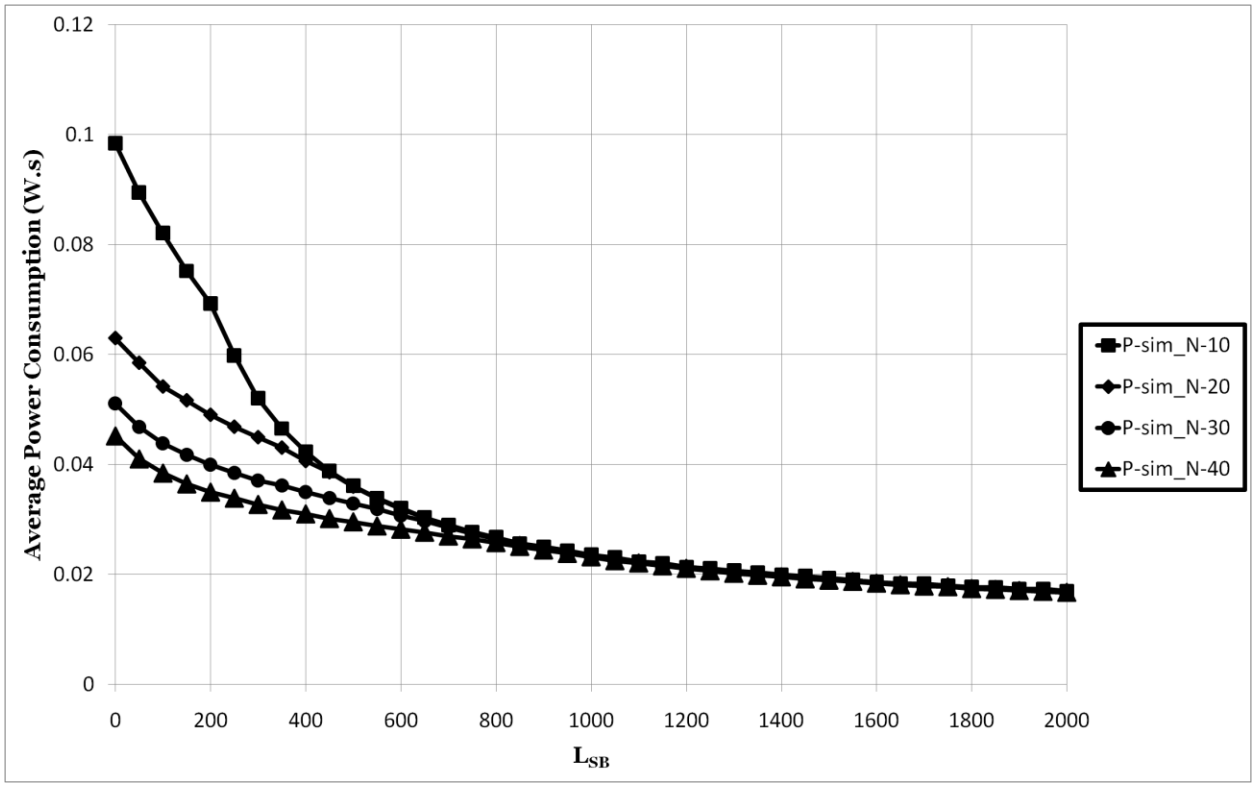

Figure 3-11: Average Power Consumption under different values of L_{SB} for different network sizes.

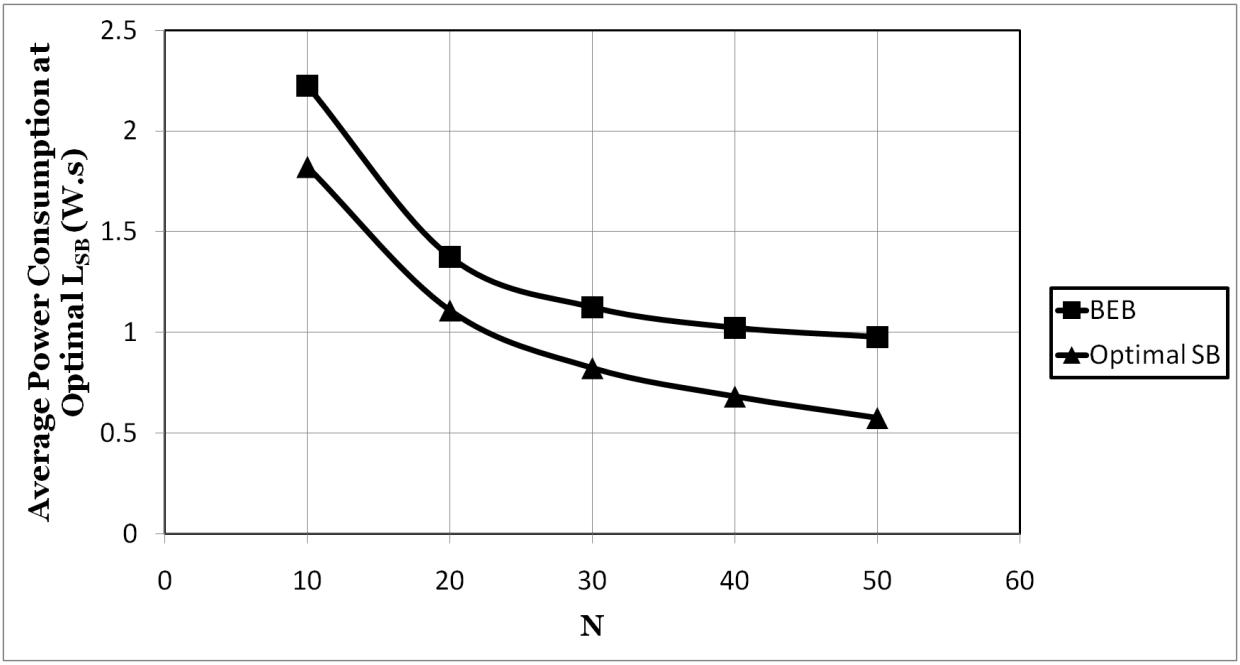

Figure 3-12: Average power consumption experienced at the optimal L_{SB} values for different network sizes.

3.4 Conclusion

In this chapter we have introduced a new backoff algorithm called the Standby-BEB (SB-BEB). With this algorithm a new *standby state* (SB state) is introduced in the mechanism of the IEEE 802.15.4 MAC protocol. The SB state is enforced after each successful transmission of a packet. That is, nodes are required to sleep for a designated time of period after each successful packet transmission. The main motivation behind this new state is to conserve more power such that the lifetime of the WSN is prolonged. We have provided both theoretical analysis and a simulation study for SB-BEB. We have proven that SB-BEB is capable of not only conserving more power for the nodes, but also improving both the channel utilization and the communication reliability. We have also found that there exists optimal durations for the SB state at which the highest channel utilization can be achieved, given the network size. With this finding, we can maintain a look-up table at each node to tune its standby period, once it knows the network size, to achieve the optimal channel utilization.

Chapter 4

Probabilistic MAC Protocol for IEEE 802.15.4-based WSNs

4.1 Introduction

In Chapter 3 we have managed to achieve an improvement in IEEE 802.15.4 MAC's performance through the incorporation of a new standby state. We have basically found an additional opportunity for each node to shut down its system such that more savings in its power resources are attained. As a matter of fact, we can think of the standby state to be part of the backoff period itself. That is, a node implementing the SB-BEB algorithm is just adding an extra duration to its randomly selected backoff period. Since maintaining a look-up table for the standby period at each node may be impractical due to memory limitations, we need to develop an algorithm that selects the standby period, or the backoff period as a whole, in an adaptive manner. This adaptive selection should be dependent on the size of the network (as we have seen in Chapter 3). In this chapter we use the findings of Chapter 3 to design the new Adaptive Backoff Algorithm (ABA) that is intended to replace BEB in IEEE 802.15.4 MAC. We use Markov chain to develop an analytical model that can accurately predict the functionality of ABA. We also conduct a simulation study to validate our proposed analytical model. The rest of this chapter is organized as follows. Section 4.2 describes ABA and provides a detailed explanation of its Markov-based analytical model. Section 4.3 describes the simulations we conducted to validate the developed model for ABA, and compares the performance of ABA

with a number of backoff algorithms proposed in the literature. Finally, Section 4.4 concludes the chapter.

4.2 The Adaptive Backoff Algorithm

The pivotal objective of ABA is to improve the channel utilization (U) in the WSN. ABA can achieve higher levels of channel utilization than is possible with BEB, while keeping the power consumption at the lowest possible level. Prior to designing/modifying any backoff algorithm, it is essential to understand the main factors that play a role in degrading U. From one side, whenever the nodes select long backoff periods, the wireless medium is forcibly kept idle for a long duration of time and thus U is affected. From another side, as the rate of packet collisions rises, the useful communication activities over the medium are affected and U is reduced as a result. Failing to consider these two factors leads to the design of less effective backoff algorithms in WSNs.

The problem with BEB is that it provides a *deterministic* solution that keeps on updating the length of the contention window based on predefined steps. This is the main shortcoming of BEB. We need a *probabilistic* solution that can involve the status over the wireless medium in the computation of the contention window. Based on that, ABA proposes that the probability of collision (P_c) be used in updating the value of the contention window. This approach guarantees that the contention window will be adapted to conditions over the communication channel. Stated differently, the value of the contention window will be updated as follows:

$$W(t) = P_c(t)W_{max} \qquad (4.1)$$

where, $W(t)$ (or W for simplicity) is the selected contention window at time t, W_{max} is IEEE 802.15.4's maximum defined contention window (set to $2^{macMaxBE}$), and $P_c(t)$ (or P_c for simplicity) is the probability of collision at time t. P_c is computed locally at each node by

knowing the proportion of packets that suffered from collisions. This proportion is computed as $n_c/(n_s + n_c)$, where n_c and n_s are, as observed by any node, the total number of collided packets and the total number of successfully transmitted packets, respectively (note that in case of unacknowledged traffic, we assume that a mechanism at higher layers is available to advise the MAC of a collision after a certain timeout). We use the concept of exponential weighted moving average (EWMA) to compute P_c before applying Equation (4.1). According to [WOO08], the use of EWMA helps in minimizing the bias against transient measurements of P_c. According to (4.1), upon having a packet to send, the node backs off for a duration that cannot exceed W_{max}. In case that CCA1 or CCA2 reveal that the medium is busy, the backoff process is repeated macMaxCSMABackoffs times before discarding the packet. On the other hand, upon experiencing an idle medium after the two CCAs, the packet is sent. In case of a packet collision, the node updates its W and attempts to resend the packet again. If the packet continues to collide more than macMaxFrameRetries times, it will be discarded. Equation (4.1) indicates that, as the rate of collisions increases (decreases), the node utilizes an extended (a shortened) backoff period. This is anticipated to significantly reduce (increase) the contention among nodes, and also allows them better chances of successful transmission. The overall result is enhanced channel utilization in the network.

ABA requires no hardware upgrades and performs simplified computations that require low power consumption (as we demonstrate in Section 4.3). Moreover, ABA can be easily implemented on sensor nodes' platform. In Figure 4-1 we show the flow diagram of ABA.

We now develop the mathematical model for ABA based on Markov chain (see [ASH11], [CHE07], [FAR10], [FAN09], [JUN09], [MAR09], [RAM07], [WIJ10], [XIA10], and [ZHU11b] for extensive studies on how to model IEEE 802.15.4's BEB using Markov chain).

The model considers both acknowledged and unacknowledged saturated traffic conditions (that is, a node has always a packet to send.).

In Figure 4-2 we show our two-dimensional Markov-based model for ABA. This model covers all the states a node goes through to access the medium and send its packets. Each state in our Markov model is distinguished by a pair (i, j), where i can be 0, -1, or -2, to refer to the backoff/CCA states, successful transmission states, or collision states, respectively. The j index will be clarified in the following. States (0, j), where $j \in [1, W-1]$, are the backoff states during which the node is involved in no activity, waiting for its backoff counter to expire. States (0, 0) and (0,-1) correspond to CCA1 and CCA2, respectively. States (-1, j), where $j \in [0, L_s\text{-}1]$, correspond to the duration spent to successfully transmit a packet. Finally, States (-2, j), where $j \in [0, L_c\text{-}1]$, correspond to the time wasted due to a packet collision. The probability of finding the medium busy during CCA1 (CCA2) is denoted as α (β) (an explanation on the difference between α and β is detailed in [MIŠ05]). The state transition probabilities of our Markov chain are as follows:

$$P(0, j-1|0, j) = 1 \qquad for \quad 0 < j \leq W-1 \quad (4.2)$$

$$P(0, j|0,0) = \frac{W-j}{W} \qquad for \quad j \geq 0 \quad (4.3)$$

$$P(0, -1|0,0) = 1-\alpha \quad (4.4)$$

$$P(-1, j|0,0) = (1-\alpha)(1-\beta)(1-P_c) \quad for \quad 0 \leq j \leq L_s - 1 \quad (4.5)$$

$$P(-2, j|0,0) = (1-\alpha)(1-\beta)P_c \quad for \quad 0 \leq j \leq L_c - 1 \quad (4.6)$$

$$P(0, j|-1, j\ or -2, j) = \frac{1}{W} \qquad for \quad j \geq 0 \quad (4.7)$$

Equation (4.2) captures how the backoff counter decrements before attempting any packet transmission. Equation (4.3) describes the probability of backing off given that the medium was

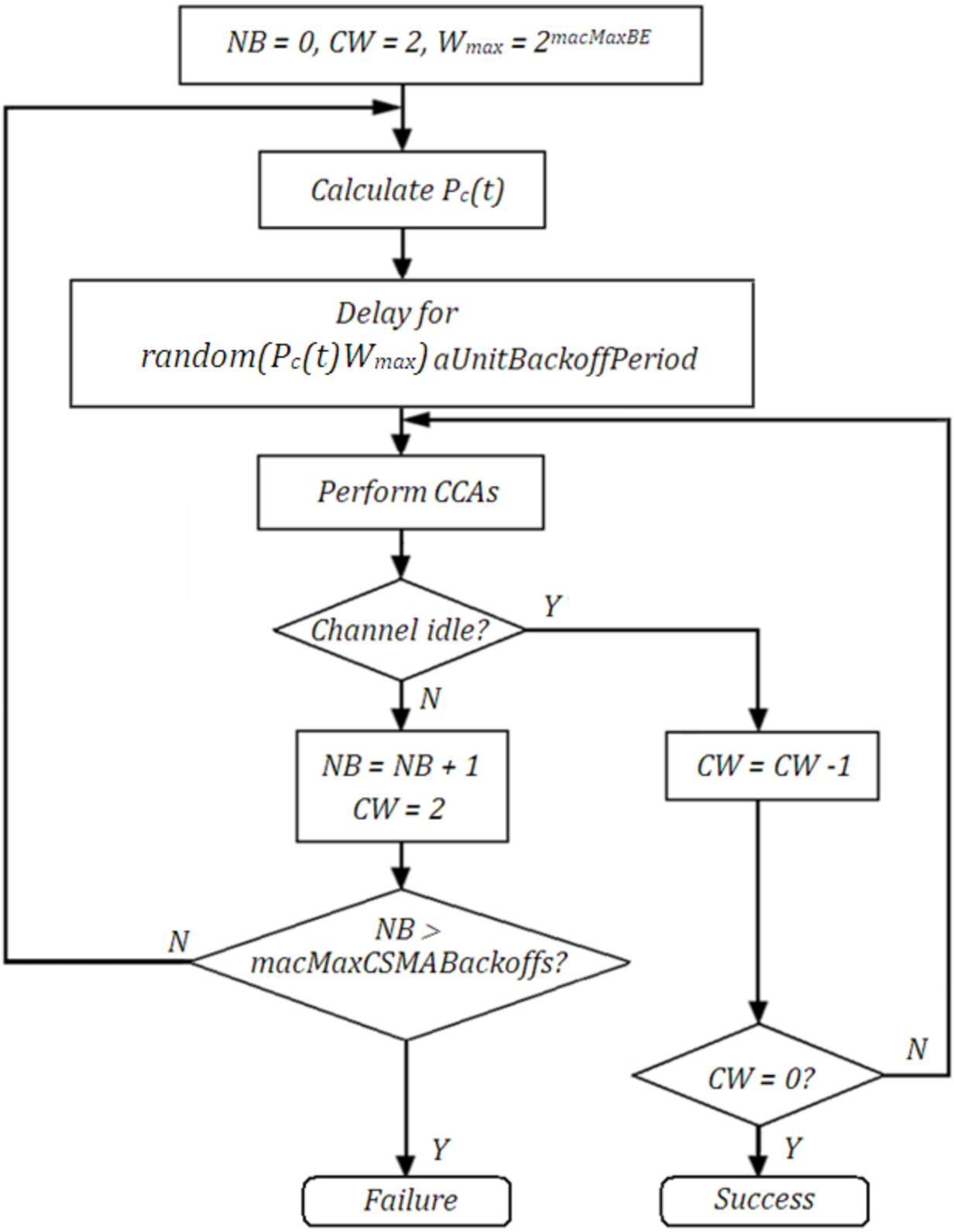

Figure 4-1: ABA Algorithm.

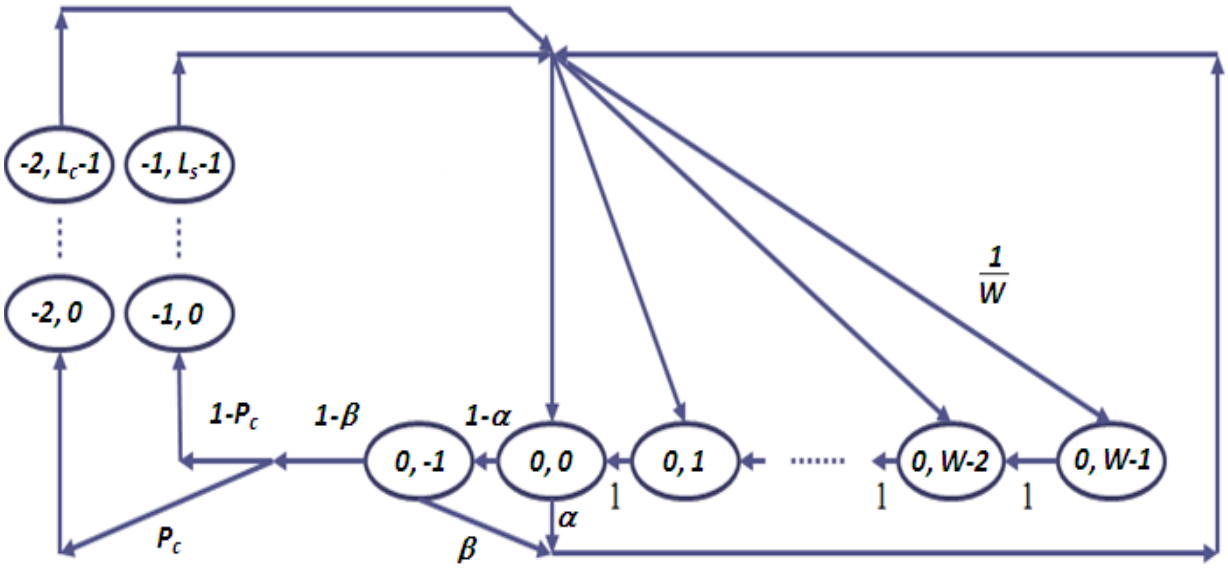

Figure 4-2: Markov chain of ABA algorithm under saturated traffic conditions.

found busy during CCA1 or CCA2. Note that W in this equation will be updated according to (4.1). It is important to point out that deriving (4.3) is attained by summing all the transition probabilities starting from state (0, 0) and ending at any of the states (0,0), … , (0, W-1). The summation includes the probabilities: $(\alpha + (1-\alpha)\beta)/W$ (to transit from state (0,0) to any of the backoff states(0, j), where j∈[0, W-1]), $(1-\alpha)(1-\beta)(1-P_c)/W$ (to transit from state (0,0) to any of the backoff states, after a successful transmission), $(1-\alpha)(1-\beta)P_c$ (to transit from state (0,0) to any of the backoff states, after a packet collision), and the probability of being at the state preceding the selected backoff state (so, if backoff state (0, 1) was randomly selected, we should include the probability of being at backoff state (0, 2) in our summation, and so on). Equation (4.4) states the probability of initiating CCA2 given that CCA1 was successful. Equation (4.5) is the probability of successfully sending a packet after two successful CCAs while Equation (4.6) is the probability of having a packet collision after those CCAs. Finally, Equation (4.7) describes the even probability of choosing a contention window after packet

transmission/collision. Assuming that s(t) and c(t) are the stochastic processes representing the backoff stage and the state of the backoff counter, respectively, we now write the stationary distribution of our Markov chain to be $b_{i,j} = lim_{t\to\infty} P(s(t) = i, c(t) = j)$, where $i \epsilon [-2,0]$ and $j \epsilon [-1, max\ (W-1, L_s-1, L_c-1)]$. We now derive the closed form expressions for this distribution.

By the normalization condition, we have the following formula:

$$\sum_{j=1}^{W-1} b_{0,j} + \sum_{j=0}^{L_s-1} b_{-1,j} + \sum_{j=0}^{L_c-1} b_{-2,j} + b_{0,0} + b_{0,-1} = 1 \qquad (4.8)$$

The first term in (4.8) refers to the backoff states, the second term refers to the packet transmission states, the third term refers to the packet collision states, and the fourth and the fifth terms refer to the CCA1 and CCA2 states, respectively. We depend on the Equations (4.2)-(4.7) to find the mathematical formula for each of these terms. All of the derived formulas will be expressed in terms of $b_{0,0}$, for which a closed form expression will be derived later. Based on (4.2), (4.3), and (4.7) we can write:

$$\sum_{j=1}^{W-1} b_{0,j} = \sum_{j=1}^{W-1} \frac{W-j}{W} b_{0,0} = \frac{W-1}{2} b_{0,0} \qquad (4.9)$$

Next, based on (4.5) and (4.6) we have:

$$\sum_{j=0}^{L_s-1} b_{-1,j} = L_s(1-\alpha)(1-\beta)(1-P_c)b_{0,0} \qquad (4.10)$$

$$\sum_{j=0}^{L_c-1} b_{-2,j} = L_c(1-\alpha)(1-\beta)P_c b_{0,0} \qquad (4.11)$$

Finally, based on (4.4) we obtain the following formula:

$$b_{0,-1} = (1-\alpha)b_{0,0} \qquad (4.12)$$

The probability of collision, P_c, is formulated in [PAR10] and [POL08] as follows:

$$P_c = 1 - (1 - \tau)^{N-1} \qquad (4.13)$$

Equation (4.13) is formulated based on the observation that a collision will not happen if, out of N nodes, only one node is at CCA1, while the remaining N-1 nodes are at any state other than CCA1. Assuming that the probability that a node initiates CCA1 is τ, the probability of having no collisions in the network will be $(1 - \tau)^{N-1}$. Therefore, P_c will be the complement of the latter term, which gives Equation (4.13). We point out, however, that when a certain node is initiating its CCA1, it is not quite accurate to assume that the remaining N-1 nodes can be at any state other than CCA1. These nodes can only be in the backoff states. They cannot be, for example, in the state (-2, 0). Otherwise, the original node, at the CCA1 state, cannot send out its packet in the first place. Therefore, we accept that Equation (4.13) provides a reasonable approximation of P_c in the network, but we expect that it may cause some deviations from the actual behaviour, as we demonstrate later in Section 4.3.

The abovementioned definition of τ indicates that it is equal to $b_{0,0}$. Therefore, we can now substitute Equations (4.9)-(4.13) into (4.8) and solve for τ. The substitution results in the following formula:

$$\tau = \frac{2}{3 - 2\alpha + 2(1-\alpha)(1-\beta)[L_s + P_c(L_c - L_s)] + W} \qquad (4.14)$$

Both L_s and L_c are defined in the IEEE 802.15.4 standard (see [ZIG06]). W and P_c has already been defined in (4.1) and (4.13), respectively. Therefore, we need to find mathematical expressions for α and β to solve for τ. These expressions strongly depend on whether the communicated traffic is acknowledged or not. Pollin et al. have provided in [POL08] (also, see [ZHU11a]) a detailed study in this direction and we adopt their findings in this chapter. In case of unacknowledged traffic, we have the following expressions:

$$\alpha = L(1-(1-\tau)^{N-1})(1-\alpha)(1-\beta) \qquad (4.15)$$

$$\beta = \frac{1-(1-\tau)^{N-1}}{2-(1-\tau)^{N-1}} \qquad (4.16)$$

where, L in (4.15) refers to the length of the packet to be sent. On the other hand, for acknowledged traffic we have the following expressions:

$$\alpha = P_c(1-\alpha)(1-\beta)\left(L + L_{ack}\frac{N\tau(1-\tau)^{N-1}}{1-(1-\tau)^{N}}\right) \qquad (4.17)$$

$$\beta = \frac{1-(1-\tau)^{N-1}+N\tau(1-\tau)^{N-1}}{2-(1-\tau)^{N}+N\tau(1-\tau)^{N-1}} \qquad (4.18)$$

where, L_{ACK} in (4.17) refers to the length of the ACK packet. We should mention that Equations (4.16) and (4.18) are approximated for large N (see [POL08] and [ZHU11a] for details).

Equation (4.14) along with Equations (4.15)-(4.16) (or Equations (4.17)-(4.18)) for unacknowledged (or acknowledged) traffic form a nonlinear equation system of three variables, namely, τ, α, and β. This system of equations can be solved using numerical methods to find the operating point of the network.

It is worth mentioning that the Markov model depicted in Figure 4-2 is much simpler than the one provided in [PAR10], [POL08], [MIŠ05], and [ZHU11a]. In these studies, the authors show all of the stages of backoff and transmission retries to study the functionality of the IEEE 802.15.4 MAC. However, although our model shows these stages augmented as one stage, yet, as we show later, we are able to capture the main characteristics of the MAC sub-layer and derive all the formulas that describe its functionality. We will see in the next section that showing the backoff and retries stages is just needed for the sake of computing the reliability of the system. We will follow a methodology that helps in deriving a mathematical formula for the reliability without undermining the validity of the model in Figure 4-2.

4.2.1 Channel Utilization under ABA

The Channel Utilization (U) parameter measures how efficiently we are utilizing the wireless medium to successfully transmit packets. In an unacknowledged traffic situation, U refers to the probability that a node manages to send a packet successfully. However, in an acknowledged traffic situation, the node should receive back the ACK packet in order to consider the transmission successful. By examining the model in Figure 4-2, we notice that channel utilization is defined as follows:

$$U = NL\tau(1-\alpha)(1-\beta)(1-P_c)$$

which reduces to:

$$U = NL\tau(1-\alpha)(1-\beta)(1-\tau)^{N-1} \qquad (4.19)$$

where, N is included in the computation in order to find the total U achieved from the successful transmissions of all the nodes in the network.

4.2.2 Power Consumption under ABA

It is essential to study the performance of ABA in terms of power consumption. This is because sensor nodes are battery-powered and any proposed algorithm for WSNs should not deplete the nodes' power resources at a high pace.

Under ABA, a node can be in any of the following states: backoff states, CCA states, packet transmission (with either success or collision) states. The average power consumed at a node, denoted E_{total}, is the total summation of the average power consumed at each of these states:

$$E_{total} = E_{idle} + E_{CCA} + E_{tx} + E_{rx} \qquad (4.20)$$

E_{idle} is the total power consumed during the backoff states:

$$E_{idle} = P_{idle} \sum_{j=1}^{W-1} b_{0,j} = P_{idle} \frac{W-1}{2} b_{0,0} \qquad (4.21)$$

E_{CCA} is the total power consumed during the two CCA states:

$$E_{CCA} = P_{CCA}\left(b_{0,0} + b_{0,-1}\right) = P_{CCA}(2-\alpha)b_{0,0} \qquad (4.22)$$

where, P_{idle} and P_{CCA} refer to the average power consumed during a backoff state and a CCA state, respectively.

We should pay a careful attention to E_{tx}, the total power consumed during packet transmission. The value of E_{tx} depends on the type of traffic assumed, whether it is acknowledged or not. According to IEEE 802.15.4 [ZIG06], if the traffic is acknowledged, the node, after sending a packet (thus, P_{tx} is considered), becomes idle for a period of one time slot (thus, P_{idle} is considered) before it starts sensing the ACK packet. If the ACK packet is sensed, we should consider the average power consumed while receiving it (P_{rx}). If the ACK packet is not sensed after a period of L_{ACK}, or in case of having a collision, the node becomes idle for an extra time slot (thus, P_{idle} is considered) before proceeding to sending the next packet. Therefore, as already noted in [PAR10], to compute the total power consumed while sending acknowledged traffic, we have the following formula:

$$E_{tx} = P_{tx}\left(\sum_{j=0}^{L_s-1} b_{-1,j} + \sum_{j=0}^{L_c-1} b_{-2,j}\right) + P_{idle}\left(b_{-1,L_s} + b_{-2,L_c}\right)$$
$$+P_{rx} \sum_{j=L_s+1}^{L_s+L_{ack}} b_{-1,j} + P_{idle} \sum_{j=L_c+1}^{L_c+L_{ack}+1} b_{-2,j} \qquad (4.23)$$

The first term in Equation (4.23) considers the transmission of the packet, whether it is successful or not. The second term corresponds to the additional time slot in waiting for the ACK packet. The third term evaluates the average power consumed while receiving the ACK packet.

Therefore, the summation starts at $L_s + 1$, which takes into consideration that we wait for L_s time slots and then one extra time slot before receiving the ACK. Finally, the fourth term corresponds to the time slot spent while experiencing a collision or in case of losing the ACK packet. In case of unacknowledged traffic, only the first term of Equation (4.23) is considered.

Finally, E_{rx}, the average power consumed during reception of packets, for both acknowledged and unacknowledged traffics, is expressed as follows:

$$E_{rx} = P_{rx} \sum_{j=0}^{L_s-1} b_{-1,j} \qquad (4.24)$$

4.2.3 Reliability under ABA

Reliability (R) is defined in [PAR10] as the probability of achieving a successful packet reception. In other words, R is useful in measuring how efficient ABA is in improving the possibility of delivering a packet to its destination. Under ABA, a packet is dismissed if we exceed either macMaxCSMABACKoffs or macMaxFrameRetries. That is, a node goes through multiple backoff stages, in case of busy CCAs, and/or multiple transmission retries, in case of repeated collisions, before dismissing a packet. Therefore, formulating R depends on finding the probability of avoiding the dismissal of a packet. As the likelihood of dismissing a packet diminishes, it means that the system is more reliable. Therefore, the reliability is defined as follows:

$$R = \frac{\pi_s}{\pi_s + \pi_f} \qquad (4.25)$$

Where, π_s is the probability of having successful transmissions and π_f is the probability of having failed transmissions. Note that failed transmissions include both collided packets and discarded packets. While π_s is known from Equation (4.5), special attention is needed to

formulate π_f. We develop the finite-state machines (FSMs) shown in Figure 4-3 and use them to accomplish that. The FSM in Figure 4-3(a) shows that a node, as it goes from state $(0, 0)$ and ends back at it, may encounter a successful transmission (S), a packet collision (C), or a busy channel (B). Figure 4-3(a), however, does not show the multiple backoff stages and packet transmission retries a node may experience while attempting to send a packet. In other words, the B and C states are in fact constituted by multiple stages. These stages are shown in Figures 4-3(b) and 4-3(c). Note that these two FSMs can be merged to show the complete system, but we avoid that to simplify our derivations. Based on Equations (4.3)-(4.6), we can directly see that $x = \alpha + (1 - \alpha)\beta$, $y = (1 - \alpha)(1 - \beta)P_c$, and $z = (1 - \alpha)(1 - \beta)(1 - P_c)$. These equations can be also inferred by noticing the transitions in Figure 4-3(a). The FSM in this figure is interpreted as follows. As a node finds the channel busy, it has a probability of x to find the channel busy again. On the other hand, it may succeed to send its packet or face a packet collision with probabilities z and y, respectively. After succeeding in sending a packet, a node may be successful in sending the next packet with a probability of z. Otherwise, the node may find the channel busy with probability x or suffer from a collision with probability y. Finally, as the node experiences a collision, it may encounter another collision with probability y, succeed in sending the packet with probability z, or find the channel busy with probability x.

