January 2021

Versatility Of Low-Power Wide-Area Network Applications

Dali Ismail
Wayne State University

VERSATILITY OF LOW-POWER WIDE-AREA NETWORK APPLICATIONS

by

DALI ISMAIL

DISSERTATION

Submitted to the Graduate School

of Wayne State University,

Detroit, Michigan

in partial fulfillment of the requirements

for the degree of

DOCTOR OF PHILOSOPHY

2021

MAJOR: COMPUTER SCIENCE

Approved By:

_____

Advisor Date

_____

_____

_____

_____

DEDICATION

Dedicated to Elamin, Siham, Sahar, Eiman, Mohamed, and my wife Khiloud

ACKNOWLEDGEMENTS

First of all, I would like to thank my advisor, Dr. Abusayeed Saifullah, for his exceptional guidance and continuous support throughout my Ph.D. journey. I believe I would not be able to complete my Ph.D. without his encouragement. To that, I admire him. I would also like to thank my co-advisor, Dr. Sanjay Madria, for his guidance and support.

To my family, I thank you all for your patience, unconditional love, and for believing in me despite all the difficulties we overcame over the past six years.

To my lab mates, Dr. Mahbubur Rahman, Dr. Prashant Modekurthy, and Sezana Fahmida thank you for your support. I would like to especially thank Dr. Mahbubur Rahman for being a great friend throughout my Ph.D. journey.

I would also like to thank all the faculty members in the Department of Computer Science at Wayne State University.

I am truly grateful for the financial support from my advisor, the Department of Computer Science at Wayne State University, and the National Science Foundation (NSF)

Lastly, I would like to extend my thanks to all the committee members for their valuable time and advice.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

The Internet of Things (IoT) has emerged as a way to revolutionize the future of communication and change the way we interact with things around us. IoT promises to enhance human lives by connecting all the devices that benefit from an Internet connection, improves sustainability, and safety for industry and society, by sensing the environment and making decisions based on the acquired information. It is expected that by 2025 there will be around 22 billion connected devices [40]. To realize the future of IoT, the need for new communication technologies connecting the massive number of devices to support the wide variety of IoT applications is critical.

Along with the traditional cellular (e.g., 2G, 3G, LTE [121]) and existing wireless technologies (e.g., WiFi [53], Bluetooth [16], IEEE 802.15.4 [1], WiMax [138, 146, 100]), the recently emerged Low-Power Wide-Area Network (LPWAN) technology promises to support the diverse requirements for IoT applications. LPWAN is characterized by long-range, low-power, low-cost, for both the devices and infrastructure, and support for massive number of devices [40]. Due to their increasing demand, several competing technologies are being developed including LoRa [77], SigFox [115], IQRF [58], RPMA (Ingenu) [57], DASH7 [32], Weightless-N (nWave) [135], Weightless-P [135], SNOW (Sensor Network Over White Spaces) [106, 107, 108], LTE Cat M1 [79], EC-GSM-IoT [49], NB-IoT [88], and 5G [90]. Despite their popularity, LPWANs are designed for low-power and low data rate operations. Most LPWANs use narrowband channels to decrease the noise level and extend their transmission range, limiting their adaptability in many IoT applications. Furthermore, some LPWANs are required to duty cycle (e.g., LoRa) or operate in a dynamic spectrum (e.g., SNOW).

As the number of IoT devices increases, many devices in an LPWAN can be mobile. The usage of drones, tractors, and vehicles makes mobility a key concern for several applications (e.g., agricultural IoT). Most LPWAN technologies are not designed to handle mobility. Cellular-based LPWANs rely on the existing wired infrastructure to enable mobility where such infrastructure does not exist/is limited in many rural areas. For example, in remote areas (e.g., farms, oil fields), often there is weak or no cellular coverage at all. The high cost of subscribing to cellular services is also hindering the adoption of cellular-based technologies. In other LPWANs, handling mobility is quite challenging and not well-addressed yet.

In this dissertation, we first identify the key opportunities of LPWAN, highlight the challenges, and show potential directions for future research. Second, we exploit LPWANs to demonstrate the versatility of their applications. Specifically, we develop a novel approach to enable applications that involve mobility in LPWAN. We propose the following work.

To enable efficient inter-network mobility, we propose to handle mobility in LPWAN over white spaces. Specifically, we consider SNOW. Our approach enables inter-SNOW mobility by designing a dynamic CFO (Carrier Frequency Offset) estimating and compensation technique that considers the impact of the Doppler shift. Also, we proposed a mobility-aware subcarrier assignment to circumvent the impact on the geospatial variation of white space within the same SNOW. Finally, we propose an energy-efficient and fast base station (BS) discovery approach which utilizes the signal features to distinguish between the TV station and SNOW BS and a lightweight cross-layer technique to associate the mobile nodes with the BS. Finally, To demonstrate the feasibility of our inter-SNOW mobility, we implement and evaluate our approach using USRP and Texas

Instruments (TI) CC1310 devices in different environments.

Finally, we present RnR (Reverse & Replace Decoding), a novel PHY-link layer collision detection and recovery technique designed for Wireless Sensor Network (WSN). RnR can recover packets from a single collision and can be easily adapted in LPWAN.

The rest of the dissertation is organized as follows. Chapter 2 presents the opportunities and challenges in LPWANs. Chapter 3 describes handling mobility in LPWAN. Chapter 4 presents the design of RnR. Chapter 5 discusses future work. Chapter 6 concludes the dissertation.

CHAPTER 2 LOW-POWER WIDE-AREA NETWORKS: OPPORTUNITIES, CHALLENGES, AND DIRECTIONS

LPWAN is an emerging network technology for IoT which offers long-range and wide-area communication at low-power. It thus overcomes the range limits and scalability challenges associated with traditional short range wireless sensor networks. Due to their escalating demand, LPWANs are gaining momentum, with multiple competing technologies currently being developed. Despite their promise, existing LPWAN technologies raise a number of challenges in terms of spectrum limitation, coexistence, mobility, scalability, coverage, security, and application-specific requirements which make their adoption challenging. In this chapter, we identify the key opportunities of LPWAN, highlight the challenges, and show potential directions of the future research on LPWAN.

2.1 Introduction

To support IoT, recent developments in communication technologies have given rise to LPWAN. Complementary to cellular (e.g. 2G, 3G, LTE [121]) and existing wireless technologies (e.g. WiFi [53], Bluetooth [16], IEEE 802.15.4 [1], WiMax [138]), the LPWAN technologies promise to support long-range, low-power consumption, low cost for both the devices and infrastructure, and connect a massive number of devices [40]. Due to their increasing demand, several competing technologies are being developed including LoRa [77], SigFox [115], IQRF [58], RPMA (Ingenu) [57], DASH7 [32], Weightless-N (nWave) [135], Weightless-P [135], SNOW (Sensor Network Over White Spaces) [106, 107], LTE Cat M1 [79], EC-GSM-IoT [49], NB-IoT [88], and 5G [90]. Cellular based LPWANs (LTE Cat M1, EC-GSM-IoT, NB-IoT, 5G) operate in licensed

band. The unlicensed sub-GHz ISM band is the operation band for most non-cellular LPWANs except SNOW that operates in the TV white spaces.

The LPWAN technologies are still in their infancy with some still being developed (e.g, 5G, NB-IoT, LTE Cat M1, Weightless-P), some having only uplink capability (e.g, SigFox, Weightless-N), while, for some, there is still no publicly available documentation (e.g., SigFox). Despite their promise, existing LPWAN technologies raise a number of challenges in terms of spectrum limitation, coexistence, mobility, scalability, coverage, security, and application-specific requirements such as data rates and real-time communication which make their adoption challenging. As LPWAN is considered to be one of the key technologies of today to drive the IoT of tomorrow, it is critical to address these challenges. In this chapter, we identify the key opportunities of LPWAN, highlight the challenges, and show potential directions of the future research on LPWAN.

In the rest of the chapter, Section 2.2 presents the characteristics of LPWANs. Section 2.3 overviews the state-of-the-art LPWAN technologies. Section 2.4 describes the opportunities of LPWAN. Section 2.5 presents the research challenges and future directions in LPWANs. Section 2.6 concludes the chapter.

2.2 Characteristics of LPWANs

2.2.1 Long-Range Connectivity

In contrast to traditional short-range wireless sensor networks, the design goal of LPWANs is to offer wide-area coverage at low-power, and low cost. Most LPWANs [77, 115, 106, 135, 49] achieve long communication range and thus form a star topology where the devices directly communicate with the base station (BS). Excluding Ingenu RPMA (2.4GHz) [57], most non-cellular

LPWANs operate on low frequencies (sub-GHz band) that provide long communication range (from few kilometers in urban areas to tens of kilometers in rural areas). Lower frequencies have better propagation characteristic through obstacles. These properties made sub-GHz band attractive for LPWANs technologies.

2.2.2 Low-Power

IoT devices are expected to operate for a very long time (several years) without the need to replace the battery. LPWANs achieve low-power operation using several approaches. **First**, they usually form a star topology, which eliminates the energy consumed through packet routing in multihop networks. **Second**, they keep the node design simple by offloading the complexities to the BS/gateway. **Third**, they use narrowband channels, decreasing the noise-level and extending the transmission range [106, 88].

2.2.3 Low Deployment and Operational Cost

A major factor contributed to the rise of LPWANs is its low cost. Non-cellular LPWANs require no (or limited) infrastructure and operate on unlicensed spectrum, providing an excellent alternative to the cellular network. In addition, the advances in the hardware design and the simplicity of LPWAN end-devices makes LPWANs economically viable [3].

2.2.4 Reliability and Robustness

LPWANs are designed to provide reliable and robust communications. Most LPWANs adopt robust modulation techniques and spread-spectrum techniques to increase the signal resistance to interference and provide a level of security. In spread-spectrum, narrowband signal is spread in the frequency domain with the same power density resulting in a wider bandwidth signal [133].

