Receiver-Assigned CDMA in Wireless Sensor Networks

Eric Edward Petrosky

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Electrical Engineering

Alan J. Michaels, Chair
Jeffery H. Reed, Co-chair
Joseph M. Ernst
Ryan M. Gerdes

April 30, 2018
Blacksburg, Virginia

Keywords: Wireless Sensor Networks (WSNs), Medium Access Control (MAC), Receiver-Assigned Code Division Multiple Access (RA-CDMA), IEEE 802.15.4

Copyright 2018, Eric Edward Petrosky
A new class of Wireless Sensor Networks (WSNs) is emerging within the Internet of Things (IoT) that features extremely high node density, low data rates per node, and high network dependability. Applications such as industrial IoT, factory automation, vehicular networks, aviation, spacecraft and others will soon feature hundreds of low power, low data rate (1-15 kbps) wireless sensor nodes within a limited spatial environment.

Existing Medium Access Control (MAC) layer protocols, namely IEEE 802.15.4, may not be suitable for highly dense, low rate networks. A new MAC protocol has been proposed that supports a Receiver-Assigned Code Division Multiple Access (RA-CDMA) physical (PHY) layer multiple access technique, which may enable higher network scalability while maintaining performance and contributing additional robustness.

This thesis presents a comparison of the contention mechanisms of IEEE 802.15.4 non-beacon enabled mode and RA-CDMA along with a Matlab simulation framework used for end-to-end simulations of the protocols. Simulations suggest that IEEE 802.15.4 networks begin to break down in terms of throughput, latency, and delivery ratio at a relatively low overall traffic rate compared to RA-CDMA networks. Results show that networks using the proposed RA-CDMA multiple access can support node densities on the order of two to three times higher than IEEE 802.15.4 within the same bandwidth.

Furthermore, features of a new MAC layer protocol are proposed that is optimized for RA-CDMA, which could further improve network performance over IEEE 802.15.4. The protocol’s simple and lightweight design eliminates significant overhead compared to other protocols while meeting performance requirements, and could further enable the deployment of RA-CDMA WSNs.
Factories, automobiles, planes, spacecraft and other systems in the future will require hundreds of sensors within a relatively small area for data gathering purposes. The sensors, which form Wireless Sensor Networks (WSNs), must have some method of wireless communication that allows each of them to transmit information when needed without obstructing other sensors’ transmissions. Wireless communication protocols provide a method for doing so. Some recognizable examples of wireless communication protocols include Bluetooth, WiFi, 3G and LTE.

For WSNs in the future, the industry’s leading candidate protocol is called IEEE 802.15.4, but it may not be most suitable because it is known to break down as large amounts of sensors are added to its networks. Because of this, a new protocol has been proposed around a channel sharing technique called Receiver-Assigned Code Division Multiple Access (RA-CDMA), which uses a different strategy to efficiently distribute network resources among sensors.

This work analyzes the differences between IEEE 802.15.4 and RA-CDMA, focusing specifically on how each protocol allows sensors to transmit without conflicting with one another. A simulation framework is introduced for complete simulations of each protocol. The result of the simulations shows that IEEE 802.15.4 breaks down in dense sensor networks. RA-CDMA, however, is able to support very large networks, on the order of two to three times the size of IEEE 802.15.4. This result could be an enabling technology for large wireless sensor networks in the future.

Additionally, a new protocol optimized for RA-CDMA is presented. Its simple design could further enable the deployment of RA-CDMA WSNs.
Acknowledgments

I must offer sincere gratitude to my numerous advisors, mentors, colleagues, and friends at the Hume Center for National Security and Technology, especially Dr. Alan Michaels and Dr. Joseph Ernst. Their guidance has been instrumental to the completion of this work, and it has been a true pleasure to be associated with the Hume Center for the last several years. I also send thanks to Devin Ridge, Joe Ziegler, and the rest of the team for the countless enlightening technical discussions. Lastly, I thank my parents and family, for without their endless support and encouragement I could not have accomplished this.
Contents

List of Figures viii

List of Tables xi

1 Introduction 1

1.1 Motivation .............................................. 2
1.2 Scope .................................................. 3
1.3 Contributions and Publications ............................ 4

2 Multiple Access and Medium Access Control in IoT 7

2.1 Multiple Access in WSNs ................................. 8
2.1.1 ALOHA .............................................. 9
2.1.2 Carrier Sense Multiple Access .......................... 10
2.1.3 Time Division Multiple Access .......................... 12
2.1.4 Frequency Division Multiple Access ....................... 13
2.1.5 Code Division Multiple Access .......................... 15
2.2 MAC Protocols for WSNs ................................. 17
2.3 Receiver-Assigned CDMA ................................. 20
3 Network Scalability Comparison of IEEE 802.15.4 and RA-CDMA

3.1 Contention Processing ........................................ 25
   3.1.1 IEEE 802.15.4 Contention Processing .................... 25
   3.1.2 RA-CDMA Contention Processing .......................... 27
   3.1.3 Multiple Access Performance Metrics ..................... 31

3.2 Simulation Frameworks ........................................ 33
   3.2.1 IEEE 802.15.4 Simulation Framework ..................... 34
   3.2.2 RA-CDMA Simulation Framework ......................... 45

3.3 Simulation Results ........................................... 54
   3.3.1 IEEE 802.15.4 vs. RA-CDMA Results .................... 55
   3.3.2 IEEE 802.15.4 Network Behavior ...................... 59
   3.3.3 RA-CDMA Network Behavior ............................... 60

3.4 Analysis ..................................................... 61
   3.4.1 IEEE 802.15.4 Analysis ................................. 62
   3.4.2 RA-CDMA Analysis ...................................... 63

4 A MAC Layer Protocol for RA-CDMA 65

4.1 Network Topology .............................................. 65

4.2 Frame Format .................................................. 67

4.3 Edge Node Profiles ............................................ 69
4.4 Error Handling ................................................................. 69
4.5 Network Formation .......................................................... 71

5 Conclusions and Future Work .............................................. 73

Bibliography ........................................................................... 75
## List of Figures

1.1 Focus of this work is a cloud of randomly distributed wireless sensors (black circles) that transmit to a central data gathering sink (open circle) over a shared channel .................................................. 4

2.1 Generalized Carrier Sense Multiple Access with Collision Avoidance Algorithm .................................................. 11

2.2 Time Division Multiple Access ................................................................. 12

2.3 Frame Repetition of Time Division Multiple Access ................................................................. 13

2.4 Frequency Division Multiple Access ................................................................. 14

2.5 Code Division Multiple Access ................................................................. 16

2.6 High Level Code Division Multiple Access System Diagram ................................................................. 16

2.7 Comparison of IoT Multiple Access Techniques – Red is poor, Green is satisfactory, Blue is excellent [45] ................................................................. 17

2.8 RA-CDMA Code Assignment Scheme .................................................. 21

3.1 IEEE 802.15.4 CSMA-CA Contention Mechanism .................................................. 26

3.2 RA-CDMA physical layer in the case of nominal SINR (left) and low SINR (right) caused by other transmitters .................................................. 28

3.3 Timing of a sample eight-finger RAKE Receiver showing properly received packets in green and dropped packets due to overload in red\(^1\) .................................................. 29
3.4 High-level diagram of the LRWPAN library representing function calls as tabbed arrows - blue text represents classes or inherited classes, green represents class functions, and red represents methods within functions 35

3.5 Interface between PHY and MAC layer illustrating step duration 38

3.6 Corrections made to the LRWPAN Library to produce behavior conforming with IEEE 802.15.4 protocol 41

3.7 Sample 802.15.4 time plots showing a collision at time 290 ms 43

3.8 QPSK bit error rate curve used to map $\frac{c}{N_0}$ to BER 50

3.9 Sample RA-CDMA time plots showing simultaneous transmissions with no collisions 54

3.10 Throughput Comparison of IEEE 802.15.4 and RA-CDMA 56

3.11 Packet Delivery Ratio Comparison of IEEE 802.15.4 and RA-CDMA 57

3.12 Average Packet Latency Comparison of IEEE 802.15.4 and RA-CDMA 58

3.13 Total Dropped Packets and Causes in IEEE 802.15.4 59

3.14 Avg Number of Simultaneous Transmitters and Corresponding BER and PER 60

3.15 Total Dropped Packets and Causes in RA-CDMA 61

4.1 Star-of-stars hierarchical topology supported by the proposed MAC protocol 66

4.2 Relationship of edge nodes with primary and secondary data concentrators, showing redundancy 67

4.3 Comparison of frame formats with gray area showing eliminated fields 68

4.4 Proposed MAC Error Handling Flowchart 70
4.5 Network formation sequence chart
List of Tables

2.1 Pros and cons list for ALOHA .............................................. 10
2.2 Pros and cons list for CSMA-CA ........................................... 11
2.3 Pros and cons list for TDMA ................................................. 13
2.4 Pros and cons list for FDMA ............................................... 15
2.5 Pros and cons list for CDMA ............................................... 17

3.1 List and descriptions of tracking and counting variables used to pull results from, verify and debug the simulation framework ........................................... 40
3.2 Signal-to-interference-plus-noise ratio corresponding to the number of users transmitting simultaneously in an RA-CDMA channel, according to Equations 3.7 and 3.10 ......................................................... 49
3.3 Packet error rates corresponding to the number of users transmitting simultaneously in an RA-CDMA channel, according to Equation 3.11 ......................................................... 51
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>BER</td>
<td>Bit Error Rate</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>CCA</td>
<td>Clear Channel Assessment</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>CSMA</td>
<td>Carrier Sense Multiple Access</td>
</tr>
<tr>
<td>CSMA-CA</td>
<td>Carrier Sense Multiple Access with Collision Avoidance</td>
</tr>
<tr>
<td>CSMA-CD</td>
<td>Carrier Sense Multiple Access with Collision Detection</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear to Send</td>
</tr>
<tr>
<td>DAMA</td>
<td>Demand Assignment Multiple Access</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame Check Sequence</td>
</tr>
<tr>
<td>FDMA</td>
<td>Frequency Division Multiple Access</td>
</tr>
<tr>
<td>FEC</td>
<td>Forward Error Correction</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>FFT</td>
<td>Fast Fourier Transform</td>
</tr>
<tr>
<td>FPGA</td>
<td>Field Programmable Gate Array</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ISM</td>
<td>Industrial, Scientific, Medical</td>
</tr>
<tr>
<td>IVWSN</td>
<td>Intra-Vehicular Wireless Sensor Network</td>
</tr>
<tr>
<td>kbps</td>
<td>Kilobits Per Second</td>
</tr>
<tr>
<td>LEACH</td>
<td>Low Energy Adaptive Clustering Hierarchy</td>
</tr>
<tr>
<td>LoRaWAN</td>
<td>Long Range Wide Area Network</td>
</tr>
<tr>
<td>LPD</td>
<td>Low Probability of Detection</td>
</tr>
<tr>
<td>LPE</td>
<td>Low Probability of Exploitation</td>
</tr>
<tr>
<td>LPI</td>
<td>Low Probability of Intercept</td>
</tr>
<tr>
<td>LR-WPAN</td>
<td>Low Rate Wireless Personal Area Network</td>
</tr>
<tr>
<td>MAI</td>
<td>Multiple Access Interference</td>
</tr>
<tr>
<td>MPDU</td>
<td>MAC Protocol Data Unit</td>
</tr>
<tr>
<td>NB-IoT</td>
<td>Narrowband Internet of Things</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiple Access</td>
</tr>
<tr>
<td>OQPSK</td>
<td>Offset Quadrature Phase Shift Keying</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PAPR</td>
<td>Peak-to-Average Power Ratio</td>
</tr>
<tr>
<td>PER</td>
<td>Packet Error Rate</td>
</tr>
<tr>
<td>QPSK</td>
<td>Quadrature Phase Shift Keying</td>
</tr>
<tr>
<td>RA-CDMA</td>
<td>Receiver-Assigned Code Division Multiple Access</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indication</td>
</tr>
<tr>
<td>RTS</td>
<td>Request to Send</td>
</tr>
<tr>
<td>S-MAC</td>
<td>Sensor-MAC</td>
</tr>
<tr>
<td>SINR</td>
<td>Signal-to-Interference-plus-Noise Ratio</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-Noise Ratio</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>WAIC</td>
<td>Wireless Avionics Intra-Communications</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

The Internet of Things (IoT) refers to the growing amount of consumer and industry devices with some connection to the outside world, primarily via wireless communication networking. The possibilities of IoT are near endless as wireless device technology becomes ever-increasingly affordable and available. Some predict that the IoT may encompass 125 billion devices by the year 2030 [17], further supporting the idea of a massive, pervasive, all-inclusive network that connects billions of commonplace devices.