In Figures 4-3(b) and 4-3(c) we capture the fact that, during a single cycle, a node may go through macMaxCSMABACKoffs (denoted as m in Figure 4-3(b)) backoff stages and macMaxFrameRetries (denoted as n in Figure 4-3(c)) collisions before discarding a packet (note that π_{C_i} denotes the probabilities to suffer from a collision after finding the channel busy for i times). Therefore, in order to find R, we need to find the probability that the system backs off

for $m+1$ times or experiences collisions for $n+1$ times. If we assume A to be a random variable that denotes the number of backoff stages the node has gone through, and B to be a random

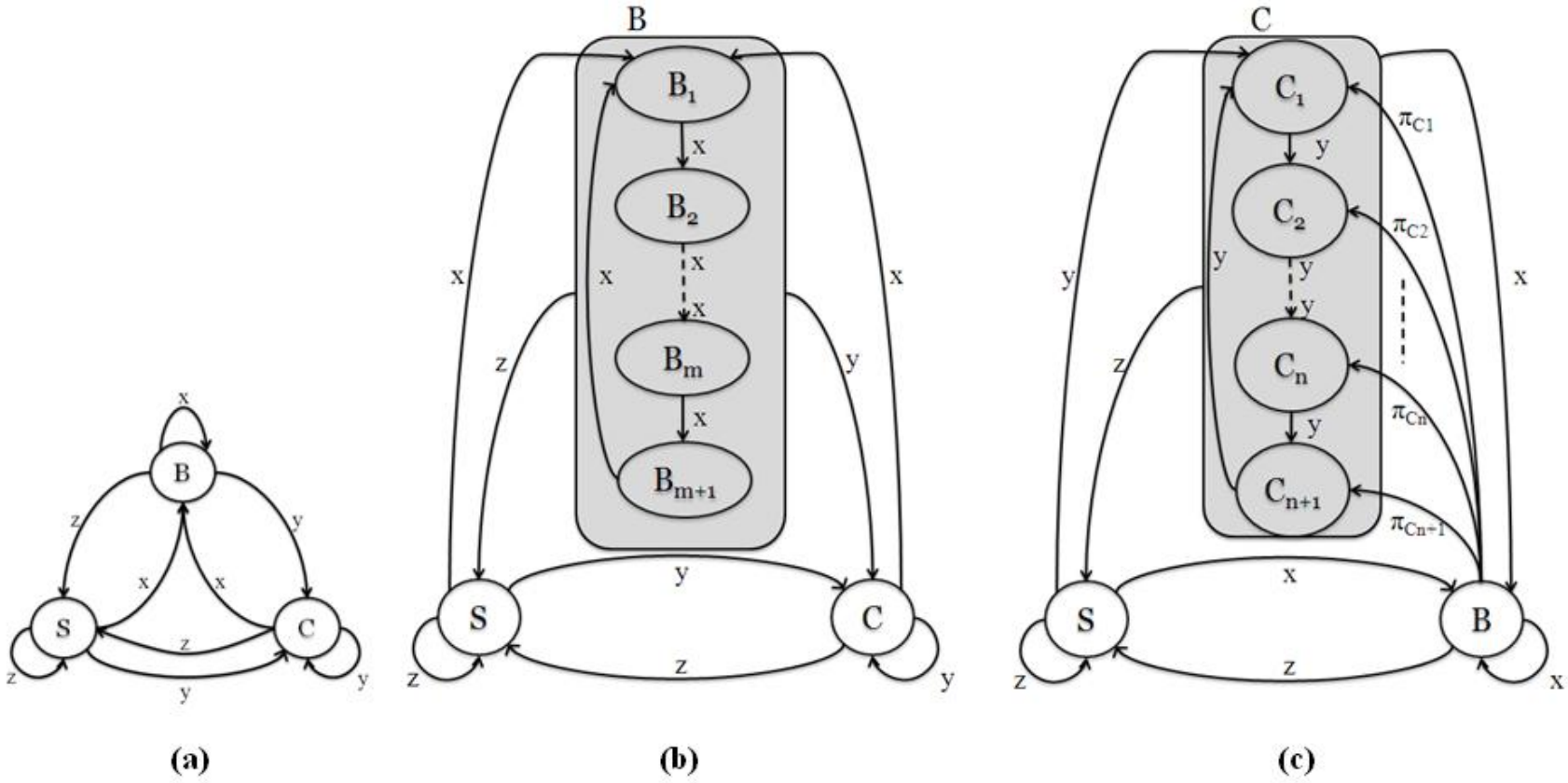

Figure 4-3: (a) States encountered during one complete cycle, (b) Break down of the B state into multiple backoff stages, and (c) Break down of the C state into multiple packet transmission retries.

variable that denotes the number of collisions occurred, then Equation (4.25) can be rewritten as follows:

$$R = \frac{\pi_s}{\pi_s + P(A = m+1) + P(B = n+1)} \qquad (4.26)$$

$P(A = m + 1)$ and $P(B = n + 1)$ can be found using the FSMs in Figures 4-3(b) and 4-3(c), respectively. Towards that end, if we have the transition matrices P_1 (for Figure 4-3(b)) and P_2 (for Figure 4-3(c)), then there exist the stationary distributions π_1 and π_2, such that $P_1 \times \pi_1 = \pi_1$ and $P_2 \times \pi_2 = \pi_2$. The latter relationships are expanded, respectively, as follows:

$$\begin{array}{c} \\ S \\ B_1 \\ B_2 \\ \vdots \\ B_m \\ B_{m+1} \\ C \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} S & B_1 & B_2 & \cdots & B_m & B_{m+1} & C \end{array} \\ \begin{bmatrix} z & z & z & \cdots & z & z & z \\ x & 0 & 0 & \cdots & 0 & x & x \\ 0 & x & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & x & 0 & 0 \\ y & y & y & \cdots & y & y & y \end{bmatrix} \end{array} \times \begin{bmatrix} \pi_s \\ \pi_{B1} \\ \pi_{B2} \\ \vdots \\ \pi_{Bm} \\ \pi_{Bm+1} \\ \pi_C \end{bmatrix} = \begin{bmatrix} \pi_s \\ \pi_{B1} \\ \pi_{B2} \\ \vdots \\ \pi_{Bm} \\ \pi_{Bm+1} \\ \pi_C \end{bmatrix} \qquad (4.27)$$

$$\begin{array}{c} \\ S \\ C_1 \\ C_2 \\ \vdots \\ C_m \\ C_{m+1} \\ B \end{array}\!\!\begin{array}{c} \begin{array}{ccccccc} S & C_1 & C_2 & \cdots & C_m & C_{m+1} & B \end{array} \\ \begin{bmatrix} z & z & z & \cdots & z & z & z \\ y & 0 & 0 & \cdots & 0 & y & \pi_{C1} \\ 0 & y & 0 & \cdots & 0 & 0 & \pi_{C2} \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & 0 & \pi_{Cn} \\ 0 & 0 & 0 & \cdots & y & 0 & \pi_{Cn+1} \\ x & X & x & \cdots & x & x & x \end{bmatrix} \end{array} \times \begin{bmatrix} \pi_s \\ \pi_{C1} \\ \pi_{C2} \\ \vdots \\ \pi_{Cm} \\ \pi_{Cm+1} \\ \pi_B \end{bmatrix} = \begin{bmatrix} \pi_s \\ \pi_{C1} \\ \pi_{C2} \\ \vdots \\ \pi_{Cm} \\ \pi_{Cm+1} \\ \pi_B \end{bmatrix} \qquad (4.28)$$

In (4.27) the stationary distribution π_1 is defined as $[\pi_S \quad \pi_{B_1} \quad \pi_{B_2} \quad \cdots \quad \pi_{B_{m-1}} \quad \pi_{B_m} \quad \pi_C]$, where, π_{B_k} is the probability of being in the *k*th backoff stage. On the other hand, π_2 is defined as $[\pi_S \quad \pi_{C_1} \quad \pi_{C_2} \quad \cdots \quad \pi_{C_{n-1}} \quad \pi_{C_n} \quad \pi_B]$ for (4.28), where π_{C_r} is the probability of experiencing the *r*th collision.

Based on (4.27) and (4.28), we can write the following formulas (see Appendix C for the detailed derivations):

$$P(A = m+1) = \pi_{B_{m+1}} = \frac{x^{m+1}(1-x)}{1-x^{m+1}} \qquad (4.29)$$

$$P(B = n+1) = \pi_{C_{n+1}} = \frac{(1-x-y)y^{n+1}}{(1-x)^{n+1}-y^{n+1}} \qquad (4.30)$$

Finally, with the knowledge of Equations (4.26), (4.29), and (4.30), we can now formulate the reliability as follows:

$$R = \frac{1}{1+\frac{(1-x)x^{m+1}}{(1-x^{m+1})(1-x-y)}+\frac{y^{n+1}}{(1-x)^{n+1}-y^{n+1}}} \qquad (4.31)$$

4.2.4 Channel Collisions Time under ABA

An efficient backoff algorithm should prove effectiveness in reducing the rate of collisions in the wireless medium. This is essential because not only it improves the utilization of the communication channel, but also reduces the consumption of power due to useless activities.

We aim in this subsection at investigating the percentage of time the channel is getting busy due to collisions. This is different from what Equation (4.13) reflects. Equation (4.13) describes the probability of collision from each node's perspective. In other words, this equation describes the average probability of collision that any node will face when communicating over the medium. However, that equation does not consider the channel's perspective. The latter recognizes the fact that a collision involves at least two nodes, and therefore, even if three or more nodes send their packets at the same instant, the channel will experience a busy period of only L_c time units. Stated differently, by examining Figure 4-2, we notice that the proportion of time a node spends in the collision state is $L_c(1-\alpha)(1-\beta)P_c\tau$ (recall Equation (4.11)). Then, if N_c nodes (out of N) have collided at the same instant, the channel collision time, T_{CC}, is the non-

overlapping period of time during which the channel is busy with a collision event. The latter is defined as follows:

$$T_{cc} = \frac{L_c N\tau(1-\alpha)(1-\beta)P_c}{N_c} \qquad (4.32)$$

where, N_c is the expected number of collided nodes. To determine the value of N_c, we should calculate the expected number of collided nodes, given that a collision has happened. This is a conditional probability that we compute as follows. The probability of having k nodes involved in a collision requires that while a node is at CCA1, $k-1$ nodes should also be at CCA1 while the remaining $N-k$ nodes should be in any state other than CCA1. This probability is expressed as $\tau^{k-1}(1-\tau)^{N-k}$. The problem of selecting $k-1$ nodes out of $N-1$ nodes under the conditions just mentioned is a typical binomial distribution. Given all of these facts, and by noticing that we may have from 2 to N nodes that are colliding at the same time, we can formulate N_c as follows:

$$N_c = \frac{1}{P_c}\sum_{k=2}^{N}\binom{k-1}{N-1}k\tau^{k-1}(1-\tau)^{N-k} \qquad (4.33)$$

Note that we divide by Pc because we have a condition that a collision has already happened.

From Equations (4.32) and (4.33) we can see that if k nodes have collided at the same time, the channel will be busy for only L_c time units and not kL_c. An effective backoff algorithm should be able to reduce T_{CC} as much as possible.

4.3 Simulations and Model Validation

In this section we conduct extensive simulations in order to validate the mathematical model developed in Section 4.2. Our simulations also provide a comparative study between ABA, on one side, and BEB, NO-BEB [LEE09], and KEB [WOO08] on the other side. In this comparison, we evaluate the performance of ABA in terms of channel utilization, average power

consumption, reliability, and channel collision time. Furthermore, the fairness of ABA is studied to ensure that the nodes in the network are sharing the communication medium equally.

We wrote a C-based simulator to simulate ABA and the other three algorithms mentioned above. The network under study is of a peer-to-peer topology. The network operates in the beacon-enabled IEEE 802.15.4 mode. We omit both the CFP and the inactive periods from the superframe and assume that it is constituted only by the active period.

We use the average power consumption of different wireless network interface cards (NICs) [ZOL10], [LUC99], and [RFM11]. The parameters considered in our simulations are summarized in Table 4-1[1]. Also, we always assume, except when stated differently, that $L_s = L_c = L$. In all of our simulation results a confidence interval (CI) of 95% is assumed. This CI is not shown in our graphs because it is too small to be observed (refer to Appendix B for more details). In the following subsections we present our simulations results along with discussions and comments.

[1] CCA power in this table refers to the power consumed during either of the clear channel assessment periods.

Table 4-1: ABA Simulation Parameters

Average Power Consumed (mW.s)	Rx	30
	Tx	40
	CCA	30
	Sleep	0.8
Durations	1 timeslot	0.32 ms (80 bits)
	Packet Length (L)	14 or 28 timeslots
	ACK Packet Length (L_{ACK})	2 timeslots
	Simulation Time	320 s
IEEE 802.15.4 Parameter Settings	*macMinBE*	3
	macMaxBE	8

4.3.1 Model Validation

In this subsection we validate our theoretical Markov model by comparing the behavior it predicts to the behavior extracted from simulations. Similar to Chapter 3, we compute the coefficient of variation of the root-mean-square deviation RSMD $\left(CV(RMSD)\right)$ of our performance metrics to measure the accuracy of our mathematical model. $CV(RMSD)$ measures the differences between the mathematical model and the simulations and is defined as follows:

$$CV(RSMD) = \frac{\sqrt{\frac{\sum_{i=1}^{n}(V_{theo} - V_{sim})^2}{n_{sample}}}}{\bar{V}}$$

where, V_{theo} is the predicted theoretical value, V_{sim} is the simulated value, $\bar{V}$ is the average of the sample values, and n_{sample} is the total number of the sample values used. An accurate theoretical model should achieve low values for $CV(RMSD)$.

4.3.1.1 Channel Utilization

We validate the mathematical expression that we derived for U in Equation (4.19). Figures 4-4 and 4-5 compare the theoretical behavior with the simulated behavior under unacknowledged traffic conditions. Figures 4-6 and 4-7 show the comparison under acknowledged traffic conditions. We can clearly see that Equation (4.19) is very accurate in predicting the behavior U of as the network size increases. We do see, however, a discrepancy for small networks ($N \leq 20$). In fact, we explain this discrepancy by recalling that Equations (4.16) and (4.18) are approximated for large N (see Section 4.2), and therefore, as the network gets smaller the model we provided may become less accurate.

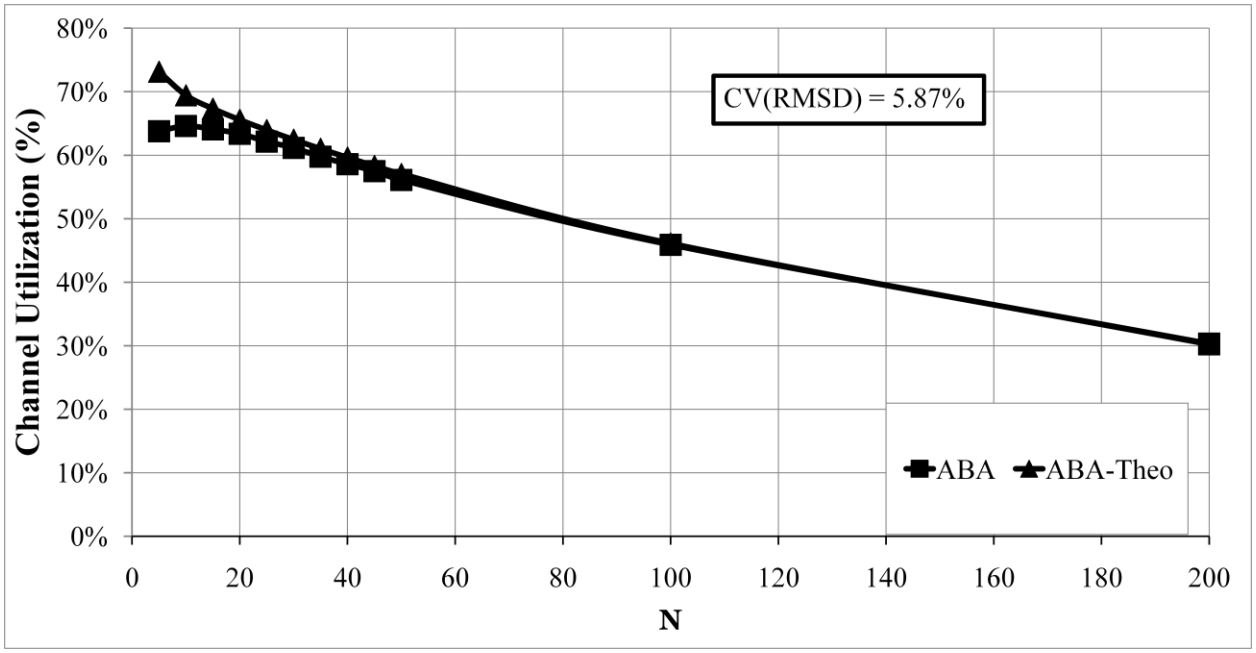

Figure 4-4: Channel utilization of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

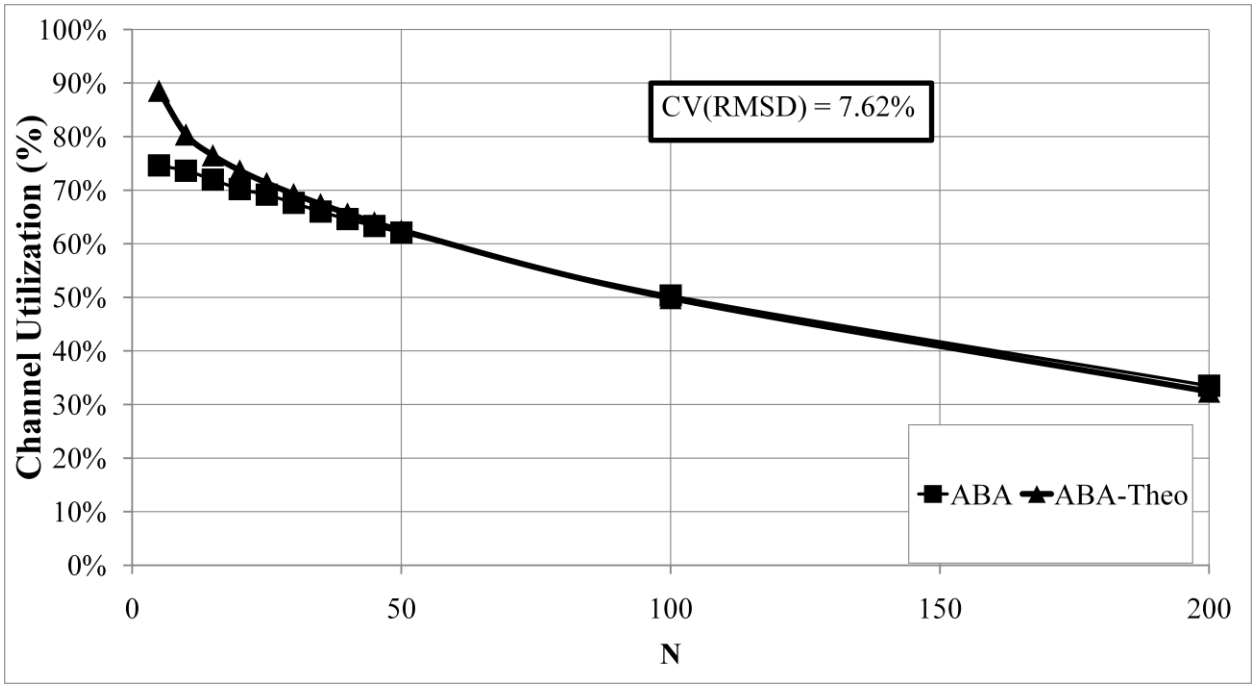

Figure 4-5: Channel utilization of ABA under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

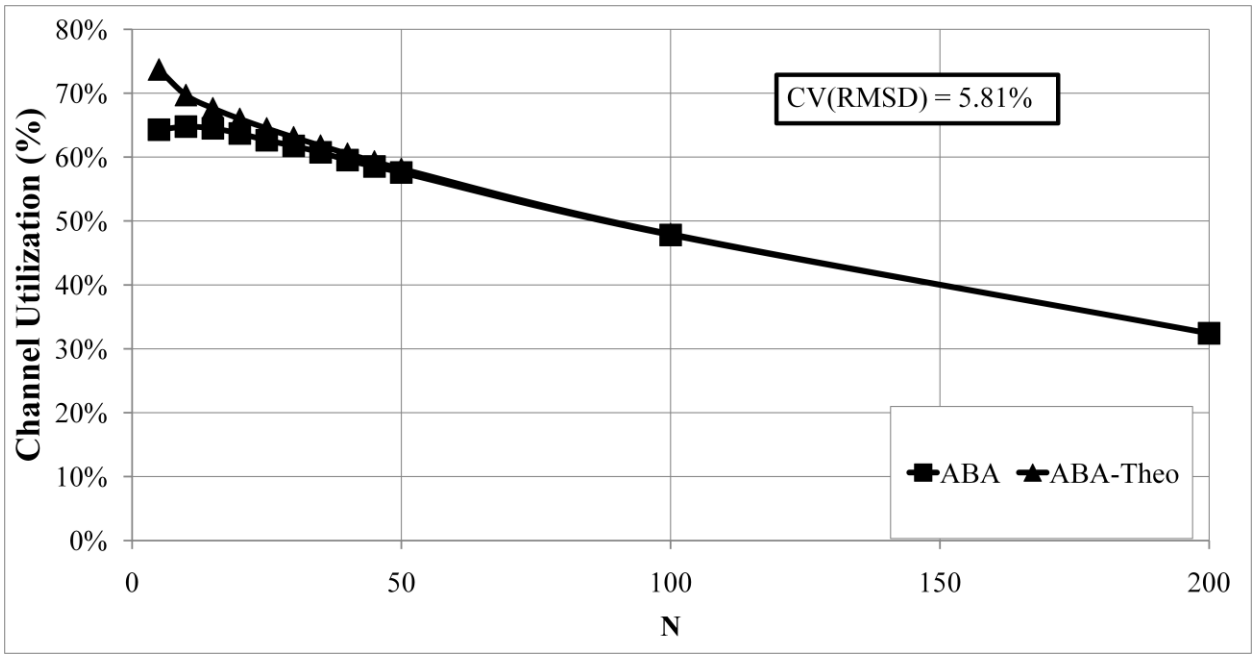

Figure 4-6: Channel utilization of ABA under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

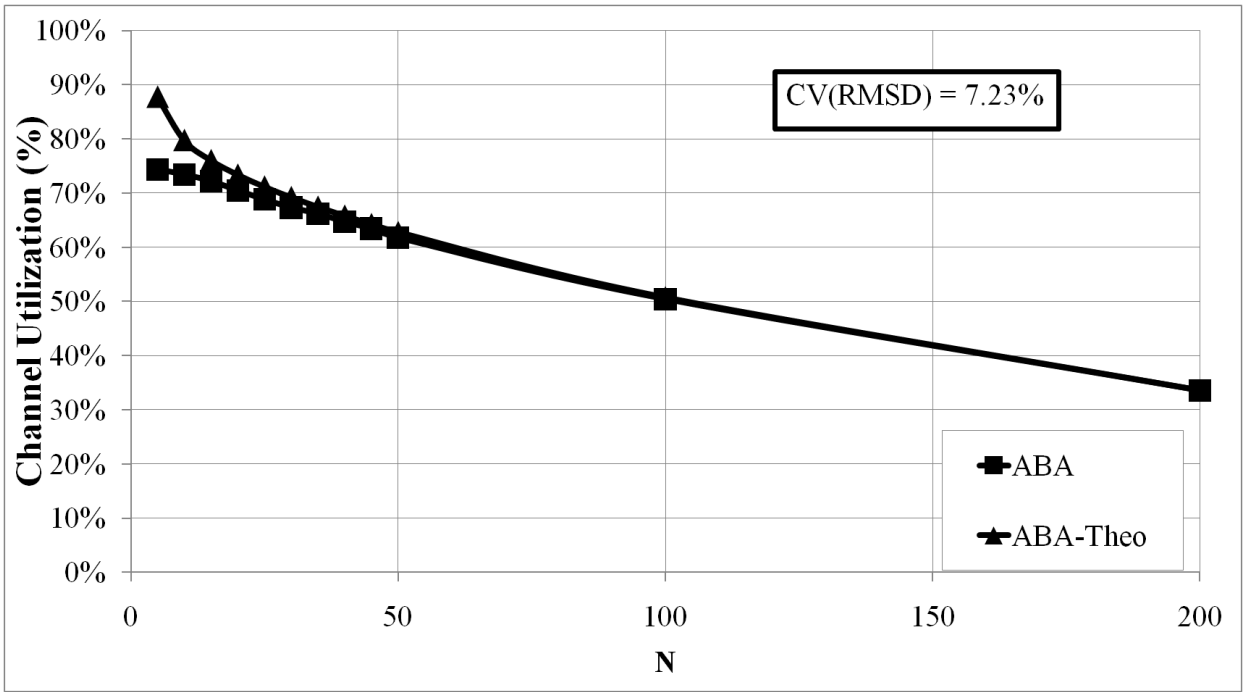

Figure 4-7: Channel utilization of ABA under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.1.2 Average Power Consumption

Figures 4-8 and 4-9, for unacknowledged traffic, and Figures 4-10 and 4-11, for acknowledged traffic, show a perfect match between our mathematical expressions and the simulations for the total power consumption under ABA.

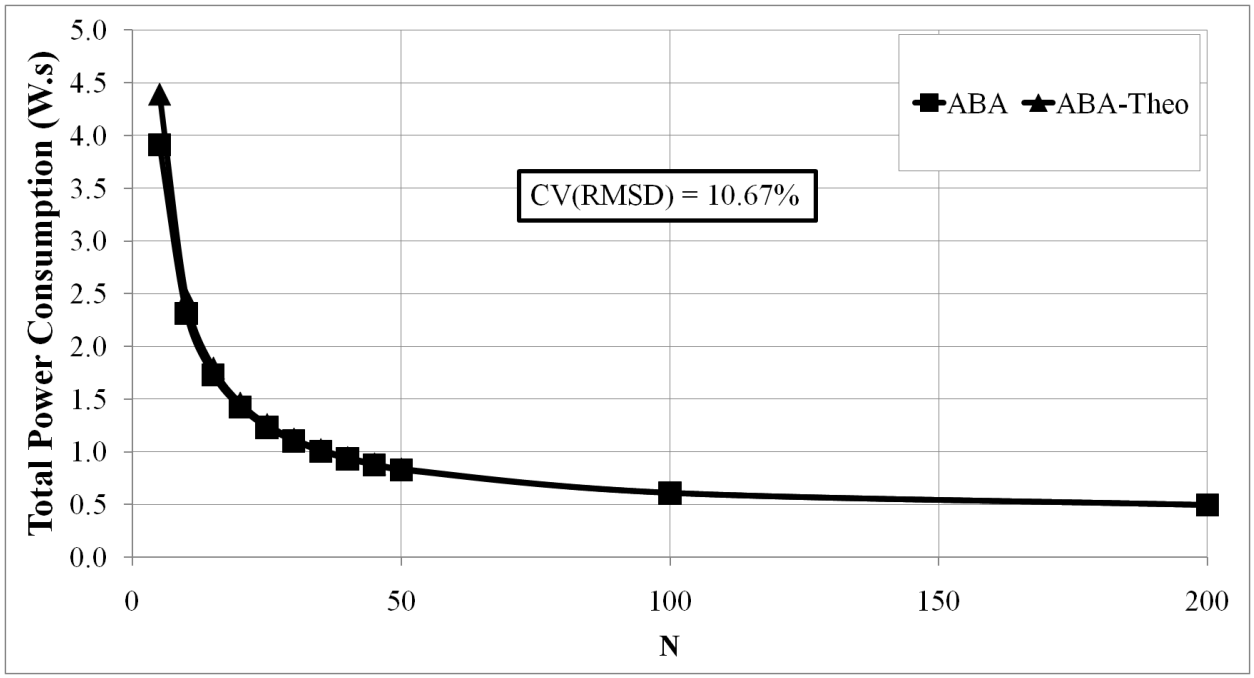

Figure 4-8: Total power consumption (W.s) of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

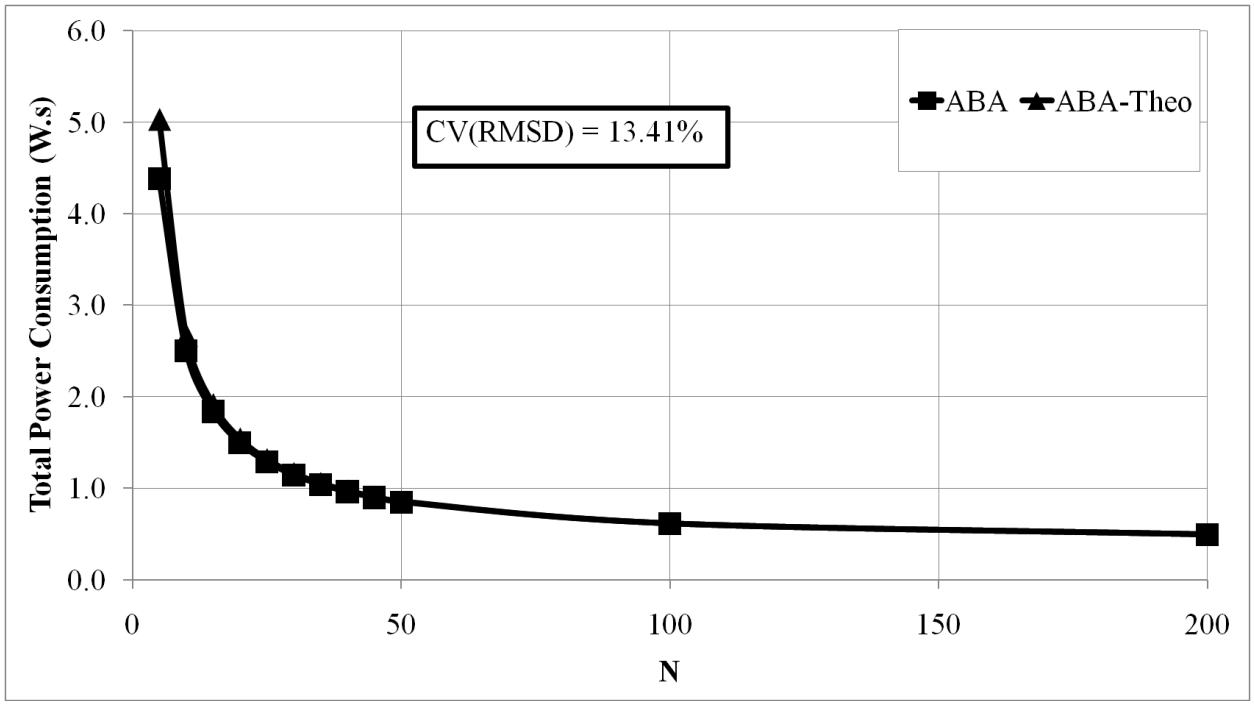

Figure 4-9: Total power consumption (W.s) of ABA under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

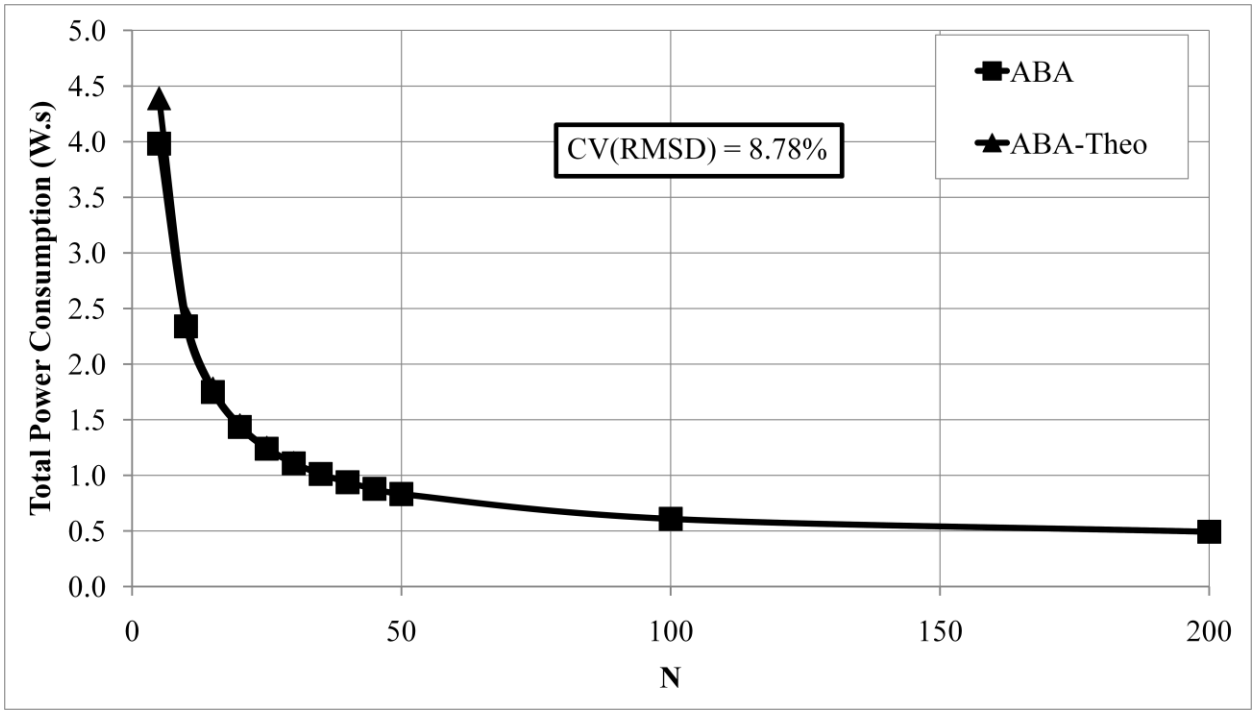

Figure 4-10: Total power consumption (W.s) of ABA under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

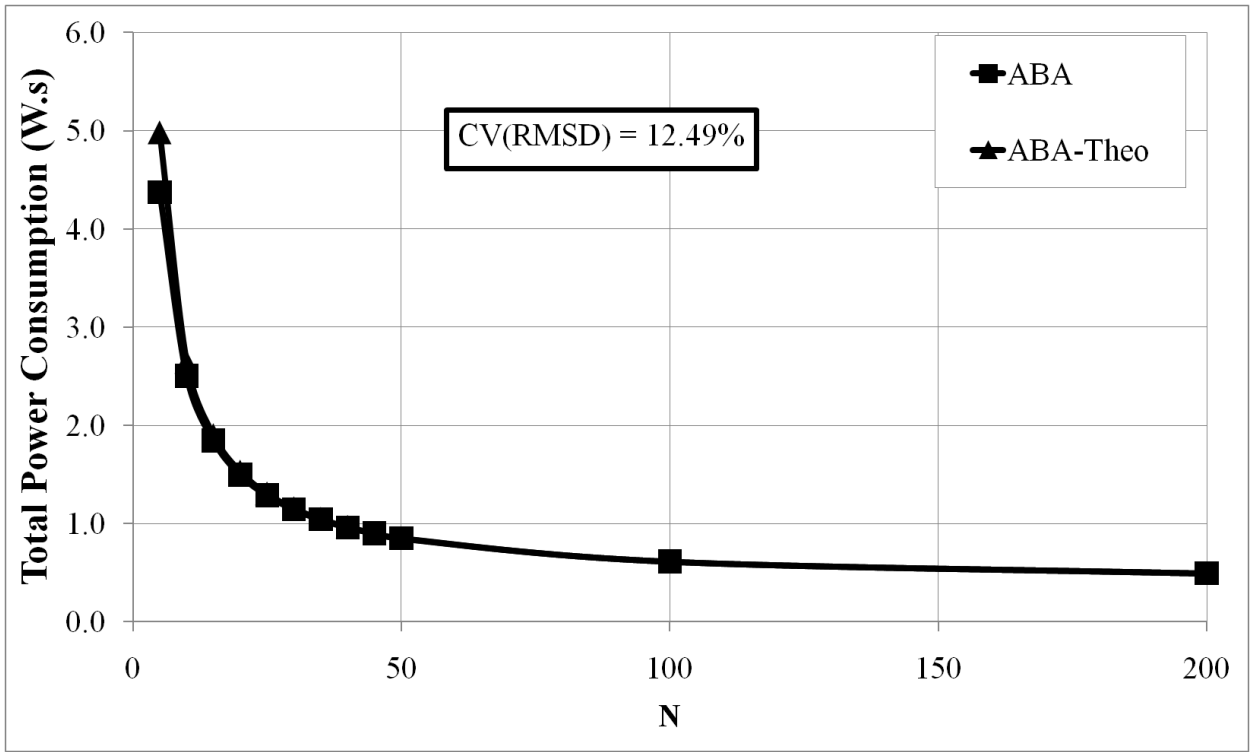

Figure 4-11: Total power consumption (W.s) of ABA under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.1.3 Average Power Wasted in Collisions

Figures 4-12 and 4-13, for unacknowledged traffic, and Figures 4-14 and 4-15, for acknowledged traffic, depict the theoretical and simulated performance in terms of the average power wasted due to packet collisions. These figures illustrate an accurate matching between our Markov model and the simulations.