2.2.5 Potential to Scale

Avoidance of multihop topology gives high potential to scale the LPWANs. In addition, LPWANs use narrowband to support a massive number of devices to efficiently utilize the limited spectrum. Besides some LPWANs (e.g., LoRa) use multiple antenna systems to enable the BS to support large number of nodes. Some adopts massively parallel communications in both directions using single antenna system (e.g., SNOW), thus providing opportunities to scale. Scalability of LPWAN is also affected by a number of factors such as the underlying MAC (media access control) protocol, duty-cycle, and reliability requirement.

2.3 Overview of Existing LPWANs

Here we overview the current LPWAN technologies. Figure 2.1 classifies them. A summary of these technologies is shown in Table 2.1.

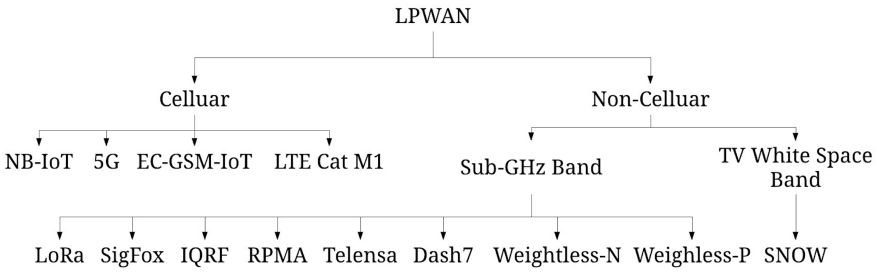


Figure 2.1: LPWAN technologies classification

2.3.1 Infrastructure Based LPWAN Technologies

NB-IoT. NB-IoT (Narrowband IoT) [88, 127] is a 3rd Generation Partnership Project (3GPP) LPWAN technology offering flexibility of deployment by allowing the use of a small portion of the available spectrum. It supports up to 50k devices per cell, and requires minimum 180 kHz of bandwidth to establish communication. It can be deployed as a stand-alone carrier with available

	NB-IoT	EC-GSM-IoT	LTE Cat M1	LoRa	SigFox	IQRF	RPMA	Telensa	DASH7	Weightless-N	Weightless-P	SNOW
Modulation	QPSK, OFDMA (UL), SC-FDMA (DL)	GMSK, 8PSK	QPSK	CSS	DBPSK, GFSK	GFSK	DSSS, CDMA	FSK	GFSK	DBPSK	GMSK, OQPSK	BPSK
Band	Licensed, Sub-GHz	Licensed, Sub-GHz	Licensed, Sub-GHz	Unlicensed, Sub-GHz	Unlicensed, Sub-GHz	Unlicensed, Sub-GHz	Unlicensed, 2.4 GHz	Unlicensed, Sub-GHz	Unlicensed, Sub-GHz	Unlicensed, Sub-GHz	Unlicensed, Licensed, Sub-GHz	Unlicensed, TV white spaces
Max Range (Km)	15	15	15	15	10	0 - 5	15	1 - 10	0 - 5	0 - 3	0 - 2	5
Peak data rate (kbps)	250 kbps (UL), 170 kbps (DL)	10	375	27	1	20	80	65	9.6, 55.666, 166.766	100	100	50kbps per node
Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	N/A
Indoor	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	No	Yes	Yes
Link budget (dB)	164	164	164	164	N/A	N/A	177	N/A	N/A	N/A	N/A	N/A
Mobility	No	Yes	Yes	Yes	No	Yes	Limited	No	N/A	No	No	N/A
Battery lifetime (Years)	10	10	10	10	5	N/A	15	10	N/A	N/A	N/A	N/A

Table 2.1: Summary of LPWAN Technologies.

spectrum exceeding 180 kHz, in-band within an LTE physical resource block, or in the guard-band inside an LTE carrier. NB-IoT uses resource mapping to preserve the orthogonality of LTE signals by avoiding mapping signals to resources currently used by LTE signals [88].

EC-GSM-IoT. Extended Coverage-GSM-IoT [49] is 3GPP standard-based LPWAN technology. EC-GSM-IoT is based on enhanced GPRS (eGPRS), designed to support long-range, low-power, and high capacity communication. EC-GSM-IoT is backward compatible with existing GSM technologies. Hence, it can be added to the existing cellular network as a software upgrade, reducing the cost of infrastructure and deployment. EC-GSM-IoT extends the coverage of GPRS by 20 dB [40]. To support various application requirements, EC-GSM-IoT provides two modulation options, Gaussian Minimum Shift Keying (GMSK) and 8-ary Phase Shift Keying (8PSK). Using these two modulations, it achieves peak data rate of 10 kbps and 240 kbps receptively. Additionally, EC-GSM-IoT improves battery lifetime by using extended Discontinued Reception (eDRX) technique, which allows the device to choose the number of inactivity periods depending on the application requirements. EC-GSM-IoT can support up to 50k devices using a single BS.

LTE Cat M1. LTE Cat M1 is an LPWAN technology introduced as a part of 3GPP Release 13 offering long-range connectivity at low-power [79]. It is specifically designed to support IoT applications requiring low to medium data rate. In addition, it offers Voice over LTE (VoLTE) functionality, enabling new use cases for IoT. LTE Cat M1 make use of the existing cellular infrastructure to support mobility and seamless communication handover at similar speeds to LTE. Finally, LTE Cat M1 supports firmware updates over the air to ensure security over long distances [79].

5G. The 5th generation of mobile technology (5G) is expected to be commercially ready by the

year 2020 [90]. 5G is expected to support a wide range of existing and future use cases in addition to the legacy mobile broadband. Specifically, for massive IoT applications, 5G will provide long-range, low-power, and low cost connectivity. In this case, several improvements over the 4G system are needed in terms of end-to-end delay, spectral efficiency, network capacity, cost-efficient deployment, and interference cancellation.

2.3.2 Infrastructure-less LPWAN Technologies

Long Range (LoRa). LoRa is a proprietary physical layer (PHY) design used in Long Range Wide Area Network (LoRaWAN) specification [77]. LoRaWAN is the specification defining the protocol and network architecture. LoRa network is organized in a special star topology, called star-of-stars, where the gateway nodes relay messages between end-devices and a central network server. LoRa defines three different classes for the end-devices to serve different application with different requirements. These classes offer a trade-off between downlink communication, latency, and energy efficiency (battery lifetime). **Class A:** End-devices of Class A support bi-directional communications where each uplink transmission is followed by two short downlink receive slots depending on the application need. The end-device randomly schedule the downlink slots based on ALOHA-like protocol [2]. **Class B:** Extend Class A random receive window by allowing extra receive window at scheduled times. The gateway node transmits a time-synchronization beacon to end-devices allowing the server to know when they are listening. **Class C:** In Class C, the receive window is continuously open unless the end-device is transmitting.

SigFox. SigFox [115] is a proprietary LPWAN technology based on Ultra-Narrowband (UNB) modulation technique [141]. UNB offers efficient spectrum utilization resulting in increased net-

work capacity and low-power consumption. SigFox adopts duty-cycled transmission of %1 in Europe. SigFox supports very low data rate compared to other LPWA technologies. SigFox allows only 140 12-bytes message per day, each transmission taking 3 seconds. To provide reliability, SigFox transmits the message multiple times, resulting in high energy consumption.

IQRF. IQRF [58] is an LPWAN technology designed to support ultra-low-power operations, and low-rate, low traffic wireless connectivity. Unlike other LPWANs, it uses mesh network topology and can support up to 239 nodes using a single coordinator. It achieves hundreds of meters range per hop in the outdoors, and tens of meters in indoors. However, with a special arrangement, IQRF can achieve several kilometers per hop [58]. IQRF implements two transmission modes – *networking* and *non-networking*. The networking mode is implemented for communication with multiple nodes and non-networking mode is for single or multiple peer-to-peer communication.

RPMA (Ingenu). Ingenu [57] proposed an LPWAN technology based on Random Phase Multiple Access (RPMA) technology. It offers low-power, low cost, robust, and bi-directional communication. Operating on the globally available 2.4 GHz band, RPMA exploits the rules and regulation imposed on 2.4 GHz band, such as minimum duty-cycle, to provide long-range communications at low-power. It allows nodes to share the same transmission slot. The nodes acquire the time and frequency from the downlink frame. Then each node randomly transmits by adding random delay selected by the node itself [57]. Furthermore, it provides acknowledged transmission, adding reliability to the communication.

Telensa. Telensa is a proprietary LPWAN technology that pioneered the use of UNB operating is the unlicensed sub-GHz ISM band [123]. It provides low data rates and does not support indoor

communications. Telensa focuses on smart city application, in particular, smart lighting and smart parking. In addition, it supports integration with third-party application by providing smart city API [123]. Although there is no publicly available information regarding the implementation of Telensa, there is an ongoing effort to standardize it through the European Technical Standards Institute.

DASH7 Alliance. DASH 7 Alliance proposed an open standard for LPWAN, DASH7 Alliance protocol (D7AP) [32], developed for wireless sensor and actuator networks communication [136]. D7AP use the acronym BLAST to describe its features – Bursty (describes the data traffic pattern supported by D7AP), Light (has maximum packet size of 256 bytes), Asynchronous (indicates that the communication does not require synchronization), Stealth (meaning that D7AP device only replies to approved devices), Transitional (meaning D7AP devices are designed for mobility).

Weightless-N. Weightless Special Interest Group (Weightless-SIG) [135] proposed Weightless, an open standard offering LPWAN connectivity. Weightless-N (nWave) is similar to SigFox. Only supporting unidirectional communication for end-devices to the BS [74]. It achieves communication range of up to 3 km with maximum data rate of 100 kbps. The MAC protocol of Weightless-N is based on slotted ALOHA.

Weightless-P. Weightless-P is the latest standard introduced by Weightless-SIG. Unlike Weightless-N, it offers bi-directional communication with support for acknowledgments. It achieves data rate around 100kbps. Compared to Weightless-N, Weightless-P has shorter communication range (2 km) and shorter battery lifetime.