A broad category that falls within the IoT is Wireless Sensor Networks (WSNs). A WSN is described as a wirelessly connected group of sensor nodes used to gather information. The applications of WSNs in both traditional and cutting edge systems are extremely broad, and growing even more so as technology advances. Current WSN applications include everything from animal tracking [19] to military threat detection [40].

Practically any wired system that uses sensors to gather data is subject to replacement by a WSN. Specific examples include automobiles, planes, factories, and spacecraft, all of which are the subject of active areas of research to incorporate WSNs into each system [8, 18, 24, 44]. But the applications of WSNs will surely continue to grow into new fields that are not even currently realized. All industries rely on sensors in some form, and WSNs have the potential to revolutionize how sensors are integrated into systems.

Despite the wide variety of modern WSNs, a general trend towards common network charac-
teristics is emerging in the designs of future WSNs. First, the size and density of WSNs are growing. Not only are sensors being incorporated into more systems, but existing systems are having more sensors incorporated into their designs as well. Second, the sensors within these networks are tending to require relatively low data rates. Typical sensor applications are often gradually changing data or change detection, both of which only require sparse bursts of data. Third, the security and robustness of WSNs is becoming paramount as they are being relied on for more and more. The nominal network performance of future WSNs in automobiles, aircraft, and autonomous systems will be directly responsible for peoples’ lives.

1.1 Motivation

Perhaps the single most limiting constraint on modern WSN size and density is multiple access, which is the strategy used by a network protocol to allocate physical channel capacity amongst the sensors in a network. In other words, multiple access techniques define how transmitters in a network share a common medium. Multiple access becomes a particularly difficult problem to solve when designing WSNs in the near future, when very large networks will be desired and potentially dozens or hundreds of devices will seek to transmit on a common radio frequency (RF) channel. When considering such a dense network, the importance of effective channel sharing becomes apparent.

Multiple access in dense WSNs is clearly a serious concern. A paper investigating future Intra-Vehicular WSNs (IVWSNs), which are aimed at replacing many of the dozens of wired sensors in automobiles with wireless sensor nodes, notes, “the design of a scalable network for IVWSNs will be a big challenge,” pointing specifically to the scalability of existing multiple access techniques [35]. Likewise, an overview paper on Wireless Avionics
1.2. Scope

Intra-Communications (WAIC), a WSN concept with a similar goal in commercial airliners, presents the many possible options for multiple access in such WSNs, but also highlights severe limitations of even the most promising techniques [36].

The overall motivation behind this work is that there is no consensus on the most effective multiple access technique to be used in dense WSNs in the future. Simply put, this work aims to contribute to the discussion, along with giving a concrete analysis that suggests revisiting code division multiple access (CDMA) as a dominant fixture in industrial IoT.

1.2 Scope

There are many shapes and sizes of WSNs, almost as diverse as the applications in which they are featured. Despite a central theme of low data rates and high node densities, a wide range of network topologies, architectures, protocols, and communication techniques exist. Potential problems and proposed solutions vary accordingly. In order to reasonably constrain the work presented herein, a subset of WSN topologies and architectures will be focused upon. This work focuses on a single physical channel using a star topology, depicted in Figure 1.1, which is the very basic building block of a WSN. This scope definition excludes the consideration and discussion of mesh routing techniques, multi-hop networks, and multi-frequency channel handling. Though these topics are noteworthy, analysis and evaluation of a single channel star architecture is expected to be most relevant to future WSNs and may be extrapolated reasonably to mesh and channelized networks efficiently, hence the constraint to these types of networks. In order to properly evaluate the performance of single channel star networks, three performance metrics are selected: (1) total network throughput, (2) average packet latency, and (3) packet delivery ratio. These cumulative statistics wholly convey overall network performance and are further explained in Section 3.1.3.
In addition to constraining the types of network architectures discussed, this work is limited to discussion of the bottom two layers of the OSI telecommunications model, the Physical (PHY) layer and the data link layer. The PHY layer defines the protocol used for data transmission over the physical medium, such as specific modulation types and packet preambles for wireless communication. The data link layer contains the Medium Access Control (MAC) sublayer, which is primarily responsible for channel sharing, routing, frame formatting, and much more [22]. Multiple access is the focus of this work because it is the primary constraint to network scalability. PHY layer attributes, such as modulation and other physical signal characteristics, are not of interest and are not evaluated. Though multiple access can possibly fall under the PHY layer in some unique schemes, it is generally part of the MAC layer, and the scope of work presented herein is generally limited to the MAC layer.

1.3 Contributions and Publications

To provide background knowledge necessary for this work, Chapter 2 presents a broad overview of existing multiple access techniques and MAC layers currently in use in WSNs. A focus is given to those that are prime candidates for use in IoT networks, featuring appli-
cability to low power devices. In the same chapter, the concept of receiver-assigned CDMA in low power networks is introduced and explained. While RA-CDMA is not necessarily a novel concept in itself, its application to low power WSNs and some specific techniques used for its implementation have not previously been publicly proposed and analyzed.

Chapter 3 presents the concept, methodology, implementation, and results of a detailed comparison of RA-CDMA to the leading existing WSN MAC layer candidate, IEEE 802.15.4. The results of the comparison reinforce previous research regarding the behavior of IEEE 802.15.4 in high-traffic and high-contention networks. They also demonstrate superior performance of RA-CDMA in dense WSNs.

Chapter 4 further develops the concept of RA-CDMA in future WSNs, presenting features of a MAC layer protocol that is optimized for RA-CDMA as a multiple access technique. By constraining a WSN design with a few core assumptions, MAC overhead and overall network performance can be greatly improved.

In Chapter 5, final conclusions of this work are discussed, along with future work that can advance RA-CDMA from a conceptual design into a full hardware implementation and ultimately to productization.

The work presented in this thesis has produced three peer-reviewed publications, listed in the bibliography as [30], [31], and [32]. They are cited and briefly annotated below.

This letter discusses the contention processing and multiple access of IEEE 802.15.4 and RA-CDMA, provides details of a Matlab simulation framework used to compare the network scalability of each, and presents simulation results that show superior maximum network scalability of RA-CDMA.


This paper introduces Receiver-Assigned CDMA in the context of low power WSNs and provides motivation towards its use. An overview of existing multiple access techniques is given, followed by a technical introduction of RA-CDMA including why it is expected to outperform other techniques. Features of a new MAC layer design optimized for RA-CDMA are proposed and discussed, including topology constraints, redundancy, frame formatting, device profiles, error handling, and network formation sequences.


Accepted to IJITN as an extension to the WTS 2018 conference paper of the same title listed above, this paper presents similar concepts but includes extended discussion on current MAC layer protocols and multiple access techniques. The concept of RA-CDMA is also more thoroughly introduced and discussed.
Chapter 2

Multiple Access and Medium Access Control in IoT

Multiple access and medium access control are perhaps two of the most limiting factors in the development of the IoT, and are certainly so for dense WSNs. Simply stated, current multiple access technology does not seem to have the ability to support the large number of low duty cycle sensors that are desired in future WSNs. This theory is investigated in Section 2.1 through an overview of currently deployed state-of-the-art multiple access techniques for low power devices. By focusing on all potential existing solutions, the necessity of new techniques becomes apparent.

In addition to presenting current multiple access techniques, this chapter reviews several Medium Access Control (MAC) layer protocols currently in use on IoT devices and thus in consideration for dense WSNs. Section 2.2 lists and annotates these protocols. A brief analysis is made to compare all existing solutions, culminating with a discussion on the most likely existing MAC protocol candidate to eventually be deployed in future WSNs.

Motivated by the findings of Sections 2.1 and 2.2, Section 2.3 presents an overview and technical details of Receiver-Assigned CDMA (RA-CDMA), a newly proposed multiple access technique aimed to satisfy the technical requirements of future WSNs while also providing benefits over existing solutions.
Definitions

Given the extensive discussion of WSN topology and architecture in this work, common vocabulary terms should be clarified. The terms Personal Area Network (PAN) coordinator, data concentrator, access point, gateway, and gateway node are all used to refer to a central data gathering sink as shown in Figure 1.1. For the purposes of this thesis, these terms may be used interchangeably. Likewise, the terms sensor, sensor node, node, device, end device, and edge node all refer to a single sensor device in the cloud of sensors.

Additional clarification should be stated regarding the inferred meaning of the terms MAC layer, multiple access, and contention processing. The MAC layer, defined as one of the two sub-layers that form the data link layer in a communications network, falls directly above the physical (PHY) layer in the OSI telecommunications model. The MAC layer’s general responsibilities include packet framing for data, successful and correct data transmission, and prevention of collisions in time, space, or frequency [22]. Medium access refers specifically to the strategy used by a network to distribute physical channel capacity amongst its nodes, which can fall under the MAC layer, PHY layer, or both, as in a cross-layer architecture. Contention processing is the set of rules implemented around the multiple access technique to resolve any conflicts. This terminology is assumed throughout the chapters in this work.

2.1 Multiple Access in WSNs

One of the most difficult challenges when choosing or designing a protocol for low power devices is the selection of an appropriate multiple access technique. In general, multiple access refers to the strategy used by a protocol to give multiple devices the ability to communicate over and share a common channel. In other words, it defines the rules and guidelines put
in place to ensure network devices can efficiently communicate when necessary and without obstructing other devices.

There are a multitude of multiple access protocols in existence today, each with specific pros and cons when applied to various network architectures. This section categorizes the most commonly used multiple access techniques in low power WSNs and present general summaries of each. Also, general pros and cons are presented for each technique, with a focus on implementation in low power WSNs.

### 2.1.1 ALOHA

ALOHA is essentially true random access, perhaps the simplest form of multiple access. All devices in a network are allowed to transmit at any time, whenever necessary. There is no scheduling or coordination between nodes, so collisions between multiple transmissions become increasingly common as overall network traffic increases. As such, ALOHA contention mechanisms typically require acknowledgements or some form of feedback to guarantee packet delivery. In the case of a packet failure, or lack of acknowledgment, a random backoff period is waited before another transmission [33]. This strategy has inherent tradeoffs in WSNs, listed in Table 2.1.

Slotted ALOHA is a popular variant that assigns a common schedule for the beginning of packet transmissions as an attempt to limit packet overlapping and collisions. Still, due to a large likelihood of packet collisions, especially in high contention networks, ALOHA and slotted ALOHA are not viable multiple access options for dense WSNs.
Table 2.1: Pros and cons list for ALOHA

<table>
<thead>
<tr>
<th>ALOHA Tradeoffs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pros</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cons</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

2.1.2 Carrier Sense Multiple Access

Carrier Sense Multiple Access (CSMA) is a structured form of random access over a common channel. It defines a simple algorithm for determining when a device can transmit without obstructing other transmissions, shown in Figure 2.1. Prior to transmitting a packet, a device performs a clear channel assessment (CCA), which senses the power level of the shared channel to determine if any other device is currently transmitting. If the channel is available, the device transmits its packet. But if the channel is being used, the device pauses for some random period of time before performing a CCA again [1].

There are two main variants of CSMA that aim to improve performance, Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA), used primarily on wireless networks, and Carrier Sense Multiple Access with Collision Detection (CSMA-CD), used on wired networks. Both variants follow the same general algorithm, but some uncertainty is inherent to wireless networks, so CSMA-CA networks cannot guarantee accurate CCAs. Because CSMA-CA is the most applicable to wireless networks, it is the focus of this section.

Generally, CSMA-CA is extremely effective at providing fair and fast channel access to devices in networks operating below channel capacity [10]. It is the multiple access technique used by several industry standard MAC layer protocols, such as IEEE 802.11 and IEEE 802.15.4, because of its effectiveness.

Even though it is widely implemented, CSMA-CA is still susceptible to collisions and the hidden node problem [15]. This is because the CSMA-CA technique makes two key as-
assumptions: (1) a sensing node is within range of all other nodes in the network, so that the sensing node’s physical channel is identical to the PAN Coordinator’s channel, and (2) the CCA is accurate and the channel will not change in the time between a CCA and the transmission of a packet. Provided that these assumptions are correct, the CSMA-CA algorithm generally performs very effectively. However, in a real, physical channel, neither of these two assumptions can be presumed. Collisions occur any time more than one device is transmitting simultaneously, which occurs if two devices perform simultaneous CCAs. Also, the hidden node problem causes collisions when one node is out of range of another node in the same network, so its CCA cannot detect the other node’s transmissions. The effects of these problems are amplified as the number of nodes in a CSMA-CA network increases, up to the point that they cripple overall performance. Table 2.2 presents pros and cons of CSMA-CA in low power WSNs.