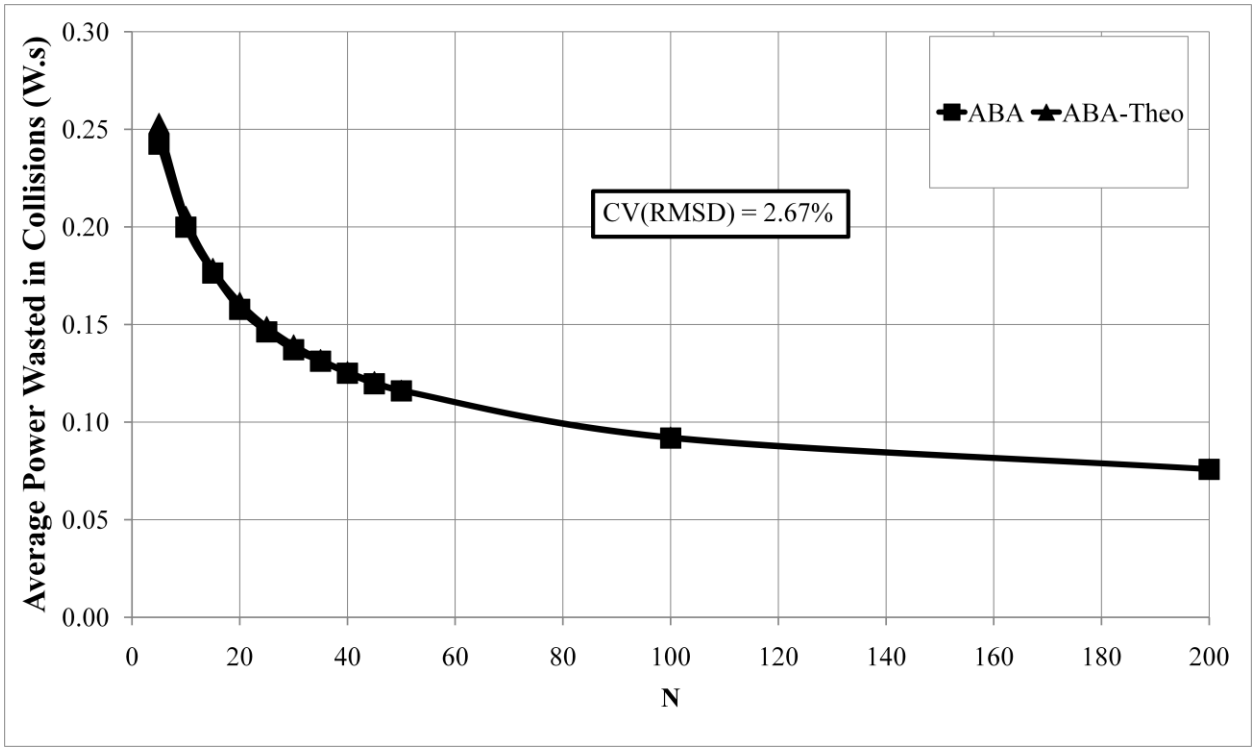

Figure 4-12: Average power wasted in collisions (W.s) under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

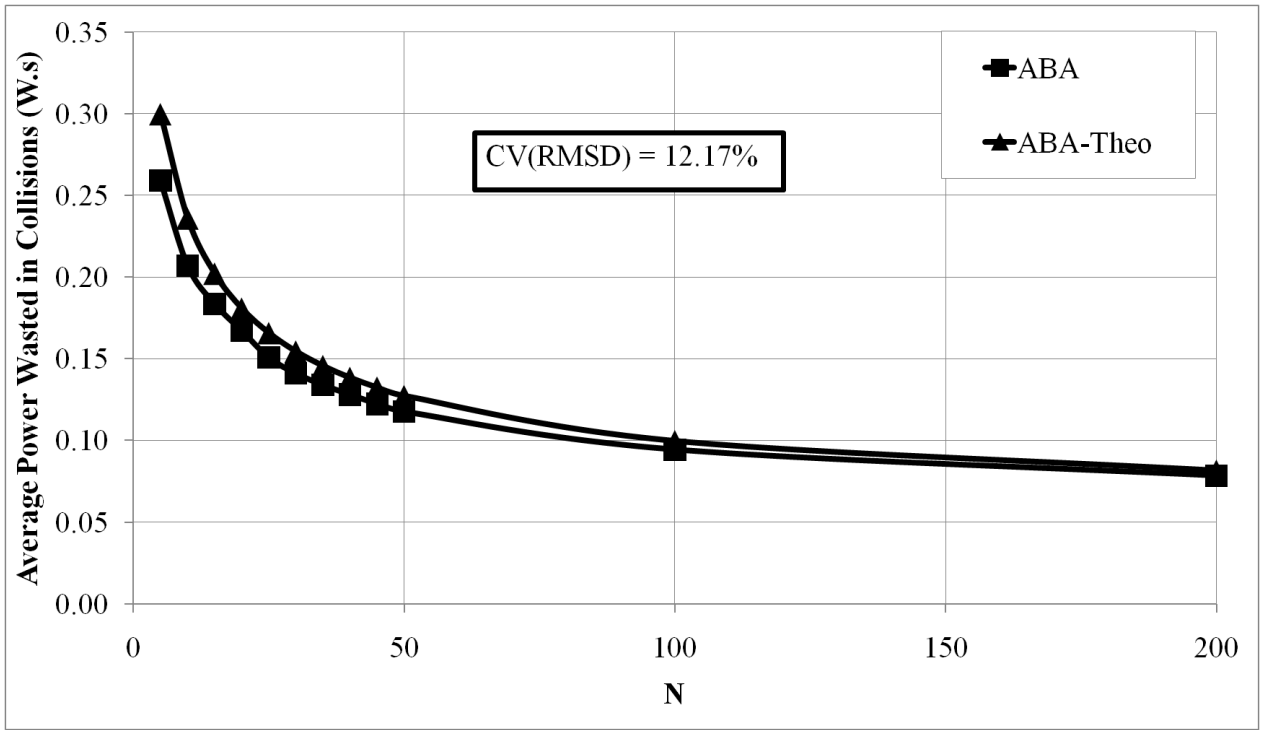

Figure 4-13: Average power wasted in collisions (W.s) under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

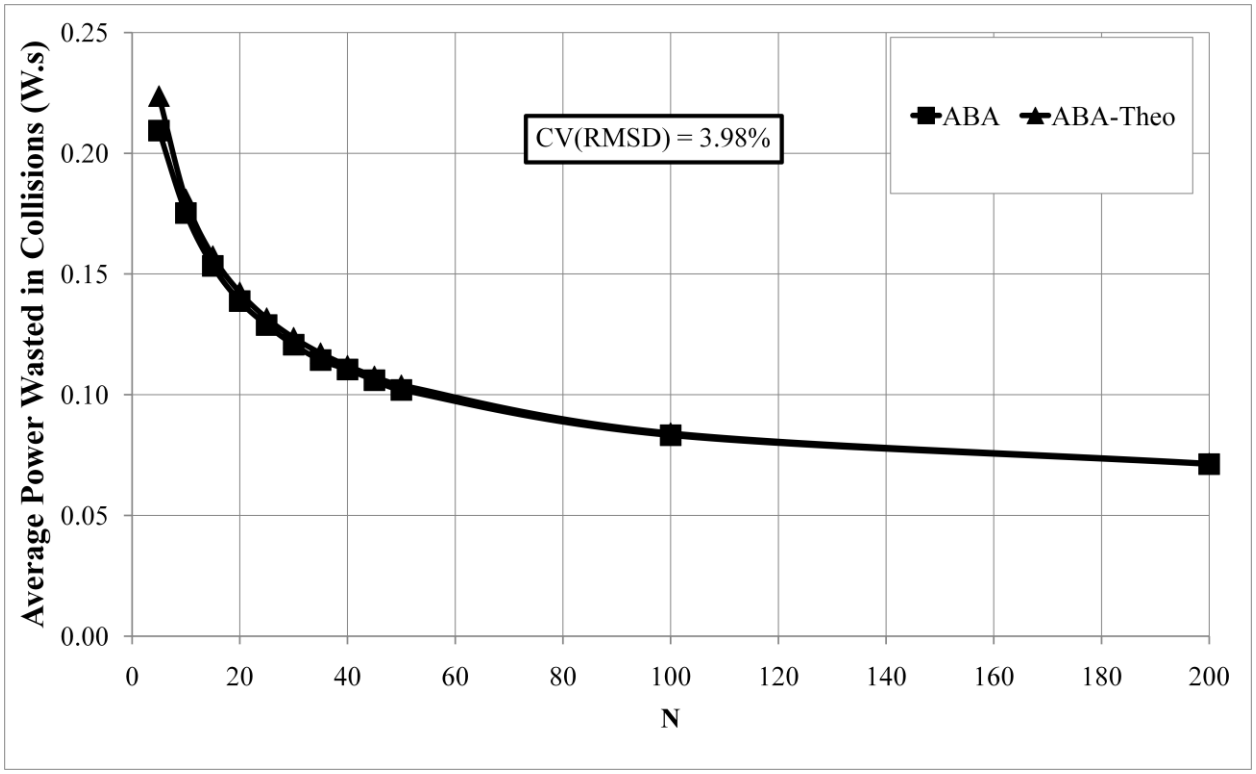

Figure 4-14: Average power wasted in collisions (W.s) under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

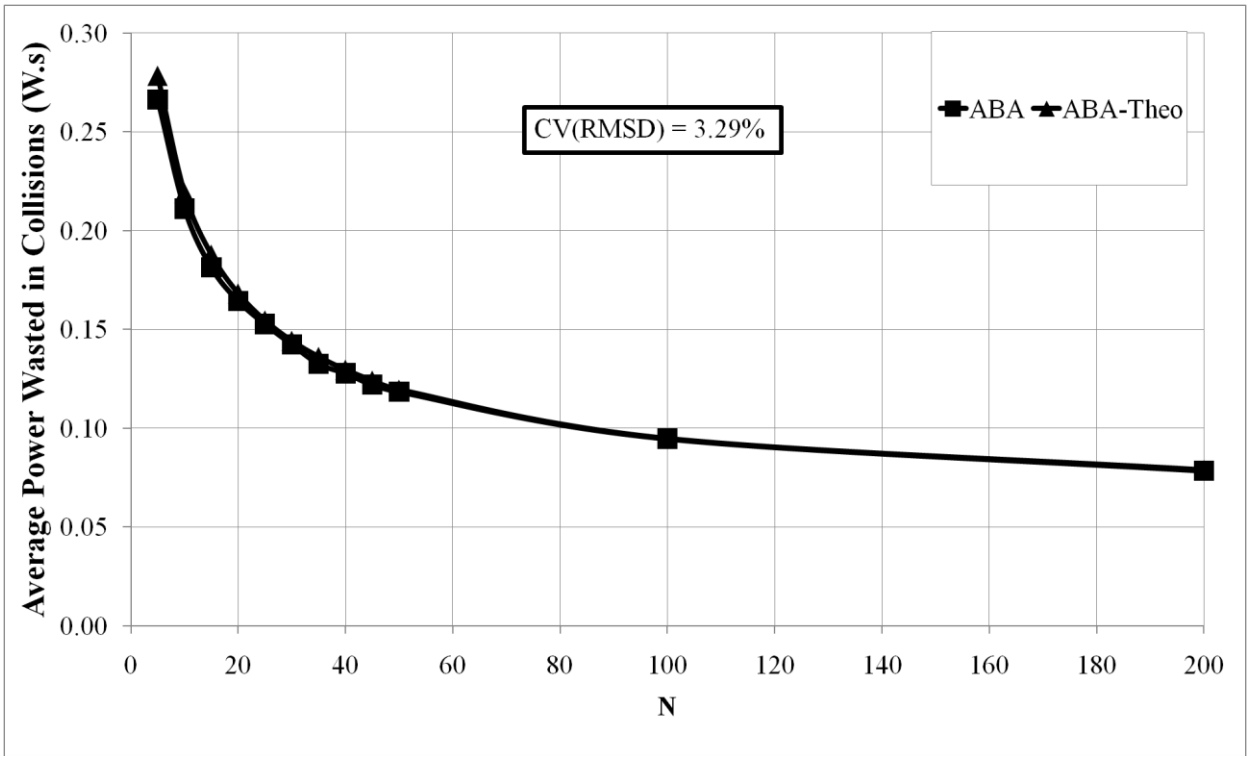

Figure 4-15: Average power wasted in collisions (W.s) under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.1.4 Reliability

Figures 4-16 and 4-17, for unacknowledged traffic, show a perfect match between our mathematical expression and the simulations for the reliability of ABA. The same observation is seen in Figures 4-18 and 4-19 for the acknowledged traffic.

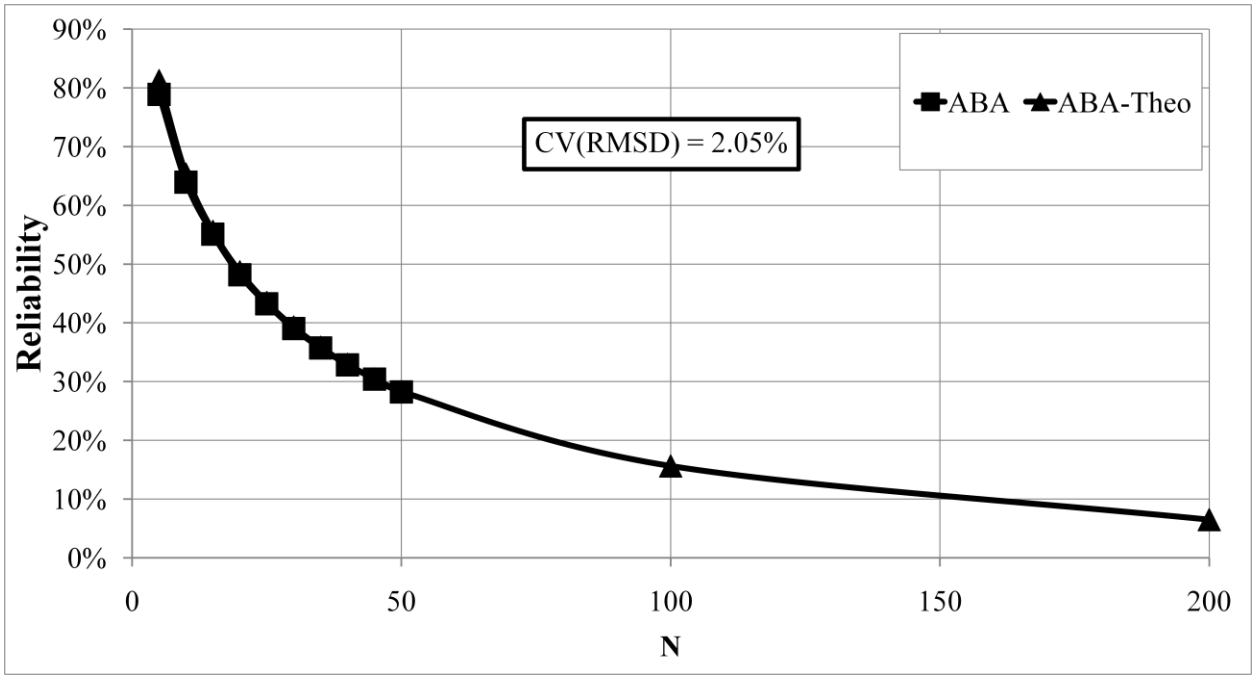

Figure 4-16: Reliability of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

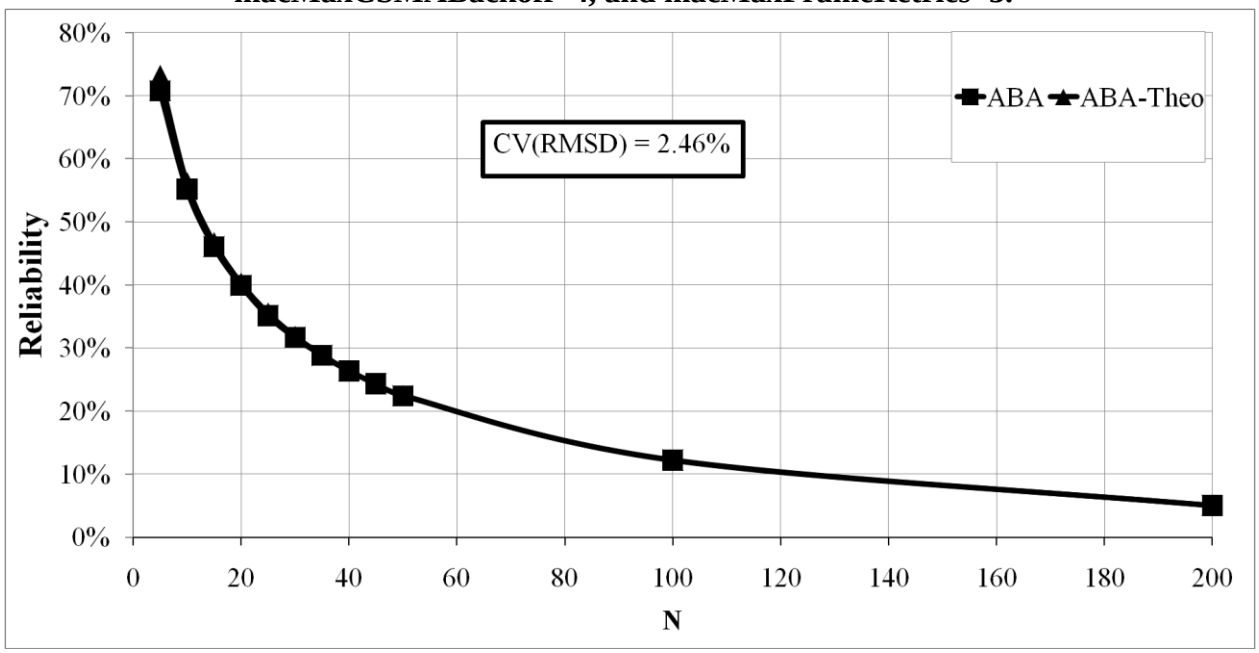

Figure 4-17: Reliability of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=3, and macMaxFrameRetries=2.

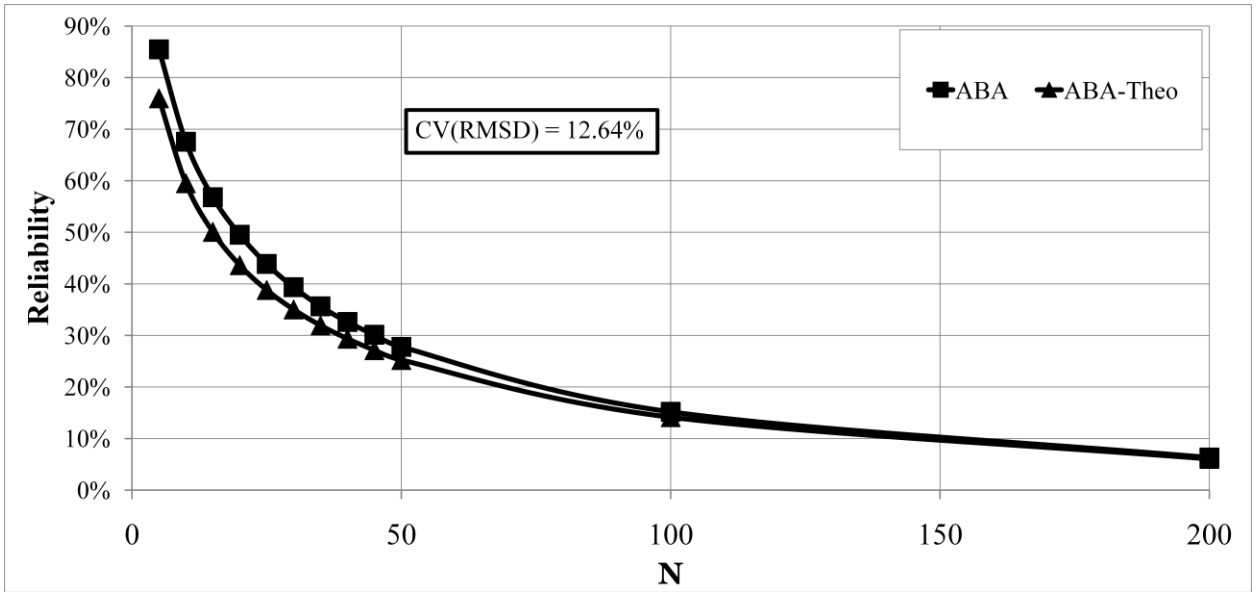

Figure 4-18: Reliability of ABA under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

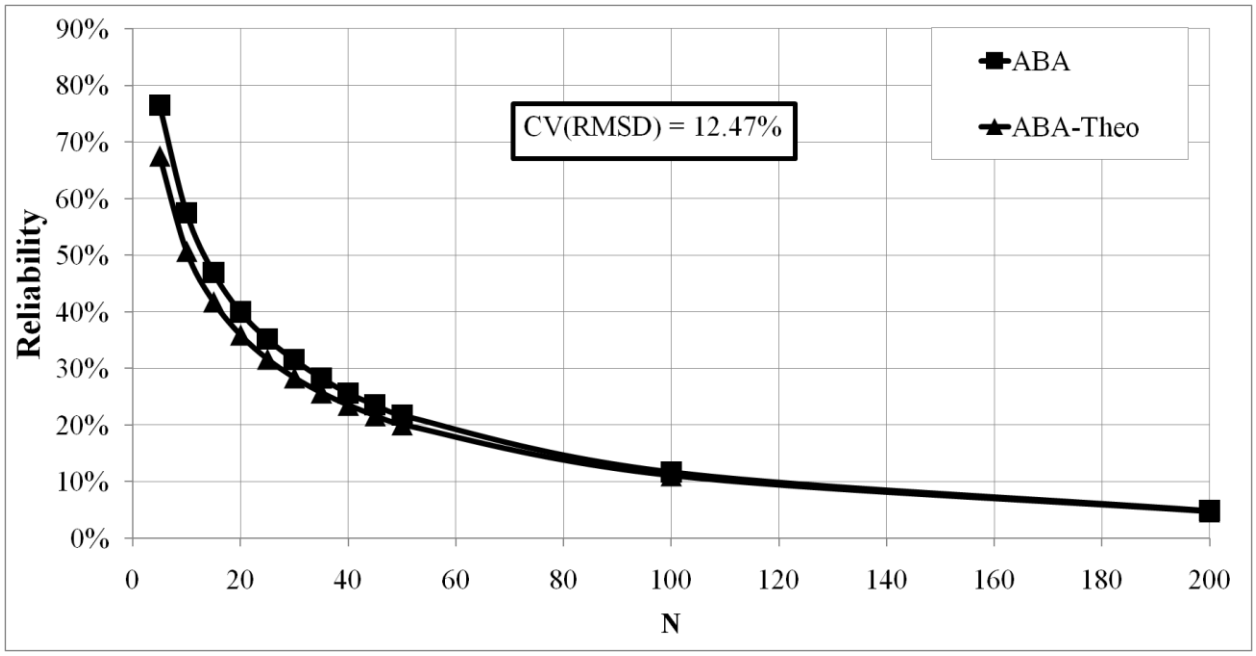

Figure 4-19: Reliability of ABA under acknowledged traffic. L=14, macMaxCSMABackoff=3, and macMaxFrameRetries=2.

4.3.1.5 Channel Collision Time

ABA's theoretical and simulated behavior in terms of the achieved channel collision time, under different traffic conditions, is depicted in Figures 4-20, 4-21, 4-22, and 4-23. Although we

observe a deviation between the theoretical curves and the simulation ones in all of these figures, the deviation is minor and does not undermine the accuracy of our model. We argue, however, that this deviation is occurring as a result of the term N_c in Equation (4.32). N_c is computed using Equation (4.33), which includes the term $(1-\tau)^{N-k}$. We discussed in Section 4.2 that this term, originally used in Equation (4.13), is formed based on the assumption that a node that is not at the CCA1 state can be at any other state in the Markov chain of Figure 4-2. This assumption provides a reasonable approximation of the probability of collision in the network, and the deviations we see in Figures 4-20, 4-21, 4-22, and 4-23 are resulting from it.

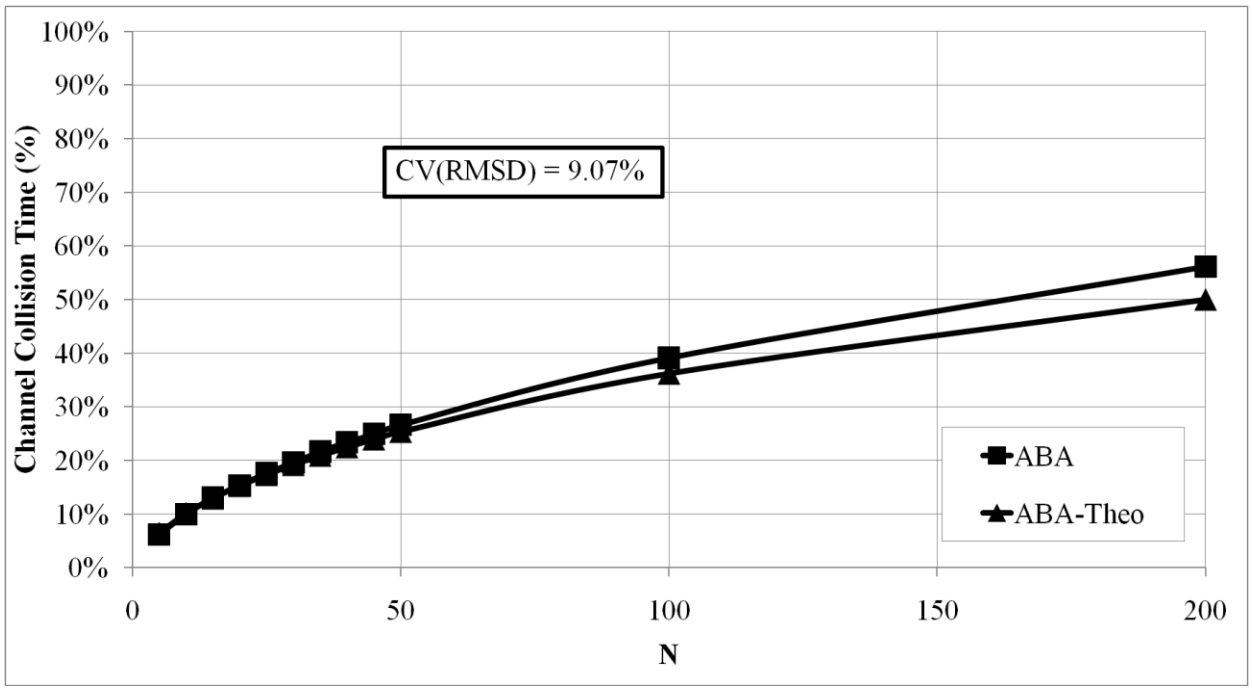

Figure 4-20: Channel collision time with ABA, under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

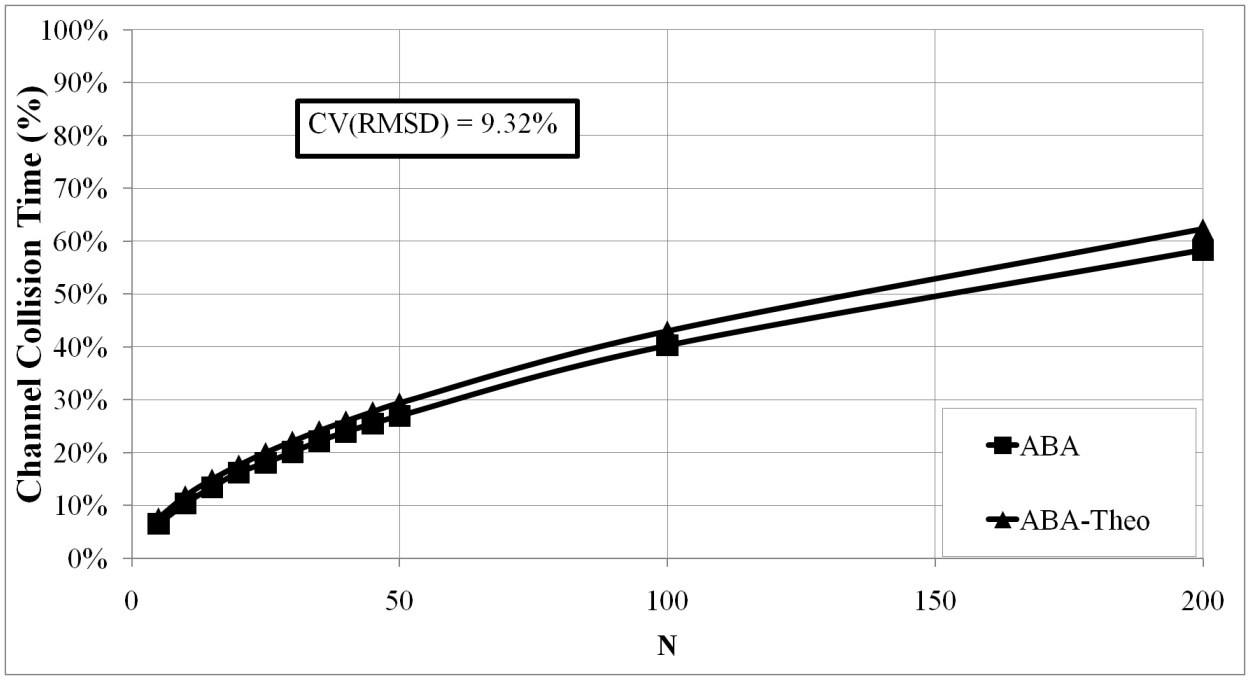

Figure 4-21: Channel collision time with ABA, under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

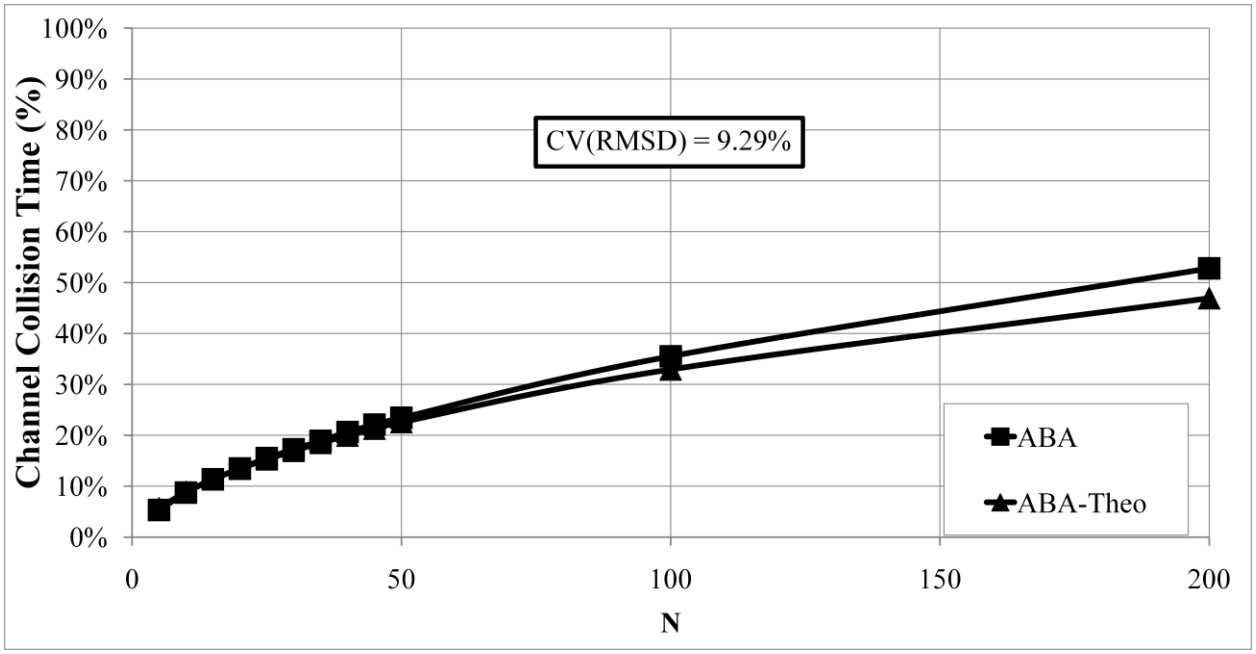

Figure 4-22: Channel collision time with ABA, under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

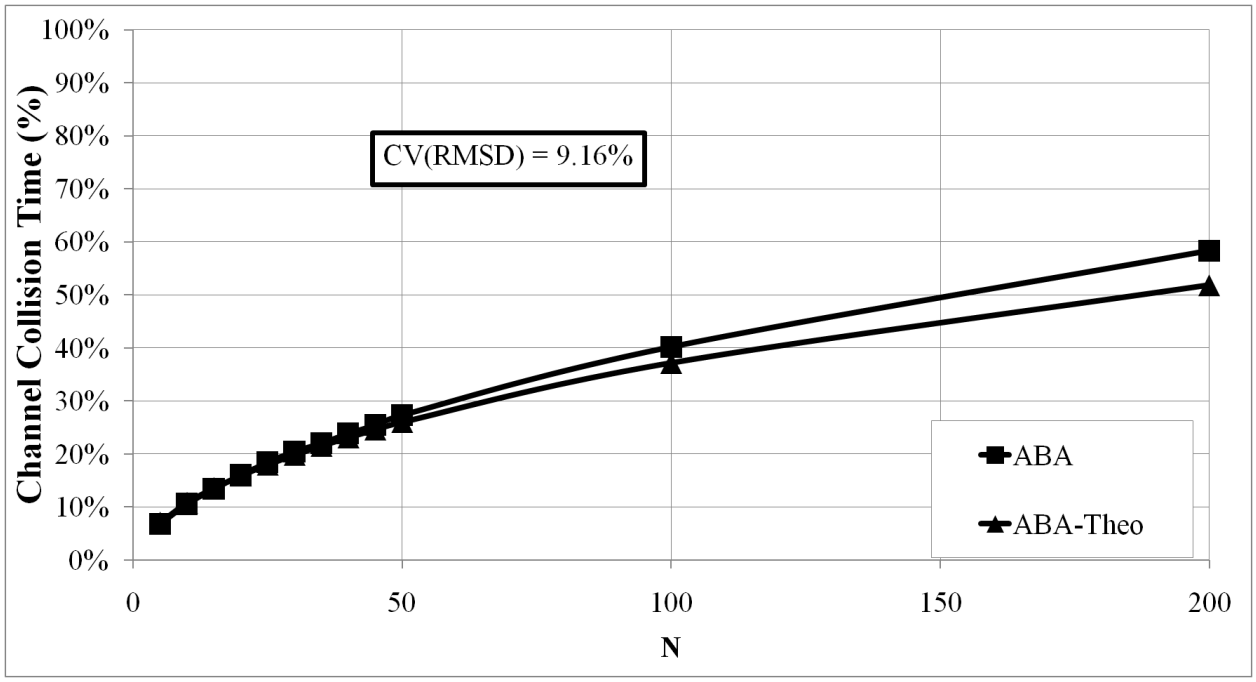

Figure 4-23: Channel collision time with ABA, under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

In general, by examining Figures 4-4 to 4-23, and by noticing the values of that we achieved, we can conclude that our Markov-based theoretical model of ABA is accurate and successful in predicting the simulated performance.