SNOW. SNOW is a new emerging asynchronous LPWAN technology with potentials to over-

come the scalability limitation of existing LPWAN technologies. SNOW has a star network topology [106, 107]. Each sensor node is equipped with a single half-duplex narrow-band white space radio. The nodes are directly connected to the BS and vice versa. The BS uses a wide channel split into orthogonal subcarriers, each of equal spectrum width (bandwidth). The BS determines white spaces for nodes by accessing a cloud-hosted database through the Internet.

The PHY layer of SNOW uses Distributed implementation of OFDM (Orthogonal Frequency Division Multiplexing) for multi-user access, called D-OFDM. If the BS spectrum is split into n subcarriers, then it can receive from n nodes simultaneously. Similarly, it can transmit n different data at a time. The BS can exploit fragmented spectrum as well. SNOW represents a novel PHY-layer design, eliminating the scalability limitations in existing LPWAN technologies. The scalability of SNOW increases with the availability of the TV spectrum.

2.4 Opportunities in LPWANs

LPWAN provides opportunities to enable a large class of IoT applications. We discuss several use cases in different domains (Figure 2.2).

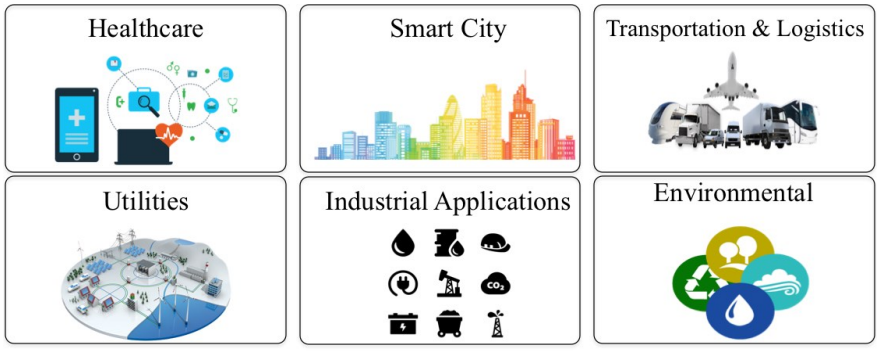


Figure 2.2: LPWAN enabled IoT applications

2.4.1 Smart City

The goal of *smart city* is to efficiently utilize the public resources, improve the quality of living, and reduce the cost of management and administrations of the public resources [147]. Multiple cities around the world have already started transitioning to smart cities [99, 6]. One example of smart city applications is **waste management.** In most cities around the world, waste management is extremely difficult and costly due to the operational service costs (e.g. trucks, fuel, and operators) and the limited storage areas [91]. Smart cities use smart waste containers, which detects the level of trash inside and send the information to a control center which then optimizes the collector truck route, eventually reducing the operational cost. Using LPWANs to provide affordable communication is beneficial to both taxpayers and city officials. Another application is **smart lighting**. Smart lighting significantly reduces the cost of street lighting by changing the light intensity according to the environment [147]. It also reduces the cost of maintenance by providing real-time fault monitoring [123]. Telensa is developed specifically for smart lighting and smart parking applications.

2.4.2 Transportation and Logistics

Today, millions of sensors and RFID tags are already deployed in vehicles, trucks, and airplanes that enable owners to track the movements of objects from the source to the destination across the supply chain in real-time [31]. One specific application is **connected vehicles**. Most of the newer vehicles include sensors, networking capability, and processor. IoT can utilize these to improve the driving experience in several ways such as enhance road sharing, accidents reporting, and parking detection. Long-range communication, low-power, low cost, and support for mobility are required

to support transportation and logistics applications.

2.4.3 Agriculture and Smart Farming

The agricultural sector is one of the earlier adopters of IoT. To enable this, a network connecting the farm devices is needed. Precision agriculture powered by IoT can help farmers better measure things like soil nutrients, fertilizer used, seeds planted, soil water, and temperature of stored produce through a dense sensor deployment, thereby almost doubling the productivity [129]. Companies like Microsoft (FarmBeats project [129, 42]), Climate Corp [27], AT&T [8], and Monsanto [84] are promoting agricultural IoT.

2.4.4 Healthcare Applications

The healthcare sector is a great market for IoT applications. Examples of IoT applications for healthcare include remote health monitoring, elderly care, chronic disease [60], etc. The key requirements for IoT in most health-related applications are noninvasive sensing and secure and reliable communication. Currently, short range wireless technologies, such as ZigBee [151], WiFi [53], 6LowPAN [113] and cellular technologies such as LTE are widely adopted in the healthcare sector. However, with the increase in the number of sensors, these technologies will not scale due to interference. The limitations in short-range wireless technologies and the high cost of cellular technologies drove the attention to LPWANs as an alternative communication solution for healthcare applications.

2.5 Challenges and future research directions

In this section, we discuss the challenges and limitations of existing LPWANs, and research directions to address the challenges.

2.5.1 Future Scalability and Coverage

Scalability in dense networks will be a big challenge for LPWANs [34]. Specifically, the performance of LoRa, widely considered as an LPWAN leader [12, 59, 21, 83, 74, 110], drops exponentially as the number of end-devices grows [17, 34, 134, 45, 9, 4]. A typical smart city deployment can support only 120 LoRa nodes per 3.8 hectares [17], which is not sufficient for future IoT applications. Without line of sight its communication range is quite low [21], specially in indoor (<100m compared to its specified 2-5km urban range [132]). SNOW has been shown to be superior to LoRa in scalability. But SNOW implementation is still on USRP devices and its hardware realization is not done yet. Scalability can also be considered in terms of coverage area. Most LPWANs are limited to star topology while the cellular based ones (EC-GSM-IoT, NB-IoT, LTE Cat M1, 5G) rely on wired infrastructure for integrating multiple networks to cover larger areas. Lack of proper infrastructure and connectivity hinders their rural applications such as agricultural IoT [129, 42], oil-field monitoring [92], smart and connected rural communities [28, 89, 76, 117] that need extended coverage.

Existing research focuses on scalability in cellular and short-range wireless networks. For LPWANs operating in unlicensed spectrum, approaches such as offloading (from licensed spectrum to unlicensed spectrum) typically adopted in cellular-based technologies are not affordable. Currently, the use of narrowband channels is common among several LPWAN technologies. While narrowband channels provide an efficient spectrum utilization and support for a larger number of devices, in the future, the increase in the number of devices and LPWAN technologies will result in a very dense spectrum limiting spectrum availability. To address the scalability problem

in LPWANs, future research would need to consider opportunistic spectrum sensing, adaption of spectral efficient modulation schemes, adaptive data rate MAC protocols, and exploring channel diversity for LPWANs. In addition, several research directions suggest the use of adaptive power control as a factor to increase the scalability [33]. Another approach is to use Non-orthogonal Multiple Access schemes (NOMA). NOMA supports multiple connections with different desired power rates by exploiting the path loss difference between multiple users, thereby increasing the spectrum utilization. For applications and deployments over very wide areas, future research needs to address wireless integration of LPWANs for extended coverage.

2.5.2 Technology Coexistence

High popularity of LPWANs brings forth a new challenge, called *coexistence*. Many independent networks will be deployed in close proximity, and interference between them must be handled to keep them operational. Today, LPWANs are not equipped to handle this imminent challenge that will make the spectrum overly crowded [102]. Studies on LoRa, SigFox, and IQRF show that coexistence severely degrades their performance [70, 45]. When four LoRa networks coexist, throughput of each reduces almost to one fourth [134]. Coexistence handling for WiFi, existing WSN, Bluetooth [143, 144, 116] will not work well for LPWANs. Due to their large coverage domains, LPWAN devices can be subject to an unprecedented number of hidden terminals. Enabling different technologies to coexist on the same spectrum is very challenging mainly due to different entities owning different technologies. One research direction is to utilize the spectrum information to detect and identify the presence of other technologies. This can be achieved using an efficient spectrum sensing method or a dedicated hardware combined with machine learning

techniques to identify interfering technologies [33].

2.5.3 Inter-Technology Communication

With the rapid growth of LPWAN technologies, there will be many coexisting LPWANs in the same geographical area and their coordination may be needed. Specifically, LPWANs from different vendors may need to communicate which would be another big challenge. Recently, cross-technology-communication (CTC) [68] without the assistance of additional hardware has been studied for communication across WiFi, ZigBee, and Bluetooth devices. Such CTC is specific to technology. Future research is needed to enable CTC in LPWANs.

2.5.4 Real-Time Communication

Many IoT applications will require real-time communication (e.g. smart grid, manufacturing, healthcare, data center energy management [109]). Such applications require very low latency and very high reliability. Most LPWANs are designed to support applications with flexible requirements. In addition, the LPWANs operating in the sub-GHz band are required to duty cycle at 0.1 or 1% which make real-time communication extremely challenging. SNOW operates on dynamic spectrum which also raises challenge for real-time communication. Future research needs to focus on finding ways to enabling real-time communication in LPWAN.

2.5.5 Support for Control Applications

LPWAN will be a major communication infrastructure for a broad range of control applications in the future. Control applications rely on reliable bi-directional communications along with their real-time requirements. Most non-cellular LPWANs (e.g., LoRa, SigFox, Weightless-N) support uplink only communication at this time. LoRa can enable bidirectional communication, but it has

to rely on time synchronized beacons and schedules, which is an overhead. DASH7 is specially designed for bidirectional communication but has only few hundred meters of communication range and has to rely on multihop. SNOW supports downlink communication but relies on dynamic spectrum availability which makes support for control extremely challenging. Investigating new techniques to enable reliable and efficient bi-directional communication represents a major direction of the future LPWAN research.