![Diagram of CSMA-CA Algorithm](image)

**Figure 2.1: Generalized Carrier Sense Multiple Access with Collision Avoidance Algorithm**

<table>
<thead>
<tr>
<th><strong>CSMA-CA Tradeoffs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pros</strong></td>
</tr>
<tr>
<td><strong>Cons</strong></td>
</tr>
</tbody>
</table>

Table 2.2: Pros and cons list for CSMA-CA
2.1.3 Time Division Multiple Access

Time Division Multiple Access (TDMA) networks divide channel capacity using assigned timeslots within which devices can utilize the entire channel. As shown in Figure 2.2, devices must transmit within their assigned slot(s), which is offset in time from other users’ slots by a short guard time to prevent errant overlaps. Figure 2.3 demonstrates the duration of a single timeslot, which is grouped with other nodes’ timeslots into a frame length that typically contains at least as many timeslots as nodes in the network. Frames are repetitive and are often begun with a broadcast beacon to denote the start of a frame.

TDMA scheduling has the inherent detriment of latency versus scalability tradeoff. With assigned timeslots, a given sensor node must wait until its assigned slot to transmit a packet, which could be a relatively long amount of time. Larger networks require more timeslots, which means more time between a given node’s slot and longer packet latencies. Demand Assignment Multiple Access (DAMA) is a technique popular in satellite communication that attempts to mitigate the latency problem by only issuing timeslots to active users, but introduces additional overhead and complexity not desired in low power WSNs. Pros and cons of TDMA are listed in Table 2.3.

![Figure 2.2: Time Division Multiple Access](image-url)
2.1.4 Frequency Division Multiple Access

Frequency Division Multiple Access (FDMA) allocates a specific frequency channel to each device in a network to communicate unobstructed within, shown in Figure 2.4. Between two adjacent channels, there is a guard channel to prevent devices from bleeding onto adjacent channels. Variants such as Orthogonal Frequency Division Multiple Access (OFDMA) expand on the basic concept by spreading data across orthogonal sub-carriers and using a Fast Fourier Transform (FFT) to recover the signal. FDMA and OFDM are used in many cellular applications and recent Narrowband-IoT standards [3].
Figure 2.4: Frequency Division Multiple Access

Though promising for some IoT applications and possibly being applied for 5G cellular standards, FDMA and OFDM are not prime candidates for use in large scale IoT WSNs for a few reasons. First, the extremely low duty cycle of sensor nodes leads to wasted channel capacity. If each sensor is allocated a unique channel, channels will be idle the vast majority of the time, which is extremely inefficient and leads to very high Peak-to-Average Power ratios (PAPR) when access points transmit multiple signals simultaneously. Second, the practicality of allocating dozens, hundreds, or thousands of individual frequency channels in a WSN is a large obstacle for FDMA. Even using relatively narrow sub-channels and guard bands, the overall network bandwidth would require sensor’s radios to be exceedingly flexible and is therefore a difficult challenge. Also, with nodes constantly entering and exiting the network as in future WSNs, channel frequency allocation becomes a difficult problem to overcome. While FDMA does offer a collision-free medium, the additional edge node flexibility needed to support the wide range of channel frequencies required in a large network is a limiting factor of FDMA and OFDM [14]. These tradeoffs are presented in Table 2.4.
FDMA Tradeoffs

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>High per-node throughput, low latency, cheap implementation</td>
<td>Vulnerable to narrowband interference, high bandwidth requirements</td>
</tr>
</tbody>
</table>

Table 2.4: Pros and cons list for FDMA

2.1.5 Code Division Multiple Access

Code Division Multiple Access (CDMA), often implemented in tandem with Direct Sequence Spread Spectrum (DSSS), is a multiple access technique that enables all users to share the entirety of a common channel simultaneously, with separation occurring via orthogonal spreading codes, shown in Figures 2.5 and 2.6. To do so, transceivers use assigned spreading codes to modulate narrowband data signals. These spreading codes, which typically take the form of orthogonal PN sequences, gold codes, Walsh codes, or Kasami codes, are used as high speed chip sequences that widen the transmitted signal’s bandwidth when multiplied with the data signal [33]. The chip rates are often 30, 200, or multiple orders of magnitude faster than the data signal [34]. Figure 2.6 shows the DSSS process and resulting wideband physical signal. A primary benefit of wideband signals is that any type of narrowband interference is easily discarded in the demodulation process. The orthogonality of spreading codes allows many transmissions to occupy a physical channel while preserving the ability to receive using a correlator in the receiver, and the processing gain associated with CDMA allows the recovery of signals from below the noise floor.

CDMA is widely used for 3G cellular network multiple access [41] and GPS [39]. The assignment of spreading codes is flexible depending on the application. GPS, for instance, assigns a repetitive code to each satellite, which they use to modulate their own signal on a shared frequency channel. GPS receivers on Earth have knowledge of each satellites’ code and can therefore autocorrelate the GPS signals [39] as part of despreading operations. Cellular standards such as IS-95, in contrast, assign a code to each handset that is used to
both transmit to a base station and receive from a base station [41].

Until recently, it has been generally accepted that CDMA is not an appropriate multiple access technique for low power WSNs, instead being overshadowed by TDMA, CSMA, and hybrid networks. CDMA networks in IoT have been considered [13], but receivers generally require increased complexity compared to other schemes and thus consume more power, which has previously disqualified CDMA from being a viable option on battery-powered nodes. Also, CDMA networks are susceptible to the near-far problem [42], which requires power control algorithms to prevent. Non-technical considerations play a large factor in the lack of CDMA deployment in low power networks as well, as companies like Qualcomm compete for business and political interests with intellectual property rights. Multiple surveys on MAC designs for WSNs don’t include analysis or evaluation of CDMA, some citing
its unsatisfactory power consumption due to complexity as the purpose for its omission [6, 14, 21]. However, recent proposed technology discussed in Section 2.3 describes techniques to overcome the drawbacks of CDMA in low power WSNs while capitalizing on its benefits, particularly for nodes operating with a low duty cycle. Table 2.5 summarizes CDMA’s tradeoffs.

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>High network scalability, robust against narrowband interference</td>
<td>High receiver complexity, potentially higher cost</td>
</tr>
</tbody>
</table>

Table 2.5: Pros and cons list for CDMA

In summary, Figure 2.7 shows a comprehensive comparison of the most popular IoT multiple access techniques as discussed in this section.

<table>
<thead>
<tr>
<th></th>
<th>Interference Mitigation</th>
<th>Network Scalability</th>
<th>Latency</th>
<th>Receiver Complexity</th>
<th>Physical Layer Security</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDMA</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
</tr>
<tr>
<td>TDMA</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
</tr>
<tr>
<td>CSMA/CSMA-CA</td>
<td>Green</td>
<td>Green</td>
<td>Blue</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
</tr>
<tr>
<td>CDMA</td>
<td>Green</td>
<td>Green</td>
<td>Blue</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
</tr>
<tr>
<td>ALOHA</td>
<td>Green</td>
<td>Green</td>
<td>Blue</td>
<td>Red</td>
<td>Red</td>
<td>Blue</td>
</tr>
</tbody>
</table>

Figure 2.7: Comparison of IoT Multiple Access Techniques – Red is poor, Green is satisfactory, Blue is excellent [45]

### 2.2 MAC Protocols for WSNs

A MAC layer protocol is typically considered distinct from the multiple access technique it employs, as described in the Definitions section of this chapter, but the two are inherently linked and their interface is the subject of investigation in this section. A MAC layer’s
responsibilities include packet framing for data, successful and correct data transmission, and especially prevention of collisions in time, space, or frequency [22], meaning it often, but not exclusively, encompasses the multiple access technique. This section introduces existing MAC layer protocols commonly included in the discussion of low power IoT networks, focusing specifically on the multiple access technique used by each. A discussion on the most likely protocol to be deployed in WSNs in the future concludes that IEEE 802.15.4 is the leading MAC layer candidate currently in existence.

**IEEE 802.15.4**

The IEEE 802.15.4 MAC protocol [1] is one of the industry standards for IoT devices and is used by ZigBee [46] for short range, low power communication. The protocol is purposely designed to be very broad, supporting both synchronous and asynchronous use as well as mesh or star topologies. IEEE 802.15.4 uses CSMA-CA for asynchronous multiple access, but can also be slotted to form a hybrid TDMA network. Many studies have been published regarding the performance of 802.15.4’s MAC layer [9, 10, 29].

One major concern presented in [7] is MAC unreliability caused by the contention mechanism. This is especially concerning when scaled to highly dense and collision-prone networks.

**Bluetooth Low Energy**

Bluetooth Low Energy (BLE) [2] is an emerging standard that uses a TDMA scheme with frequency hopping. It offers promising potential, but is relatively unproven for use in WSNs [37]. Also, it has severe jamming and security concerns that render it questionable for any security conscious network [20, 38]. Moreover, the higher layer protocols are optimized for single peer-to-peer connections rather than the star topology focused upon in this work.
2.2. MAC Protocols for WSNs

LoRaWAN

LoRa Wide Area Network (LoRaWAN) is a standard published by the LoRa Alliance that is a very applicable and widely growing protocol in the IoT, focused on long distance communication. Though it is effective in these long range low power networks which can cover hundreds of square kilometers, LoRaWAN is not designed for the type of highly contested channels of WSNs, and is not openly advertised as a WSN solution [5]. Furthermore, it is shown in [4] that sensor data rates would have to be exceedingly low, significantly lower than those used in this work, in order to support the required network densities.

Sensor-MAC

Sensor-MAC, or S-MAC, is designed specifically for low power IoT devices, using a coordinated sleep schedule to minimize idle listening time. S-MAC variants such as T-MAC point out and improve upon specific shortcomings of the protocol [43]. Still, synchronization requirements are generally not desired for WSNs.

LEACH

Low Energy Adaptive Clustering Hierarchy (LEACH) is a MAC layer for WSNs that is based on network topology management using adaptive clustering techniques. The protocol aims to support large scale WSNs by intelligently grouping nodes into hierarchies of clusters using separate channels rather than using a single high capacity channel. LEACH employs a hybrid TDMA/CSMA multiple access technique, much like the beacon-enabled mode of IEEE 802.15.4 [23]. Due to the use of this technique, synchronization requirements and CSMA-CA drawbacks are challenges faced in the protocol.
IEEE 802.11

IEEE 802.11 protocols, commonly known as WiFi, implement a similar CSMA-CA algorithm as IEEE 802.15.4 but with an added capability aimed at further reducing the probability of collisions by mitigating the hidden node problem. A Request-to-Send (RTS) and Clear-to-Send (CTS) protocol is managed by a central coordinator that prevents nodes from transmitting over hidden nodes [12]. However, RTS and CTS adds significant additional overhead to a CSMA-CA algorithm, and would likely prove less effective than IEEE 802.15.4.

Narrowband IoT LTE

Narrowband IoT (NB-IoT) is an extension of LTE protocols designed for use on low power devices in the IoT. As such, it adopts OFDM as a multiple access technique, similar to LTE [11], that is difficult to scale in the highly dense networks of future WSNs. Also, as discussed in Section 2.1, large FDMA or OFDM networks with low data rates result in significant wasted bandwidth. A large difference of NB-IoT to other protocols is that it operates in licensed spectrum rather than unlicensed, which has a large effect on non-technical deployment considerations.

2.3 Receiver-Assigned CDMA

The previous sections have built a proper background on the topics of medium access and MAC protocols. This section moves beyond the introduction and discussion of previous work, focusing on novel concepts and contributions not yet published.

The conceptual design of Receiver-Assigned CDMA (RA-CDMA) is similar to that of most CDMA networks discussed in Section 2.1.5, but with a few unique design features that enable
2.3. Receiver-Assigned CDMA

It is based on the design that a central network coordinator, or access point, is assigned a specific spreading code that all sensor nodes use to address the coordinator. The access point contains a RAKE receiver [16, 42] with a common preamble detector that is used to correlate and demodulate each packet, enabling simultaneous reception of multiple packets. Sensor nodes are similarly assigned spreading codes so that the access point can individually address them. Shown in Figure 2.8, this network architecture greatly simplifies RA-CDMA into a scheme that can be applied to low power devices. The primary benefit of this scheme is that a sensor node must only listen for its own code and optionally a common broadcast code, rather than listening for several codes.