4.3.2 Comparing ABA with other Algorithms

In this subsection we study the performance of ABA compared to that of BEB, NO-BEB, and KEB.

4.3.2.1 Channel Utilization

We show in Figures 4-24 and 4-25 ABA's performance in terms of channel utilization, under unacknowledged traffic conditions, compared to BEB, NO-BEB, and KEB. The comparison under acknowledged traffic conditions is shown in Figures 4-26 and 4-27. In all of these figures we can see that ABA achieves a superior performance compared to BEB and NO-BEB. The enhancements over the latter algorithms become significant as the network size

increases (especially beyond a size of 20 nodes). For example, in Figure 4-24, at 35 nodes, ABA achieves a U of 59.84%, while BEB and NO-BEB achieve 19.63% and 34.63%, respectively. For the KEB algorithm, we can see in Figures 4-24 to 4-27 that KEB's performance is inferior to ABA's for lower sizes of the network. However, KEB tends to match ABA's performance at high network sizes (35 nodes in Figure 4-24, 40 nodes in Figure 4-25, and 45 nodes for both Figures 4-26 and 4-27). KEB's main shortcoming is that it updates the size of the contention window based on a pre-specified threshold, which is difficult to quantify. In Figure 4-24, for example, we can see that, under KEB, U keeps decreasing with the increase of the network size till we reach 30 nodes. At that point, we can see how U switches its behaviour and starts increasing. This means that we could not cross the pre-specified threshold till we reached the size 30 nodes. As a result, we expect that different behaviour may occur if a different threshold value is used. In the case of ABA, however, we managed to make the process of updating the contention window's size to be adaptive. That is, nodes will self-adapt their windows according to the collisions they face, and this behaviour reflects in better utilization of the communication channel.

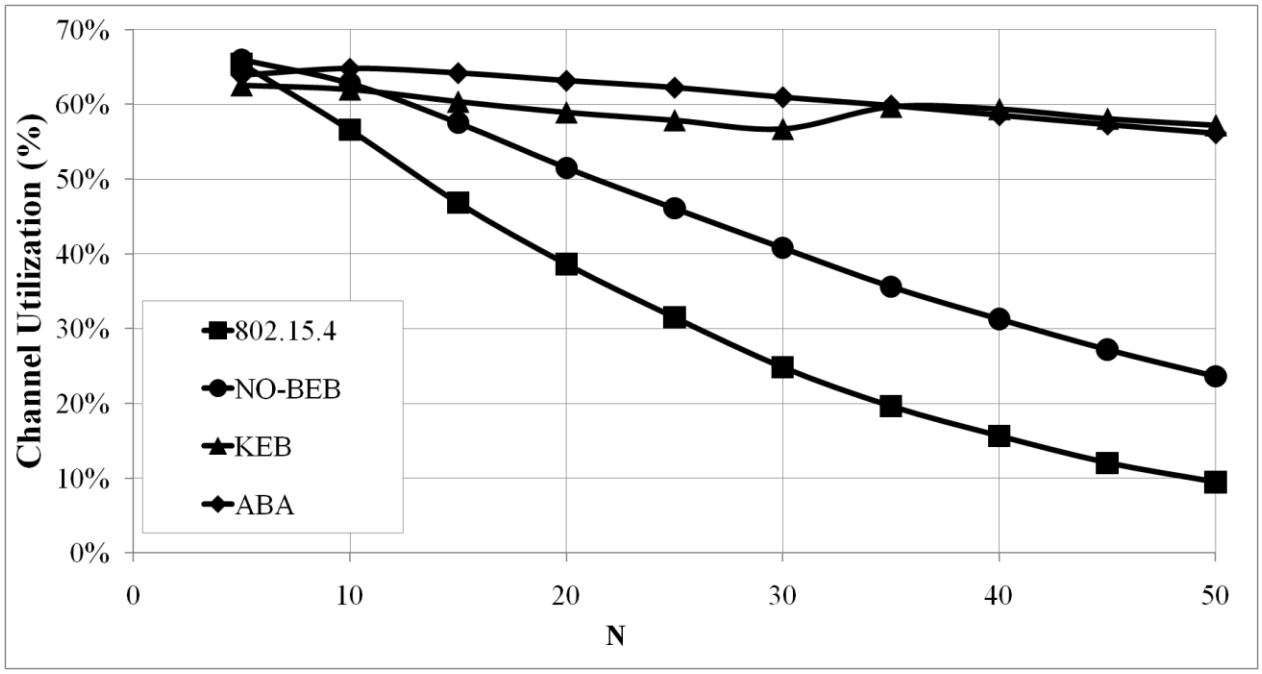

Figure 4-24: Channel utilization of ABA, BEB, NO-BEB, and KEB under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

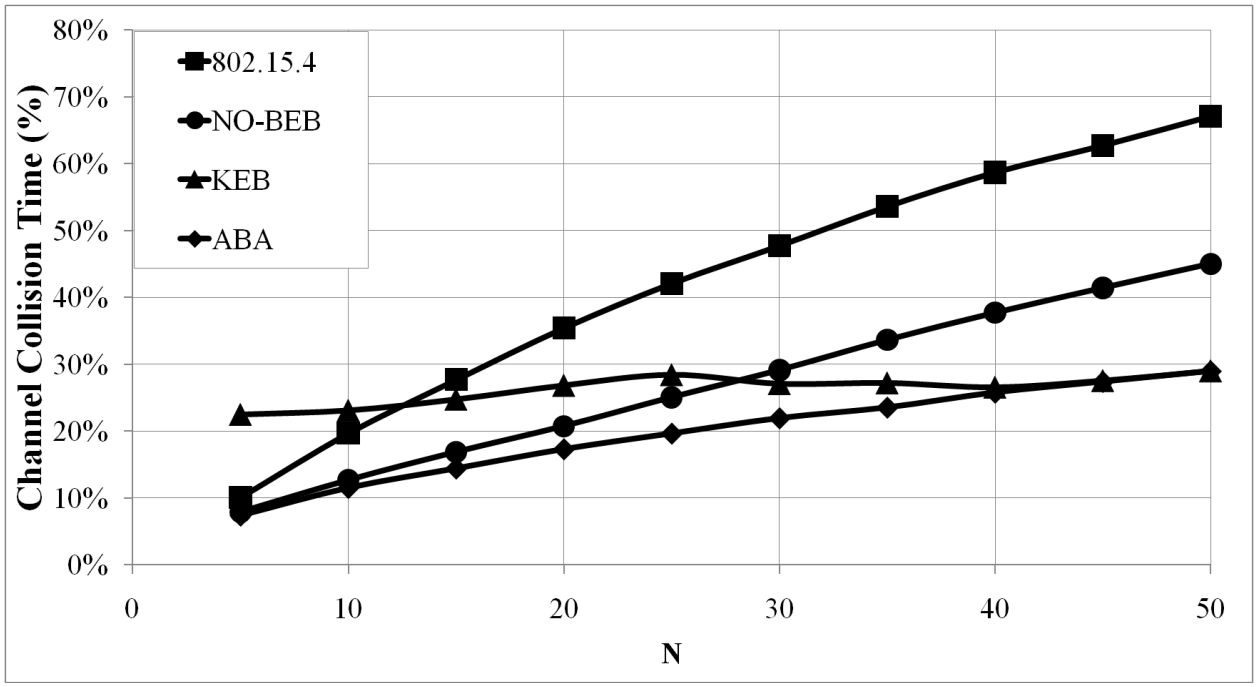

Figure 4-25: Channel utilization of ABA, BEB, NO-BEB, and KEB under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

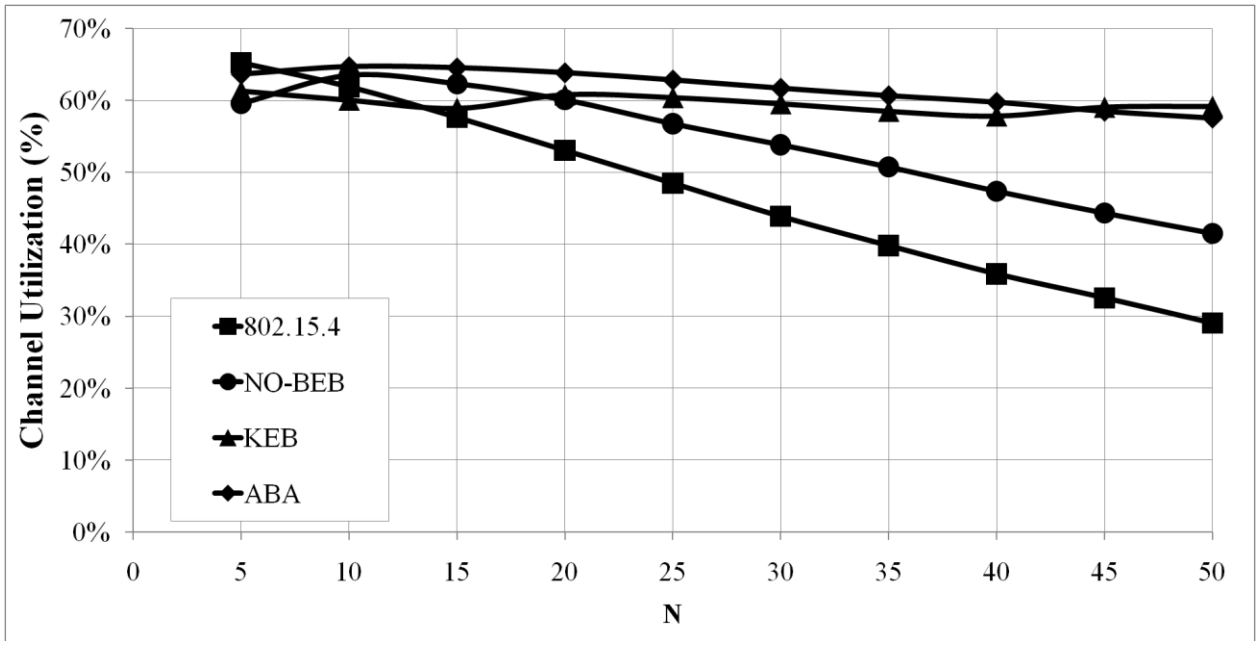

Figure 4-26: Channel utilization of ABA, BEB, NO-BEB, and KEB under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

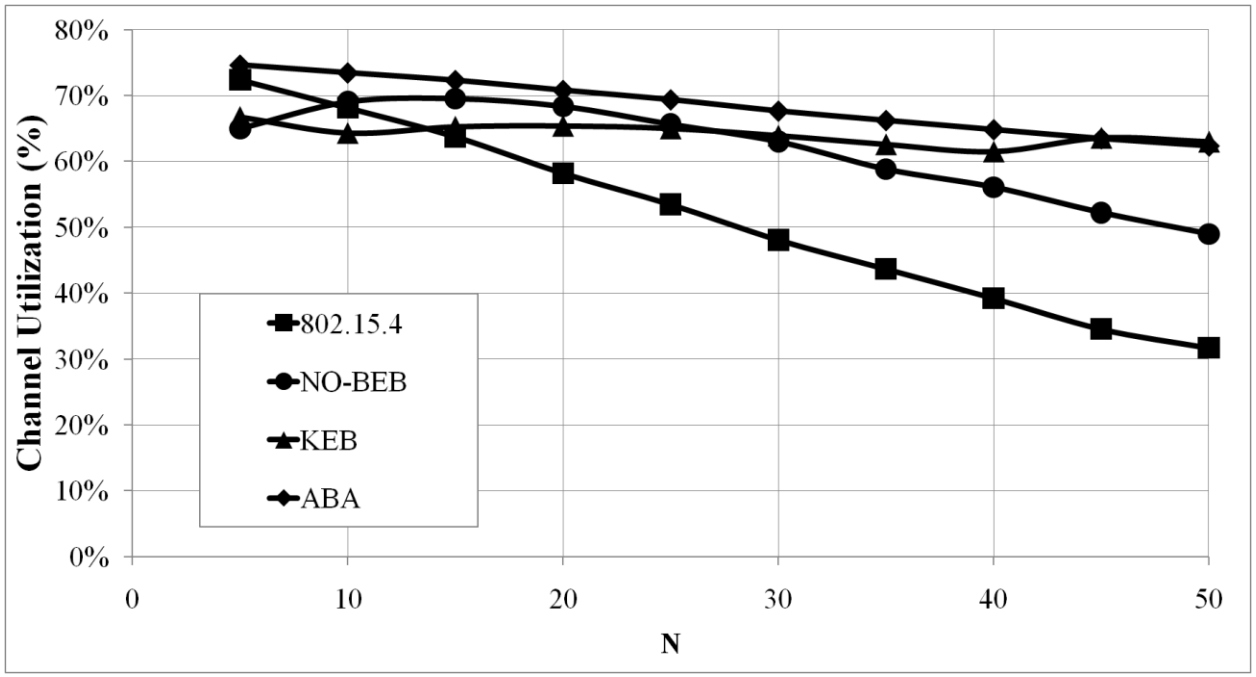

Figure 4-27: Channel utilization of ABA, BEB, NO-BEB, and KEB under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.2.2 Average Power Consumption

In Figures 4-28 to 4-31 we show the performance of ABA in terms of average power consumption. It is evident in all these figures that although ABA is consuming the least amount of power among all the algorithms, the differences in the total power consumed are minor. Therefore, it is interesting to investigate the portion of this total power that is wasted in useless activities, that is, collisions. In Figures 4-32 to 4-35 we show the amount of power lost due to collisions under each algorithm. It its quite evident that ABA is capable of lowering the percentage of collisions, and therefore, the power lost during these situations is the lowest compared to the other algorithms. We can clearly see that ABA is providing a significant improvement over BEB in terms of utilizing the power resources in useful activities. On the other hand, while NO-BEB is performing better than BEB, it is still inferior to ABA. KEB's performance in small networks (especially when $N \leq 20$) is very poor compared to ABA, even though it manages to match ABA's results at larger sizes of the network. In conclusion, we can see that ABA is proving to be more conservative in depleting the power resources of the nodes.

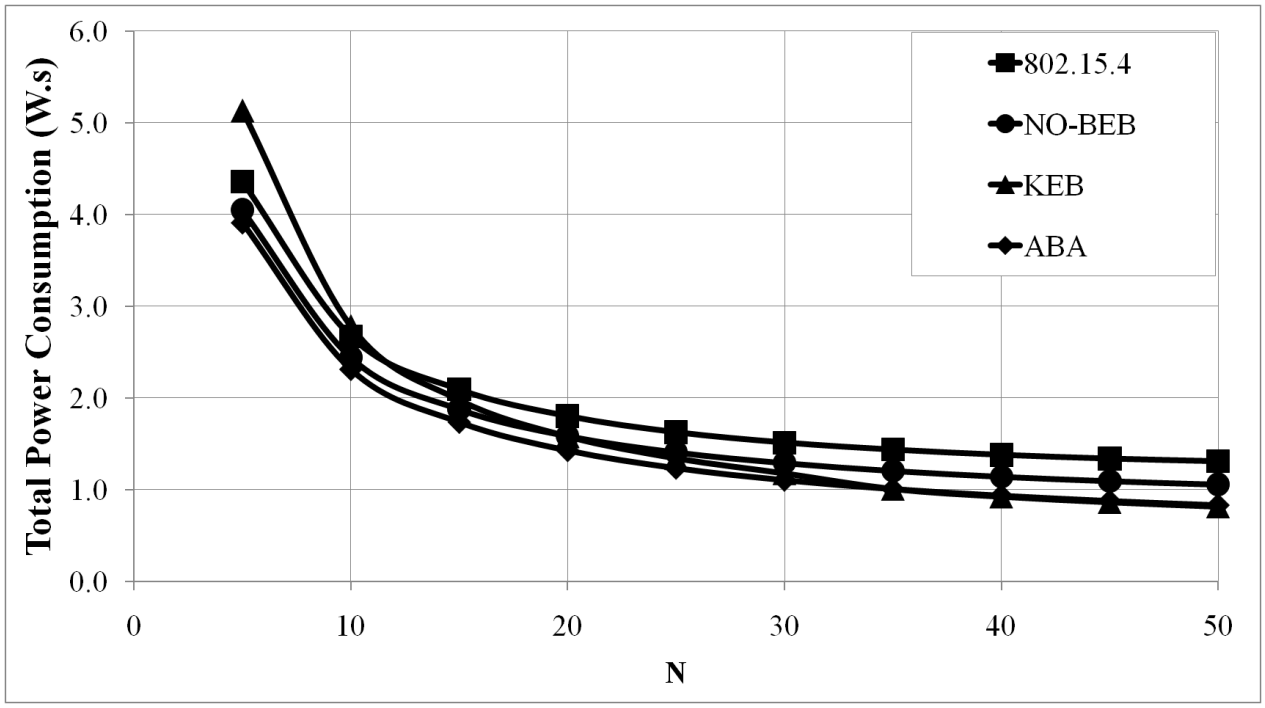

Figure 4-28: Total power consumption (W.s) of ABA, BEB, NO-BEB, and KEB under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

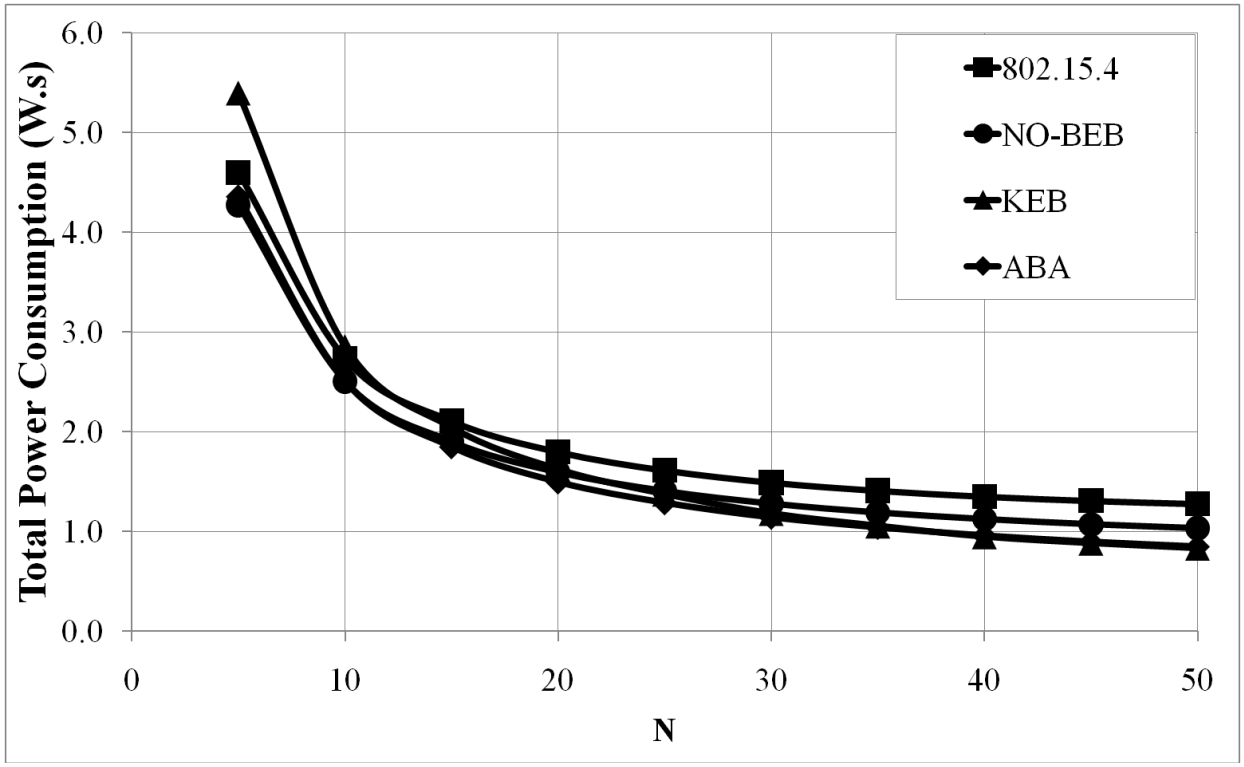

Figure 4-29: Total power consumption (W.s) of ABA, BEB, NO-BEB, and KEB under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

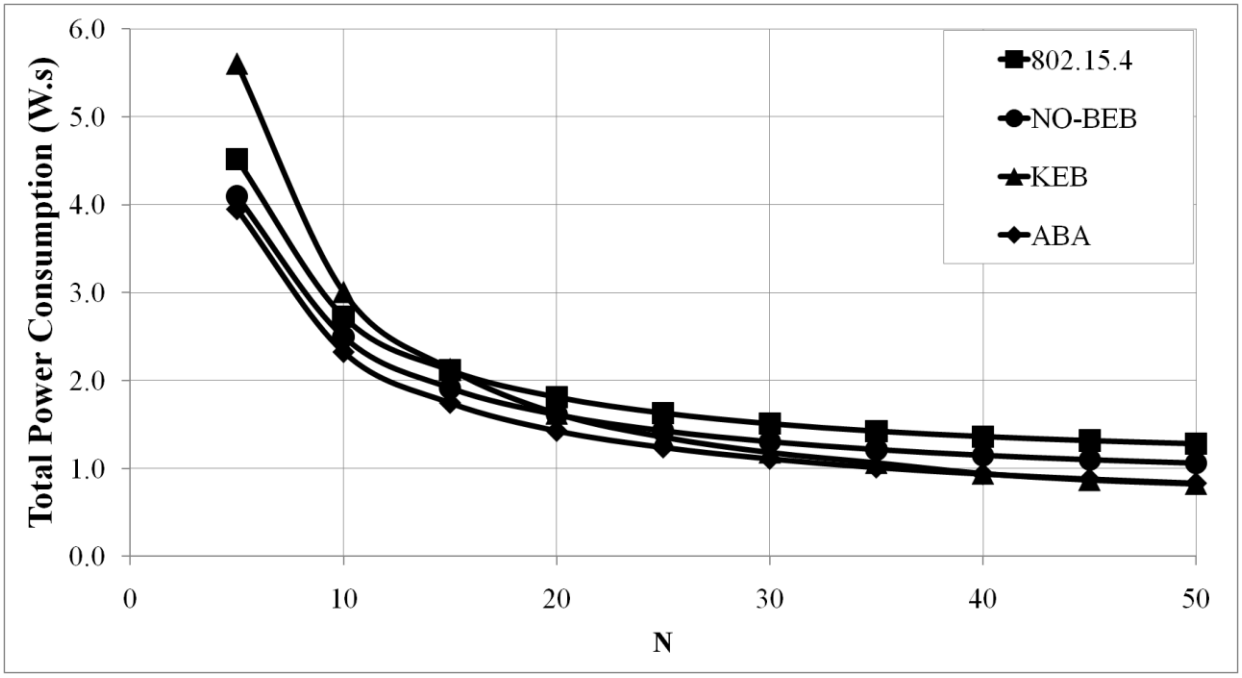

Figure 4-30: Total power consumption (W.s) of ABA, BEB, NO-BEB, and KEB under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

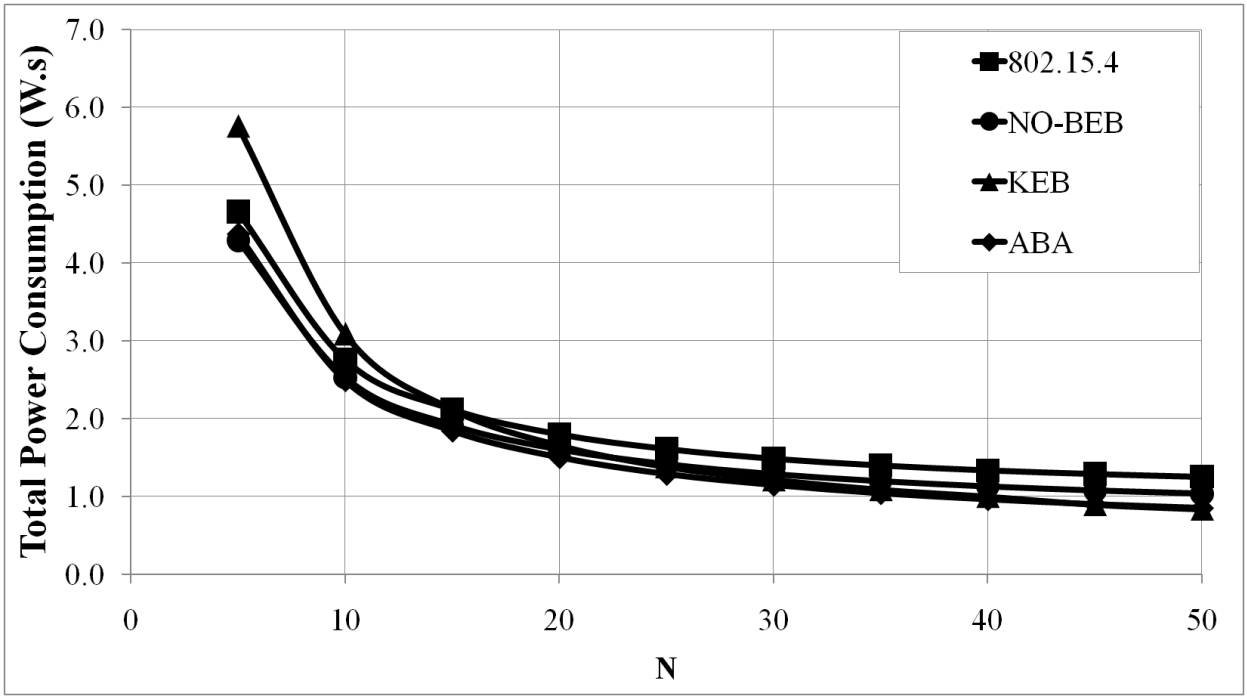

Figure 4-31: Total power consumption (W/s) of ABA, BEB, NO-BEB, and KEB under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

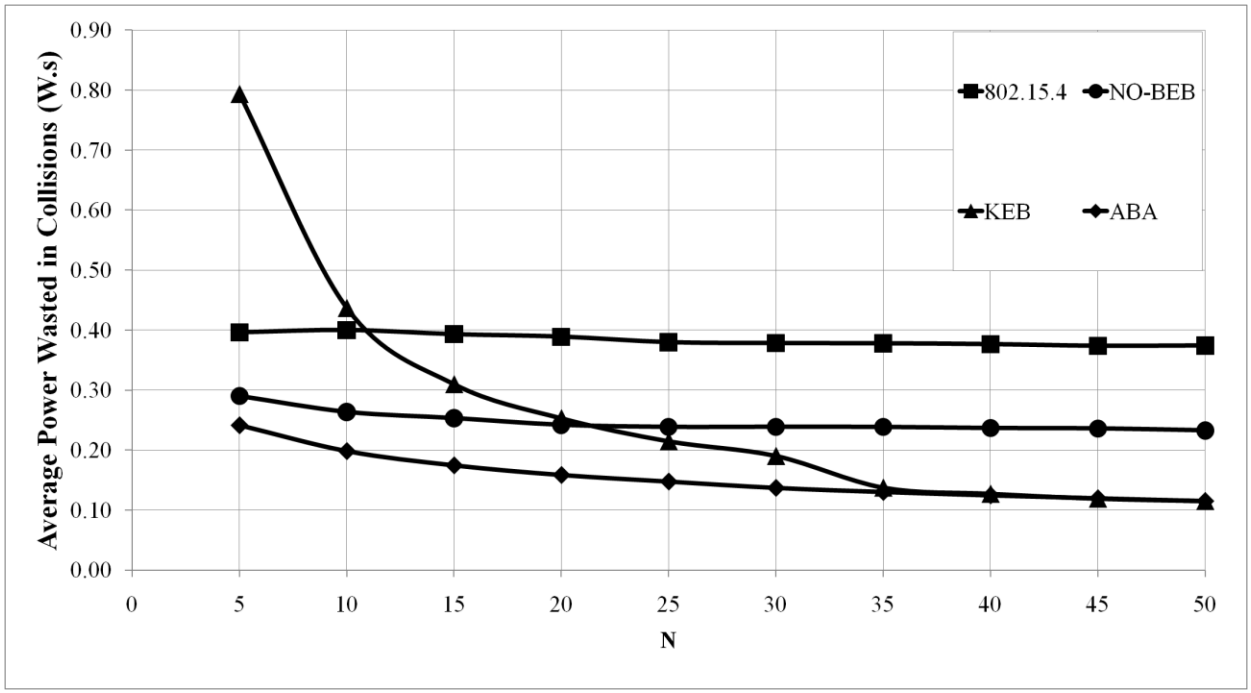

Figure 4-32: Average power wasted in collisions (W.s) under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

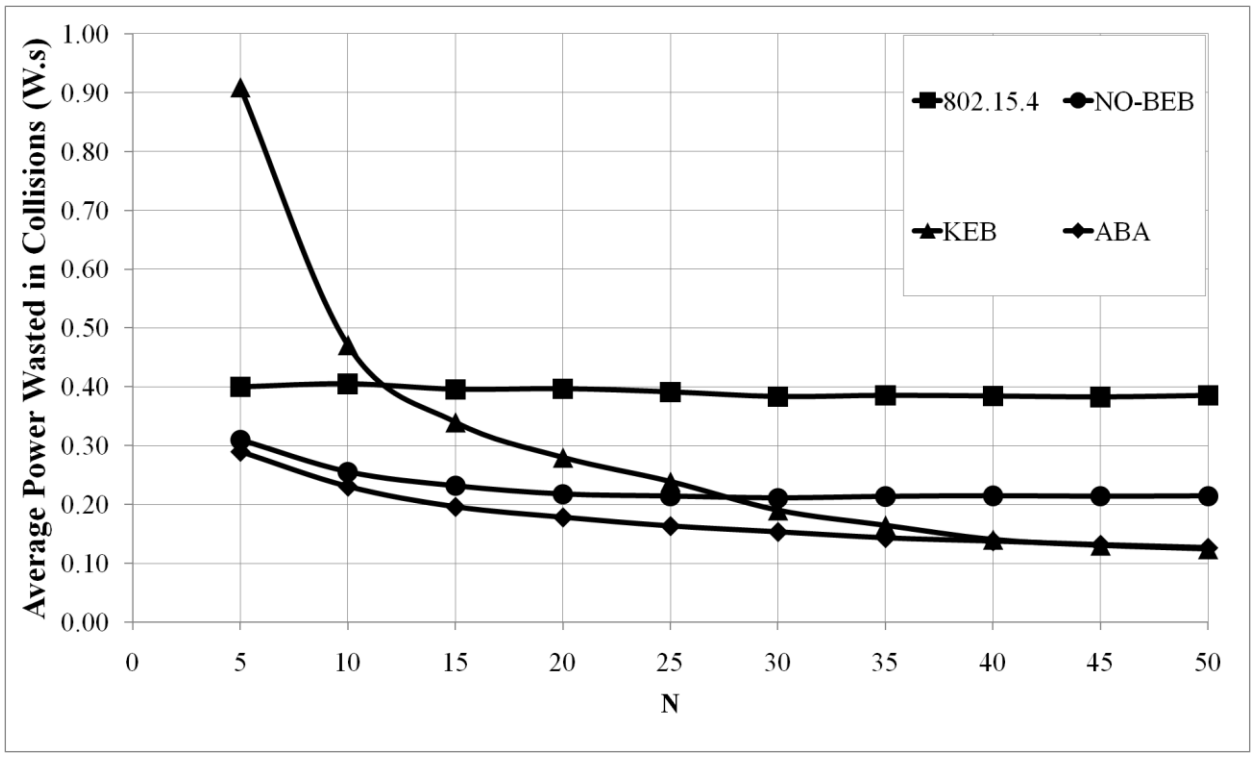

Figure 4-33: Average power wasted in collisions (W.s) under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

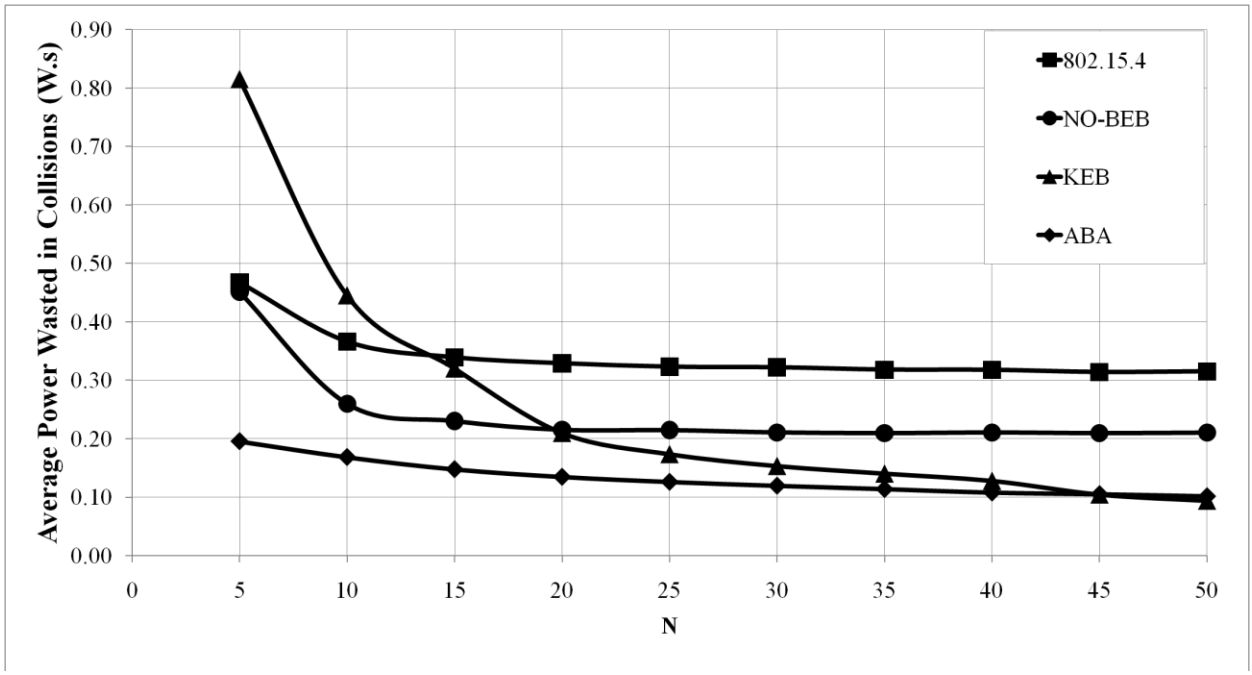

Figure 4-34: Average power wasted in collisions (W.s) under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

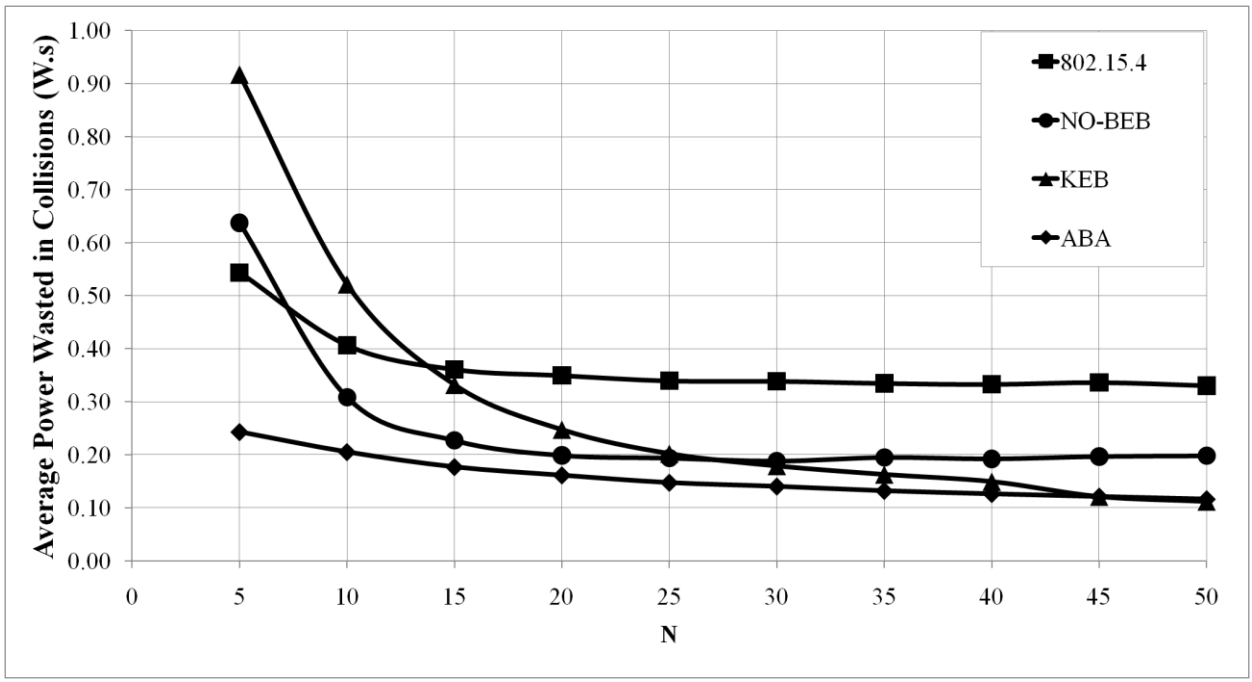

Figure 4-35: Average power wasted in collisions (W.s) under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.2.3 Reliability

In Figures 4-36 to 4-39 we depict the performance of ABA in terms of the reliability. These figures demonstrate the superiority of ABA over all the other algorithms in terms of reliability. A significant improvement can be observed over BEB and NO-BEB. Also, KEB is showing the same usual behaviour of being able to catch up with ABA as the network size gets bigger.