2.5.6 Support for Mobility

As the number of mobile devices grows, many devices in an LPWAN can be mobile. The usage of drones, tractors, vehicles, and human make mobility an immediate concern in agricultural IoT [129, 42, 84, 43]. Existing LPWAN technologies are not designed for handling mobility well except the cellular based ones that rely on wired infrastructure to handle mobility [39]. Such wired infrastructure does not exist in rural environments. Specifically, in remote areas (e.g. farms, oil fields etc.) often there is weak or no cellular signal/coverage. The high cost of subscribing to cellular service is also hindering the adoption of cellular technologies. In other LPWANs, handling mobility is quite challenging and not well-addressed yet. Their performance is susceptible even to minor human mobility [95]. Technology-specific features of each LPWAN also makes mobility issues such as base station discovery, handoff, and seamless communication quite different. The mobility feature of RPMA [104] is its transmitter's robustness to the Doppler effect, and does not mean the aforementioned mobility issues. Mobility imposes challenges for LPWAN in terms of energy consumption. The support for mobility has a direct impact on the battery lifetime of the node. Thus, the design of an energy-efficient, low cost mobility approach for LPWANs is needed.

2.5.7 Support for High Data Rate

The typical data rate supported by LPWAN technologies is ranging from 1 – 100 kbps. Narrowband offers long transmission range at the cost of low data rates. The advent of aerial imagery systems that involve drones and cameras for richer sensor data from the farms need high bandwidth in agricultural IoT [129, 42, 84, 43]. In the future, many IoT applications will evolve to include several use cases, such as video streaming, requiring very high data rate. LPWANs must investigate different approaches to support high data rate. Future research directions to enabling high data rates include enabling different modulation techniques, borrowing approaches used in technologies like WiFi, and designing new hardware to support multiple PHY layers offering different data rates.

2.5.8 Security

Transmitting a signal over the air is subject to jamming attacks, packets sniffing, eavesdropping, and variety of attacks. Most LPWAN technologies support a simple cryptography method where the device and the network share a secret key. On the other hand, cellular technologies have support for end-to-end authentication and privacy using Subscriber Identification Module (SIM). However, this comes with the high cost of cellular devices and more complex device design. The need for secure communication is essential for LPWANs. For example, enabling over the air software updates is important to ensure security for LPWAN devices. As LPWAN is a key technology driving the IoT, extensive future research is needed for the study of LPWAN security.

2.6 Summary

In this chapter, we have discussed the opportunities and challenges in LPWANs as an enabling technology for IoT applications. We have presented the state-of-the-art LPWAN technologies and discussed their characteristics which allow them to achieve long-range connectivity, low-power communication, and low deployment cost for a large number of devices. Finally, we have outlined the opportunities and challenges in realizing the LPWANs for the future IoT applications. We have provided insights and directions for the future research in LPWAN.

CHAPTER 3 MOBILITY IN LOW-POWER WIDE-AREA NETWORK OVER WHITE SPACES

Despite the proliferation of mobile devices in various wide-area Internet of Things applications (e.g., smart city, smart farming), current LPWANs are not designed to effectively support mobile nodes. In this chapter, we propose to handle mobility in SNOW, an LPWAN that operates in the TV white spaces. SNOW supports massive concurrent communication between a BS and numerous low-power nodes through a distributed implementation of OFDM. In SNOW, inter-carrier interference (ICI) is more pronounced under mobility due to its OFDM based design. Geospatial variation of white spaces also raises challenges in both intra- and inter-network mobility as the low-power nodes are not equipped to determine white spaces. To handle mobility impacts on ICI, we propose a dynamic carrier frequency offset estimation and compensation technique which takes into account Doppler shifts without requiring to know the speed of the nodes. We also propose to circumvent the mobility impacts on geospatial variation of white space through a mobility-aware spectrum assignment to nodes. To enable mobility of the nodes across different SNOWs, we propose an efficient handoff management through a fast and energy-efficient BS discovery and quick association with the BS by combining time and frequency domain energy-sensing. Experiments through SNOW deployments in a large metropolitan city and indoors show that our proposed approaches enable mobility across multiple different SNOWs and provide robustness in terms of reliability, latency, and energy consumption under mobility.

3.1 Introduction

LPWAN is an enabling technology for wide-area IoT applications such as smart city, agricultural IoT, and industrial IoT offering long-range (several miles), low-power, and low-cost communication. With the fast growth of IoT, multiple LPWAN technologies have emerged recently such as LoRa [77], SigFox [115], IQRF [58], RPMA [57], DASH7 [32], Weightless-N/P [135], Telensa [123] in the ISM band, and EC-GSM-IoT [49], NB-IoT [88], and LTE Cat M1 [79, 78] in the licensed cellular band. To avoid the *crowd* in the *limited* ISM band and the *cost* of licensed band, *SNOW* is an LPWAN architecture to support scalable wide-area IoT over the TV white spaces [108, 106, 107]. *White spaces* are the allocated but locally unused TV spectrum (54 - 698 MHz in the US) [93, 94]. Compared to ISM band, they have much wider, less crowded spectrum in rural and most urban areas, with an abundance in rural areas [10].

With a wide range of supported applications, IoT is integrating more mobile nodes/devices in different domains (e.g. agriculture [128, 130], connected vehicle [81], healthcare [60], smart city [148]). For example, in agricultural IoT, the use of drones and tractors is rapidly increasing [84, 42, 43, 130]. It is expected that by the year 2050, there will be more than 3 billion wearable sensors [95]. The cellular-based LPWANs rely on wired infrastructure to handle mobility. Such infrastructure is often not available in rural and remote areas (e.g., farms, oil fields, etc.). In others, mobility introduces challenges that are not well-addressed yet. Study on LoRa shows that its performance is susceptible even to minor human mobility [95, 97].

In this chapter, we propose to handle mobility in LPWAN in the white spaces considering SNOW. With the rapid growth of IoT, LPWANs will suffer from crowded spectrum due to long

range, making it critical to exploit white spaces. SNOW is a highly scalable LPWAN over the white spaces which enables massive concurrent communication between a BS and numerous low-power nodes. It is available as an open-course implementation [118]. Its physical layer is designed based on a Distributed implementation of OFDM (orthogonal frequency division multiplexing) for multi-user access, called D-OFDM. The BS operates on a wide band spectrum which is split into many orthogonal narrowband subcarriers. A node (non-BS) transmits and receives on a subcarrier. In SNOW, ICI is more pronounced under mobility due to its OFDM based design. Geospatial variation of white spaces also raises challenges in both intra- and inter-network mobility as the low-power nodes are not equipped to determine white space. For example, to enable mobility across different SNOWs, it is challenging for a node to scan the wide spectrum of the TV band to discover a new BS. Besides, different BSs may be using different subcarrier widths, which may result in subcarrier misalignment between the mobile node and the new BS.

In this chapter, we address the challenges mentioned above to handle mobility in SNOW. Specifically, we make the following new contributions.

- To handle mobility impacts on ICI, we propose a dynamic CFO (Carrier Frequency Offset) estimation and compensation technique for SNOW which takes into account Doppler shifts under non-uniform speeds without requiring to know the speed of the nodes. To circumvent the mobility impacts on geospatial variation of white space within the same SNOW, we propose a mobility-aware subcarrier assignment to the nodes.

- To handle inter-SNOW (inter-network) mobility, we propose an energy-efficient and fast BS discovery technique that considers the trade-off between discovery latency and energy

consumption to allow efficient handoff management. Our approach utilizes the spectrum information by combining the received signal features to distinguish between primary users (TV stations) and a SNOW BS. We also propose a lightweight cross-layer technique feasible at the energy-constrained SNOW nodes to handle subcarrier alignment by combining time and frequency domain energy-sensing.

- We implement our proposed mobility handling techniques on SNOW devices and perform experiments by deploying SNOW in two environments - a large metropolitan city and an indoor testbed. The experimental results show that our approaches enable mobility across multiple different SNOWs. The results also show an improvement of reliability from 80% to 96.6% when our dynamic CFO estimation and compensation is incorporated.

The rest of the chapter is organized as follows. Section 3.2 overviews related work. Section 3.3 presents an overview of SNOW. Section 3.4 describes the system model. Section 3.5 presents our mobility approach. Section 3.6 presents the experiments. Section 3.7 concludes the chapter.

3.2 Related Work

Many studies focused on handling mobility in Wireless Sensor Networks (WSNs) [98, 5, 62, 145, 87, 37] (more can be found in survey [36, 38]) and ad hoc network [19, 52]. In WSN or WiFi networks, a client has to scan only a limited/fixed number of channels to discover a new BS. However, those approaches are not directly applicable to LPWAN. To handle mobility across networks, cellular LPWANs rely on wired infrastructure. Non-cellular LPWANs are not yet handling it well. Real experiments show that their performance is susceptible even to minor human mobility [95]. Spectrum mobility studied in [149, 119] for cognitive networks enables secondary

users to change the operating frequencies, and is different from device mobility. Device mobility was studied in [85] for white space network, where every device primarily relies on the database to determine the white spaces. A mobile device adds a protection range of δd so that any channel blocked within distance δd of current location is not used. Note that this approach does not work for SNOW as the nodes have no direct access to the Internet (and database). It first has to discover a BS, associate with it, and rely on it for spectrum access. Additionally, there has been much work on channel rendezvous in cognitive radio [150, 114, 14, 30, 25] (more can be found in survey [35, 29]). Due to technology-specific nature of SNOW, these techniques cannot be applied to a SNOW.

Senseless [86] is an infrastructure based white space network system where the devices do not rely on sensing to determine the availability of white space. They use geo-location service to calculate white space availability at any location. Senseless then disseminates the availability information to each device in the network. To address the mobility challenges in white space, Senseless suggests that every device adds a protection range to determine the availability of white spaces while mobile. This could lead to a huge spectrum waste depending on the size of the protection area. SNOW differ from Senseless in that it considers infrastructure-less network system where BSs are not connected. Besides, the D-OFDM based design requires a different approach for mobility in SNOW. Also, we incorporate an energy-efficient sensing approach along with the geo-location service to efficiently handle nodes mobility. To date, inter-network mobility for non-cellular LPWAN remains mostly unexplored and it was never studied for SNOW.