![RA-CDMA Code Assignment Scheme](image)

Figure 2.8: RA-CDMA Code Assignment Scheme

Currently, a renewed interest in using CDMA on low powered nodes is being realized, fueled by recent advances in CDMA technology and the increasing necessity of large-scale secure WSNs. As mentioned in [14], using CDMA could mitigate the collision avoidance problem in TDMA and CSMA protocols and could be feasible for WSNs if its computational complexity is decreased. Also, CDMA in general enables the possibility of PHY layer security concepts such as Low Probability of Detection (LPD), Low Probability of Intercept (LPI),
and especially Low Probability of Exploitation (LPE). While not focused upon in this work, [27] describes specific security benefits of low power CDMA. It is proposed in [27] that a CDMA multiple access technique and unique physical layer modulation could enable the use of CDMA on IoT low power nodes with much greater scalability and security than other protocols. Due to these developments and others, CDMA is now being considered for low power IoT wireless sensor networks.

An important distinction to make in evaluating these channel capacity division techniques is that the uplink and downlink can optionally be chosen in an asymmetric fashion. For instance, an asynchronous, low latency CDMA uplink from battery powered nodes to an access point could be paired in a network with a different power-optimized downlink that offers a better overall system compromise when the primary flow of sensor traffic and primary computation complexity is apportioned to the access points’ despreading receivers.

In summary, RA-CDMA has the potential to offer greater network scalability, increased physical layer security, and robustness against interference while matching or exceeding required WSN performance. Its drawback is increased receiver complexity, which can be mitigated using techniques in [27] and a unique code assignment scheme.

**Summary**

This section has introduced the potential multiple access techniques to enable future dense WSNs along with the leading candidate MAC layer protocols to be deployed on such networks. The details of each techniques’ tradeoffs, specifically in WSNs, have been discussed, and their effect on the MAC layer has been presented. Based on this analysis and the literature presented within, the author believes IEEE 802.15.4 is the most likely existing candidate MAC protocol to be deployed in future WSNs, meaning its asynchronous CSMA-CA multiple
access will be tested in dense, contested channels in these networks.

The proposed alternative multiple access technique, RA-CDMA, has also been introduced in this section. RA-CDMA offers multiple benefits over existing IoT multiple access techniques when applied to certain networks. Its resilience against collisions, robustness against multipath interference, and its asynchronous characteristics make it a prime candidate for use in low power WSNs. RA-CDMA offers high scalability for support of large scale networks where other protocols, such as IEEE 802.15.4 may break down.

The discussion and analysis presented in this section sets the stage for a comprehensive investigation into the performance of IEEE 802.15.4 and RA-CDMA networks. The network scalability, specifically the ability of each multiple access technique to support a large number of sensor nodes, becomes the primary concern regarding deployment in WSNs.
Chapter 3

Network Scalability Comparison of IEEE 802.15.4 and RA-CDMA

Existing Medium Access Control (MAC) layer protocols, namely IEEE 802.15.4, may not be suitable for highly dense, low rate networks. A new MAC protocol has been proposed that features a receiver-assigned code division multiple access (RA-CDMA) contention mechanism, which may enable higher network scalability while maintaining performance and contributing additional dependability.

This chapter presents a comparison of the multiple access techniques of IEEE 802.15.4 non-beacon enabled mode and RA-CDMA along with a Matlab simulation framework used for end-to-end simulations of the protocols. Simulations suggest that IEEE 802.15.4 networks begin to break down in terms of throughput, latency, and delivery ratio at a relatively low overall traffic rate compared to RA-CDMA networks. Results show that networks using the proposed RA-CDMA multiple access can support node densities on the order of two to three times higher than IEEE 802.15.4.

Introduction

Having evaluated existing multiple access techniques in Chapter 2, IEEE 802.15.4 and its CSMA-CA multiple access are determined to be the leading existing candidate for WSNs.
The proposed RA-CDMA multiple access technique will be compared to it to objectively evaluate network performance in terms of scalability. Section 3.1 further explains the contention processing mechanisms of IEEE 802.15.4 and RA-CDMA and details the potential benefits and drawbacks of each. A Matlab simulation framework used for the comparison is detailed in Section 3.2, along with the numerous modifications made to accommodate the two multiple access techniques. Final results of the simulation comparison are presented in Section 3.3, followed by an analysis and takeaways in Section 3.4.

3.1 Contention Processing

The overall goal of contention processing within a wireless communication protocol is to maximize the efficiency of the protocol’s multiple access technique. This generally means collision prevention, handling, and recovery. The contention processing of 802.15.4 and RA-CDMA differ greatly, primarily because each uses a radically different form of multiple access. An overview of each contention mechanism reveals unique pros and cons that must be considered when evaluating for use in a future WSN.

3.1.1 IEEE 802.15.4 Contention Processing

The IEEE 802.15.4 protocol features two different multiple access modes with similar, but different, contention mechanisms. The focus of this comparison is asynchronous mode, also known as unslotted or non-beacon enabled mode, because it is most similar in design and behavior to RA-CDMA and most relevant to low duty cycle signals. IEEE 802.15.4 asynchronous mode employs CSMA-CA to prevent collisions that occur any time multiple nodes transmit simultaneously on the same channel. The algorithm used is shown in Figure 3.1.
IEEE 802.15.4’s CSMA-CA multiple access and contention processing are simple and require low complexity hardware to implement, enabling extremely low power and low cost networks. It has become a widely used industry standard in many IoT applications for these reasons.

However, the CSMA-CA algorithm is known to be susceptible to problems that can cause ineffective channel capacity distribution. Specifically, simultaneous collisions and the hidden node problem are both well studied issues that are known to produce undesired performance [15]. The CSMA-CA technique makes two key assumptions that cause vulnerability to these problems: (1) the sensing node is within range of all other nodes in the network, so that the
sensing nodes physical channel is identical to the PAN Coordinator’s channel, and (2) the channel will not change in the time between a clear channel assessment (CCA)/carrier sensing and the transmission of a packet. Provided that these assumptions are correct, CSMA-CA generally performs very effectively in a channel with a cumulative data rate less than the channel capacity. However, in a real, physical channel, neither of these two assumptions can be realistically presumed. Collisions at the PAN Coordinator in an 802.15.4 network generally occur when one or both of these two core assumptions break down.

Additional problems arise in 802.15.4 networks when the overall cumulative desired throughput of all nodes in a network exceeds the theoretical channel capacity. For example, if a channel’s capacity is 100 kilobits/sec (kbps) and contains twelve nodes, each with a desired data rate of ten kbps, the cumulative desired data rate of 120 kbps exceeds the channel capacity of 100 kbps. This causes problems for the contention processing algorithm.

When an 802.15.4 network is scaled to a large number of low data rate nodes, its cumulative desired data rate often exceeds its channel capacity, which results in a cascading backoff effect that severely cripples network performance [28]. Essentially, nodes can enter a near-perpetual backoff state with no likelihood of completing a successful carrier sense and packet transmission. This behavior is apparent in simulation results and is analyzed in Section 3.4. Despite the low power and low cost benefits of 802.15.4, its cascading backoff problem renders it ineffective on highly dense WSNs.

3.1.2 RA-CDMA Contention Processing

A receiver-assigned CDMA network offers several benefits over IEEE 802.15.4 in similar WSN architectures. This section will investigate the cause of its superior performance by analyzing the sources of contention and the contention processing of RA-CDMA WSNs.
Sources of Contention

Sensor nodes in RA-CDMA are essentially granted unimpeded asynchronous random access to the access point. Most usual sources of contention in TDMA and FDMA are thereby mitigated completely. However, contention does exist in RA-CDMA networks, but in different forms than traditional multiple access techniques.

The most theoretically prohibitive cause of contention is multiple access interference (MAI), which is additional noise generated by other simultaneously transmitting nodes that decreases the signal-to-interference-plus-noise ratio (SINR) of an intended signal. Figure 3.2 depicts the effect of MAI on the PHY layer.

![RA-CDMA physical layer in the case of nominal SINR (left) and low SINR (right) caused by other transmitters](image)

Additional contention can also be caused by the number of demodulators, or fingers, contained in the RAKE receiver hardware. If the number of simultaneous transmissions exceeds the number of parallel demodulators, packet drops will result. This work assumes that no packets are dropped due to RAKE receiver limitations, meaning that RAKE hardware is assumed to be sufficient enough to receive all simultaneous transmissions.

However, this may not always be the case in real network implementations, especially in cost-conscious networks, so an analysis of possible effects of RAKE hardware limitations is
3.1. Contention Processing

useful. The number of parallel demodulators in each access point is one of many tradeoffs between power consumption, cost, capacity, and performance in an RA-CDMA network.

Figure 3.3 demonstrates the timing associated with packet drops due to RAKE receiver hardware limitations, supposing a RAKE receiver with eight parallel demodulators. In the figure, immediately before Time 1, there are eight devices transmitting, which fill up completely an eight finger RAKE receiver, so the next transmission by End Device 5 cannot be demodulated after its detection and is therefore dropped. But in the period between Time 1 and Time 2, End Device 1’s transmission ends. End Device 5’s transmission is unrecoverable, but one RAKE finger becomes available. The next transmission by End Device 10 at Time 2 is therefore received properly by the one remaining open finger. Then at Time 3, End Device 1’s transmission is also dropped because all fingers are occupied.

Figure 3.3: Timing of a sample eight-finger RAKE Receiver showing properly received packets in green and dropped packets due to overload in red\textsuperscript{1}

\textsuperscript{1}The network traffic shown is purely a demonstrative sample and does not accurately represent expected network traffic. At the data rates analyzed, RAKE drops typically only occur in networks exceeding 90 or more nodes.
Finally, collisions in time within ±1 chip cycle cause a correlator failure at the correlator and detector stages of the receiver, dropping packets due to failed preambles. This occurrence is relatively unlikely based on the chipping rate implemented.

Contestion Processing

Given the three sources of contention in an RA-CDMA network (MAI, RAKE hardware limitations, and collisions in time), a question arises regarding what actions to take when a packet is dropped. The first possible solution is simply to not request acknowledgments from the coordinator for any data packets, thereby not guaranteeing successful delivery of a packet. This is by far the least complex contention processing, but many applications require strict delivery assurances.

A second possibility is adapting the backoff periods of CSMA-CA to fit RA-CDMA. Using this contention processing, if an acknowledgement packet from an access point is not received within a packet’s timeout window, the packet is retransmitted after a random backoff duration. This is the contention processing solution is implemented in the simulations in this work. Acknowledgments are expected to be received for every data packet unless it is dropped.

It is noteworthy to clarify that a RA-CDMA access point will have knowledge of the cause of contention in its network, so it can intelligently throttle network traffic based on priority as an attempt to reduce contention. Hence, a third solution for contention processing could be a system of monitoring and commanding signals that manage the overall traffic according to the level of contention. This processing, a priority-based scheme designed to keep network traffic below the channel capacity, offers perhaps the most promising potential for RA-CDMA, but is significantly more complicated to implement. Moreover, the access point is
3.1. Contention Processing

capable of sending multiple acknowledgements simultaneously using parallel modulators and code diversity.

3.1.3 Multiple Access Performance Metrics

In order to objectively compare different multiple access protocols, some quantitative performance metrics must be established. This section will introduce and discuss the three primary metrics of performance used in this work to evaluate IEEE 802.15.4 and RA-CDMA, chosen because they accurately summarize overall network behavior when considered cumulatively.

Throughput

In this work, throughput refers to the total network payload throughput, or the cumulative payload throughput of all end devices. This is sometimes referred to as goodput. It is defined according to Equation 3.1.

\[
\text{throughput} = \frac{\text{\# total successful packets} \times (\text{payload length})}{(1000 \times \text{simulation time})} \quad \text{[kbps]} \quad (3.1)
\]

Packet Delivery Ratio

Packet Delivery Ratio is defined in this work as the number of packets successfully transmitted and properly acknowledged, divided by the number of unique attempted packets, which is stated in Equation 3.2.
\[
\text{packet delivery ratio} = \frac{\text{\# total successful packets}}{\text{\# total successful packets} + \text{\# total dropped packets}} \times 100
\] (3.2) 

This definition will exclude any packets retransmitted due to a failed acknowledgement, which is the result of a packet drop or collision.

Packet failures are defined as those that are discarded as a result of reaching the maximum allowed value of either (1) four consecutive unsuccessful CCA carrier sensing attempts or (2) three consecutive unacknowledged packet transmissions. Packet delivery ratio is a good metric of the overall effectiveness of a MAC layer and contention mechanism.