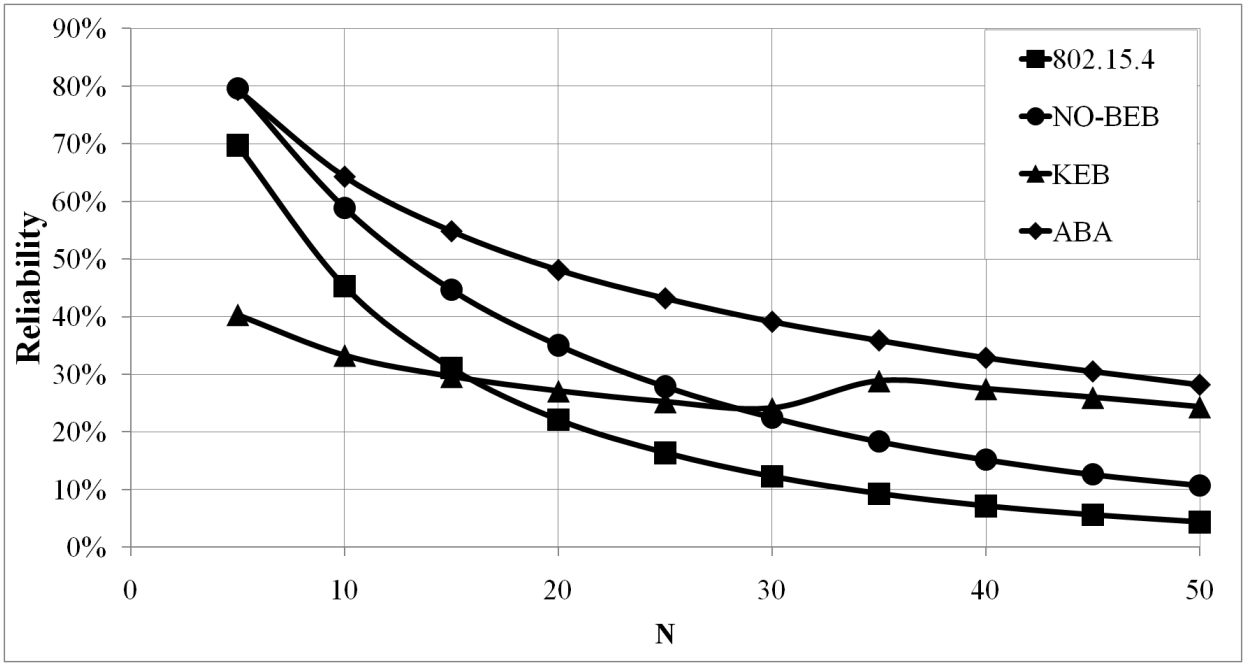

Figure 4-36: Reliability of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

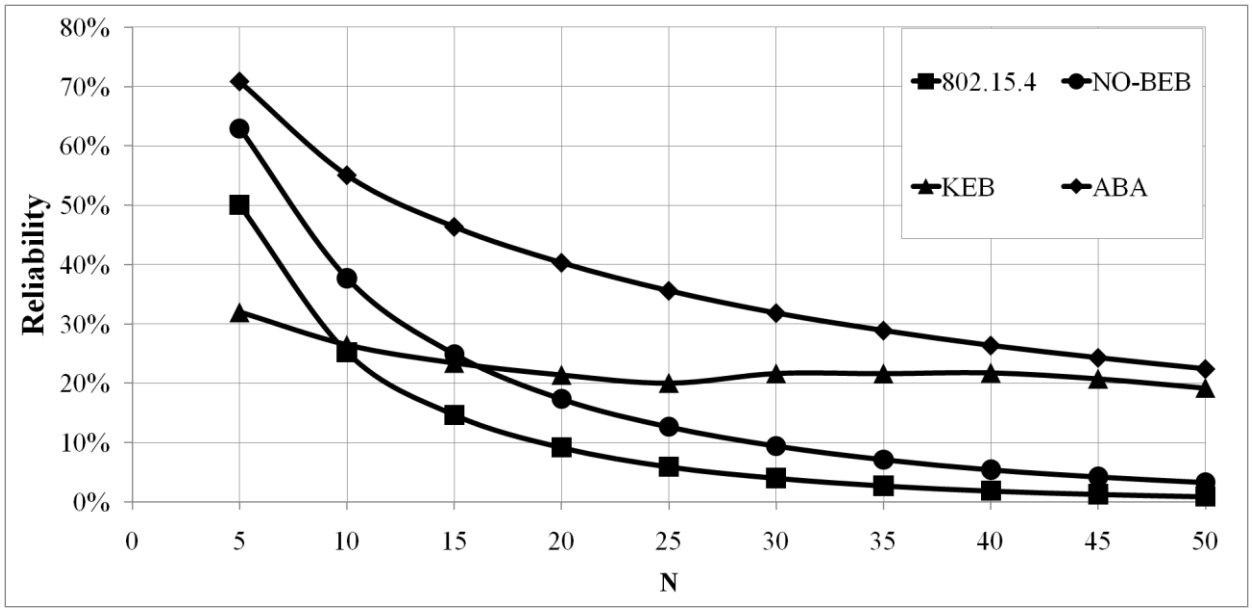

Figure 4-37: Reliability of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=3, and macMaxFrameRetries=2.

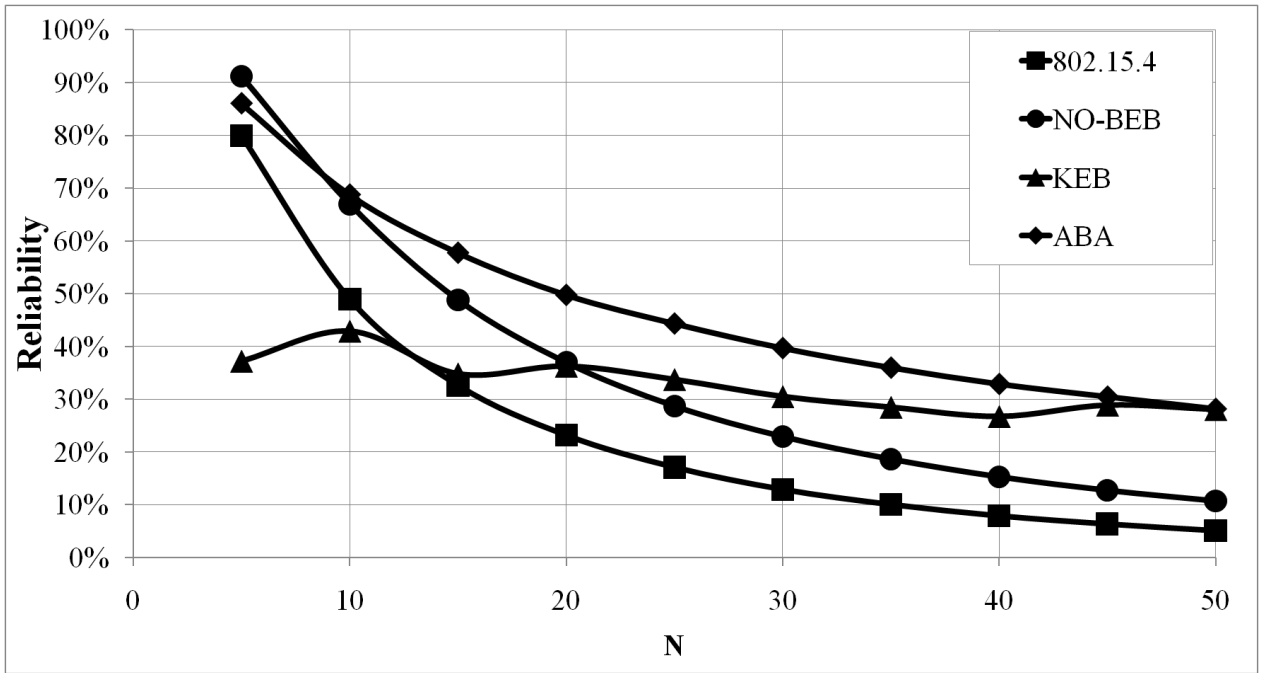

Figure 4-38: Reliability of ABA under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

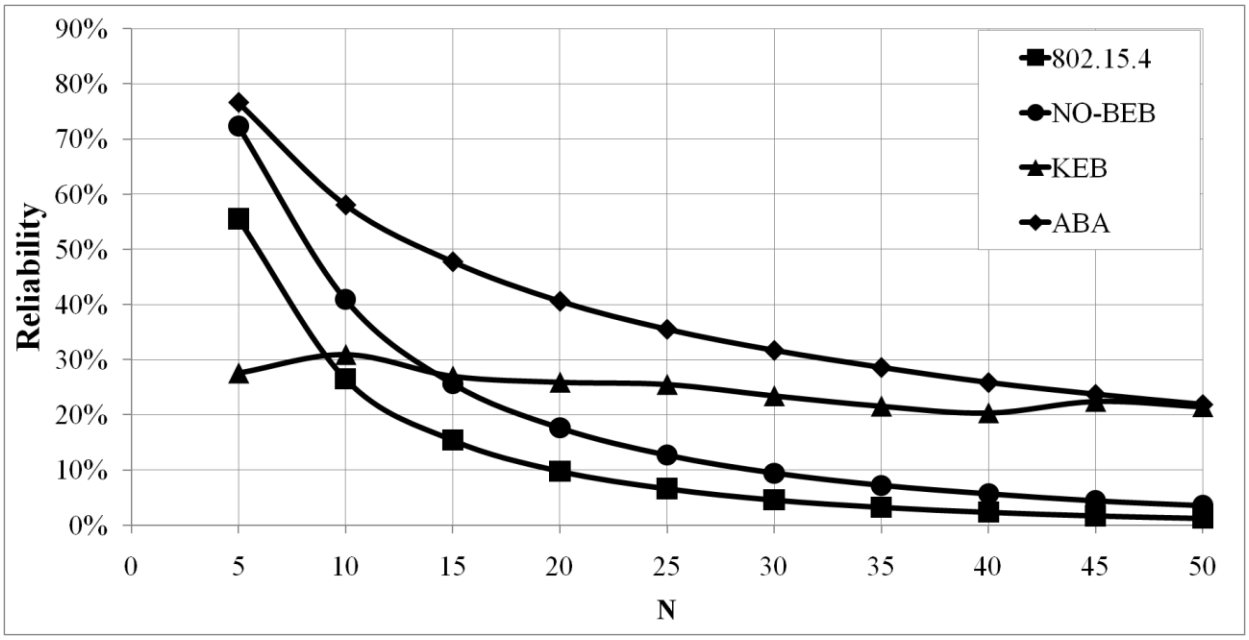

Figure 4-39: Reliability of ABA under acknowledged traffic. L=28, macMaxCSMABackoff=3, and macMaxFrameRetries=2.

4.3.2.4 Channel Collision Time

We examine the performance in terms of the channel collision time in Figures 4-40 to 4-43. Again, ABA is showing superiority in terms of its ability to keep the channel collision time at its lowest level compared to the other algorithms. KEB falls behind ABA, but manages to catch up as N keeps growing 30 nodes. ABA's ability to adapt the contention window's size in accordance with the collisions level allows for an efficient utilization of the network resources.

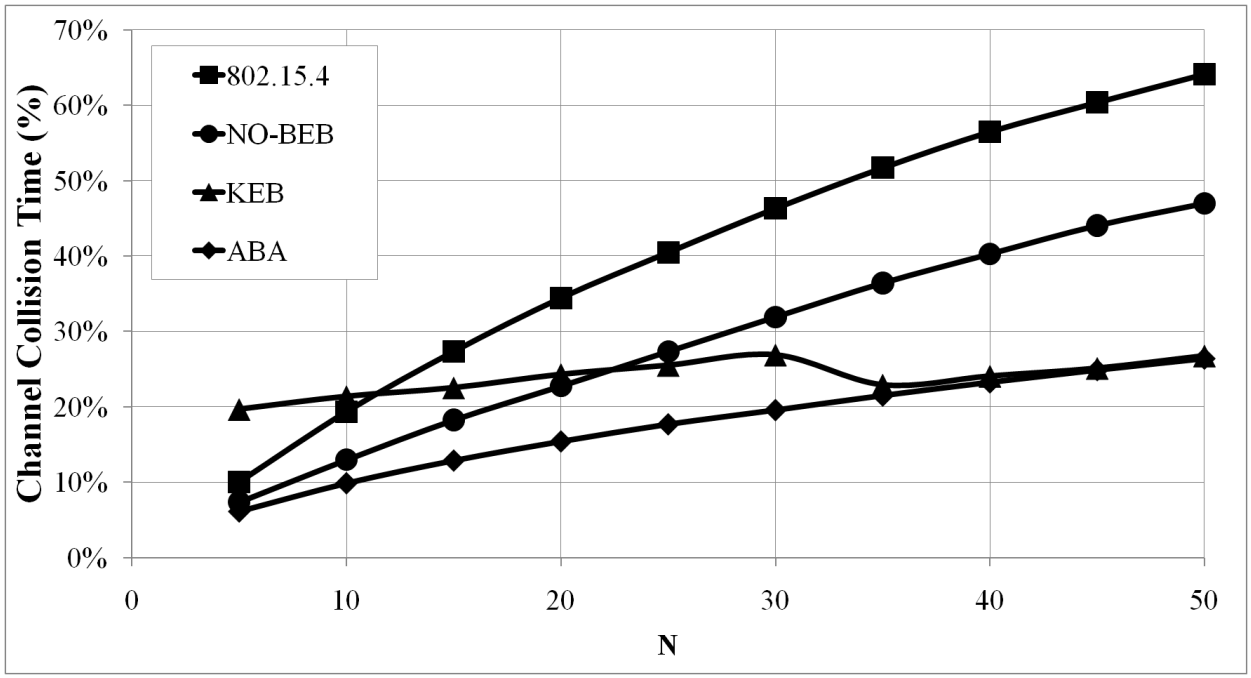

Figure 4-40: Channel collision time with ABA, under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

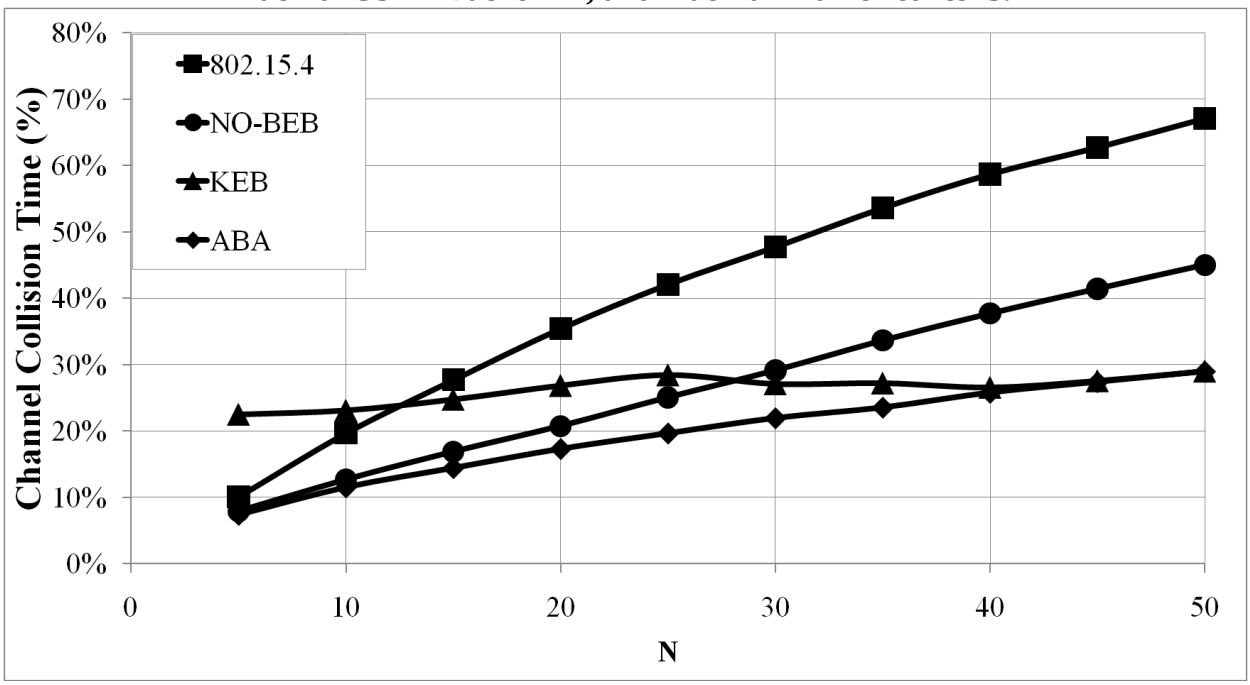

Figure 4-41: Channel collision time with ABA, under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

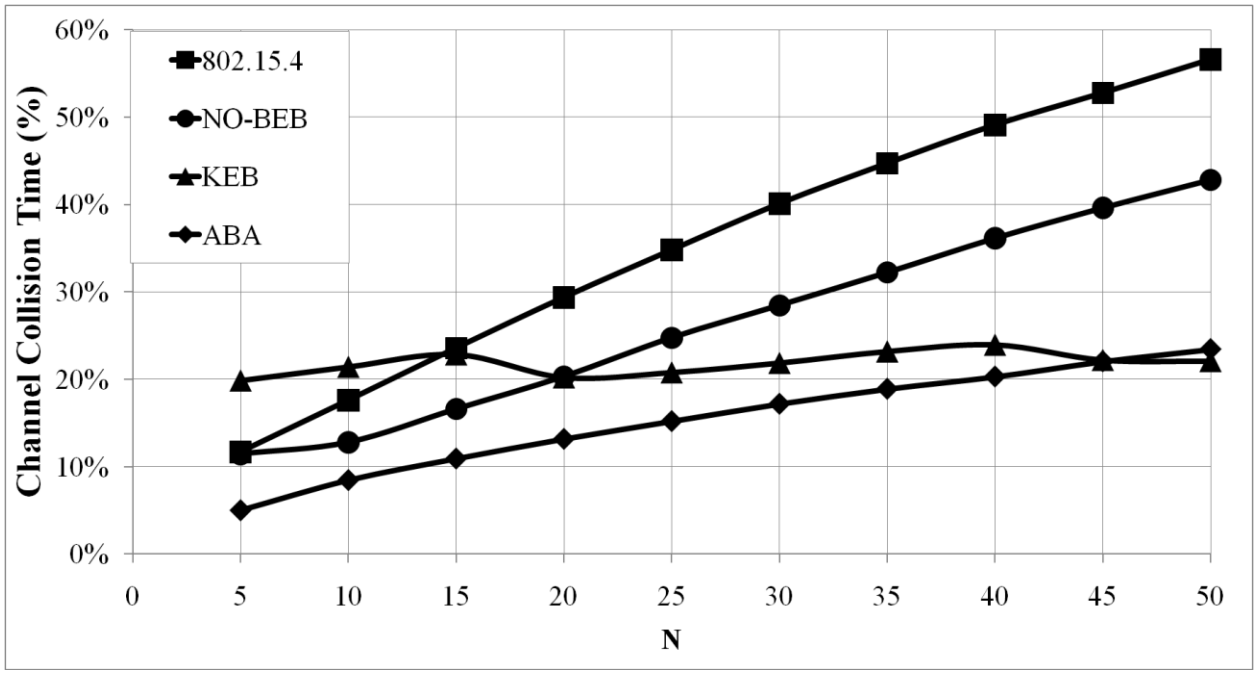

Figure 4-42: Channel collision time with ABA, under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

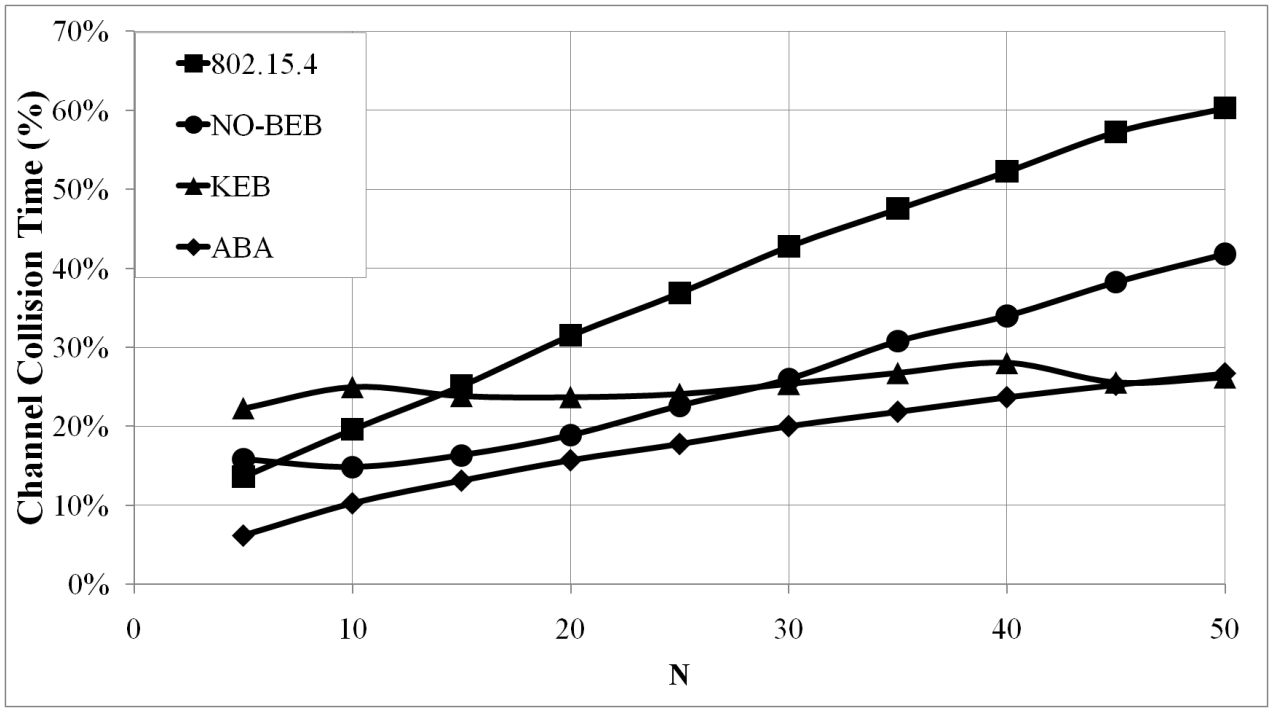

Figure 4-43: Channel collision time with ABA, under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.2.5 Fairness

Finally, we examine the fairness of ABA in order to see whether it allows nodes an equal opportunity to access the wireless medium or not. Again, we adopt Jain's fairness index [JAI84] to measure ABA's fairness:

$$fairness\ index = \frac{(\sum x_i)^2}{N \sum {x_i}^2} \qquad (4.34)$$

where, x_i denotes the ith node's share of the medium. An algorithm is achieving better sharing of the medium among the nodes if its fairness index is closer to 1. Figures 4-44 and 4-45 show the fairness of ABA, BEB, NO-BEB, and KEB under unacknowledged traffic conditions while Figures 4-46 and 4-47 show the fairness under acknowledged traffic conditions. We can clearly see that, for different packet lengths, ABA, BEB, and NO-BEB achieve a fair sharing of the medium among the nodes (only the curve of BEB is apparent because the curves have almost the same behavior and they overlap perfectly). It is interesting to see that KEB has a major problem in treating the nodes equally. The highest fairness index it achieves is barely 83% (see Figure 4-46). The dramatic degradation in KEB's fairness results from the strong dependence on the parameter α (the collisions threshold, refer to Chapter 2 for more details). The tuning of this parameter controls the behavior of KEB and highly affects the final performance of the algorithm. This is due to that the value of BE keeps on increasing, after suffering from collisions, as long as the collisions threshold is not crossed. In other words, the level of collisions over the communication medium will not have any effect on W before reaching α. Therefore, the nodes that suffer from repetitive collisions will have lower chances of accessing the medium (because their backoff periods keep on increasing). That is, these nodes will experience a case of starvation for the medium. With ABA, however, the updating of W is not subject to any

thresholds and is directly dependent on the level of packet collisions, such that we achieve an adaptive algorithm.

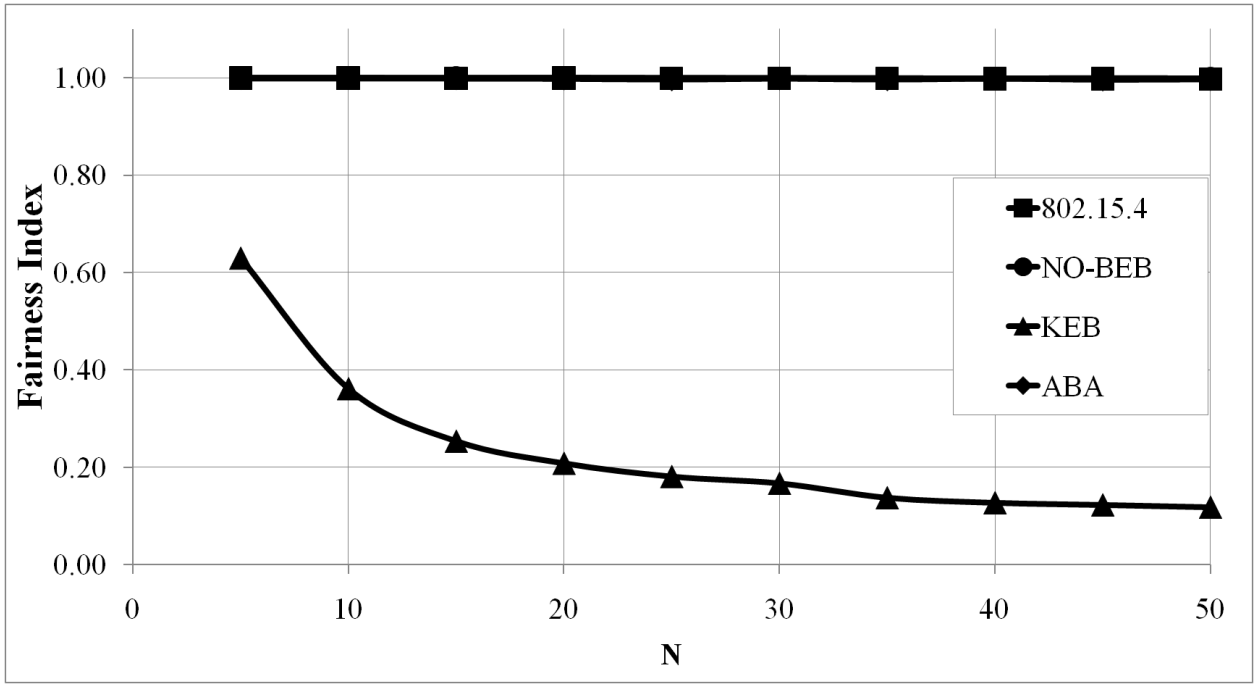

Figure 4-44: Fairness of ABA under unacknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

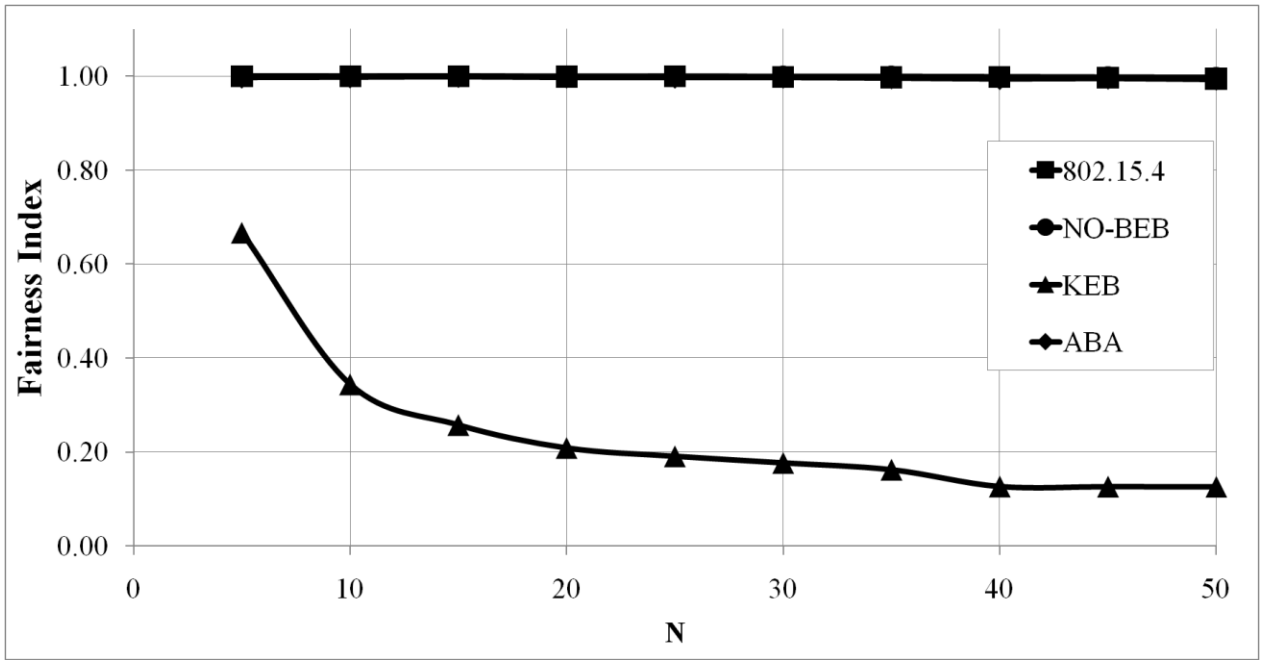

Figure 4-45: Fairness of ABA under unacknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

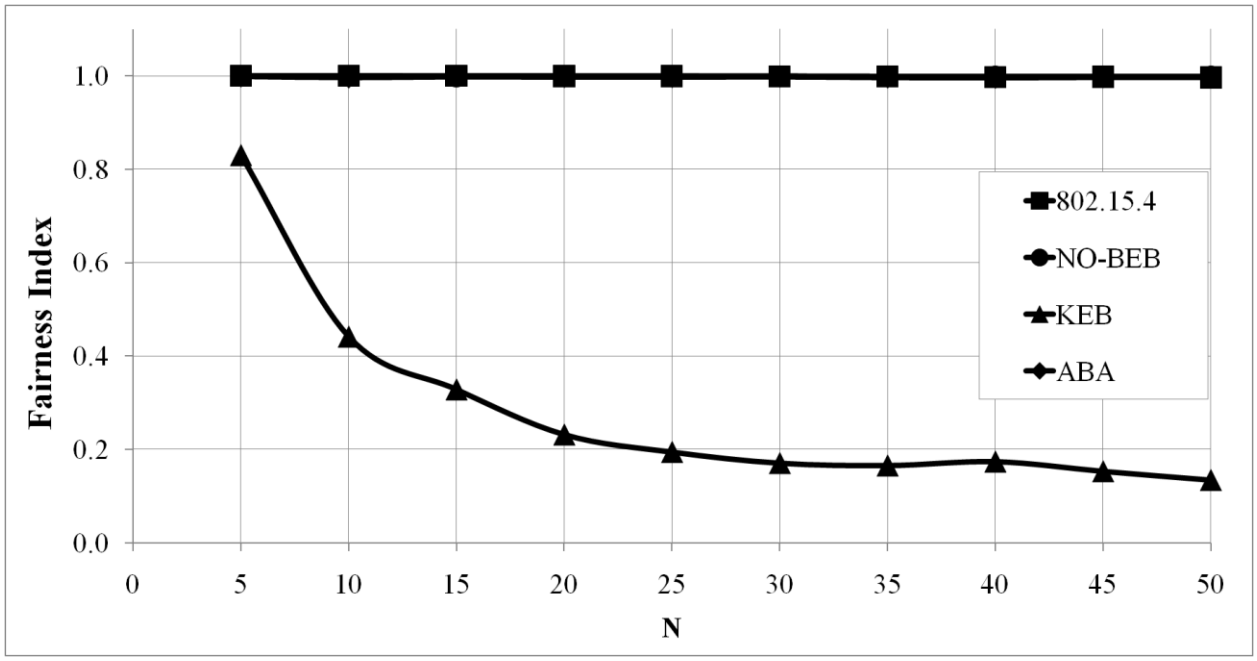

Figure 4-46: Fairness of ABA under acknowledged traffic. L=14, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

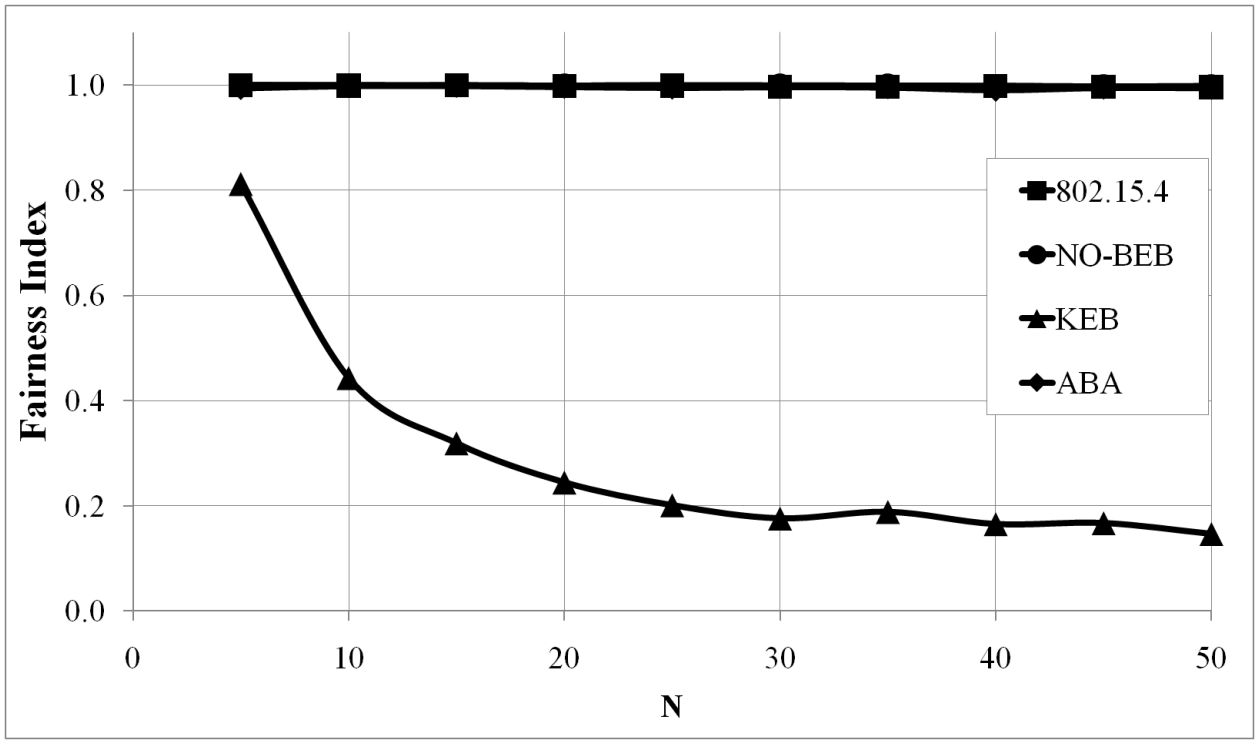

Figure 4-47: Fairness of ABA under acknowledged traffic. L=28, macMaxCSMABackoff=4, and macMaxFrameRetries=3.