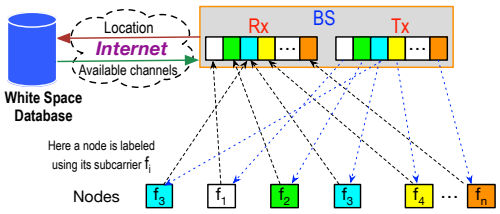


Figure 3.1: The SNOW architecture.

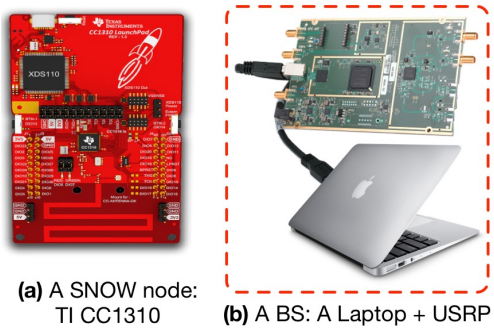


Figure 3.2: SNOW Hardware.

3.3 A Brief Overview of SNOW

Here we provide a brief overview of the SNOW architecture [106, 107, 108]. Due to long transmission (Tx) range (several miles at 0dBm), the nodes in SNOW are directly connected to the BS, forming a star topology as shown in Fig. 3.1. We use **'node'** to indicate a sensor node. The BS periodically determines white spaces by providing locations of its own and of all other nodes in a cloud-hosted database through the Internet. It uses wide white space spectrum as a single wide channel that is split into narrowband orthogonal subcarriers, each of equal spectrum width (bandwidth). Each node has a single half-duplex narrowband radio. It sends/receives on a subcarrier. The nodes are power-constrained, and do not do spectrum sensing or cloud access. As shown in Fig. 3.1, the BS uses two radios operating on the same spectrum – one for only transmission (called *Tx radio*) and the other for only reception (called *Rx radio*) – to facilitate

concurrent bidirectional communication.

The physical layer (PHY) of SNOW is designed based on a **D**istributed implementation of **OFDM** for multi-user access, called **D-OFDM**. D-OFDM splits a wide spectrum into numerous narrowband orthogonal subcarriers enabling parallel data streams to/from numerous distributed nodes from/to the BS. A subcarrier bandwidth is in kHz (e.g., 50kHz, 100kHz, 200kHz, or so depending on packet size and needed bit rate). The nodes transmit/receive on orthogonal subcarriers, each using one. A subcarrier is modulated using Binary Phase Shift Keying (BPSK) or Amplitude Shift Keying (ASK). If the BS spectrum is split into m subcarriers, it can receive from m nodes simultaneously using a single antenna. Similarly, it can transmit different data on different subcarriers through a single transmission. Currently, the sensor nodes in SNOW use a very simple and lightweight CSMA/CA based MAC (media access control) protocol like the one used in TinyOS [124].

SNOW was implemented on two hardware platforms [101] – USRP (universal software radio peripheral) [103] using GNU radio [46] and TI CC1310 [22] (Figure 3.2). A dual-radio USRP connected to Raspberry PI or Laptop is used as the BS. A CC1310 device or a single-radio USRP can be used as a SNOW node. CC1310 is a tiny, cheap (<$30), and commercially off-the-shelf (COTS) device with a programmable PHY. We have adopted the open-source implementation of SNOW that is available at [118].

3.4 System Model

We consider multiple independent and uncoordinated SNOWs. Each SNOW is having its own BS and associated nodes. The nodes are battery-powered and thus have energy constraints. We

assume the existence of both mobile and stationary nodes in SNOW. A mobile node can move from one SNOW to any SNOW, as depicted in Figure 3.3. Since the BS has a long-range, it can cover a wide area. Hence, we assume the BSs are stationary. Each node is equipped with a half-duplex white space radio. The BS and its associated nodes form a star topology where nodes can directly communicate with the BS.

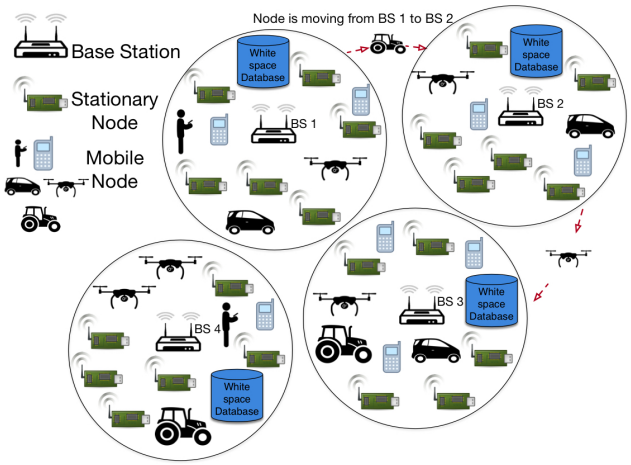


Figure 3.3: Inter-SNOW mobility: the figure shows multiple SNOWs where a mobile node is moving from one SNOW to another.

The BSs are independent, connected to the Internet, and directly connected to a power source. Each BS uses a wide channel. This channel is split into narrowband channels/subcarriers of equal width. Each node is assigned a single subcarrier for transmission and reception to/from the BS. The nodes are kept simple by offloading the complexities to the BS. The BS determines the availability of white space at its location by querying a cloud-hosted database through the Internet. We assume each BS knows the location of its associated nodes either manually or through existing localization techniques [82]. However, we are not considering localization in this work.

3.5 Handling Mobility

In this section, we present our techniques to address mobility challenges in both intra- and inter-SNOW mobility. We propose to address those through lightweight cross-layer approaches (MAC-PHY design) feasible at energy-constrained nodes. First, we present our mobility handling within the same SNOW (intra-SNOW mobility), and then we will present mobility handling across SNOWs (inter-SNOW mobility).

3.5.1 Handling Mobility within the Same SNOW

Mobility affects communication reliability even when a node moves within the same network due to ICI occurred in OFDM subcarriers and also due to geospatial variation of spectrum within the same network. We address both scenarios as described below.

Handling Mobility Impacts on ICI. ICI is introduced mainly due to the CFO, which stems from the frequency mismatch between the transmitter and receiver oscillators due to hardware imperfections and the **Doppler shift** which is a function of their relative speed. In SNOW, the subcarriers loose their orthogonality due to such CFO as shown Figure 3.4. Hence, to improve an OFDM system's performance, CFO needs to be estimated and compensated. Currently, in SNOW, CFO estimation and compensation is done considering stationary nodes or assuming node speeds are known [101]. However, SNOW nodes are energy-constrained and low-cost and may not be equipped to determine speeds. We first give an overview of the adopted CFO estimation technique and then describe our Doppler shift handling approach without the need to know the speed of the nodes or under non-uniform speed.

SNOW uses training symbols (preamble) for CFO estimation. Due to its distributed and asyn-

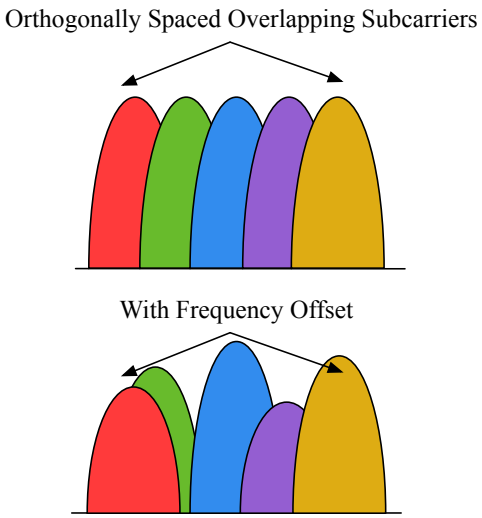


Figure 3.4: The impact of CFO on subcarriers orthogonality.

chronous nature, CFO estimation in D-OFDM is done slightly differently than traditional OFDM. CFO estimation in D-OFDM is done when a node joins the network. SNOW uses one (or more) subcarrier for a node joining the network, called *join subcarrier*, that does not overlap with any other subcarrier. Each node joins the network by first communicating with the BS on a join subcarrier. Each way, communication (BS to node and node to BS) follows a preamble used to estimate CFO on join subcarrier. Specifically, preamble from a node to BS allows to estimate CFO at the BS, and that from BS to a node allows to estimate CFO at the node on the join subcarrier. Later, based on the CFO on a join subcarrier, the CFO on a node's assigned subcarrier is determined. CFO estimation technique for both upward and downward communication is similar. However, CFO compensation approaches in upward and downward communication are different (refer to [101] for detailed explanation).