**Average Packet Latency**

Packet latency describes the timeliness of a MAC Layer’s packet delivery, which is an important requirement in many WSNs. This work defines packet latency as the time elapsed between the moment of a frame’s entrance into the frame queue and the moment of the transmission of the packet’s last symbol. To compile the average packet latency metric, the latency measurement of every packet transmitted by an end device over the entire simulation period is averaged together.

Average latency has a heavy dependence on the desired data rate of each node. If the packet generation rate of a given node exceeds the rate that the channel and its contention mechanism can support, the node’s queue will begin to fill up rapidly at a higher rate than packets being transmitted. This behavior can greatly inflate a node’s packet latency metric.

Also noteworthy is that only packets transmitted within the simulation period are included in the final metric’s value, so that any frames that remain in the frame queue at the end of
the simulation period are not included.

This metric is not bi-directional, meaning it does not account for the successful or dropped reception of each packet by the intended target node.

### 3.2 Simulation Frameworks

Beginning with the release of Matlab R2017a, Matlab’s add-on Communications System Toolbox includes a library of source code for the implementation of the ZigBee protocol [25], which will herein be referred to as the “LRWPAN library.” The ZigBee Alliance [46] provides a Network and Application layer specification that falls on top of the IEEE 802.15.4 PHY and MAC protocols, so that ZigBee’s top two layers replicate exactly an implementation of IEEE 802.15.4. The LRWPAN library is the foundation of this work’s simulations. As a part of the LRWPAN library, classes are available to create objects that fully implement the specifications of 802.15.4 and can be used for a complete end-to-end simulation of both the PHY and MAC layers.

Frame generation, decoding, and MAC layer device processing classes were used for both 802.15.4 and RA-CDMA, while the 802.15.4 PHY generation and decoding classes were used only for 802.15.4 simulation. Because RA-CDMA uses a unique spread spectrum physical layer, a PHY emulator was implemented in Matlab to model its behavior, based on measured results of an FPGA-based testbed. [27] provides details of the complete PHY design that is modeled by the emulator.


3.2.1 IEEE 802.15.4 Simulation Framework

The first step towards a full scale 802.15.4 simulation using the LRWPAN library was general familiarization with the library’s architecture and capabilities. Next, numerous modifications and corrections were put in place, then subsequently verified through a comprehensive testing and inspection process that identified any deviations from nominal 802.15.4 behavior.

Overview of Matlab LRWPAN Library

The LRWPAN Library consists of three main classes of interest that interact to produce a complete end-to-end simulation of the 802.15.4 MAC and PHY layers. The interaction of the three classes, along with some of the critical functions associated with each, are depicted in Figure 3.4.

The first class of interest is MACDevice, which provides the core functionality and processing of the entire MAC layer of a device. Two subclasses of MACDevice, MACFullFunctionDevice and MACReducedFunctionDevice, provide additional functionality unique to PAN Coordinators (full function devices) and end devices (reduced function devices).

The second class is MACFrameConfig, which contains functions for both generating and decoding formatted MAC frames. The class easily allows transition between a MAC protocol data unit (MPDU), which is a bit-level representation of a MAC frame, and a configuration object, which contains all the information of an MPDU in a more easily readable and accessible format.

Finally, the PHYDecoderOQPSK class provides the PHY layer processing necessary to interface between PHY and MAC layers, including synchronization, despreading, preamble detection, and decoding. It is important to understand that the full IEEE 802.15.4 PHY
layer is implemented simply to provide a mechanism for medium access comparison, and has no effect on multiple access performance metrics other than defining physical data rates and bandwidths. The IEEE 802.15.4 PHY layer class implements offset quadrature phase-shift keying (OQPSK), which employs 16-ary quasi-orthogonal modulation, with a symbol rate of 62.5 kHz in the 2.4 GHz ISM band, occupying approximately 2.5 MHz of bandwidth per channel. The 16-ary OQPSK uses four-to-one bit-to-symbol mapping. A key assumption made is a signal-to-interference-plus-noise (SINR) value of above 20 dB, which corresponds to a negligible bit error rate (BER) for OQPSK. Because of this, no forward error correction (FEC) is implemented in the PHY.

Figure 3.4: High-level diagram of the LRWPAN library representing function calls as tabbed arrows - blue text represents classes or inherited classes, green represents class functions, and red represents methods within functions
Simulation Framework Assumptions
Assumptions made regarding the design and modifications of the simulation framework are generally a result of the overall network constraints placed on the scope of this work. All listed assumptions that are also applicable to the RA-CDMA simulation are assumed for RA-CDMA.

- The network topology consists of a single PAN Coordinator (full function device) with a specified number of end node devices (reduced function devices) which represent sensors in a WSN.

- The framework simulates a single PAN, representing a single channel at a single carrier frequency.

- Because this simulation is purposed to evaluate only the contention mechanism of the protocol, all devices are assumed to be properly associated with the PAN Coordinator and will never become disassociated. This will be referred to as steady state.

- Network layer processing is assumed to be covered in other work. The MAC layer’s payload consists of randomly generated data.

- All devices are assumed to be within physical range of each other, thus dismissing the hidden node problem. Further, edge node power control is assumed to have reached steady state such that all edge nodes transmit with sufficient power to have constant received power levels at the access point.

- To realistically replicate the data flow of a dense WSN, end devices generate random data packets at a specified probabilistic rate using a uniform distribution, and the PAN Coordinator does not generate any data packets. Thus, the PAN Coordinator’s outbound traffic is limited to acknowledgment packets as specified by the MAC protocol.
3.2. Simulation Frameworks

- Edge nodes are technically modeled as full duplex devices; however, simultaneous transmit and receive is not expected behavior due to the assumed data flow and assumed acknowledgement protocol.

- The payload length of all data packets is 50 bytes.

- The simulations represent 2 seconds of real time in steady state.

- Given the asynchronous nature of both protocols, no assumptions on MAC layer timing or timeslot synchronization are made.

Simulation Timing

As with any computer simulation of a real time system, efforts must be made to discretize the system’s behavior into steps that are reasonably manageable for a processor. Especially in wireless network simulations, this is commonly done by performing complex processes at less frequent intervals than in a real-time system.

In the LRWPAN library, MAC processing is performed at batch intervals separated by the duration of a single CSMA backoff period, which is defined as the duration of 20 OQPSK symbols. Using a rate of 65.5 kHz as the top-level MAC layer simulation rate, the MAC processing step size is 0.00031 seconds. This selection of step size simplifies the implementation of the CSMA algorithm, allowing backoff duration variables to count in terms of steps rather than individual symbols.

In addition to simplifying MAC layer processing, a step size of 20 symbols serves as a reasonable representation of an actual embedded system that would be implemented in hardware. Low power wireless nodes operate on a similar time scale, with physical processing occurring at a high sample rate and MAC layer processing occurring during update loops that can last as long 20 symbols, or 0.00031 seconds.
It should be emphasized that this step size defines the repetition frequency of MAC layer processing, meaning the rate at which the MAC layer processes the last 20 symbols received, and does not represent the smallest resolution in time in the simulation. Physical layer processing requires resolution down to the sample level. Figure 3.5 shows this relation.

Figure 3.5: Interface between PHY and MAC layer illustrating step duration

**Modifications to LRWPAN Library for IEEE 802.15.4**

Though the LRWPAN library has much utility, several modifications to the source code were needed before complete network simulations were possible. Necessary modifications include both additional capabilities added to the existing framework and correctional modifications to patch bugs or anomalous behavior, all of which have been confirmed, but not yet addressed by Matlab.

First, the addition of a top-level simulation script was necessary to interface the different devices, which are represented as objects of the classes detailed in Section 3.4. Matlab provides a good starting point with a simple example, which is available on their website [26]. But additional modifications were necessary to create a fully flexible and nominally behaving framework. Variable length cell arrays are used to provide flexibility in the number of nodes
3.2. Simulation Frameworks

joining the network. Also, because this simulation framework is intended to focus solely on steady state network contention, a network formation phase of the simulation was added to run separately before a steady state phase so that all performance metrics exclude any artifacts from network formation. Additional top-level script functionality includes debugging and statistic gathering, calculation, and display.

The most significant modification made to the LRWPAN library was the placement of statistic tracking variables throughout the source code for the purpose of verification, performance metric gathering, and debugging. These variables track network behavior and also help reveal anomalous behavior in the simulation. Table 3.1 contains a list of these variables and brief descriptions.

Another added capability was creating a flexible packet generation rate, which defines the likelihood that a random data packet is generated on a given simulation step cycle. This variable is also known as packet arrival rate. It has a random uniform distribution that essentially defines a node’s desired data throughput, which greatly affects the network’s behavior.

As mentioned, several corrections were necessary to fix erroneous behavior non-conforming to the 802.15.4 protocol. In the interest of enabling the reader to fully replicate the simulation framework and obtain similar results, Table 3.6 details each correction made to the publicly available LRWPAN library. Note that this table is not a comprehensive list of modifications to the source code, but rather just includes the corrections made to the LRWPAN library source code to produce network behavior that complies with IEEE 802.15.4.
### Table 3.1: List and descriptions of tracking and counting variables used to pull results from, verify and debug the simulation framework

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Packets</td>
<td>Total number of packets successfully transmitted by an end device then properly received and acknowledged by the PAN Coordinator</td>
</tr>
<tr>
<td>Failed Packets</td>
<td>Total number of packets discarded due to a CSMA give-up or ACK give-up</td>
</tr>
<tr>
<td>Attempted Packets</td>
<td>Total number of packets processed from the frame queue</td>
</tr>
<tr>
<td>Unique Attempted Packets</td>
<td>The total number of packets processed from the frame queue that are not duplicates (retransmissions) or are not ACK’d by the end of simulation</td>
</tr>
</tbody>
</table>
| Packet Delivery Ratio            | \[
|                                | \[
| ACK Timeouts                    | Total number of packets not properly acknowledged within the ACK timeout window, prompting a packet retransmission or ACK give-up                                                                            |
| Collided Packets                 | Total number of packets that collide with another packet                                                                                                                                                   |
| Number of Collisions             | Total number of instances in which two or more packets collide                                                                                                                                              |
| CSMA Give-Ups                   | Total number of packets discarded due to reaching the maximum allowed number of carrier sensing attempts                                                                                                 |
| ACK Give-Ups                    | Total number of packets discarded due to reaching the maximum allowed number of retransmissions                                                                                                           |
| CRC Check Failures              | Total number of packets containing an incorrect CRC when received                                                                                                                                           |
| Frames Remaining in Queue        | Total number of frames remaining in a frame queue at the end of the steady state simulation                                                                                                                  |
| Frames Remaining in Processing   | Total number of frames in either a backoff state or pending acknowledgment at the end of steady state simulation                                                                                           |
| Total Network Throughput         | \[
|                                | \[
| Average Throughput per Device   | \[
|                                | \[
<p>| Average Packet Latency          | Average of the time elapsed between the moment of a frame’s entrance into the frame queue and the moment of the transmission of the packet’s last symbol                                                      |
| Total Idle Time                 | Total number of steps in idle state by all end devices                                                                                                                                                     |
| Total Transmit Time              | Total number of steps in transmitting state by all end devices                                                                                                                                              |
| Total Backoff Time               | Total number of steps in backoff state by all end devices                                                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>File</th>
<th>Line</th>
<th>Code inserted</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSMAStateMachine.m</td>
<td>33, 35</td>
<td>Add &quot;end&quot; at line 33 to close the InitTransmit if statement. At line 35, change else if to if</td>
<td>The InitTransmit stage of the CSMA algorithm need not take an entire step – if no backoff is necessary, the algorithm should advance to next stage within the same step</td>
</tr>
<tr>
<td>CSMAStateMachine.m</td>
<td>77</td>
<td>Insert line:</td>
<td>Without clearing obj pTxBuffer, the device will cease transmitting altogether if a CSMA reaches max attempts because the idleProcessing.m line 11 will always return false</td>
</tr>
<tr>
<td>PHYDecoderOQPSK.m</td>
<td>376</td>
<td>Insert lines:</td>
<td>Rarely, line 377 will error due to an overflow of the demodulated() array. This patch will simply extend the index of demodulated() with appended zeros so there is no index error</td>
</tr>
<tr>
<td>decodeReceived.m</td>
<td>10</td>
<td>Delete line 13 and add the following at line 10:</td>
<td>Necessary to facilitate changes below</td>
</tr>
<tr>
<td>decodeReceived.m</td>
<td>11</td>
<td>Add the following lines after line 10:</td>
<td>IEEE 802.15.4 specifies that an ACK should be sent SIFS duration after the last symbol of a packet that requests acknowledgement arrives. The unedited version incorrectly makes a decision between SIFS and LIFS before sending an ACK.</td>
</tr>
<tr>
<td>decodeReceived.m</td>
<td>After line 11 above</td>
<td>Add the following lines after the edits made above:</td>
<td>IFS Symbols should be decreased each step, not only if device is idle</td>
</tr>
<tr>
<td>idleProcessing.m</td>
<td>26</td>
<td>if obj pSymbolsToWait &gt;= obj SYMBOLSTEP &amp; &amp; strcspn(obj pState, 'BackOff')</td>
<td>Same as above</td>
</tr>
</tbody>
</table>

Figure 3.6: Corrections made to the LRWPAN Library to produce behavior conforming with IEEE 802.15.4 protocol
Verification of Simulation Results

The process of verifying the accuracy of the simulation results was iterative. It consisted of building up the framework to allow the extraction of the many network performance statistics shown in Table 3.1, then carefully examining those statistics over a comprehensive series of test cases, and comparing the experimental results with expected results. Inspection of network activity plots, shown in Figure 3.7, visually demonstrates network behavior and is useful in the debugging process. On the bottom plots, collisions are shown as any instance more than one device is transmitting, such as at time 290 ms visible in the zoomed-in plot. Also in the zoomed-in plot, the acknowledgment protocol is apparent, as all end device data packet transmissions are followed immediately by a short ACK transmission from the PAN Coordinator. Note that collided packets do not receive an ACK.