4.3.3 Discussions

In the previous subsection we found that the ABA algorithm is achieving a promising performance in terms of enhancing channel utilization, conserving power resources, improving reliability, reducing the level of collisions, while preserving the fairness among the nodes in the network. The superiority of ABA over the other algorithms, especially BEB, comes from the fact that it indirectly relates the contention window (W) to the number of nodes in the network. This can be understood by recalling Equation (4.13) in which we have a direct relation between the probability of collision (P_c) and the number of nodes in the network (N). P_c increases with the increase of N, and therefore, the value of the W should be changed taking into consideration the size of the network. Thus, the main strength of ABA is that it controls W probabilistically, in such a way that it self-adapts to the network size and the activity over the communication

channel. Depending on a deterministic methodology, as in BEB, to change W without any consideration for the network size gives a poor performance as we demonstrated. The same problem is found with NO-BEB which adopts from BEB the idea of resetting W to a predefined minimum. Although NO-BEB shows a considerable improvement over BEB's performance, resetting W to its minimum without taking into consideration the current status over the medium will degrade the performance. Finally, KEB is an innovative methodology that includes the status of the medium in its calculation of W. The main drawback of KEB is its dependence on a pre-specified threshold, and we showed that the final performance depends solely on it. As we examine all the graphs in the previous subsection we can easily notice that KEB suffers from oscillations that cannot reflect a steady and stable behavior. In contrast, ABA managed to provide stable and smooth results as the network size changed.

4.4 Conclusion

In this chapter we have pointed out that BEB's methodology of updating the size of the contention window is highly deterministic and cannot cope with the changing levels of activity over the communication channel. Based on these observations, we have introduced a novel backoff algorithm, the Adaptive Backoff Algorithm (ABA), which introduces an adaptive, probabilistic methodology to control the size of the contention window. ABA depends on including the probability of collisions, as computed locally by each sensor node, in the computation of the size of the contention window. In this way, the number of nodes competing to access the medium is involved indirectly in the process of updating the contention window. Therefore, we have ended up with a backoff algorithm that can self-adapt to the size of the network, and therefore, manage the medium access in a way that improves the overall performance.

Chapter 5

Prioritization of MAC for IEEE 802.15.4-based WSNs

5.1 Introduction

In Chapter 1 we have discussed the fact that IEEE 802.15.4 does not define clear measures to preserve the priority of traffics or nodes. Instead, all of the nodes are treated the same and each node receives the same opportunity to access the medium. That is, no measures are taken to distinguish between nodes based on how long they have been attempting to gain medium access or how urgent their traffics are. The problem of enhancing the MAC protocol of IEEE 802.15.4, such that the priority among the nodes is preserved, has received a considerable attention in the research community (see Chapter 2). In this chapter we elaborate on the probabilistic approach we developed in Chapter 4 and use it to propose the Priority-Based BEB, a modified version of BEB that can adaptively prioritize the access to the medium such that nodes are treated more fairly. We provide a simulation-based study to evaluate the performance of Priority-Based BEB compared to BEB. We defer the development of an analytical model for PB-BEB for a future study. The rest of this chapter is organised as follows. In Section 5.2 we describe the new Priority-Based BEB algorithm. In Section 5.3 we detail the simulations we conducted to compare the performance of Priority-Based BEB and BEB. Finally, Section 5.4 concludes the chapter.

5.2 The Priority-Based BEB Algorithm

The MAC layer of IEEE 802.15.4 *implicitly* recognizes two classes of priority. In particular, the first class (lower priority) is assigned to the data packets while the second class (higher priority) is given to their associated ACK packets. This can be noticed by observing that the CCA1 state is firstly needed to avoid any collision with an ongoing data packet transmission. After that, the CCA2 state is imposed such that the ACK for that packet is transferred successfully. However, this functionality does not consider the number of failed attempts that certain nodes encounter while trying to access the medium. These nodes are more prone to deplete their power resources at a higher pace and for useless activities. Different nodes should be treated *fairly* such that those that experience repeated access failures are given higher priority to access the medium.

In the Priority-Based BEB (PB-BEB) algorithm we propose to extend the BEB algorithm such that the number of CCAs is not confined to only two. Instead, the number of CCAs will be dictated by the level of collisions over the communication medium. The flow diagram of PB-BEB is shown in Figure 5-2. After a node conducts its regular BEB-defined CCAs, it will be required to conduct more CCAs before being able to start its transmission. The total number of CCAs conducted by a node will be determined by the following formula:

$$n_{CCA} = 2 + AP_c \qquad (5.1)$$

where, P_c is the probability of collision and A is a constant value. The first term in Equation (5.1) indicates that PB-BEB keeps the two CCAs of BEB without modification. This is required in order preserve the aforementioned functionality of BEB in which the highest priority is assigned to the ACK packet. The second term in Equation (5.1) indicates that the addition of the extra

CCAs will be dependent on the collisions experienced by the packets. That is, we adapt the number of extra CCAs in accordance with the activities over the wireless channel. P_c is computed as follows:

$$P_c = \frac{n_s}{n_s+n_f} \qquad (5.2)$$

where, n_s is the total number of successfully transmitted packets and n_f is the total number of failed packets. The latter refers to packets discarded due to either channel access failure (when exceeding macMaxCSMABackoffs) or transmission failures (when exceeding macMaxFrameRetries). Equation (5.2) is computed locally at each node. In Equation (5.1), A is a constant that is set to the value macMaxCSMABackoffs. We use the latter value to indicate that we need the number of extra CCAs to be below the maximum number of backoff stages allowed. In Figure 5.1 we illustrate the CAA timeslots of our system.

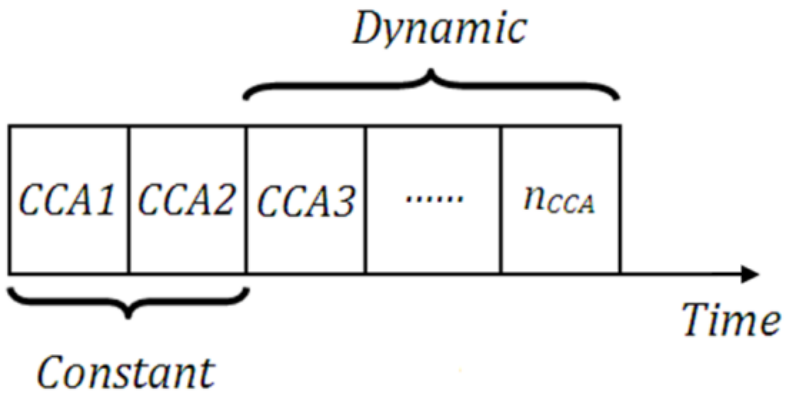

Figure 5-1: PB-BEB uses the original CCAs of BEB and adds extra CCAs, the number of which is dynamically changing.

As the node starts conducting its extra CCAs, it may find the medium busy, and therefore, it will backoff again. Once the backoff counter expires, the node will not restart the CCAs from CCA1. Instead, it will continue from exactly the same CCA it stopped at. The only exception of

this rule is if the node stopped previously at CCA2. In that case, the node will have to restart from CCA1. Again, this keeps unchanged the original functionality of BEB to give priority to the ACK packet over all other packets. In brief, PB-BEB applies the following formula to find the next CCA the node will conduct:

$$CCA_{new} = \max(2, CCA_{old}) \qquad (5.3)$$

where, $\mathrm{CCA_{new}}$ refers to the next CCA to start at and $\mathrm{CCA_{old}}$ is the last CCA at which the medium was found busy.

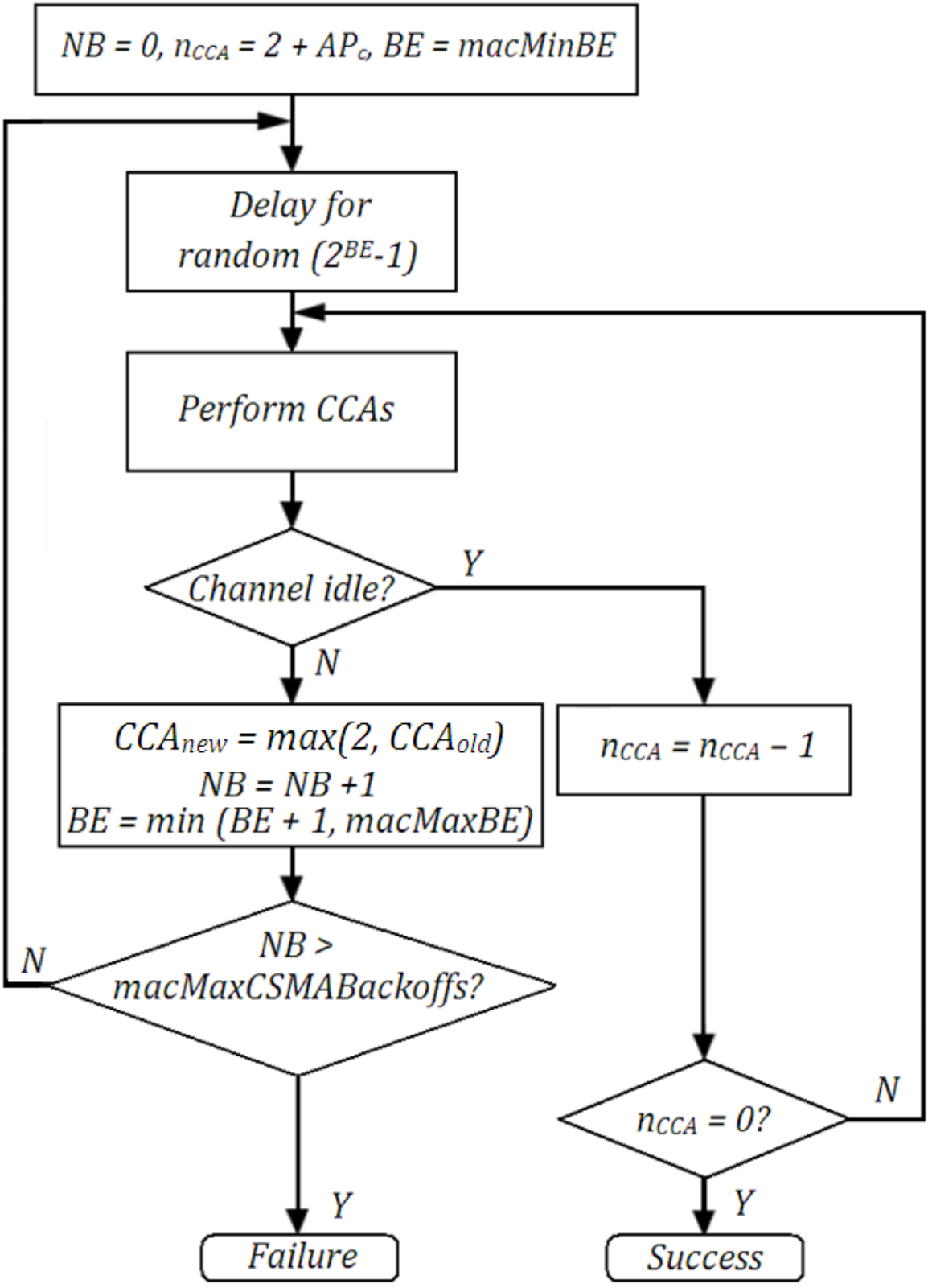

Figure 5-2: PB-BEB Algorithm.

The result of imposing Equation (5.3) is that the node that has been experiencing multiple backoffs while trying to send a packet is given a higher priority to access the medium. This means that we are able to incorporate a degree of priority that has been absent in BEB.

5.3 Simulations

In this section we conduct simulations to compare the performance of PB-BEB and BEB. The performance parameters we concentrate on are fairness, channel utilization, reliability, average power consumption, channel collision time, delay, and channel idle time. We use the simulation parameters listed in Table 5-1. The network is assumed to be of a peer-to-peer topology. We operate the network under the beacon-enabled mode with the superstructure constituted by only the CAP. The traffic used is assumed to be saturated (i.e., nodes has always packets to send). In all of our simulation results a confidence interval (CI) of 95% is assumed. This CI is not shown in our graphs because it is too small to be observed (refer to Appendix B for more details). In the following subsections we show and discuss the results of our simulations.

Table 5-1: ABA Simulation Parameters

Average Power Consumed (mW.s)	Rx	30
	Tx	40
	CCA	30
	Sleep	0.8
Durations	1 timeslot	0.32 ms (80 bits)
	Packet Length (L)	14 timeslots
	ACK Packet Length (L_{ACK})	2 timeslots
	Simulation Time	320 s
IEEE 802.15.4 Parameter Settings	*macMaxFrameRetries*	3
	macMaxCSMABackoffs	4
	macMinBE	3
	macMaxBE	8

5.3.1 Fairness

Testing the fairness of any backoff algorithm is essential to assert that nodes are getting equal opportunity to access the wireless medium. In measuring the fairness, we again depend on Jain's fairness index [JAI84], which is expressed as follows:

$$fairness\ index = \frac{(\sum x_i)^2}{N \sum {x_i}^2} \qquad (5.4)$$

where, N is the total number of nodes available in the network and x_i is the *i*th node's share of the medium. A backoff algorithm is deemed fair if it can achieve a fairness index close 1. In Figure 5-3 we show the fairness index for both PB-BEB and BEB. The graph clearly shows that as the network size grows beyond 100 nodes, BEB falls behind PB-BEB in treating the nodes fairly. In fact, we can see that PB-BEB is achieving a significant improvement over BEB. For example, at N = 200, BEB achieves a fairness index of 0.77 while PB-BEB achieves a fairness index of 1. This behavior is consistent with other studies that highlighted and proved the *short-term unfairness* of BEB (see [KOK00] for example).

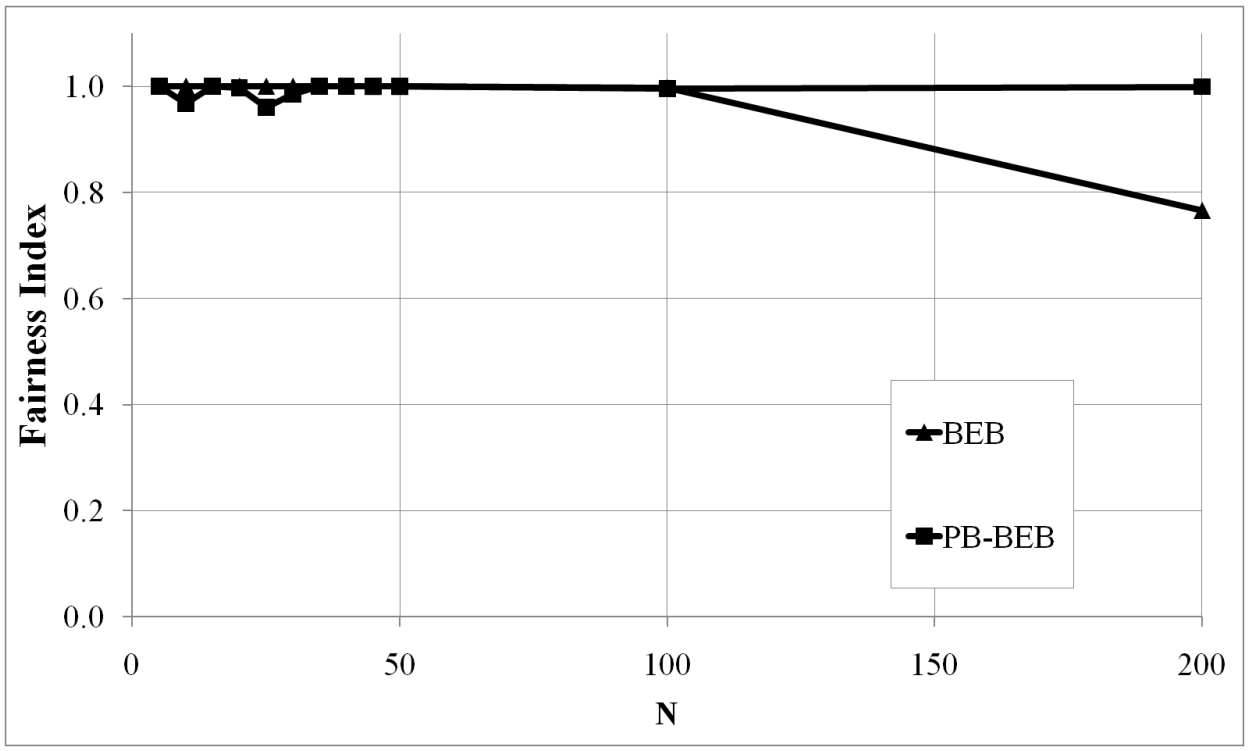

Figure 5-3: Fairness of PB-BEB compared to BEB.

5.3.2 Channel Utilization

Channel Utilization (U) is the proportion of time the wireless channel is being used to successfully transmit packets. We define U as follows:

$$U = \frac{L}{T} \qquad (5.5)$$

where, L is the packet length and T is the total duration spent to deliver the packet to its destination. This duration includes the backoff periods, packet transmission time, and the time wasted while retrying (due to experiencing multiple collisions) to send the packet. In Figure 5-4 we show the performance in terms of U for both BEB and PB-BEB. We can quite observe that PB-BEB is significantly outperforming BEB. At a network size of 100 nodes, for instance, PB-BEB achieves a U of 53.3% while BEB utilizes the channel by as low as 3.3%.

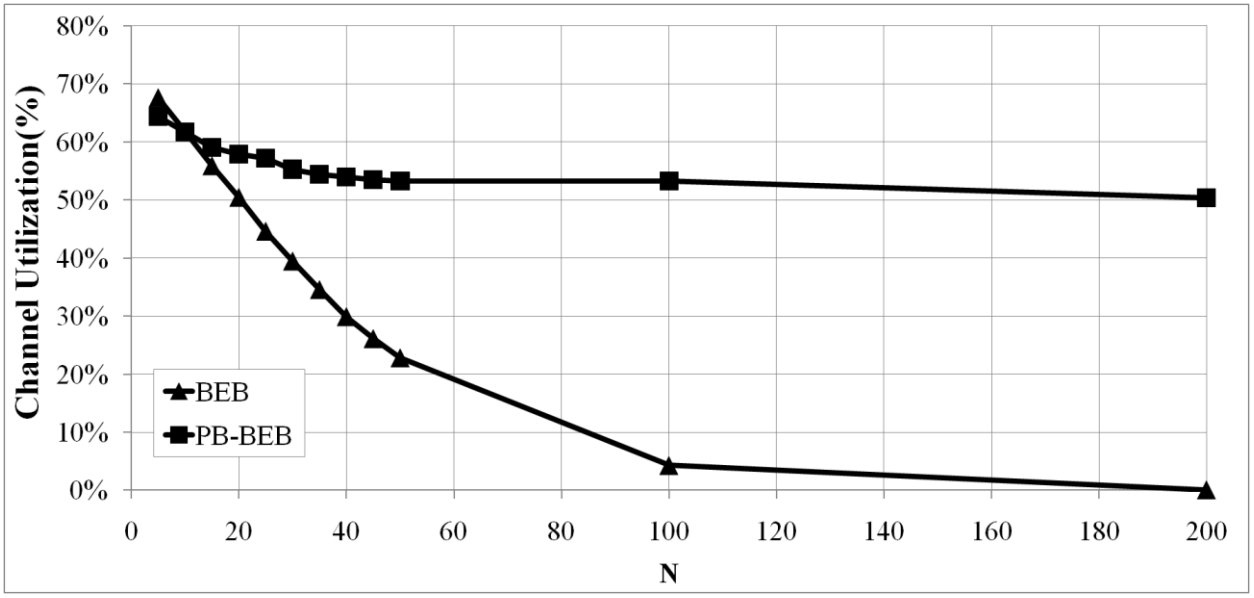

Figure 5-4: Channel utilization of PB-BEB compared to BEB.

5.3.3 Reliability

Reliability (R) is the probability of transmitting a packet successfully. Stated differently, R is the probability of *not* discarding a packet. The latter reflects the fact that nodes may backoff multiple times and/or suffer from multiple collisions before managing to send the packet. An algorithm of high R is one that can reduce the possibility of repetitive backoffs and/or collisions while attempting to send a packet. We illustrate in Figure 5-5 the performance of PB-BEB and

BEB in terms of R. PB-BEB is able to achieve higher R than BEB as the size of the network grows. At a network size of 50 nodes, PB-BEB achieves a reliability of 10% while BEB's reliability is only 3.4%.

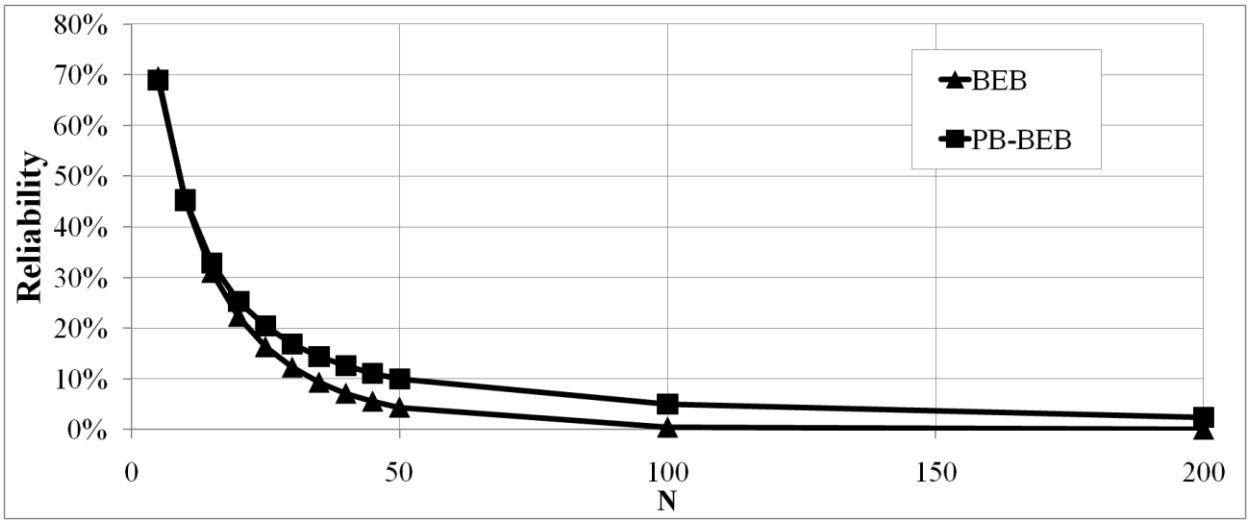

Figure 5-5: Reliability of PB-BEB compared to BEB.

5.3.4 Average Power Consumption

It is essential to study the power requirements of any algorithm devised for WSNs. This is because of that sensor nodes are battery-powered and we need to be conservative in power usage in order to prolong the lifetime of the sensor node, and thus the network. In Figure 5-6 we show the average power consumption required by PB-BEB and BEB. The graph shows that the performance of both PB-BEB and BEB is generally comparable. Therefore, it is interesting to investigate the activities during which the nodes' power resources are consumed to see what activities are contributing more to that consumption. In Figure 5-7 we show the average power wasted due to collisions when the network operates under PB-BEB or BEB. It is quite evident that BEB is wasting a large amount of power in collisions. For instance, at a network size of 45 nodes, the average power consumption of BEB is 1.34 W/s (Figure 5-6). From Figure 5-7, we

observe that 0.38 W/s is wasted due to collisions, which contributes to 28.4% of the average power consumed. The contribution becomes 30.6% at N = 100. However, under PB-BEB, the average power wasted due to collisions contributes to only 10% (at N = 45) and 6% (at N = 100) of the average power consumption.

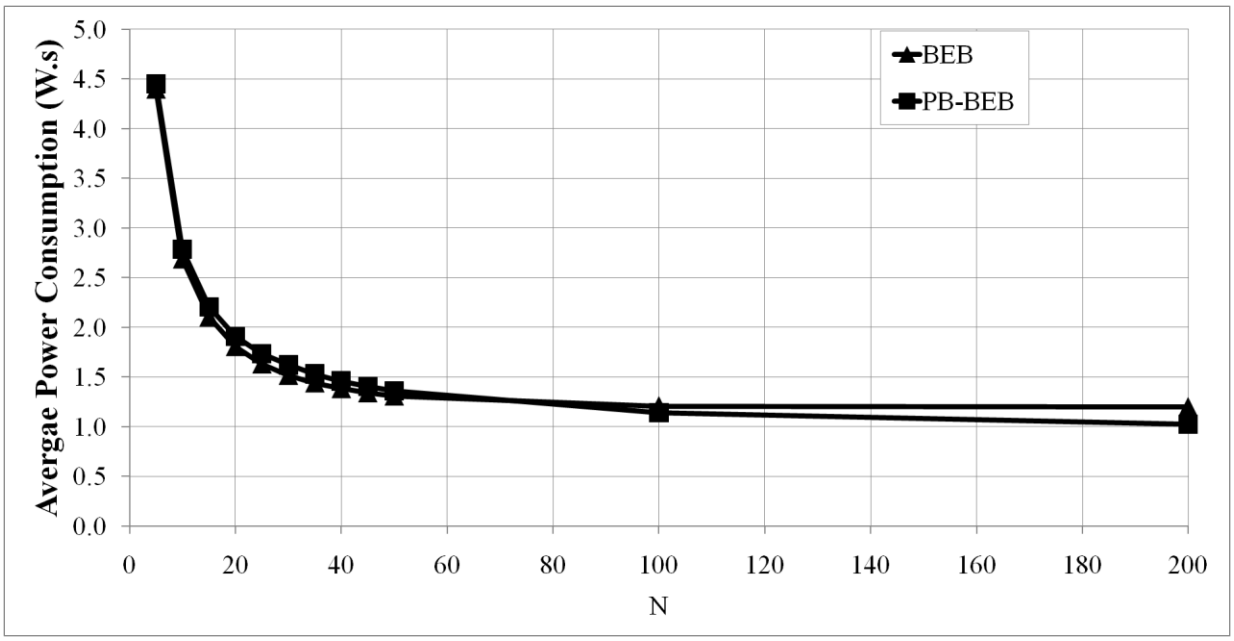

Figure 5-6: Average power consumption under PB-BEB compared to BEB.

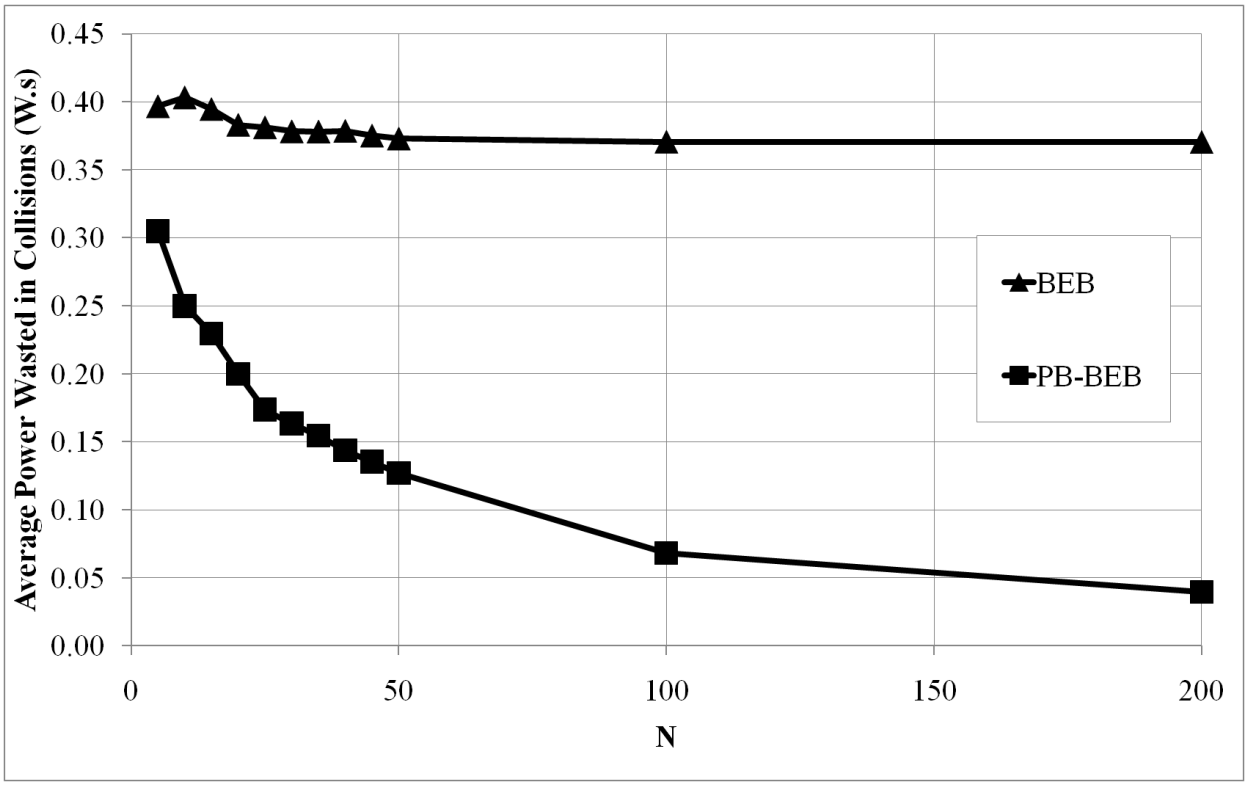

Figure 5-7: Average power wasted in collisions with PB-BEB compared to BEB.