First, we explain how CFO is estimated on a join subcarrier f. Since it does not overlap with other subcarriers, it is ICI-free. If f_{Tx} and f_{Rx} are the frequencies at the transmitter and at the

receiver, respectively, then their frequency offset $\Delta f = f_{Tx} - f_{Rx}$. For transmitted signal $x(t)$, the received signal $y(t)$ that experiences a CFO of Δf is given by

$$y(t) = x(t)e^{j2\pi\Delta f t} \tag{3.1}$$

Δf is estimated based on short and long preamble approach using time-domain samples. A 32-bit preamble is divided into two equal parts, each of 16 bits. First part is for coarse estimation and the second part is for finer estimation of CFO [120]. Considering δt as the short preamble duration,

$$y(t - \delta t) = x(t)e^{j2\pi\Delta f(t-\delta t)}.$$

Since $y(t)$ and $y(t - \delta t)$ are known at the receiver,

$$\begin{aligned} y(t - \delta t)y^*(t) &= x(t)e^{j2\pi\Delta f(t-\delta t)}x^*(t)e^{-j2\pi\Delta f t} \\ &= |x(t)|^2 e^{j2\pi\Delta f - \delta t} \end{aligned}$$

Taking angle of both sides,

$$\sphericalangle y(t - \delta t)y^*(t) = \sphericalangle |x(t)|^2 e^{j2\pi\Delta f - \delta t} = -2\pi\Delta f\delta t.$$

Thus, $$\Delta f = -\frac{\sphericalangle y(t - \delta t)y^*(t)}{2\pi\delta t}$$

A SNOW node calculates the CFO on join subcarrier f using the preambles from the BS to

the node using the above approach. In upward communication, the time-domain samples are used for CFO estimation on the join subcarrier f at the BS based on the above approach. Then the *ppm (parts per million)* on the receiver's (BS or SNOW node) crystal is given by ppm = $10^6 \frac{\Delta f}{f}$. Thus, the receiver (BS or a node) calculates Δf_i on subcarrier f_i as

$$\Delta f_i = \frac{f_i * \text{ppm}}{10^6}.$$

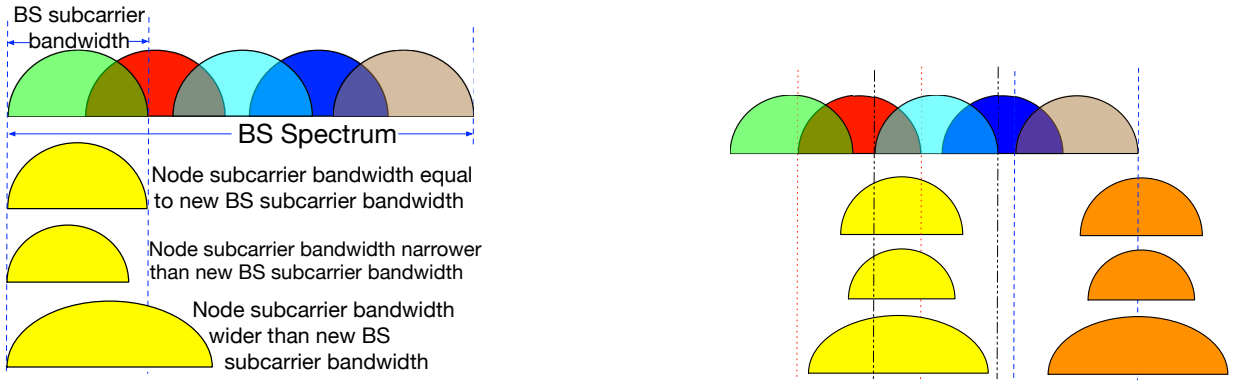
Thus the BS and a SNOW node that is assigned subcarrier f_i calculates CFO on f_i on its respective side. As the nodes asynchronously transmit to the BS, doing the CFO compensation for each subcarrier at the BS is quite tricky. Hence, a simple feedback approach for proactive CFO correction in upward communication is adopted. In this approach, a transmitting node adjusts its frequency based on Δf_i when transmitting on subcarrier f_i so that the BS does not have to compensate for Δf_i.

Since mobility causes Doppler shift in frequency contributing further to CFO, CFO has to be estimated using the above approach while a node moves. If a node moves at speed v, such Doppler Frequency Offset (DFO), denoted by $\delta_f(v)$, is upper-bounded by

$$\delta_f(v) = \frac{v}{c} f_c \tag{3.2}$$

where, c is the speed of light, and f_c is the carrier frequency. Therefore, considering Δf_i as the CFO when a node is stationary, it experiences a total CFO of $\Delta f_i + \delta_{f_i}(v)$ when it moves at speed v. Therefore, to account for this total CFO, the node needs to know its speed. Besides, when the speed

changes, δ_{f_i} has to be recalculated. But, being energy-constrained and low-cost, SNOW nodes are not equipped to determine their speeds. Hence, we rely on the observation that when CFO is estimated for a moving node using the above CFO estimation technique, its estimation includes both Δf_i and δ_{f_i}, resulting in a CFO of $\Delta f_i + \delta_{f_i}$. Thus, the node does not need to know its speed. If the node's speed changes, then the total CFO changes and we need re-estimate. However, the node has no way to determine if its speed increases or decreases. To handle this challenge, we enable each node to periodically estimate the CFO. This period can be set as a tunable system parameter. Estimating CFO periodically will ensure that if the speed changes, the new CFO calculation takes the new speed into account.



(a) Subcarrier aligned with BS

(b) Scenarios showing misalignment

Figure 3.5: Alignment between the node subcarrier and BS subcarrier.

Handling Mobility Impacts on Geospatial Variation of White Spaces. Due to long range, a node's mobility even within the same network affects the spectrum availability. For example, a subcarrier that is assigned to a node at a particular place may not be available if the node moves to another location within the range of the same BS (i.e., within the same SNOW). Currently, the BS assigns subcarriers to the nodes without considering their mobility. This may affect the communi-

cations of the mobile nodes. Namely, if a node is highly mobile and may move anywhere inside the network but is assigned a subcarrier which is available only in a few locations, its subcarrier assignment is not much useful. To handle this problem due to geospatial variation of white spaces, we propose a mobility-aware subcarrier assignment policy as follows.

Note that the BS is already assumed to know the location information of its coverage area. We also assume that the BS knows the degree or rate of mobility of each node (i.e, how much mobile the node is). A node can provide a rough estimate of its mobility when it joins the network. The BS orders the nodes based on their mobility, where the stationary nodes come first and the most mobile node is the last. The BS then orders the subcarriers based on their availability, from the least widely available (inside its communication range) subcarrier to the most widely available one. That is, the subcarrier that is available in the minimum number of locations comes first and that available in the maximum number of locations (inside the network) comes at the last of this order. If there are m subcarriers and n nodes, each subcarrier is roughly shared by $\lceil \frac{n}{m} \rceil$ nodes. Starting from the beginning of the ordered subcarriers, each subcarrier is then assigned roughly to $\lceil \frac{n}{m} \rceil$ nodes that are not yet assigned a subcarrier starting from the beginning of the ordered nodes. In this way, we ensure that the widely available subcarriers are assigned to highly mobile nodes and the least widely available subcarriers are assigned to stationary or less mobile nodes.

3.5.2 Handling Mobility across SNOWs

In this section, we present our approach to addressing the mobility across different SNOWs. Specifically, we handle mobility problem that arises when a node goes out of the range of a BS. When a node goes out of the range of a BS, it needs to discover a new BS and get associated with

it. Handoff becomes an issue when a node moves to an uncoordinated SNOW whose operating spectrum is unknown.

For SNOW, the white space range is very wide, and the SNOW BS may be using a channel anywhere in that spectrum. A node operates on a narrowband subcarrier. Two subcarriers at center frequencies f_i and f_j, $f_i \neq f_j$, are orthogonal when over time T' [24]:

$$\int_0^{T'} \cos(2\pi f_i t)\cos(2\pi f_j t)dt = 0. \tag{3.3}$$

For example, when the overlap between subcarriers is 50%, the BS bandwidth is 6 MHz, and the subcarrier width is 200 kHz, we can have 59 orthogonal subcarriers. Thus, to discover a new BS, it is very energy and time consuming for a low-power node as the node may need to scan thousands of subcarriers. Our approach has to deal with the following challenges as well. **(1)** Spectrum dynamics due to primary user activity is handled using backup subcarriers in SNOW. However, such an approach does not work under mobility as the backup channels may be unavailable in a new location. A SNOW node has no access to the database and thus does not know the white space spectrum availability in its location. Spectrum sensing is highly energy consuming and is not feasible for it. **(2)** It cannot transmit any probing message to explore a BS as it can interfere with primary users. The node hence needs to depend only on listening to SNOW's communication. **(3)** The nearby BS may be using subcarriers of different bandwidth, and thus the node subcarrier may be unaligned (as depicted in Figure 3.5) and listening to nothing. Aligning with a BS channel is quite difficult as the BS subcarrier bandwidth is unknown to the moving node. **(4)** The node should

be able to distinguish between a primary user and a secondary user (BS). Our steps to address these challenges are as follows.

BS Discovery. A direct approach to minimizing BS discovery overhead is that the current BS can provide a node, before it moves, the channels that the BS would find at 8 locations $(0, \pm r), (\pm r, 0), (\pm r, \pm r)$, considering its (estimated) communication range r and location at $(0, 0)$ assuming a Cartesian plane as shown in Fig. 3.6. After a node moves out of the current BS range, it can scan only those channels to find a neighboring BS. However, this approach would only work if it can inform the BS of its intention to move before it starts to move. Second, the node needs to know the direction of its movement and inform the BS. Hence, we also propose another energy-efficient and fast BS discovery technique that does not depend on these requirements. It utilizes the spectrum information by combining the received signal features to distinguish between primary users (TV stations) and a SNOW BS, and considers the trade-off between discovery latency and energy consumption to allow efficient handoff management.

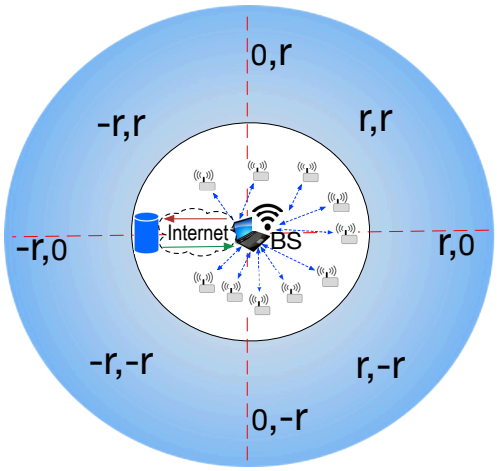


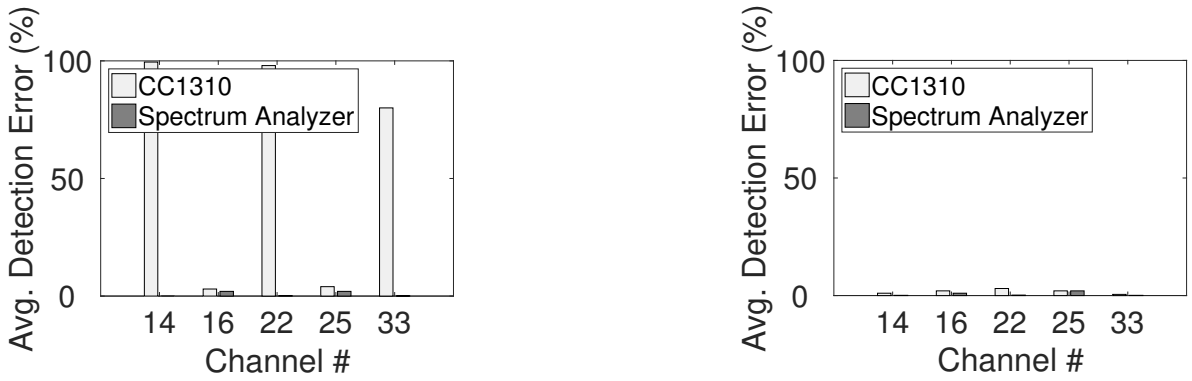
Figure 3.6: Channel availability information in 8 locations.