One effective verification test case is the comparison of the theoretical maximum throughput possible with the absolute maximum throughput achieved by the simulation in any network configuration. These two values should closely match. The simulation’s data rate is defined at 62.5 symbols per second, which for 16-ary OQPSK equates to 250 kilobits/sec. This serves as the maximum possible throughput assuming a single node is transmitting constantly with no gaps in transmitted symbols. This is unachievable in practice, however, because the 802.15.4 protocol overhead assumes acknowledgment packets, inter-frame spacing, and header/footer overhead in the MAC layer.

In an open channel with one end node and one PAN Coordinator, the process of generating a data packet, transmitting it, waiting the proper inter-frame spacing periods, and receiving an ACK takes between 180 and 320 symbols, depending on the initial CSMA-CA backoff time. With a mean initial backoff period of 70 symbols according to 802.15.4’s backoff algorithm, the time for one total successful packet transmission, including backoff, interframe spacing,
and acknowledgement, is 260 symbols. Though the data packet itself is only 134 symbols, the MAC overhead adds an average of 126 symbols. Also, our simulation framework assumes a fixed data payload length of 50 bytes. Thus, the following calculation in Equation 3.3 is made to determine the maximum expected throughput for a test case with one end device and one PAN Coordinator, assuming the end device uses an infinite packet generation rate, i.e. its frame queue is always filled.
This theoretical throughput represents the maximum channel capacity of the IEEE 802.15.4 simulated PAN. The simulation was shown to achieve this calculated throughput in the given scenario.

Other statistics were similarly calculated, analyzed, and compared to expected results. For example, the number of overall attempted packets should equal the sum of successful packets, CSMA give-ups, ACK give-ups, and packet retransmissions, all of which are independently gathered. The many relationships like these amongst the tracking and counting variables are all nominal in the simulations, providing confidence in the simulation framework’s accuracy.

**Limitations of Simulation Framework**

Despite the full scope of the simulation framework, there still exist some inherent limitations that must be acknowledged.

The functionality of the LRWPAN library is limited to simulating the IEEE 802.15.4 MAC layer in asynchronous mode, also known as non-beacon enabled mode or unslotted mode. It does not include implementation of 802.15.4 beacon-enabled mode, which uses synchronization beacons and a superframe structure to potentially improve upon contention in some network configurations and architectures. For this reason, IEEE 802.15.4 beacon-enabled mode is not addressed in this work. However, non-beacon enabled mode serves as an adequately commensurate comparison to RA-CDMA because it is most similar in design and behavior to RA-CDMA and most relevant to low duty cycle signals. Synchronous MAC layers are undesirable in WSNs due to generally higher latency.
An additional drawback of the simulation framework is its inability to model the hidden node problem. This problem, discussed in Section 3.1.1, is well documented for CSMA techniques, and could negatively affect network performance by inflating the probability of collisions. The simulation framework simply assumes all nodes to be within sensing range of all other nodes in the network.

Though the selection of a MAC simulation step size of 20 symbols is within reason and makes sense to model a real world hardware implementation, it presents a few limitations that may adversely affect network performance. Of specific concern is the duration of a clear channel assessment (CCA), which is used in carrier sensing to determine if the channel is currently in use or not. According to the IEEE 802.15.4 standard [1], a CCA should last the duration of 8 symbols and return channel idle if the power level over those 8 symbols is below a certain threshold. However, the simulation framework implementation performs a CCA over an entire step size of 20 symbols, which could potentially inflate the likelihood of the channel being sensed as busy.

Despite this deviation from the protocol and the other mentioned issues, the author has a high level of confidence in the validity of the simulation results and its realistic simulation of a real world network.

### 3.2.2 RA-CDMA Simulation Framework

Because the proposed RA-CDMA is more of a multiple access technique than a complete MAC Layer protocol, steps must be taken to limit the scope of performance evaluation strictly to the performance of the multiple access, rather than a protocol as a whole. If two separate MAC layer protocols were used, the final performance metrics would reflect the difference in performance of the entire MAC protocols, not just the multiple access
Chapter 3. Network Scalability Comparison of IEEE 802.15.4 and RA-CDMA

technique. Furthermore, many factors affect the performance of a MAC protocol, but do not represent the performance of multiple access, such as frame formats, acknowledgement protocol, error handling, CRC checking, topology, and many others. In order to prevent these ancillary MAC protocol characteristics from affecting the multiple access evaluation results, the aspects of the proposed RA-CDMA were plugged in to the LRWPAN simulation, replacing all aspects of multiple access but retaining the parts of the MAC layer unrelated to multiple access.

Similar to Equation 3.3, a theoretical calculation of RA-CDMA channel throughput is a useful verification tool in understanding network behavior. The calculation assumes a single end device transmitting continuous packets with acknowledgment, which represents the maximum per-node theoretical throughput. In RA-CDMA, the maximum network throughput is therefore a function of this per-node throughput and the number of nodes connected in the network. However, the theoretical network throughput is bounded by noise and bit error rates, as further discussed later in this section.

Because acknowledgement packets are addressed on separate spreading codes and can be transmitted simultaneously on separate modulators, the end devices can continually occupy a demodulator. Additionally, RA-CDMA networks have no initial CSMA backoff period prior to the transmission of a packet. Due to these deviations from IEEE 802.15.4, RA-CDMA transmissions take 134 symbols from frame processing and transmit initialization to completion. Equation 3.4 calculates the maximum theoretical channel capacity of RA-CDMA for a single end device. This value should then be multiplied by the number of nodes in the network to find maximum network capacity. However, this capacity value is bounded by the bit error rate.
Physical Layer Emulation

In the case of RA-CDMA, there is no readily available end-to-end simulation of the spread spectrum physical layer detailed in [27], so a PHY emulator must be designed in Matlab to replicate exactly the behavior of the PHY as seen from the perspective of the MAC layer. The primary function of the emulator is modeling MAI and time collisions. In a deviation from the OQPSK PHY layer of 802.15.4, which uses four-to-one bit-to-symbol mapping, the RA-CDMA PHY layer employs standard Quadrature Phase Shift Keying (QPSK), which uses two-to-one bit-to-symbol mapping. QPSK requires a lower SINR for equal BER compared to OQPSK, so its use can help decrease the effect of MAI on network performance. A single channel of the QPSK PHY layer occupies 10 MHz of bandwidth using the chipping rates specified below. The following sections detail the design of the PHY emulator.

Multiple Access Interference Modeling

The primary function of the PHY emulator, other than acting as a pass-through between devices’ MAC layers, is to accurately model the bit error rate (BER) of a physical channel on an RA-CDMA system. Note that the BER of IEEE 802.15.4 is assumed to be negligible, which is not the case in RA-CDMA. In a CDMA system, the interference caused by other nodes using different spreading codes is an important factor. This interference is called multiple access interference (MAI). Figure 3.2 provides context for the following calculations.
Chapter 3. Network Scalability Comparison of IEEE 802.15.4 and RA-CDMA

To model the bit error rate caused by both background noise and MAI, some assumptions must first be made:

- Background noise power = 0 dB (same as 802.15.4)
- RA-CDMA Spreading Ratio = 175
- RA-CDMA Spread SNR = 0 dB

Then the de-spread signal-to-noise (SNR) of the desired RA-CDMA signal becomes:

\[
\frac{\epsilon_s}{N_0} = 10 \log_{10}(175) \approx 22.4 \text{ dB}
\]  

And the overall interference, both background noise and MAI, becomes:

\[
0 \text{ dB} + 10 \log_{10}(1 + n)
\]  

where \( n = \text{Average number of interferers across the duration of a packet transmission} \)

Thus, the effective SINR, \( \frac{\epsilon_s}{N_0} \), is:

\[
22.4 \text{ dB} - 10 \log_{10}(1 + n)
\]  

And a conversion from \( \frac{\epsilon_s}{N_0} \) to \( \frac{\epsilon_b}{N_0} \) is performed under the assumption of a QPSK PHY layer, which represents two bits as one symbol:
3.2. Simulation Frameworks

\[
\frac{\epsilon_b}{N_0} = \frac{\epsilon_s}{N_0} \quad (3.8)
\]

\[
10\log_{10}(\frac{\epsilon_b}{N_0}) = 10\log_{10}(\frac{\epsilon_s}{N_0} + \frac{\epsilon_s}{N_0} - 3\ dB) \quad (3.9)
\]

\[
\frac{\epsilon_b}{N_0} = \frac{\epsilon_s}{N_0} - 3 \ dB \quad (3.10)
\]

Based on Equations 3.7 and 3.10, Table 3.2 is completed below.

<table>
<thead>
<tr>
<th>Average Number of Interferers</th>
<th>SINR (dB) = \frac{\epsilon_s}{N_0}</th>
<th>\frac{\epsilon_b}{N_0}</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>22.4</td>
<td>19.4</td>
</tr>
<tr>
<td>1</td>
<td>19.4</td>
<td>16.4</td>
</tr>
<tr>
<td>2</td>
<td>17.6</td>
<td>14.6</td>
</tr>
<tr>
<td>3</td>
<td>16.4</td>
<td>13.4</td>
</tr>
<tr>
<td>4</td>
<td>15.4</td>
<td>12.4</td>
</tr>
<tr>
<td>5</td>
<td>14.6</td>
<td>11.6</td>
</tr>
<tr>
<td>6</td>
<td>13.9</td>
<td>10.9</td>
</tr>
<tr>
<td>7</td>
<td>13.4</td>
<td>10.4</td>
</tr>
<tr>
<td>8</td>
<td>12.9</td>
<td>9.9</td>
</tr>
<tr>
<td>9</td>
<td>12.4</td>
<td>9.4</td>
</tr>
<tr>
<td>10</td>
<td>12.0</td>
<td>9.0</td>
</tr>
</tbody>
</table>

Table 3.2: Signal-to-interference-plus-noise ratio corresponding to the number of users transmitting simultaneously in an RA-CDMA channel, according to Equations 3.7 and 3.10.
Based on the SINR for each number of transmitting users, a BER vs SINR curve for QPSK can be used to map the number of transmitting users directly to an expected BER. Using the QPSK BER vs. SINR curve in Figure 3.8, the BER column of Table 3.3 is obtained.

![Figure 3.8: QPSK bit error rate curve used to map $\frac{Eb}{No}$ to BER](image)

Then, a calculation from expected bit error rate to expected packet error rate must be made, as in Equation 3.11.

$$P_p = 1 - (1 - P_b)^N$$  \hspace{0.5cm} (3.11)

where \( P_p \) = Packet Error Rate

\( P_b \) = Bit Error Rate

\( N \) = Number of bits in MPDU
Finally, there is a direct connection between the average number of interferers across the
duration of a transmission and the expected probability of a packet drop, which is applied
to each packet as it passes through the PHY emulator. Table 3.3 shows each step taken to
calculate the probability of a given packet being dropped based on the number of simulta-
neous transmitters, summarizing the MAI modeling performed by the PHY emulator. Note
that a data packet’s MPDU length is 488 bits, while an ACK packet’s MPDU length is 80.
In the simulation, a simple lookup table is used to map column 1 with column 5. This is
how MAI is modeled in the emulator, with the emulator’s lookup table extending up to 40
simultaneous interferers.