5.3.5 Channel Collision Time

Channel Collision Time (T_{CC}) refers to the proportion of time the channel is busy due to collisions. This parameter measures the percentage of time the channel is being utilized in useless activities. Therefore, T_{CC} should be reduced as much as possible. We illustrate the performance in terms of T_{CC} in Figure 5-8. This figure demonstrates the significant reduction in T_{CC} that PB-BEB can achieve compared to BEB. For example, at N = 100, PB-BEB and BEB result in a T_{CC} of 27.7% and 83.1%, respectively. This means that PB-BEB can considerably reduce the percentage of time during which the wireless channel is wasted due to collisions.

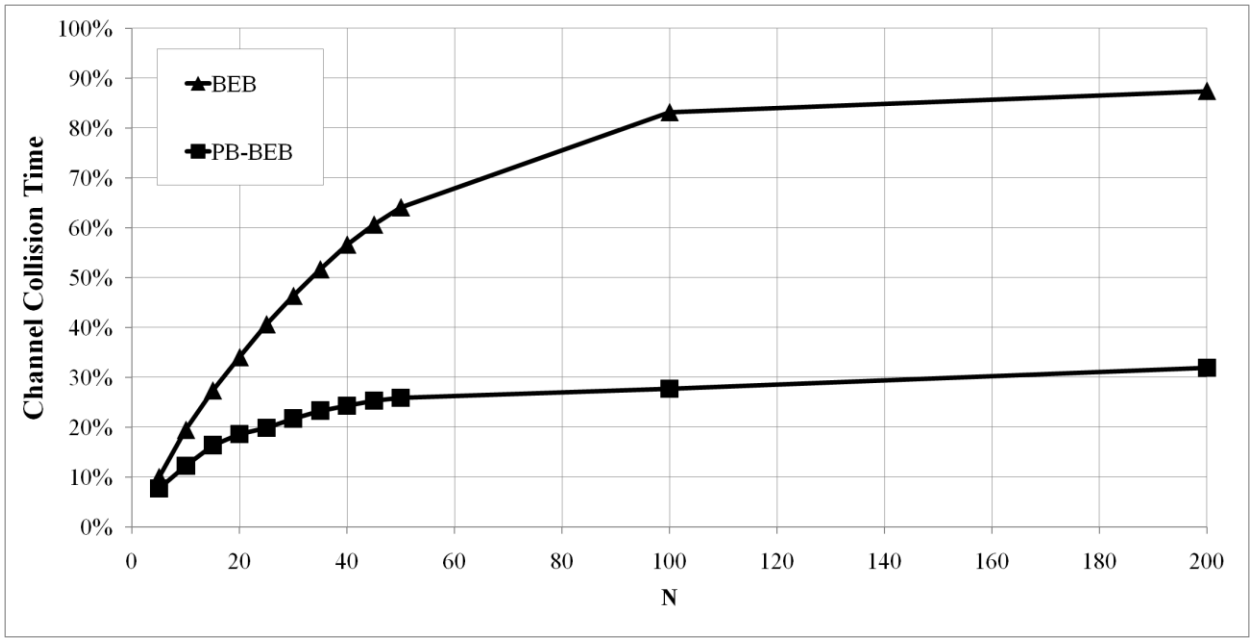

Figure 5-8: Channel collision time with PB-BEB compared to BEB.

5.3.6 Delay

The delay encountered to deliver a packet to its destination is an important metric that gives more insight into the performance of PB-BEB. The delay is measured starting from the instant the packet is available at the node till it is finally received at its destination. That is, the time spent in backoff stages, transmission retries, and CCAs is included in this measurement. In Figure 5-9 we can see that PB-BEB is causing an increase in the delay. At N = 200, PB-BEB increases the delay by 22.3% compared to BEB. This outcome is expected since PB-BEB is introducing extra CCA states, and therefore, the node is forced to spend more time before accessing the medium.

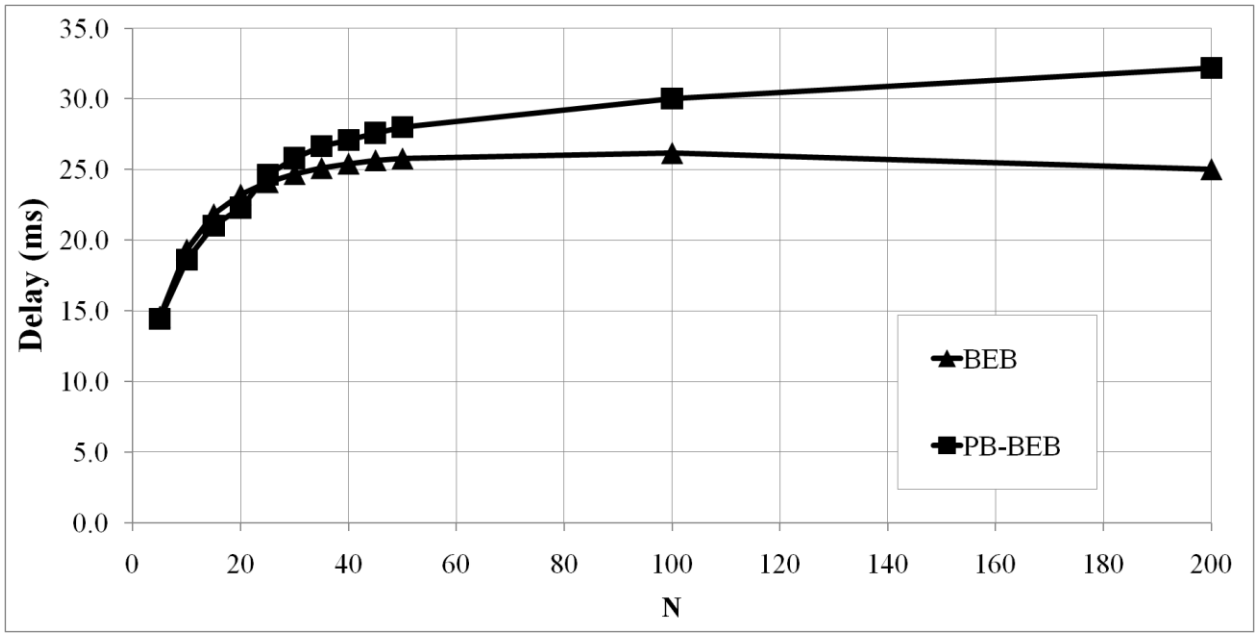

Figure 5-9: Delay under PB-BEB compared to BEB.

5.3.7 Channel Idle Time

Channel idle time (T_{CI}) refers to the proportion of time the channel is free of any packet transmissions of collisions. This metric measures the percentage of time during which all nodes are either in backoff or CCA states. Therefore, T_{CI} should be reduced as much as possible because it indicates that the wireless channel is free of any activity. From the definition of T_{CI} we can see that it is the complement of both U and T_{CC}. That is, we compute T_{CI} as follows:

$$T_{CI} = 1 - U - T_{CC} \qquad (5.6)$$

In Figure 5-10 we show the performance of PB-BEB and BEB in terms of T_{CI}. It comes as no surprise that PB-BEB is resulting in excessive amount of idle time. Again, this behavior is due to that we are introducing extra CCAs with which nodes are encountering additional waiting periods before being able to send their packets. However, although BEB results in lower T_{CI}, it is causing excessive collisions, as is evident in Figure 5-10.

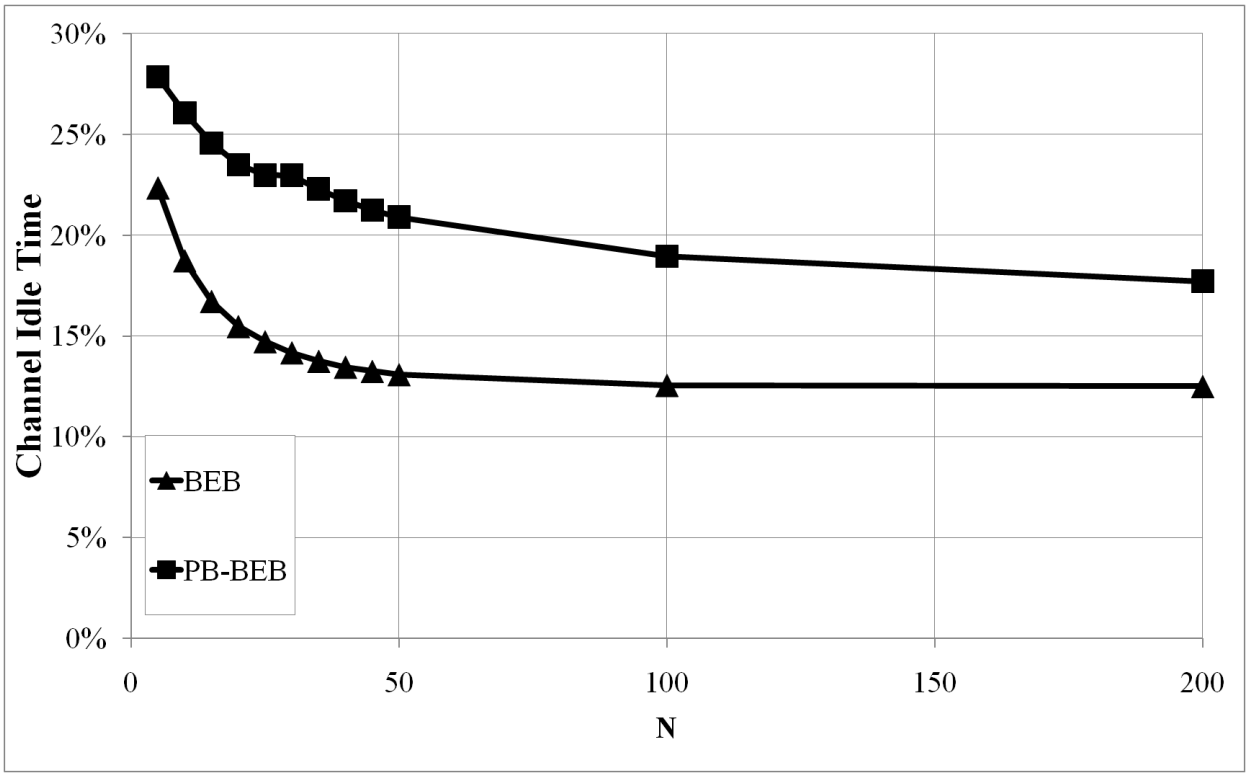

Figure 5-10: Channel idle time with PB-BEB compared to BEB.

5.3.8 Discussions

Our simulation results showed a superior performance for PB-BEB over BEB, except for the delay. The reason behind these enhancements in the performance is that as we preserve the priority of certain nodes, we basically increase their opportunity to access the communication medium. That is, as different nodes commence their channel sensing at different CCAs, the number of nodes contending to access the channel is reduced and therefore the probability of collision is reduced. This is reflected in improved U, R, and T_{CC} as well as reduced power consumption due to collisions. The fact that introducing extra CCAs does not result in increased power consumption is a direct result of making n_{CCA} change probabilistically. This is because of that the second term in Equation (5.1) will be eliminated in case of having relatively low level of collisions. In fact, this term will make PB-BEB highly adaptive to the level of activities in the

network, which is directly related to the size of the network. As the network size increases, the probability of collision increases, and thus the number of CCAs will increase, which plays a role in reducing collisions and therefore enhancing the overall performance.

5.4 Conclusion

In this chapter we have tackled the problem of prioritizing the BEB algorithm in the IEEE 802.15.4 MAC protocol. The problem with BEB is that it treats all the nodes equally without giving any consideration to the repeated channel access failures or transmission failures experienced by some nodes. We have proposed the Priority-Based BEB (PB-BEB) to fill that gap in the design of BEB. In PB-BEB, the number of CCAs is controlled probabilistically according to the collision level over the communication medium. In fact, the major finding in this chapter is that the concept of controlling the parameters of BEB probabilistically is capable of making the algorithm more adaptive. Nodes can tune the number of CCAs they conduct in accordance with the conditions over the communication medium. This finding is confirmed by the simulations that show that PB-BEB is able to outperform BEB in terms of fairness, channel utilization, reliability, average power wasted in collisions, and channel collision time. However, the main drawback of PB-BEB, compared to BEB, is that it leads to increased delay. The latter is an expected outcome since nodes are forced to conduct extra number of CCAs, which delays the transmission of packets.

Chapter 6

Conclusions and Future Research

6.1 Concluding Remarks

In this thesis we have provided an in-depth study of the beacon-enabled IEEE 802.15.4 MAC protocol in the context of Wireless Sensor Networks (WSNs). We have described in details the characteristics of WSNs and the major requirements that drive the design of any protocol or system for these networks. The deployment of IEEE 802.15.4 in WSNs is encouraged by the fact that the specifications it defines for the PHY layer and the MAC sub-layer are in harmony with the unique characteristics of WSNs. We have shed the light on the pros and cons of the IEEE 802.15.4 MAC protocol and the challenges it faces when implemented in WSNs. By delving into an extensive review of the research contributions that put this protocol under its scope, we could draw a high-level idea of what capabilities are missing in the protocol and which aspects need to be enhanced. Based on that, we have pictured a roadmap for designing efficient MAC protocols for the standard. This roadmap has clearly determined that we need to design distributed, adaptive, and power-efficient backoff algorithms to mitigate several problems associated with IEEE 802.15.4 MAC. Also, the roadmap has advocated IEEE 802.15.4-centred solutions that enhance the performance of the standard's MAC protocol while preserving the latter's core functionality and features. The latter methodology, which emerges from the envisioned roadmap, has paved the way for the design of a set of backoff algorithms that managed to achieve promising performance. Although each of these algorithms has been

oriented towards resolving a different problem in IEEE 802.15.4 MAC, we have seen that the development of the third backoff algorithm (PB-BEB) emerges as a natural, accumulative step that builds on top of the methodology followed in the first algorithm (SB-BEB).

The first backoff algorithm we have proposed is the Standby-BEB (SB-BEB). The motivation behind this algorithm is to discover new opportunities to save sensor nodes' power resources. SB-BEB forces nodes to go into a mandatory sleep (or standby (SB)) state after each successful transmission. This way, we could reduce the number of nodes that will be contending to access the wireless medium for the next packet transmission. We have analytically modeled SB-BEB using Markov chain and have validated the model by running extensive simulations. We have found that our analytical model is accurate in predicting the behavior of SB-BEB, and the simulations have confirmed that the algorithm could outperform the standard BEB in terms of power conservation, channel utilization, and communication reliability. We could also draw a relationship between the duration spent in the new standby state and the optimal channel utilization level that can be achieved with the knowledge of the network size. This fact allows sensor nodes to tune SB-BEB with the appropriate duration of standby, once the network size is known, to achieve better utilization of the communication channel.

The second backoff algorithm we have proposed is the Adaptive Backoff Algorithm (ABA). ABA builds on the idea that the SB state can be merged with the backoff periods that are chosen randomly by the contending sensor nodes. Since the SB state is a tunable state that can assist in improving the performance, ABA works on making this tuning more adaptive and directly related to the communication activities over the communication channel. However, the level of these activities is directly related to the size of the network. Therefore, if we could relate the duration of the backoff periods to that level, we would end up with a relationship that

dynamically controls the length of the backoff period based on the network size (which takes the methodology of SB-BEB to the next level). ABA chooses the probability of collision (P_c) to be the factor that realizes the relationship we desire. P_c is directly dependent on the number of nodes in the network, and using it to control the length of the backoff period allows us to adapt the latter in accordance with the activities over the communication channel. ABA has managed to convert the backoff methodology from a deterministic process (in which the backoff period is updated in the same way under all circumstances) to a collision-aware, probabilistic process that is highly adaptive. ABA has been modeled using an accurate Markov chain that has provided accurate prediction of the algorithm's behavior. We have also run extensive simulations that have proven the superiority of ABA over the standard BEB in terms of the power wasted in collisions, channel utilization, and communication reliability. Also, ABA has been found to achieve lower channel idle time and channel collision time.

The third backoff algorithm we have proposed is the Priority-Based BEB (PB-BEB). This algorithm exploits the probabilistic approach followed by ABA to recognize the priorities among the nodes in the network. The probability of collision is used to dynamically increase the number of Clear Channel Assessments (CCAs) beyond the standard defined CCAs. Similar to ABA, the PB-BEB benefits from P_c to associate the CCAs with the size of the network. As a node persistently attempts to access the wireless medium, it should be given higher priority of medium access than other nodes that join the contention at a later time. By allowing that node to conduct extra CCAs and commence their medium sensing from the last CCA they reached, we could preserve the node's priority of access. The simulations we have run showed that PB-BEB could outperform the standard BEB in terms of the short-term fairness among the contending nodes. Also, the performance of PB-BEB has been superior in terms of the power wasted in collisions,

channel utilization, communication reliability, and channel collision time. The only drawback we have observed is that an increase in the end-to-end delay is encountered due to the extra CCAs that a node initiates.

The major conclusion we come to is that employing the collision-aware concept to tune the different parameters of the IEEE 802.15.4 MAC protocol can have a significant effect on the overall performance in the WSNs.

6.2 Future Research

Based on our findings in this thesis, we foresee the following areas to be strong candidates for further future research:

1. Running experiments on sensor platforms that implement our three new backoff algorithms is important to examine their performance in more realistic scenarios. It is an interesting research topic to build a test-bed of these sensors to conduct various research studies.
2. The unsaturated traffic conditions have not been considered in our analytical models. These conditions are realistic for certain WSN-based applications and their implementation can be investigated.
3. It will be an interesting area of research to investigate the impact of uniting both ABA and PB-BEB in one comprehensive protocol.
4. Prioritizing the different types of traffics is still an open area in the context of IEEE 802.15.4. We have focused in this thesis on prioritizing the nodes based on their channel access failures, regardless of the urgency of their traffics. One can take the opportunity to exploit the collision-aware concept in developing a traffic-priority aware IEEE 802.15.4 MAC protocol.

5. The PB-BEB algorithm has been studied through simulations only. It is an important point of research to develop an analytical model to capture the details of this algorithm and predict its behavior.
6. Although our backoff algorithms have been designed without targeting certain applications, it will be interesting to investigate the WSN-based applications that can benefit more from these algorithms.
7. All of the algorithms we have proposed did not tackle the issue of security in the WSNs. It is an implicit assumption that all of the nodes in the network are trustworthy and will not commit any attempts to manipulate the algorithms parameters. However, we have demonstrated in Chapters 1 and 2 the vulnerabilities of the IEEE 802.15.4 standard that can be exploited by intruders and put the overall network at risk. It is an interesting and important research to strengthen the security measures taken by the three backoff algorithms we have proposed in this thesis.

Bibliography

[AKY02] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, vol. 40, no. 8, pp. 104–112, Aug. 2002.

[BAK07] C.R. Baker, K. Armijo, S. Belka, M. Benhabib, V. Bhargava, N. Burkhart, A.D. Minassians, G. Dervisoglu, L. Gutnik, M.B. Haick, C. Ho, M. Koplow, J. Mangold, S. Robinson, M. Rosa, M. Schwartz, C. Sims, H. Stoffregen, A. Waterbury, E.S. Leland, T. Pering, P.K. Wright, "Wireless Sensor Networks for Home Health Care", in Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), vol. 2, pp. 832-837, Niagara Falls, Ontario, Canada, May 2007.

[BHA08] G. Bhatti, A. Mehta, Z. Sahinoglu, J. Zhang, and R. Viswanathan, "Modified Beacon-Enabled IEEE 802.15.4 MAC for Lower Latency," Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'08), pp. 875-880, Nov./Dec. 2008.

[BHU07] V. S. Bhuse, "Lightweight Intrusion Detection: A Second Line of Defence for Unguarded Wireless Sensor networks", PhD dissertation, Western Michigan University, Kalamazoo, Michigan, USA, Jan. 2007.

[BIA96] G. Bianchi, L. Fratta, and M. Oliveri, "Performance Evaluation and Enhancement of the CSMA/CA MAC Protocol for 802.11 Wireless LANs," in Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'96), pp. 392–396, Taipei, Taiwan, Oct. 1996.

[BIA00] G. Bianchi, "Analysis of the IEEE 802.11 Distributed Coordination Function," IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[BOU07] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Localization Systems for Wireless Sensor Networks", IEEE Wireless Communications, special issue on wireless sensor networks, vol. 14, no. 6, pp. 6-12, Dec. 2007.

[CAL00] F. Calì, M. Conti, and E. Gregori, "Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit," IEEE/ACM Transactions on Networking, vol. 8, no. 6, pp. 785-799, Dec. 2000.

[CAL03] E. H. Callaway, "Wireless Sensor Networks – Architectures and Protocols", Auerbach, Boca Raton, Florida, USA, 2003.

[CHA07] Z. Chaczko1, R. Klempous, J. Nikodem, and M. Nikodem, "Methods of Sensors Localization in Wireless Sensor Networks", in Proceedings of the 14th Annual IEEE International Conference and Workshops on the Engineering of Computer-Based Systems (ECBS'07), pp. 145-152, Tucson, Arizona, USA, Mar. 2007.

[CHE06] W. Chen, L. Chen, Z. Chen, and S. Tu "WITS: A Wireless Sensor Network for Intelligent Transportation System", 1st International Multi-Symposiums on Computer and Computational Sciences (IMSCCS '06), vol. 2, pp. 635-641, Jun. 2006.

[CHE07] Z. Chen, C. Lin, H. Wen, and H. Yin, "An Analytical Model for Evaluating IEEE 802.15.4 CSMA/CA Protocol in Low-Rate Wireless Application," in Proceedings of the 21st International Conference on Advanced Networking and Applications Wokshops (AINAW'07), vol. 2, pp. 899-904, Niagara Falls, Ontario, Canada, May 2007.

[DEN04] J. Deng, P. K. Varshney, and Z. J. Hass, "A New Backoff Algorithm for the IEEE 802.11 Distributed Coordination Function," in Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS '04), pp. 215-225, San Diego, California, USA, Jan. 2004.

[DEP11] R. de Paz Alberola and D. Pesch, "Duty Cycle Learning Algorithm (DCLA) for IEEE 802.15.4 Beacon-Enabled Wireless Sensor Networks," Elsevier Ad Hoc Networks, doi:10.1016/j.adhoc.2011.06.006, pp. 217–232, available online: Jul. 7th, 2011.

[FAE08] K. Faez and M. Khanjary, "UTOSPF: A Distributed Dynamic Route Guidance System Based on Wireless Sensor Networks and Open Shortest Path First Protocol", IEEE 8th International Symposium on Wireless Communication Systems (ISWCS '08), pp. 558-562, Oct. 2008.

[FAN09] S. Fang, L. Rong, Q. Xu, and Y. Du, "Analysis of Performance of Unsaturated Slotted IEEE 802.15.4 Medium Access Layer," in Proceedings of Progress In Electromagnetics Research Symposium (PIERS), pp. 348-352, Beijing, China, Mar. 2009.

[FAR10] A. Faridi, M. R. Palattella, A. Lozano, M. Dohler, G. Boggia, L. A. Grieco, and P. Camarda,"Comprehensive Evaluation of the IEEE 802.15.4 MAC Layer Performance With Retransmissions," IEEE Transactions on Vehicular Technology, vol. 59, no. 8, pp. 3917–3932, Oct. 2010.

[FRA11] M. D. Francesco, G. Anastasi, M. Conti, S. K. Das, and V. Neri, "Reliability and Energy-Efficiency in IEEE 802.15.4/ZigBee Sensor Networks: An Adaptive and Cross-Layer Approach," IEEE Journal on Selected Areas in Communictaions, vol. 29, no. 8, pp. 1508 –1524, Sept. 2011.

[GAD10] Y. Gadallah and M. Jaafari, "A Reliable Energy-Efficient 802.15.4-Based MAC Protocol for Wireless Sensor Networks," Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'10), pp. 1-6, Sydney, Australia, Apr. 2010.

[GIL11] M. H. S. Gilani, I. Sarrafi, and M. Abbaspour, "An adaptive CSMA/TDMA hybrid MAC for energy and throughput improvement of wireless sensor networks," Elsevier Ad Hoc Networks, doi:10.1016/j.adhoc.2011.01.005, pp. 1-8, available online: Jan. 11th, 2011.

[GUA06] L. Guang and C. Assi, "Mitigating Smart Selfish MAC Layer Misbehaviour in Ad Hoc Networks," in Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking, and Communications (WiMob '06), pp. 115-123, Montreal, Quebec, Canada, Jun. 2006.

[GUA08] L. Guang and C. Assi, "MAC Layer Misbehavior in Wireless Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 15, no. 4, pp. 5-14, Aug. 2008.

[HA07] J. Y. Ha, T. H. Kim, H. S. Park, S. Choi, and W. H. Kwon, "An Enhanced CSMA-CA Algorithm for IEEE 802.15.4 LR-WPANs," IEEE Communications Letters, vol. 11, no. 5, pp. 461-463, May 2007.

[HEI00] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," in Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS'00), pp. 1-10, Jan. 2000.

[HUA08] Y.-K. Huang, A.-C. Pang, and H.-N. Hung, "An Adaptive GTS Allocation Scheme for IEEE 802.15.4," IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 5, pp. 641-651, May 2008.

[JAI84] R. Jain, D. Chiu, and W. Hawe, "A Quantitative Measure of Fairness and Discrimination for Resource Allocation in Shared Computer Systems", DEC-TR-301, Sept. 1984.

[JAR10] S. Jardosh, P. Ranjan, D. Rawal, "Prioritized IEEE 802.15.4 for Wireless Sensor Networks," Proceedings of the 6th Conference on Wireless Advanced (WiAD'10), pp. 1-7, London, UK, Jun. 2010.

[JIN11] H. Jing and H. Aida, "An Analytical Approach to Optimization of Throughput for IEEE 802.15.4 Slotted CSMA/CA Networks," Proceedings of the 8th Annual IEEE Consumer Communications and Networking Conference (CCNC'11), pp. 1021-1025, Las Vegas, Nevada, USA, Jan. 2011.

[JUN09] C. Y. Jung, H. Y. Hwang, D. K. Sung, and G. U. Hwang, "Enhanced Markov Chain Model and Throughput Analysis of the Slotted CSMA/CA for IEEE 802.15.4 Under Unsaturated Traffic Conditions," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 473-478, Jan. 2009.

[KAC02] O. Kachirski and R. Guha., "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", Proceedings of the IEEE Workshop on Knowledge Media Networking (KMN '02), pp. 153-158, Kyoto, Japan, Jul. 2002.

[KAM08] V. V. Kamath, "An Approach to Increase Channel Utilization in the IEEE 802.11 Networks by Improving Fairness at the Medium Access Control Sub-Layer," Master's thesis, George Mason University, Dec. 2008.

[KAR04] C. Karlof, N. Sastry, and D. Wagner, “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks,” in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys’04), pp. 162-175, Baltimore, MD, Nov. 2004.

[KAR05] H. Karl and A. Willig, “Protocols and Architectures for Wireless Sensor Networks”, John Wiley & Sons, Ltd, 2005.

[KAV10] T. Kavitha and D. Sridharan, “Security Vulnerabilities in Wireless Sensor Networks: A Survey”, Journal of Information Assurance and Security (JIAS), vol. 5, no. 1, pp. 31-44, 2010.

[KHA09] M. Khanafer, M. Guennoun, H. T. Mouftah, **“**WSN Architectures for Intelligent Transportation Systems,” Proceedings of the 3rd IFIP International Conference on New Technologies, Mobility, and Security (NTMS ’09), pp. 1-8, Cairo, Egypt, Dec. 2009.

[KHA10a] B.M. Khan, F.H. Ali, E. Stipidis, “Improved Backoff Algorithm for IEEE 802.15.4 Wireless Sensor Networks,” in Proceedings of the 3rd IFIP Wireless Days (WD’10), pp. 1-5, Italy, Oct. 2010.

[KHA10b] M. Khanafer, M. Guennoun, H. T. Mouftah, “Intrusion Detection System for WSN-based Intelligent Transportation Systems,” Proceedings of IEEE Global Communications Conference (GLOBECOM ’10), pp. 1-6, Miami, Florida, USA, Dec. 2010.

[KHA11a] M. Khanafer, M. Guennoun, H. T. Mouftah, “A Probabilistic, Collision-Aware MAC Protocol for Wireless Sensor Networks,” submitted.

[KHA11b] M. Khanafer, M. Guennoun, H. T. Mouftah, "Priority-Based CCA Periods for Efficient and Reliable Communications in Wireless Sensor Networks," Wireless Sensor Network, vol. 4, no. 2, pp. 45-51, Feb. 2011.

[KHA11c] M. Khanafer, M. Guennoun, H. T. Mouftah, "An Efficient Adaptive Backoff Algorithm for Wireless Sensor Networks," Proceedings of IEEE Global Communications Conference (GLOBECOM '11), pp. 1-6, Houston, Texas, USA, Dec. 2011.

[KHA11d] M. Khanafer, M. Guennoun, H. T. Mouftah, "Adaptive Sleeping Periods in Slotted IEEE 802.15.4 for Efficient Energy Savings: Markov-Based Theoretical Analysis," Proceedings of IEEE International Conference on Communications (ICC '11), pp. 1-6, Kyoto, Japan, Jun. 2011.

[KHA11e] M. Khanafer, M. Guennoun, H. T. Mouftah, "Extending Beacon-Enabled IEEE 802.15.4 to achieve Efficient Energy Savings: Simulation-Based Performance Analysis," Proceedings of the 4th IFIP International Conference on New Technologies, Mobility and Security Program (NTMS '11), pp. 1-5, Paris, France, Feb. 2011.

[KIM10] M. Kim and C.-H. Kang, "Priority-Based Service-Differentiation Scheme for IEEE 802.15.4 Sensor Networks in Nonsaturation Environments," IEEE Transactions on Vehicular Technology, vol. 59, no. 7, pp. 3523-3535, Sept. 2010.

[KO06] J.-G. Ko, Y.-H. Cho, and H. Kim, "Performance Evaluation of IEEE 802.15.4 MAC with Different Backoff Ranges in Wireless Sensor Networks," in Proceedings of the 10thIEEE International Conference on Communications Systems (ICCS'06), pp. 1-5, Singapore, Oct. 2006.

[KOU08] A. Koubâa, A. Cunha, M. Alves, and E. Tovar, "TDBS: A Time Division Beacon Scheduling Mechanism for ZigBee Cluster-Tree Wireless Sensor Networks," Real-Time Systems, vol. 40, no. 3, pp. 321-354, 2008.

[KOK00] C. E. Koksal, H. Kassab, and H. Balakrishnan, "An Analysis of Short Term Fairness in Wireless Media Access Protocols," in Proceedings of the ACM International Conference on Measurements and Modeling of Computer Systems (SIGMETRICS'00), vol. 28, no. 1, pp. 118-119, Santa Clara, California, USA, Jun. 2000.

[KRE07] K. Kredo and P. Mohapatra, "Medium Access Control in Wireless Sensor Networks", Computer Networks, vol. 51, no. 4, pp. 961-994, Mar. 2007.

[KRO08] I. Krontiris "Intrusion Prevention and Detection in Wireless Sensor Networks", PhD dissertation, University of Mannheim, Mannheim, Germany, Nov. 2008.

[LEA07] J. Leal, A. Cunha, M. Alves, and A. Koubaa, "On IEEE 802.15.4/ZigBee to IEEE 802.11 Gateway for the ART-Wise Architecture", IEEE Conference on Emerging Technologies and Factory Automation (ETFA'07), pp. 1388-1391, Sept. 2007.

[LEE08] B.-H. Lee and H.-K. Wu, "Study on Backoff Algorithm for IEEE 802.15.4 LR-WPAN," in Proceedings of the 22nd International Conference on Advanced Information Networking and Applications (AINA'08), pp. 403 - 409, Okinawa, Japan, Mar. 2008.

[LEE09] S.-Y. Lee, Y-S. Shin, J.-S. Ahn, and K-W. Lee, "Performance Analysis of a Non-Overlapping Binary Exponential Backoff Algorithm over IEEE 802.15.4," in Proceedings of the 4th International Conference on Ubiquitous Information Technologies & Applications (ICUT'09), pp. 1-5, Japan, Dec. 2009.

[LI06] B. Li, H. Wang, B. Yan, and C. Zhang, "The Research of Applying Wireless Sensor Networks to Intelligent Transportation System (ITS) Based on IEEE 802.15.4", Proceedings of the 6th International Conference on ITS, pp. 939-942, Jun. 2006.

[LI07] L. Li, L. Yuan-an, and T. Bi-hua "SNMS: An Intelligent Transportation System Network Architecture Based on WSN and P2P Network", China Universities of Posts and Telecommunications, vol. 14, no. 1, pp. 65-70, Mar. 2007.

[LI11] X. Li, C. J. Bleakley, and W. Bober, "Enhanced Beacon-Enabled Mode for Improved IEEE 802.15.4 Low Data Rate Performance," Wireless Networks, Online First, published online: Sept. 10th, 2011.

[LIN04] P. Lin, C. Qiao, and X. Wang, "Medium Access Control with a Dynamic Duty Cycle for Sensor Networks", in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'04), vol. 3, pp. 1534–1539, Atlanta, Georgia, USA, Mar. 2004.

[LUC99] Lucent Technologies, WaveLAN/EC-S User's Guide, http://wireless.ictp.it/ school_2001/docs/specs/orinoco/station_adapter.pdf, Apr. 1999.

[MAO07] G. Mao, B. Fidan, and B. D.O. Anderson, "Wireless Sensor Network Localization Techniques", Computer Networks, vol. 51, pp. 2529-2553, Jan. 2007.

[MAR09] M. Martalò, G. Ferrari, and S. Busanelli, "Markov Chain-Based Performance Analysis of Multihop IEEE 802.15.4 Wireless Networks," Performance Evaluation, vol. 66, no. 12, pp. 722-741, Dec. 2009.

[MAR10] P. D. Marco, P. Park, C. Fischione, and K. H. Johansson, "TREnD: a Timely, Reliable, Energy-efficient and Dynamic WSN Protocol for Control Applications," in

Proceedings of the IEEE International Conference on Communications (ICC'10), pp. 1-6, Cape Town, South Africa, May 2010.

[MER09] M. Meribout and A. Al Naamany, "A Collision Free data Link Layer Protocol for Wireless Sensor Networks and its Application in Intelligent Transportation Systems", Wireless Telecommunications Symposium (WTS'09), pp. 1-6, Apr. 2009.

[MIN02] R. Min, M. Bhardwaj, S. H. Cho, N. Ickes, E. Shih, A. Sinha, A. Wang, and A. Chandrakasan, "Energy-Centric Enabling Technologies for Wireless Sensor Networks", IEEE Wireless Communications, vol. 9, no. 4, pp. 28-39, Aug. 2002.