After a node goes out of range of its BS, it will scan one or more of its subcarriers. In either case, if it senses signal strength on a subcarrier, then it has to determine whether it is a BS or a primary user. If its subcarrier is not aligned with that subcarrier (in case of BS), it may not decode the received packets. To distinguish between the TV signal and the BS signal, we first need to detect the presence of primary users. The FCC regulation for protecting primary incumbents define a protection contour for TV station as the area where the received signal strength (RSS) is > -84dBm [93]. We follow an approach similar to the one presented in Waldo [105]. Waldo's results show that low-cost sensors can efficiently detect white spaces ignored in the databases and existing approaches. Furthermore, depending on the white space device's antenna height, further separation (6 km for portable devices) is required to protect the primary incumbent. To detect white spaces, FCC recommends a typical antenna height of 10 meters. We consider an antenna height of 2 meters and compensate for the difference (8 meters) using the antenna correction factor using Hatas' urban area propagation model [105] considering h_m as the antenna height in meters as follows.

$$a(h_m) = 3.2(\log 11.5h_m)^2 - 4.97 \tag{3.4}$$

Using Hata's model, the calculations result in $a(h_m) = 7.5$dB, which will be added uniformly to the RSS measurements. The addition of the antenna correction factor directly impacts the noisy measurements by making it closer to the threshold. Hence, improving the probability of false TV channel detection. We also follow Waldo's approach by considering the location safe for white space operation if the RSS ≥ -84dBm, and the nearest measurement is 6 km away [105]. We record the measurements in a large metropolitan city for five different TV channels (14, 22, 33 are

occupied by TV stations, 16 and 25 are white spaces). Additionally, we use the spectrum analyzer measurements and Google spectrum database as the ground truth to evaluate the SNOW nodes' TV channel detection performance. We collect 1500 spectrum measurements using four low-cost SNOW nodes (TI CC1310 [22]) over a period of 48 hours. Figure 3.7 shows the results for TV station detection. It is clear from Figure 3.7(a) that without considering the antenna correction factor, CC1310 fails to detect TV transmission in all occupied channels.



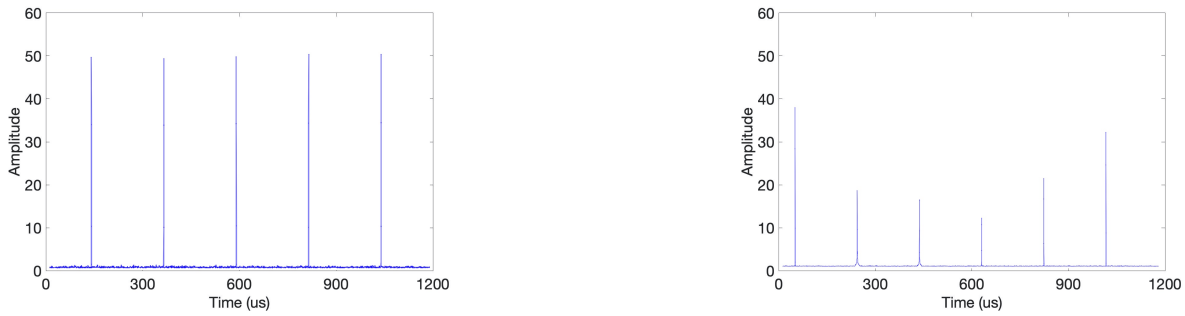
(a) Channel detection before adding antenna correction factor

(b) Channel detection after adding antenna correction factor

Figure 3.7: Performance of TV detection

We utilize a number of features of the received signals to distinguish between primary users (TV stations) and a SNOW BS. In addition to the common observation that RSS of the TV transmission is high and the signal amplitude is constant, primary user communication is observed to be continuous over a long duration (see Figure 3.8(a)). In contrast, SNOW BS signal amplitude is fluctuating during transmission and the BS may not have continuous communication for long periods as shown in Figure 3.8(b). In addition, if multiple consecutive channels have similar RSS, it is likely to be a BS because a BS typically uses more than one TV channel. For primary users,

two consecutive channels should belong to two different primary users, and their signal strengths on two consecutive channels should be a lot different. To enable faster discovery, we also consider using a wider band for sensing, which will enhance the BS detection probability but will consume more energy. Since using a narrow subcarrier for searching can take a longer time, thus consuming much energy, such tradeoff is left as a design choice.



(a) TV transmission (b) SNOW transmission

Figure 3.8: TV and SNOW signal transmission recorded using a spectrum analyzer.

Subcarrier Alignment. Different SNOWs can have different subcarrier bandwidth, e.g., camera or audio may use a wider subcarrier. Thus upon discovery of a new BS, as shown in Figure 3.5, a node's subcarrier may not be aligned with a BS subcarrier. Alignment is needed to start communication. Existing channel rendezvous techniques are not applicable as they consider the channels of equal bandwidth. Thus, this problem is specific to SNOW. By Equation (3.3), an overlap can start from many points of a nearby subcarrier. Such an overlap makes the problem highly challenging. To solve the problem, we exploit several characteristics of SNOW design. Even though SNOW can use any subcarrier bandwidth, we consider that subcarrier bandwidth does not vary arbitrarily, and we assume each BS uses a subcarrier bandwidth from the values 100kHz, 200kHz, 400kH, or 600kHz. Upon discovering the presence of a BS, this assumption helps us simplify the

synchronization with its subcarrier. This will be done using a wider bandwidth at the node and combining time and frequency domain energy-sensing.

The time-domain sensing is the typical carrier sensing that calculates the energy level using a moving average of the digital signals, i.e., the sequence of discretized, complex samples from the analog-to-digital converter, within a short period. A channel is considered *busy* if the output exceeds the predefined threshold. The moving average's window size is set to half of the length of the preamble to ensure prompt sensing of a packet. Although time-domain sensing alone can sense a busy channel, it does not distinguish between different subcarriers. A node needs to analyze the frequency domain of the signals further. Specifically, it calculates the power spectrum density (PSD) of the recent M samples using Fast Fourier Transformation (FFT). The node analyzes the power distribution and compares it with all possible channel-overlapping patterns based on the PSD. Intuitively, if the power is uniformly distributed over the entire spectrum, then the signals on the air come from a fully-overlapped subcarrier; otherwise, only a fraction of the channel is occupied. The exact fraction of channel in use is hard to calculate because different subcarriers may exhibit different power levels due to frequency-selective fading, and the imperfect hardware filter (used to confine the radio's bandwidth) spreads over the boundary of the PSD curve. But considering a limited number of bandwidths, the node can explore possible overlapping patterns and select the one with maximum matching with the PSD. The number of such patterns will also be limited as it is done after determining the presence of a BS.

In SNOW, a node is less powerful and energy-constrained. The complexity of time-domain sensing is the same as the RSSI calculation in typical communications systems, which is linear

with respect to the number of incoming samples. Since frequency sensing is performed only after a sequence of signals pass the time domain sensing, it takes constant time irrespective of the number of samples. The constant depends on the number of packets that cause the time-domain sensing to return *busy*. Note that such an approach is needed only when a node moves to an uncoordinated SNOW. Once the node is aligned with any subcarrier of the new BS, it can use CSMA/CA approach to transmit to the BS and ultimately join the network. Figure 3.9 shows the subcarrier alignment latency for different subcarrier bandwidths.

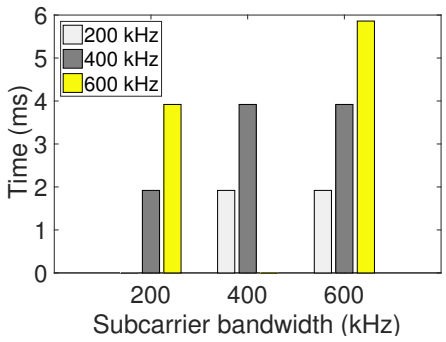


Figure 3.9: Subcarrier alignment latency

3.6 Experiments

We have first implemented our mobility approaches using TI CC1310 devices as SNOW nodes. TI CC1310 is a tiny, low-cost, and low-power COTS device with a programmable PHY which was recently adopted as SNOW node [101]. To perform experiments at much longer communication ranges, we have also implemented our mobility approaches using USRP devices as SNOW nodes based on its current open-source implementation in GNU Radio [118]. GNU Radio is an open-source development toolkit that provides signal processing blocks to develop software-defined radio [46]. USRP is a hardware platform designed for RF application [103]. We have used two

USRP 210 devices, each having a dual radio, as two BSs in each experiment for inter-SNOW mobility experiments. In the first set of experiments, we have used 10 TI CC1310 devices as SNOW nodes. In the other set of experiments, we have used 7 USRP 200 devices, each with a single radio, as SNOW nodes. The USRP devices operate in the band 70MHz – 6GHz. Packets generation, decoder, and other implementation are adopted from SNOW open source implementation [118].