<table>
<thead>
<tr>
<th>Average Number of Interferers</th>
<th>SINR (dB) = $\frac{\epsilon_s}{N_0}$</th>
<th>$\frac{\epsilon_b}{N_0}$</th>
<th>Bit Error Rate</th>
<th>Data Packet Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>22.4</td>
<td>19.4</td>
<td>$1^{-9}$</td>
<td>4.88$^{-7}$</td>
</tr>
<tr>
<td>1</td>
<td>19.4</td>
<td>16.4</td>
<td>$1^{-9}$</td>
<td>4.88$^{-7}$</td>
</tr>
<tr>
<td>2</td>
<td>17.6</td>
<td>14.6</td>
<td>$1^{-9}$</td>
<td>4.88$^{-7}$</td>
</tr>
<tr>
<td>3</td>
<td>16.4</td>
<td>13.4</td>
<td>$1^{-9}$</td>
<td>4.88$^{-7}$</td>
</tr>
<tr>
<td>4</td>
<td>15.4</td>
<td>12.4</td>
<td>$5^{-9}$</td>
<td>2.44$^{-6}$</td>
</tr>
<tr>
<td>5</td>
<td>14.6</td>
<td>11.6</td>
<td>$6^{-8}$</td>
<td>2.93$^{-5}$</td>
</tr>
<tr>
<td>6</td>
<td>13.9</td>
<td>10.9</td>
<td>$2.75^{-7}$</td>
<td>1.34$^{-4}$</td>
</tr>
<tr>
<td>7</td>
<td>13.4</td>
<td>10.4</td>
<td>$1.49^{-6}$</td>
<td>7.27$^{-4}$</td>
</tr>
<tr>
<td>8</td>
<td>12.9</td>
<td>9.9</td>
<td>$5.63^{-6}$</td>
<td>2.7$^{-3}$</td>
</tr>
<tr>
<td>9</td>
<td>12.4</td>
<td>9.4</td>
<td>$1.47^{-5}$</td>
<td>7.1$^{-3}$</td>
</tr>
<tr>
<td>10</td>
<td>12.0</td>
<td>9.0</td>
<td>$3.38^{-5}$</td>
<td>1.63$^{-2}$</td>
</tr>
</tbody>
</table>

Table 3.3: Packet error rates corresponding to the number of users transmitting simultane-
ously in an RA-CDMA channel, according to Equation 3.11
RAKE Receiver and Time Collision Modeling

As previously discussed, the simulations herein do not assume a limited number of RAKE demodulators. However, a real hardware system must be constrained, so the simulation framework does include the capacity to model receivers with a limited number of demodulators. Refer to Figure 3.3 in Section 3.1.2 for a diagram on the RAKE timing and explanation of RAKE receiver overloads.

If a RAKE receiver is chosen to be constrained to a limited number of demodulators, the PHY emulator tracks the number of transmitters across the duration of a transmission and flags any new packet transmissions that exceed the number of fingers of the RAKE receiver. Flagged packets are simply dropped in the emulator and are not passed to the access point’s MAC layer processing, so they do not receive an ACK and proceed through the contention mechanism detailed in Section 3.1.2.

In the order to detect packet collisions at the detector, which cause a packet drop, the emulator detects and flags any two or more packet transmissions that begin within ±1 chip cycle of each other. Due to simulation artifacts, the likelihood of a time collision is technically about three times more probable in the simulation than in a real RA-CDMA network. Still, time collisions account for a negligible amount of total dropped packets in the simulation.

CSMA-CA Elimination

Along with the PHY emulator, the elimination of the CSMA algorithm is the second significant modification to the IEEE 802.15.4 simulation framework to accommodate RA-CDMA. The modification of the simulation framework to cut out the CSMA-CA processing was very straightforward, allowing the preservation of the majority of MAC layer processing while eliminating the CSMA-CA multiple access. When an idle node pulls a frame from the frame
queue for processing, the node is put directly into a transmitting state rather than a CSMA processing state, representing an accurate model of an RA-CDMA node’s state machine. A few additional modifications were needed due to the elimination of CSMA-CA processing, such as an implementation of the contention mechanism’s random backoff algorithm, but these modifications were minor. The simple elimination of CSMA-CA allows the comparison of IEEE 802.15.4 and RA-CDMA to truly be limited to multiple access techniques rather than MAC layer protocols.

With the Matlab framework properly modified for RA-CDMA simulations, through the addition of a PHY emulator and elimination of CSMA-CA, network behavior was verified using similar means as in the 802.15.4 simulation, outlined in Section 3.2.1. Figure 3.9 shows RA-CDMA network activity time plots. Compare with Figure 3.7 to see the differences in behavior between between 802.15.4 and RA-CDMA. Specifically note the overlapping packet transmissions in RA-CDMA that result still with a successful acknowledgement, demonstrating RA-CDMA’s multiple access.
Figure 3.9: Sample RA-CDMA time plots showing simultaneous transmissions with no collisions

### 3.3 Simulation Results

The final results of the network scalability comparison of IEEE 802.15.4 and RA-CDMA, obtained through Matlab end-to-end simulations, are presented in this section. The primary means of directly comparing IEEE 802.15.4 and RA-CDMA is through the performance metrics explained in Section 3.1.3: (1) Total Network Throughput, (2) Packet Delivery Ratio, and (3) Average Packet Latency. Plots of each metric are included for each multiple
access technique, allowing an objective analysis. A closer look at the network behavior of each protocol is also presented through supplemental plots that offer insight and explanation of the network performance metrics.

### 3.3.1 IEEE 802.15.4 vs. RA-CDMA Results

The performance metric plots for IEEE 802.15.4 networks are presented as a function of both the number of nodes in the network and the desired data rate of each node. The simulated per-node data rates are 1, 5, 10, and 15 kbps, meaning each node in the network is generating data packets and adding them to their frame queues at a rate to satisfy these throughputs, respectively. RA-CDMA performance metric results are likewise presented as a function of the number of nodes in the network and the desired data rate per node.

Of specific interest when analyzing the plots is the channel capacity of the networks. As explained in Section 3.2.1, the maximum theoretical data rate of the modeled IEEE 802.15.4 network is 250 kbps, but the maximum channel capacity is 96 kbps due to protocol overhead, as calculated in Equation 3.3. The single-node capacity in RA-CDMA is 186 kbps, which can be scaled to as many nodes as are in the network until MAI becomes prohibitive.

Another crucial element to consider when analyzing results in this section are the channel bandwidths of each protocol. The modeled IEEE 802.15.4 PHY layer assumes a 2.5 MHz channel bandwidth while the emulated RA-CDMA PHY layer is based on a 10 MHz channel bandwidth. In order to practically compare network scalability, channel bandwidths must be factored in because four IEEE 802.15.4 channels could be implemented within the same bandwidth as a single RA-CDMA channel. So, while analyzing the throughput plots, a factor of four should be considered for the IEEE 802.15.4 plots in order to form a comparison in terms of channel bandwidth.
Figures 3.10a and 3.10b show the total throughput of the single-channel networks. It is apparent that IEEE 802.15.4 networks reach peak throughput at significantly lower network sizes than RA-CDMA, even after incorporating a factor of four to normalize bandwidth.
3.3. Simulation Results

Figures 3.11a and 3.11b present packet delivery ratio results. The trend seen in the throughput graphs is also apparent in the delivery ratio, as packet failures occur in smaller network sizes in IEEE 802.15.4.

(a) IEEE 802.15.4 packet delivery ratio of a single 2.5 MHz channel

(b) RA-CDMA packet delivery ratio of a single 10 MHz channel

Figure 3.11: Packet Delivery Ratio Comparison of IEEE 802.15.4 and RA-CDMA
Along with the other deteriorating performance metrics, packet latency increases in 802.15.4 for smaller network sizes than does that of RA-CDMA, shown in Figures 3.12a and 3.12b.

Figure 3.12: Average Packet Latency Comparison of IEEE 802.15.4 and RA-CDMA
### 3.3.2 IEEE 802.15.4 Network Behavior

Beyond the performance metrics, an informative indicator of network behavior in an IEEE 802.15.4 network is the total number of dropped packets and the cause of each packet drop. Packet drops are the primary source of decreased performance, so they offer a good perspective into cumulative trends across edge nodes.

Figure 3.13 contains plots showing the overall packet drops as a percentage of overall network traffic. This is different from packet delivery ratio, which does not account for packet retransmissions. Also included in the plots is the cause of packet drops, which is shown to be primarily timeouts of 802.15.4’s CSMA-CA algorithm.

![IEEE 802.15.4 Packet Drops](image)

Figure 3.13: Total Dropped Packets and Causes in IEEE 802.15.4
3.3.3 RA-CDMA Network Behavior

This section contains plots to convey the network behavior of RA-CDMA and further explain the trends seen in Section 3.3.1. Because MAI is the primary cause of dropped packets in RA-CDMA networks, degraded performance is directly traced to high levels of MAI. Further, MAI is a direct function of the number of simultaneously transmitting devices, so the number of transmitting devices is very closely related to overall network performance. Plots in Figure 3.14 show the average number of simultaneous transmitters and the corresponding BER and PER. Some interesting behavior is apparent once the average number of transmitters exceeds the initial linear region, where a sudden non-linear increase in traffic occurs.

![Average Number of Simultaneously Transmitting Devices](image1)

![Average Bit Error Rate](image2)

![Average Packet Error Rate](image3)

Figure 3.14: Avg Number of Simultaneous Transmitters and Corresponding BER and PER
3.4. Analysis

Plots conveying the overall packet drops and their causes, shown in Figure 3.15, provide more insight into the degradation of network performance and further exemplify the trends seen throughout this section. The only cause of dropped packets in RA-CDMA is shown to be bit errors caused by MAI. Plots for 1 and 5 kbps desired per-node throughputs are not included because these simulations do not have any packet drops.

![Figure 3.15: Total Dropped Packets and Causes in RA-CDMA](image)

Figure 3.15: Total Dropped Packets and Causes in RA-CDMA

3.4 Analysis

The overarching takeaway from the results presented in Section 3.3 is that IEEE 802.15.4’s CSMA-CA multiple access and contention processing seems to break down at lower network sizes than RA-CDMA. Using the plots presented, this section will find the extent to which RA-CDMA performance exceeds 802.15.4 and explain why this happens.

It is difficult to generalize the network scalability comparison to a single conclusion because the actual number of supported nodes is very dependent on specific network features. Throughput, delivery ratio, and latency all offer different metrics with which to compare scalability. The desired data rate of each sensor is another factor to consider. In order to
best attempt a generalized conclusion, consider the 15 kbps case in Figure 3.10. The peak throughput value of about 90 kbps is reached at a network size of eight nodes. Extrapolating this value to the same bandwidth of an RA-CDMA network, a factor of four, while maintaining the same peak throughput per channel, results in an IEEE 802.15.4 maximum network size of about 32 nodes. Focusing on RA-CDMA’s corresponding plot, peak throughput is reached at about 60 nodes in the network. The ratio of 32:60 leads to the conclusion that RA-CDMA can support roughly twice the number of nodes as IEEE 802.15.4. The same process can be performed for the 10 kbps data rates and leads to a ratio of about 48:90, a ratio of just under 1:2. So it is a reasonable conclusion to say that RA-CDMA is capable of supporting approximately twice the number of nodes while maintaining linear network throughput.

The packet delivery ratio provides another method of comparison between IEEE 802.15.4 and RA-CDMA network sizes. Assuming a WSN must maintain a packet delivery ratio above 90 percent and focusing on a 15 kbps data rate, an IEEE 802.15.4 channel can support about six end devices, which is extrapolated to 24 devices after factoring channel bandwidth. In the same scenario, RA-CDMA can support 65 nodes, a factor of just under 1:3. Likewise, for the 10 kbps case, the IEEE 802.14.5-to-RA-CDMA ratio is about 24:90, slightly above a 1:3 ratio. If packet delivery ratio is a WSN’s constraint, a single RA-CDMA channel can support around three times more nodes than IEEE 802.15.4 channels within the same bandwidth.

3.4.1 IEEE 802.15.4 Analysis

Referring to Figure 3.10a, the plot conveys that 802.15.4 network throughputs perform linearly as a function of the number of nodes in the network, up until the channel capacity is reached. For the simulations, maximum theoretical channel capacity is calculated in Equa-
tion 3.3 to be 96 kbps, and the results show a general adherence to that value, with slight loss as expected due to simulation overhead and the CSMA-CA algorithm. Once the channel capacity is exceeded by the cumulative data rate of the end nodes, throughput begins to decrease to the point of ruin.