[MIN07] H. Minooei and H. Nojumi, "Performance Evaluation of a New Backoff Method for IEEE 802.11", Computer Communications, vol. 30, no. 18, pp. 3698–3704, Dec. 2007.

[MIŠ05] J. Mišić and V. B. Mišić, "Access Delay for Nodes with Finite Buffers in IEEE 802.15.4 Beacon Enabled PAN with Uplink Transmissions," Computer Communications, vol. 28, no. 10, pp. 1152-1166, Jun. 2005.

[MOR11] K. Mori, K. Naito, and H. Kobayashi, "Distributed Backoff Mechanism for Traffic Adaptive Active Period Control in Cluster-based IEEE 802.15.4 WSNs," Proceedings of IEEE 73rd Vehicular Technology Conference (VTC 2011-Spring), pp. 1-5, Budapest, Hungary, May 2011.

[MUR04] C. Murthy, B. Manoj, "Ad Hoc Wireless Networks – Architectures and Protocols", Prentice Hall, 2004.

[MUT09] P. S. Muthukumaran, R. de Paz, R. Špinar, and D. Pesch, "MeshMAC: Enabling Mesh Networking over IEEE802.15.4 Through Distributed Beacon Scheduling", In J. Zheng et al. (Eds.): ADHOCNETS 2009, LNICST 28, pp. 561–575, 2009.

[NDI09] E. D. N. Ndih, N. Khaled, G. D. Micheli, “An Analytical Model for the Contention Access Period of the Slotted IEEE 802.15.4 with Service Differentiation,” in Proceedings of IEEE International Conference on Communications (ICC’09), pp. 1-6, Dresden, Germany, Jun. 2009.

[NOH10] K.-C. Noh, S.-Y. Lee, Y.-S. Shin, K.-W. Lee, and J.-S. Ahn, “Performance Evaluation of an Adaptive Congestion Avoidance Algorithm for IEEE 802.15.4,”in Proceedings of the IEEE 13th International Conference on Computational Science and Engineering (CSE’10), pp. 13-19, Hong Kong, China, Dec. 2010.

[PAR10] P. Park, P. D. Marco, C. Fischione, and K. H. Johansson, "Adaptive IEEE 802.15.4 Protocol for Reliable and Timely Communications," in Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN’10), pp. 327-338, Stockholm, Sweden, Apr. 2010.

[POL08] S. Pollin, M. Ergen, S. C. Ergen, B. Bougard, L. Van der Perre, I. Moerman, A. Bahai, P. Varaiya, and F. Catthoor, “Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Medium Access Layer,” IEEE Transactions on Wireless Communications, vol. 7, no. 9, pp. 3359-3371, Sept. 2008.

[PRI01] N. B. Priyantha et al., “The Cricket Compass for Context-Aware Mobile Applications,” in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM’07), pp. 1-14, Rome, Italy, Jul. 2001.

[RAM07]I. Ramachandran, A. K. Das, and S. Roy, “Analysis of the Contention Access Period of IEEE 802.15.4 MAC,” ACM Transactions on Sensor Networks, vol. 3, no. 4, article 4, Mar. 2007.

[RAY06]M. Raya, I. Aad, J.-P. Hubaux, and A. El Fawal, "DOMINO: Detecting MAC Layer Greedy Behaviour in IEEE 802.11 Hotspots," IEEE Transactions on Mobile Computing, vol. 5, no. 12, pp. 1691-1705, Dec. 2006.

[RFM11] RFM ZPM3570 ZigBee Pro Module datasheet, http://www.rfm.com/ products/data/zpm3570-e.pdf, May 2011.

[ROY10] F. Royo, T. Olivares, M. Lopez-Guerrero, L. Orozco-Barbosa, and A. M. Ortiz, "Enhancing Collision Resolution for Large-Scale IEEE 802.15.4 Networks," Proceedings of the 3rd Joint IFIP Wireless and Mobile Networking Conference (WMNC'10), pp. 1-6, Budapest, Hungary, Oct. 2010.

[SAV01] A. Savvides, C.-C. Han, and M. B. Strivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," in Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM'07), pp. 166-179, Rome, Italy, Jul. 2001.

[SER10] P. Serrano, A. Banchs, V. Targon, and J. F. Kukielka, "Detecting Selfish Configurations in 802.11 WLANs," IEEE Communications Letters, vol. 14, no. 2, pp. 142-144, Feb. 2010.

[SEV10] R. Severino, M. Batsa, M. Alves, and A. Koubaa, "A Traffic Differentiation Add-On to the IEEE 802.15.4 Protocol: Implementation and Experimental Validation over a Real-Time Operating System," Proceedings of 13th Euromicro Conference on Digital System Design: Architectures, Methods, and Tools (DSD'10), pp. 501-508, Lille, France, Sept. 2010.

[SHI11] A. Shi, G. Tan, G. Chen, and L. Xu, “An Improved CSMA/CA Protocol for Real-Time Abnormal Events Monitoring,” Journal of Computational Information Systems, vol. 7, no. 9, pp. 3299-3308, Sept. 2011.

[SHU08] M. Shuai, K. Xie, X. Ma, and G. Song “An On-Road Wireless Sensor Network Approach for Urban Traffic State Monitoring”, Proceedings of the 11th International IEEE Conference on Intelligent Transportation Systems (ITSC’08), pp. 1195-1200, Oct. 2008.

[SIM04] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai, K. Frampton, “Sensor Network-Based Countersniper System”, Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys’04), pp. 1-12, Baltimore, MD, USA, Nov. 2004.

[SON03] N.-O. Song, B.-J. Kwak, J. Song, and L. E. Miller, “Enhancement of IEEE 802.11 Distributed Coordination Function with Exponential Increase Exponential Decrease Backoff Algorithm,” in Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference (VTC’03), vol. 4, pp. 2774-2778, Apr. 2003.

[SON07a] L. Song and D. Hatzinakos,“Architecture of Wireless Sensor Networks with Mobile Sinks: Sparsely Deployed Sensors”, IEEE transactions on Vehicular Technology, vol. 56, no. 4, Part 1, pp. 26-1836, Jul. 2007.

[SON07b] L. Song and D. Hatzinakos,“A Cross-Layer Architecture of Wireless Sensor Networks for Target Tracking”, IEEE/ACM Transactions on Networking (TON), vol. 15, no. 1, pp. 145-158, Feb. 2007.

[SUT98] R.S. Sutton and A.G. Barto, “Reinforcement Learning: an Introduction”, Artificial Intelligence, The MIT Press, Cambridge, Massachusetts, 1998.

[TAC07] D. Tacconi, I. Carreras, D. Miorandi, A. Casile, F. Chiti, and Romano Fantacci, “A system Architecture Supporting Mobile Applications in Disconnected Sensor Networks”, Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '07), pp. 833-837, Nov. 2007.

[TAK10] M. Takaffoli, E. Elmallah, and W. Moussa, “Scheduled Access Using the IEEE 802.15.4 Guaranteed Time Slots,” in Proceedings of IEEE International Conference on Communications (ICC’10), pp. 1-5, Cape Town, South Africa, May 2010.

[TUB09] M. Tubaishat, P. Zhuang, Q. Qi, and Y. Shang, “Wireless Sensor Networks in Intelligent Transportation Systems”, Wireless Communications & Mobile Computing, vol. 9, no. 3, pp. 287-302, Mar. 2009.

[VAD08] P. R. Vaddina, www.ifn.et.tu-dresden.de/~marandin/ZigBee/ZigBeeTutorial.html, Apr. 2008, last accessed: Dec. 2011.

[VAL10] M. Valero, A. Bourgeois, and R. Beyah, “DEEP: A Deployable Energy Efficient 802.15.4 MAC Protocol for Sensor Networks,” Proceedings of IEEE International Conference on Communications (ICC’10), pp. 1-6, Cape Town, South Africa, May 2010.

[VAN03] T. van Dam and K. Langendoen, “An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks”, in Proceedings of the 1st ACM International Conference on Embedded Networked Sensor Systems (SenSys’03), pp. 171–180, Los Angeles, California, USA, Nov. 2003.

[WAN11] F. Wang, D. Li, and Y. Zhao, “On Analysis of the Contention Access Period of IEEE 802.15.4 MAC and its Improvement,” Wireless Personal Communications, Online First, published online: Apr. 2011.

[WIJ10] S. Wijetunge, U. Gunawardana, R. Liyanapathirana, “Performance Analysis of IEEE 802.15.4 MAC Protocol for WSNs with ACK Frame Transmission Under Unsaturated Traffic Conditions,” in Proceedings of the 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP’10), pp. 54-60, Brisbane, Australia, Dec. 2010.

[WON10a] C.-M. Wong and W.-P. Hsu, “An Additional Clear Channel Assessment for IEEE 802.15.4 Slotted CSMA/CA Networks,” Proceedings of IEEE International Conference on Communication Systems (ICCS’10), pp. 62-66, Singapore, Nov. 2010.

[WON10b] C.-M. Wong, R.-L. Lai, and I-T. Lai, “An Enhanced Carrier Sensing Algorithm for IEEE 802.15.4 Low-Rate Wireless Sensor Networks,” in Proceedings of IEEE Symposium on Industrial Electronics and Applications (ISIEA’10), pp. 10-15, Penang, Malaysia, Oct. 2010.

[WOO08] S. Woo, W. Park, S.Y. Ahn, S. An, and D. Kim, “Knowledge-Based Exponential Backoff Scheme in IEEE 802.15.4 MAC,” Lecture Notes in Computer Science (LNCS), vol. 5200, pp. 435-444, 2008.

[XIA10] Z. Xiao, C. He, and L. Jiang, “Slot-Based Model for IEEE 802.15.4 MAC with Sleep Mechanism,” IEEE Communications Letters, vol. 14, no. 2, pp. 153-156, Feb. 2010.

[XU01] S. Xu and T. Saadawi, “Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?,” IEEE Communications Magazine, vol. 39. no. 6, pp. 130-137, Jun. 2001.

[YAP05] K.K. Yap, V. Srinivasan, M. Motani, "MAX: Human-Centric Search of the Physical World", in Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems (SenSys'5), pp. 165-179, San Diego, CA, USA, Nov. 2005.

[YED08] K. Yedavalli and B. Krishnamachari, "Enhancement of the IEEE 802.15.4 MAC Protocol for Scalable Data Collection in Dense Sensor Networks," in Proceedings of the 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT'08), pp. 152–161, Berlin, Germany, Apr. 2008.

[YIC08] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless Sensor Network Survey", Computer Networks, vol. 52, no. 12, pp. 2292-2330, Aug. 2008.

[ZHA03] Y. Zhang, W. Lee, and Y.-A. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks", Wireless Networks, vol. 9, no. 5, pp. 545-556, Jan. 2003.

[ZHA04] P. Zhang, C.M. Sadler, S.A. Lyon, M. Martonosi, "Hardware Design Experiences in ZebraNet", in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys'04), pp. 227–238, Baltimore, MD, Nov. 2004.

[ZHA05] M. Zhang, J. Song and Y. Zhang,"Three-Tiered Sensor Networks Architecture for Traffic Information Monitoring and Processing", IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS'05), pp. 2291-2296, Aug. 2005.

[ZHA10] X. Zhao, W. Zhang, W. Niu, Y. Zhang, and L. Zhao, "Power and Bandwidth Efficiency of IEEE 802.15.4 Wireless Sensor Networks," Proceedings of the 7th International Conference on Ubiquitous Intelligence and Computing (UIC'10), pp. 243-251, Xi'an, China, Oct. 2010.

[ZHO08] Y. Zhou, Y. Fang, and Y. Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, vol. 10, no. 3, pp. 6-28, Jan.-Oct. 2008.

[ZHU11a] J. Zhu, Z. Tao, and C. Lv, "Delay Analysis for IEEE 802.15.4 CSMA/CA Scheme with Heterogeneous Buffered Traffic," in Proceedings of the 3rdInternational Conference on Measuring Technology and Mechatronics Automation (ICMTMA'11), vol. 1, pp. 834-845, Shangshai, China, Jan. 2011.

[ZHU11b] J. Zhu, Z. Tao, and C. Lv, "Performance Evaluation of IEEE 802.15.4 CSMA/CA Scheme Adopting a Modified LIB Model," Wireless Personal Communications, Online First, pp. 1-27, published online: Jan. 30th, 2011.

[ZIG06] IEEE Std 802.14.3-2006, September, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). Available online at: www.ieee.org/Standards (Last accessed in Jan. 2012).

[ZOL10] Zolertia Z1 datasheet, http://zolertia.sourceforge.net/wiki/images/e/e8/ Z1_RevC_Datasheet.pdf, Mar. 2010.

Appendix A

The IEEE 802.15.4 Standard

The IEEE 802.15.4 standard has received a considerable attention in the research of WSNs. This is due to its suitability for deployment in these networks. In this chapter we describe the IEEE 802.15.4 MAC protocol standard in details and highlight both its strengths and shortcomings.

The IEEE 802.15.4 standard defines the specifications of the PHY layer and the MAC sub-layer for low-rate personal area networks (LR-WPANs) [ZIG06]. This standard suits the functionality of WSNs as it conforms to their distinguished requirements (like the need to preserve the resources of the sensor nodes [KRE07]). In the rest of this thesis our focus is on the MAC protocol in the IEEE 802.15.4 standard. The standard supports both star and peer-to-peer network topologies. In the star topology, communications among nodes should go through a designated controller node called the PAN coordinator (or the *coordinator* for simplicity). In the peer-to-peer topology, direct communication between nodes is possible, although the coordinator still exists. The standard can operate in a non-bacon-enabled or beacon-enabled mode. In the nonbeacon-enabled mode, the unslotted CSMA-CA mechanism is employed. In this mechanism, a node wishing to transmit a packet backs off for a random period of time and then senses the communication medium. If the latter is found idle, the node sends its packet. Otherwise, the node backs off for another random period and repeats the process. In the beacon-enabled mode utilizes a superframe structure to control the communications over the wireless medium in a way that reduces packet collisions. In this thesis, we concentrate only on the beacon-enabled mode of the

IEEE 802.15.4 standard[1]. In Figure A-1, we depict the general structure of the superframe [VAD08]. As shown in the figure, the superframe is delimited by beacons that the coordinator sends periodically to synchronize the nodes. Also shown are the two main periods that constitute the superframe, namely, the mandatory contention access period (CAP) and the optional contention free period (CFP). The structure of the superframe is specified by two attributes, namely, macBeaconOrder (BO) and macSuperframeOrder (SO). The BO specifies the time period during which the coordinator can communicate the beacon frames. The value of BO is related to the beacon interval (BI) as follows [ZIG06]:

$$\text{for } 0 \leq BO \leq 14$$

$$BI = \text{aBaseSuperframeDuration} \times 2^{BO} \text{ symbols}$$

where aBaseSuperframeDuration is the number of symbols constituting a superframe when the SO is set to zero [ZIG06]. If BO is set to 15, the value of macSuperframeOrder is ignored and beacon frames will not be sent except upon request (see [ZIG06] for more details). The SO specifies the duration of the active portion of the CAP (including the beacon frame). The value of the SO is related to the superframe duration (SD) as follows:

$$\text{for } 0 \leq SO \leq BO \leq 14$$

$$SD = \text{aBaseSuperframeDuration} \times 2^{SO} \text{ symbols}$$

During the CAP, nodes contend among themselves to secure an access to the wireless medium. The slotted CSMA-CA mechanism, that employs the BEB algorithm, is utilized here. The basic functionality of BEB is explained as follows. Before any transmission attempt three parameters are initializes, namely, the Number of Backoff stages (NB), the Contention Window

[1] In the rest of the thesis, the use of the terms *IEEE 802.15.4* or *standard* refer solely to the IEEE 802.15.4 MAC protocol operating in the beacon-enabled mode, except when stated otherwise.

(CW) that designates the number of backoff periods during which the channel is assessed for activities, and the Backoff Exponent (BE) that represents the number of backoff periods waited before assessing the channel's status. These parameters are initialized with zero, two, and macMinBE [1], respectively. After that, the node backs off for a duration chosen randomly from the range [0, 2^{BE}-1].

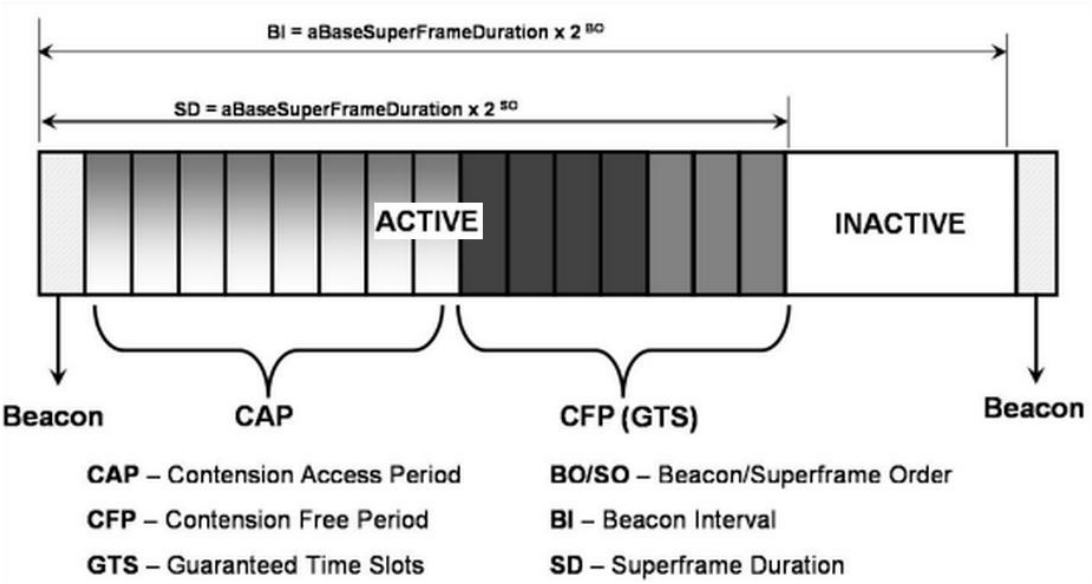

Figure A-1: Superframe structure.

Once the backoff period expires, the node proceeds for two clear channel assessments (CCA1 and CCA2). The number of CCAs is controlled by the parameter CW, such that CCAs are conducted as long as CW is not zero. If either CCA reveals that the medium is busy, CW is reset to two. The CCAs are needed to check whether the wireless medium is free from any activity before commencing a transmission. Packet transmission starts only if the medium is found to be clear during the two CCAs (provided that the remaining time slots in the current CAP are

[1] macMinBE is a MAC attribute defined in the IEEE 802.15.4 standard with a default value of 3.

sufficient to transmit the packet and its ACK. Otherwise, the node has to postpone the packet transmission to the next superframe). However, if either of the CCAs results in finding the medium busy, the value of BE will be increased by one (up to a maximum of macMaxBE[1]) and the node backs off again (that is, NB is increased by one and can reach a maximum of macMaxCSMABackoffs [2]). If BE reaches its maximum, it cannot change unless a successful/failed packet transmission occurs or packet retransmission commences. In that case, BE is reset to macMinBE. The packet will be dismissed if macMaxCSMABackoffs is crossed, and the CSMA-CA mechanism will start the BEB process over. Upon succeeding in transmitting a packet, an acknowledgement (ACK) packet is sent back by the receiver node. If the ACK packet is not received, the node attempts (up to a maximum of macMaxFrameRetries attempts) to retransmit the packet. With every retry, the complete BEB procedure is re-applied. If macMaxFrameRetries [3]is crossed, the packet will be dismissed. It should be mentioned that the basic time unit used by CSMA-CA is the aUnitBackoffPeriod, which we refer to it as time slot or time unit in the rest of the thesis. Figure A-2 shows the flow chart of the CSMA-CA mechanism, including the BEB algorithm, with more details (the flow chart is a modified version of the one available in the standard taken from [ZIG06]).

The CFP is used to support QoS requirements (low-latency, specific data bandwidths...etc). Basically, the coordinator may dedicate a number time slots of the superframe active period for these requirements. These time slots, which constitute the CFP, are called the Guaranteed Time Slots (GTSs). The GTSs start immediately following the CAP, as shown in Figure 2-1. The

[1] macMaxBE is a MAC attribute defined in the IEEE 802.15.4 standard with a default value of 5.
[2] macMaxCSMABackoffs is a MAC attribute defined in the IEEE 802.15.4 standard with a default value of 4.
[3] macMaxFrameRetries is a MAC attribute defined in the IEEE 802.15.4 standard with a default value of 3.

maximum number of GTSs a coordinator can assign is seven, and a single GTS may span more than one time slot. GTSs are assigned to nodes based on their request. Once assigned to a node, the GTS is dedicated to that node and no other node can contend for the medium or transmit a packet during that GTS. Nodes activity during its GTS should be completed before the start of the next GTS or the end of the CFP. In this thesis, we omit the CFP and consider the active period of the superframe to include only the CAP.

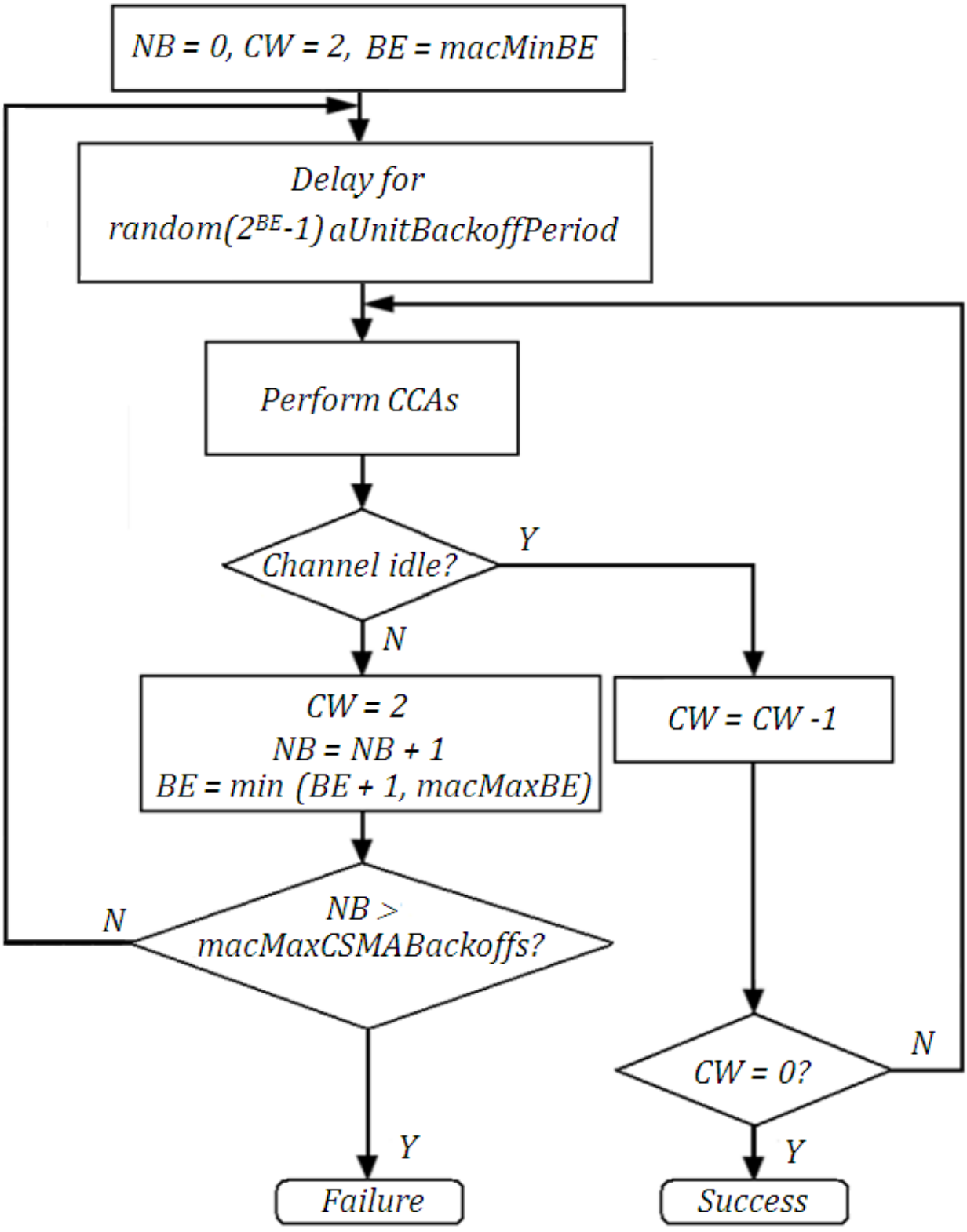

Figure A-2: CSMA-CA mechanism.

Appendix B

Confidence Interval Computation

A confidence interval (CI) is used to quantify the uncertainty in any collected sample of data. It is defined as the estimated range of values within which a generated data lies with a specified probability. This probability is usually set to 95%, which means that we have a confidence of 95% that the collected data lay in a certain (confidence) interval. The end points of the CI are known as the confidence limits. The confidence limits for a *normally* distributed sample of data *n* are computed as follows:

$$\mu \pm z \frac{\sigma}{\sqrt{n}} \qquad \text{(B.1)}$$

where, μ is the mean value of *n*, σ is the standard deviation of *n*, and *z* is the significance level (described shortly). Equation B.1 states that the CI is centered at the mean value of the collected sample data.

The significance level *z* is used to specify the area under the normal distribution curve, shown in Figure B.1, that corresponds to the desired confidence level. Therefore, to find the 95% CI for the shown normal distribution, we need to exclude 5% of the total area under the curve from our computation. This means that we should exclude 2.5% of the area on both sides of the mean μ. Then, we need to find the area that corresponds to 95% of the sample of data *n*. This area can be found using the z-table that is populated with the values of z (or areas) that correspond to the desired confidence level. A partial snapshot of the z-table is shown in Table B-1. To read z from this table, we firstly specify the percentage of the sample data needed to

achieve a 95% of confidence. This corresponds to 1-0.025 = 0.975. Thus, from the table we can see that z = 1.96 (once we locate the 0.975 in the table, we read the first two digits of z from the leftmost column. Then, we get the third digit from the first row of the column where 0.975 is located).

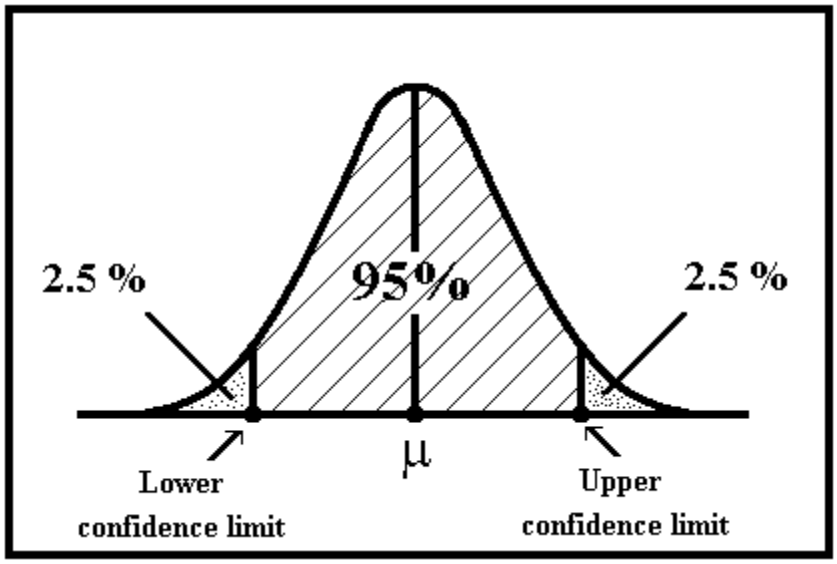

Figure B-1 An illustration of the normal distribution function of the sample data *n*. Only 95% of the area under the curve is considered to compute a CI of 95% centered at the mean value μ.

Table B-0-1: z-table.

z	0	0.01	0.02	0.03	0.04	0.05	0.06	0.07
1.8	0.96407	0.96485	0.96562	0.96638	0.96712	0.96784	0.96856	0.96926
1.9	0.97128	0.97193	0.97257	0.97320	0.97381	0.97441	0.97500	0.97558
2	0.97725	0.97778	0.97831	0.97882	0.97932	0.97982	0.98030	0.98077

In this thesis, we have considered a CI of 95%. For each graph generated, we have run our simulations three independent runs to assert that our results fall within the computed CI. However, our confidence limits have been too small to be observable on the provided graphs.

We hereby exemplify the computation of the CI for the *channel utilization* (U) metric that has been depicted in graphs 3-7 (Chapter 3) in Table B-2. In this table, U_1, U_2, and U_3, correspond to the values of U (at N = 30) generated in the first, second, and third simulation run, respectively.

L_{SB}	Simulation Runs			μ	σ	Confidence Interval	
	U_1	U_2	U_3			Upper Limit	Lower Limit
0	0.5069	0.51253	0.50225	0.507225	0.005145	0.510047	0.504403
50	0.588	0.5789	0.5761	0.581	0.006222	0.584413	0.577587
100	0.61275	0.60305	0.61625	0.610683	0.006838	0.614434	0.606933
150	0.64095	0.63085	0.63875	0.63685	0.005311	0.639763	0.633937
200	0.65193	0.65388	0.65235	0.652717	0.001025	0.653279	0.652154
250	0.65038	0.6538	0.65538	0.653183	0.002556	0.654585	0.651781
300	0.66745	0.65133	0.65588	0.658217	0.008314	0.662777	0.653657
350	0.66445	0.6495	0.6601	0.658017	0.00769	0.662234	0.653799
400	0.6559	0.6552	0.65255	0.65455	0.001767	0.655519	0.653581
450	0.6489	0.65015	0.649	0.64935	0.000695	0.649731	0.648969
500	0.63803	0.6468	0.63863	0.64115	0.004902	0.643839	0.638461

Appendix C

Derivations for Chapter 4

In Chapter 4, Equations (4.27) and (4.28) are used to formulate the reliability (*R*) for a WSN operating the Adaptive Backoff Algorithm (ABA). In this appendix we show the detailed derivations of the probabilities of having *m+1*backoffs and/or *n+1* transmission retries.

Based on Equation (4.27), we can write the following set of equations:

$$z\left(\pi_s + \pi_{B_1} + \cdots + \pi_{B_{m+1}} + \pi_C\right) = \pi_s \quad \text{(C.1)}$$

$$y\left(\pi_s + \pi_{B_1} + \cdots + \pi_{B_{m+1}} + \pi_C\right) = \pi_C \quad \text{(C.2)}$$

$$x\pi_S + x\pi_{B_{m+1}} + x\pi_C = \pi_{B_1} \quad \text{(C.3)}$$

$$x\pi_{B_1} = \pi_{B_2} \quad \text{(C.4)}$$

$$x\pi_{B_m} = \pi_{B_{m+1}} \quad \text{(C.5)}$$

The summation $\pi_s + \pi_{B_1} + \cdots + \pi_{B_{m+1}} + \pi_C$ is equal to 1 because it includes all the states that a node can encounter while attempting to send a packet. Therefore, Equations (C.1) and (C.2) reduce to:

$$z = \pi_s \quad \text{(C.6)}$$

$$y = \pi_C \quad \text{(C.7)}$$

Based on this, Equation (C.3) can now be re-written as follows:

$$xz + x\pi_{B_{m+1}} + xy = \pi_{B_1} \quad \text{(B.8)}$$

From Equations (C.4) and (C.5), and by clearly examining Equation (4.27), we can directly see that $\pi_{B_{m+1}}$can be expressed in terms of π_{B_1} as follows:

$$\pi_{B_{m+1}} = x^m \pi_{B_1} \quad \text{(B.9)}$$

By solving both Equations (C.8) and (C.9) for $\pi_{B_{m+1}}$, we end up with the following expression:

$$\pi_{B_{m+1}} = \frac{x^{m+1}(z+y)}{(1-x)^{m+1}} \quad \text{(B.10)}$$

Based on Equation (4.28), we can write the following set of equations:

$$z\left(\pi_s + \pi_{C_1} + \cdots + \pi_{C_{n+1}} + \pi_B\right) = \pi_s \quad \text{(B.11)}$$

$$x\left(\pi_s + \pi_{C_1} + \cdots + \pi_{C_{n+1}} + \pi_B\right) = \pi_B \quad \text{(B.12)}$$

$$y\pi_S + y\pi_{C_{n+1}} + \pi_{C_1}\pi_B = \pi_{C_1} \quad \text{(B.13)}$$

$$y\pi_{C_1} + \pi_{C_2}\pi_B = \pi_{C_{n+1}} \quad \text{(B.14)}$$

$$y\pi_{C_n} + \pi_{C_{n+1}}\pi_B = \pi_{C_{n+1}} \quad \text{(B.15)}$$

The summation $\pi_s + \pi_{C_1} + \cdots + \pi_{C_{n+1}} + \pi_B$ is equal to 1 because it includes all the states that a node can encounter while attempting to send a packet. Therefore, Equation (C.11) reduces to (C.6) while Equation (C.12) reduces to:

$$x = \pi_B \quad \text{(B.16)}$$

Based on this, Equations (C.13)-(C.15) can now be re-written as follows:

$$yz + y\pi_{C_{n+1}} + x\pi_{C_1} = \pi_{C_1} \quad \text{(B.17)}$$

$$y\pi_{C_1} + x\pi_{C_2} = \pi_{C_{n+1}} \quad \text{(B.18)}$$

$$y\pi_{C_n} + x\pi_{C_{n+1}} = \pi_{C_{n+1}} \quad \text{(B.19)}$$

From Equations (C.18) and (C.19), and by clearly examining Equation (4.28), we can directly see that $\pi_{C_{n+1}}$ can be expressed in terms of π_{C_1} as follows:

$$\pi_{C_{n+1}} = \left(\frac{y}{1-x}\right)^n \pi_{C_1} \quad \text{(B.20)}$$

By solving both Equations (C.17) and (C.20) for $\pi_{C_{c+1}}$, we end up with the following expression:

$$\pi_{C_{n+1}} = \frac{z\left(\frac{y}{1-x}\right)^{n+1}}{1-\left(\frac{y}{1-x}\right)^{n+1}} \qquad (B.21)$$

Finally, by knowing Equations (C.10) and (C.21), Equation (4.26) from Chapter 4, and by noticing that $z = 1 - x - y$, we can formulate R as follows:

$$R = \frac{1}{1 + \frac{(1-x)x^{m+1}}{(1-x^{m+1})(1-x-y)} + \frac{y^{n+1}}{(1-x)^{n+1}-y^{n+1}}}$$