The cause of decreasing network performance beyond the channel capacity is explained in Figures 3.11a, 3.12a, and 3.13. Beginning at the point of maximum channel capacity, the packet delivery ratio trends downward from 100 percent, meaning that packets are beginning to be dropped in the CSMA algorithm, as proved in Figure 3.13. Also, as packet drops begin, average packet latency increases. This behavior makes sense as packets are spending more time in backoff states as they struggle to complete a successful CCA.

IEEE 802.15.4 network behavior is best summarized as linearly increasing as a function of network density until the point that cumulative network data rates exceed the theoretical channel capacity, when overall network performance decreases due to the CSMA-CA cascading backoff effect.

3.4.2 RA-CDMA Analysis

It is clear when examining Figures 3.10b-3.15 that the general trend of linear network throughput as a function of number of nodes in a network is maintained in RA-CDMA simulations similarly to IEEE 802.15.4 simulations; however, the RA-CDMA trend continues much farther into larger networks than does 802.15.4. It is able to support the higher node densities because its channel capacity is significantly larger, bounded only by the effects of MAI, which is far less prohibitive than the CSMA algorithm.

A close analysis of Figure 3.14 reveals some interesting details of the method in which RA-CDMA networks break down due to MAI. Networks with each data rate grow linearly as a
function of the number of nodes in the network. This linear region is the nominal operating region below the channel capacity. Packet latency is minimal and delivery ratio is perfect in this region because MAI is small and packet drops are not present. As more nodes join the networks, a transition region is reached when the channel capacity is approached by the cumulative throughput desired by all end devices. The region is non-linear because it represents the division between perfect network behavior and complete channel saturation. The transition region is followed by a saturation region in which so many devices are transmitting that the BER is prohibitive and no packets are successful. Dropped packets then cause retransmissions and backed up frame queues, which causes a cascading effect that raises the overall MAI to a level that is completely prohibitive.

A noteworthy takeaway from RA-CDMA simulations is the effect of the contention processing algorithm on network performance, especially when approaching channel capacity. A poorly optimized algorithm can trigger the beginning of the transition region at a surprisingly small network size, which causes prohibitive MAI at a relatively low number of nodes. To the contrary, a well optimized contention algorithm can extend network performance far beyond the expected capacity. Optimization is highly dependent on the inherent tradeoffs of contention processing. A throughput-optimized algorithm can cause extremely high latencies while a latency-optimized algorithm will cause lower packet delivery ratio.

It is clear that the IEEE 802.15.4 contention processing algorithm applied to RA-CDMA is not optimized for RA-CDMA, and yet RA-CDMA still outperforms 802.15.4 in the same channel bandwidth. An optimized algorithm for RA-CDMA would be expected to increase RA-CDMA performance over IEEE 802.15.4 even more so.
The previous section shows that in dense WSNs, RA-CDMA is a superior multiple access and contention processing technique than CSMA-CA. But the comparison does not account for MAC protocol optimization to RA-CDMA; rather, the comparison assumes a nearly identical MAC layer with similar MAC processing. If a MAC protocol is designed to be optimized for use with the RA-CDMA multiple access scheme, performance is expected to improve even more over CSMA-CA and specifically IEEE 802.15.4. This chapter will introduce some key features of a MAC layer design optimized for RA-CDMA.

4.1 Network Topology

A fundamental contributor to a MAC design is the assumed network topology, which defines the flow of packets from node to node. In this proposed MAC layer, the network topology is a hierarchical network with defined wired access points commanding and collecting data from a large grouping of wireless sensors, or edge nodes. The terminology of edge node refers to a single sensor transceiver at the bottom of the hierarchy, while access point refers to the wired nodes at the next higher layer of the hierarchy. At the top layer of the hierarchy is a central computing hub which manages the network at the application layer, thus relieving
the edge nodes and access points of much of the application-level processing.

Despite the inherent master-slave relationship between the hierarchy of nodes, the overall link characteristics are envisioned as symmetric (all packets are equally prioritized), with data primarily flowing upward from the large collection of edge nodes to the access points. Figure 4.1 shows the network topology.

![Figure 4.1: Star-of-stars hierarchical topology supported by the proposed MAC protocol](image)

By constraining the network topology to this fully standardized hierarchy, significant network overhead is eliminated in comparison to other IoT MAC layers.

The motivation towards this type of hierarchical topology is driven directly by intended use cases involving the physical environments. For example, a vehicular wireless sensor network using this topology may have an access point in the engine compartment, passenger cabin, and trunk, all of which are physically separated. In a factory environment, sensor and actuator nodes may be distributed densely, but each primary collection of nodes for a machine can be treated as a distinct subnet with one access point per machine.

Theoretically, this topology could be modified to permit mesh networking by using destination addresses and other routing protocols, but these additional considerations increase overhead and computation, likely negating the core benefits of RA-CDMA.
4.2. Frame Format

Redundancy

For the purpose of redundancy, each edge node should be allowed to connect with both a primary access point, which serves as its master, and at least one additional secondary access point to serve as a backup. This relationship is shown in Figure 4.2. Note that Figure 4.1 contains only primary access point links for visual simplicity.

![Relationship of edge nodes with primary and secondary data concentrators, showing redundancy](image)

Figure 4.2: Relationship of edge nodes with primary and secondary data concentrators, showing redundancy

4.2 Frame Format

The frame formatting adopted for the proposed MAC layer is largely based on that of the IEEE 802.15.4 MAC protocol. Some modifications to the IEEE 802.15.4 general frame format are made to minimize the MAC header for optimization to RA-CDMA and a hierarchical topology while retaining many of the core functions for low power wireless sensor networks.

A general frame format for this MAC protocol is shown in Figure 4.3b along with an 802.15.4 frame in Figure 4.3a for reference. Each grayed-out field could be eliminated from the frame for specific reasons related to the standardized topology and application to CDMA. For example, by utilizing RA-CDMA, the destination address need not be plainly transmitted.
over-the-air. Rather, the physical layer uses the destinations spreading code, which is based on its address, to send a packet to its targeted destination. This is a key feature and benefit of CDMA. Note also that though the destination address is passed in the packet between MAC and physical layers, the physical layer treats it as a control parameter and therefore does not transmit it.

In total, modifications to the MAC Header result in a MAC overhead of between 2-9 bytes per packet, compared to 5-39 bytes per packet for IEEE 802.15.4.

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>Frame Control</th>
<th>Sequence Number</th>
<th>Source Address</th>
<th>Payload Length</th>
<th>Frame Payload</th>
<th>Frame Check Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>0/1</td>
<td>0/1/2</td>
<td>0/1</td>
<td>0-255</td>
<td>1/2/4</td>
</tr>
<tr>
<td></td>
<td>MAC Header (MHR)</td>
<td>MAC Payload</td>
<td>MAC Footer (MFR)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(a) RA-CDMA MAC General Frame Format

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Sequence Number</th>
<th>Destination PAN ID</th>
<th>Destination Address</th>
<th>Source PAN ID</th>
<th>Source Address</th>
<th>Auxiliary Security Header</th>
<th>Information Elements (IE)</th>
<th>Frame Payload</th>
<th>Frame Check Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addressing fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>MHR</td>
<td>MAC Payload</td>
</tr>
</tbody>
</table>

(b) IEEE 802.15.4 General Frame Format

Figure 4.3: Comparison of frame formats with gray area showing eliminated fields
4.3 Edge Node Profiles

Each edge node is defined by a comprehensive list of network parameters that completely defines the nodes communication behavior and characteristics, from physical layer parameters to application layer details. The comprehensive list is known as a node profile. By having memory of node profiles, the central processing hub can better manage the network and overall communication overhead is reduced from the bottom up. Examples of edge node parameters include frame check sequence (FCS) length and various packet flags that may affect an access points actions.

The overall concept of node profiles is that an edge node should not be wasting transmitted energy on repetitive information that could be memorized and maintained by the central hub without frequent transmission. A simple example of such a policy is to incorporate change detection into the reporting of sensor values by reporting only up/down indicators for slowly changing values like temperature, provided their values do not exceed pre-defined control limits.

Another purpose for edge node profiling is the potential implementation of priority-based contention. If cumulative network traffic climbs to near the channel capacity, the central hub can intelligently throttle the traffic of low-priority nodes as an attempt to curb overall network traffic.

4.4 Error Handling

The proposed MAC layers error handling is very flexible to allow for optimization to many different types of nodes with varying error tolerances. For example, a highly critical temperature sensor should have a low tolerance for packet errors while a video sensor may be
allowed more lost data.

The error handling process is generalized for all edge nodes, but specific error thresholds are customizable to allow flexibility. For instance, all messages should be positively acknowledged, but the timeout threshold for acknowledgment for each edge node can be different, depending on the edge node’s profile. Figure 4.4 shows the error handling algorithm used. Though the algorithm itself is similar to other MAC standards, the flexibility allowed by edge node profiles is specifically optimized for RA-CDMA networks.

Figure 4.4: Proposed MAC Error Handling Flowchart
4.5 Network Formation

Upon power-up, edge nodes and access points default into network formation mode. This mode is purposed to initialize the network’s topology and form all necessary communication links, as well as maintain them throughout all network phases. Due to the nature of low power nodes, especially if energy harvesting is a source of power, edge nodes must be able to enter or exit the network at any time.

While in network formation mode, each access point transmits an advertisement beacon at a rate defined by the central hub. When an unconnected edge node, which monitors the advertising channel, receives a beacon from an access point, it transmits a response after a back-off period that contains the received signal strength indicator (RSSI) of the received beacon. A back-off is necessary to prevent collisions because unconnected edge nodes do not yet know their assigned access point and thus must use a broadcast spreading code. The SNR of the received beacon and the edge nodes response is used by the central hub to determine the optimal primary and secondary access point assignments. Then the primary access point initiates an association request, authentication, and configuration. This sequence is shown in Figure 4.5.

This network formation and maintenance process is designed for simplicity and fits well into a RA-CDMA protocol. Access points can use a broadcast spreading code, which all edge nodes listen for, to address the advertising beacon to all edge nodes within range. This is a benefit over other protocols that have timing and synchronization requirements for broadcast beacons.
Summary

A MAC layer specifically optimized for RA-CDMA multiple access will allow increased network performance over the simulation results shown in Chapter 3, which uses features from the IEEE 802.15.4 MAC protocol instead. An optimized MAC protocol will be extremely simple and lightweight to complement the random access-like RA-CDMA multiple access. The proposed MAC protocol greatly reduces overhead and complexity compared to existing MAC layers while still meeting WSN requirements.
Chapter 5

Conclusions and Future Work

In the near future, wireless sensor networks will grow increasingly large and dense, with a necessity to support dozens or hundreds of sensor nodes in a single network. Current multiple access techniques in IoT WSNs are thoroughly investigated in this work and determined to have insufficient network scalability to support dense WSNs. Because of this, a new multiple access technique based on receiver-assigned CDMA is proposed, which could satisfy network scalability requirements and contribute the added benefits of interference mitigation and physical layer security.

The work presented compares the leading candidate multiple access technique, CSMA-CA, used by the IEEE 802.15.4 MAC layer, with the proposed RA-CDMA technique. The two schemes are simulated using a Matlab-based end-to-end simulation framework. Results show that RA-CDMA outperforms IEEE 802.15.4 in all three performance metrics analyzed - total network throughput, packet delivery ratio, and average packet latency - in large and dense networks.

Given that RA-CDMA is a higher performing multiple access technique in WSN architectures of interest, a logical next step is the optimization of an entire MAC layer protocol for RA-CDMA. The main focus of such a MAC layer is a lightweight and simple design to complement the random access properties of RA-CDMA. Key features of the protocol include a topology definition, frame formatting, error handling, and other specifications that significantly reduce overhead compared to industry standards.
**Future Work**

The future outlook on the technology detailed in this work is very bright and could turn in many possible directions. RA-CDMA multiple access is a potential enabling technology for WSNs incorporating hundreds of sensors into a single network, especially when coupled with an optimized MAC design to further improve performance.

Specifically, future work includes defining the details of the RA-CDMA MAC layer and reaching a complete implementation. It is shown that contention processing optimization has an enormous effect on network scalability. Optimizing RA-CDMA’s backoff durations and other algorithm parameters could potentially increase performance significantly. Next steps could include further testing and evaluation of RA-CDMA, with focus on power consumption and receiver complexity, or integration into FPGA or ASIC hardware.

Steps towards the productization of RA-CDMA for low power, scalable WSNs are imminent, and the results presented herein support the movement towards the integration of these networks into industrial systems.
Bibliography

[1] IEEE standard 802.15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans), 2011.


[43] Tijs van Dam and Koen Langendoen. An adaptive energy-efficient mac protocol for...