Note that our experiments are performed mainly considering inter-SNOW mobility to show that our approach can enable such mobility. We cannot compare the results against the scenario when our approaches are not adopted because inter-SNOW mobility cannot be enabled without our approaches. However, we compare the performance against the stationary scenario to observe the performance degradation under mobility. In our experiments we shall demonstrate that such degradations are not high and our approaches show robustness in terms of reliability, latency, and energy consumption under various mobility scenarios.

3.6.1 Default parameters

Parameters of interests are calibrated in different experiments based on requirements and the rest are left as defaults. The default experimental parameter settings are as follows.

- Frequency band: varying (470 MHz - 599 MHz)
- Modulation: ASK/OOK
- Packet size: 40 bytes
- BS bandwidth: 6 MHz
- Node bandwidth: TI CC1310: 200 kHz, USRP: 400 kHz

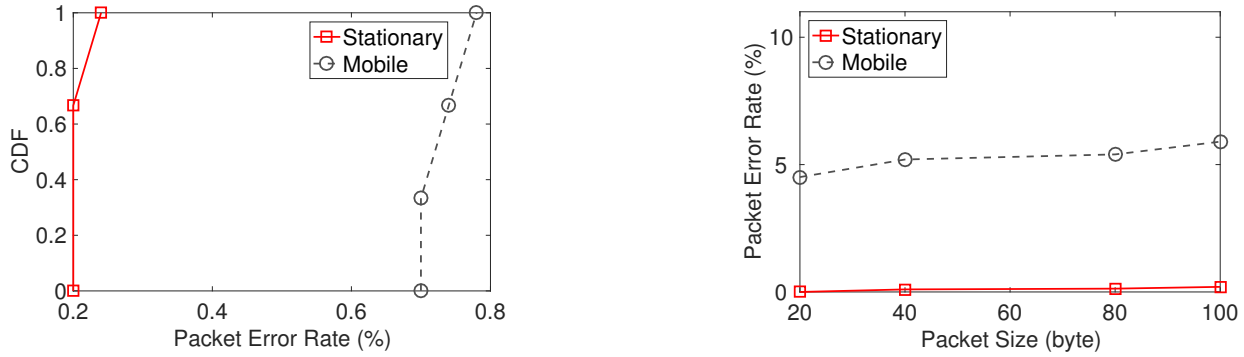
- TX power: TI CC1310: 15 dBm, USRP: 0 dBm
- Receiver sensitivity: -110 dBm
- Signal-to-noise ratio (SNR): 6 dB
- Distance: Indoor: 10 - 50 m, Outdoor: 900 m

3.6.2 Experiments with TI CC1310: Indoor and Outdoor Deployment

Indoor Deployment. The experiments with CC1310 were carried out in a hallway on the third floor inside a building in our location. We fixed the position of the BSs while a person is continuously moving at average walking speed from one end of the hallway to the other for 30 minutes. We kept the antenna height at 2 meters above the ground for all experiments. In all the experiments, the CFO and CSI are estimated and compensated based on SNOW implementation in [101]. We used the default setting for all the experiments.

Reliability under Mobility. We kept the distance between the node and BSs at approximately 10 meters to observe our proposed mobility approach's reliability. One node is stationary at this distance, and another node is continuously moving from one BS towards the other. The stationary node transmits 5000 packets to the BS while the mobile node transmits 2500 packets to the first BS and 2500 to the second BS after the joining process. The results in Figure 3.10(a) demonstrate that with minor human mobility, the Packet Error Rate (PER) slightly increases under our approach. For the stationary node, the PER is around 0.02%, while the mobile node is 0.72%. Also, we observe reliability with varying packet sizes. Figure 3.10(b) demonstrates the impact of packet size on our mobility approach. With 20-byte packet, the stationary node PER is 0% (no packet loss). For the

same packet size, the mobile node PER is around 4.5%. Furthermore, for the 40-byte packet, the PER is 0.1% and 5.2% for the stationary and mobile node. With a 100-byte packet, the mobile node achieves 5.4% PER, while the PER for the stationary node is 0.39%. This result shows that packet size has an impact on reliability. Larger packets require more air time to receive, resulting in more interference leading to increased PER. For the mobile node, moving from one BS to another might increase the PER due to the channel condition at the new location, which might increase the PER. However, the results prove that our approach offers reliable communication under mobility.



(a) Reliability under mobility

(b) Reliability with varying packet size

Figure 3.10: Reliability under mobility and varying packet size.

Maximum Achievable Throughput. The maximum achievable throughput is the total maximum number of bits the BS can receive per second. In this experiment, we calculate the maximum achievable throughput using our approach compared to the stationary nodes. In both scenarios, each node transmits 1000 40-byte packets. Figure 4.12 shows that in a stationary scenario, the maximum achievable throughput is 240 kbps compared to 174 kbps during mobility when ten nodes transmit simultaneously. This result is not surprising since mobility increases the packet loss rate, which affects the throughput.

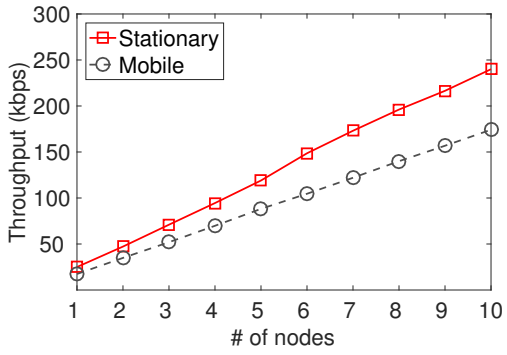


Figure 3.11: Throughput with varying # of nodes.

Energy Consumption and Latency. To estimate the energy consumption and latency of CC1310 during mobility, we measure the average energy consumed at the nodes and the time it takes to transmit 1000 packets per node successfully. We placed ten nodes, each 50 m away from BS1. We performed two sets of experiments (stationary nodes and mobile nodes). In the mobility experiment, the nodes are placed 10 m away from BS1 and 50 m away from BS2. And the nodes move from BS1 to BS2. Also, we measure the overhead of the BS discovery and sub-carrier alignment offline and add the results accordingly. To calculate the energy consumption, we use the energy model of CC1310 (Voltage is 3.8v, RX 5.4mA, and TX 13.4mA). We measure the time required to collect 10.000 packets at BS1 for the stationary nodes and 2500 packets and 7500 packets at BS1 and BS2, respectively, in the mobile scenario. Figure 3.12 shows that in a stationary scenario, the average energy consumed by the node is 81.4mJ compared to 87.1mJ in during mobility. We observe similar behavior for the latency. As shown in Figure 3.13, the average latency for stationary nodes is 1.6s compared to 1.712s in mobile nodes. This result indicates that the number of nodes has an insignificant impact on the energy and latency regardless of mobility. This is due to the capability of SNOW BS, which allows multiple nodes to transmit in parallel.

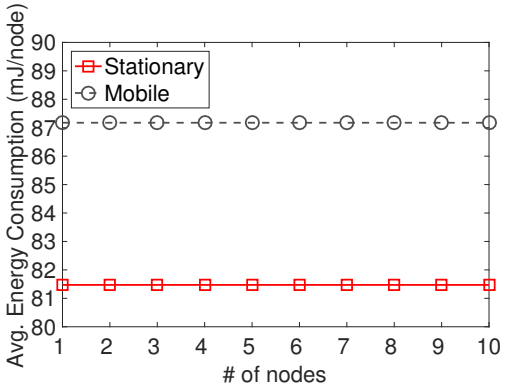


Figure 3.12: CC1310 Energy consumption

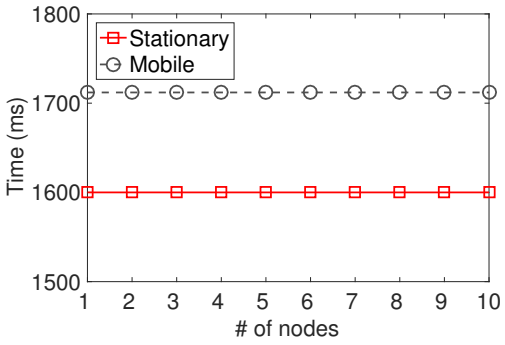


Figure 3.13: CC1310 Latency

Outdoor Deployment. In this experiment, we evaluate the performance of our mobility approach in terms of maximum achievable throughput, energy consumption, and latency using CC1310 devices in outdoor deployments. We fix the location of the BSs and place the node inside a moving vehicle. The distance between the node and the BSs is approximately 900 meters. The vehicle speed varies between 5 mph and 40 mph. The data is collected at the BSs for further analysis.

Maximum Achievable Throughput. In this experiment, we compare the maximum achievable throughput at different speeds (5 mph, 20 mph, 40 mph). Each node transmits 1000 40-byte

packets, and we calculate the combined throughput at the BSs. Figure 3.14 shows that the maximum achievable throughput is approximately 12.5 kbps at 5 mph speed compared to 11.89 kbps and 11.83 kbps At 20 mph and 40 mph, respectively. This shows that the speed (up to 40 mph) has an insignificant impact on the nodes' maximum achievable throughput.

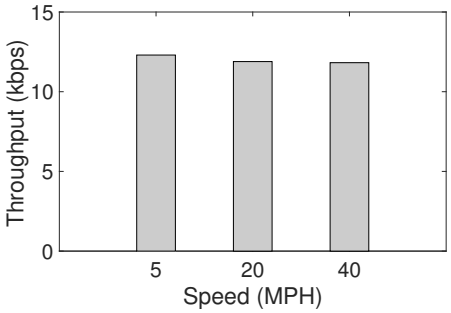


Figure 3.14: Throughput vs. node speed

Energy Consumption and Latency. To estimate the energy consumption and latency in outdoor deployment, we place the BSs at varying distances from the nodes (up to 900 meters). We set the nodes inside a moving vehicle. We measure the average energy consumed at each node and the time it takes to transmit 1000 packets per node successfully. Figure 3.15 shows that the average energy consumed by the node moving 5 mph is to 87.1mJ and 87.3 mJ at 100 m and 900 m, respectively. At 20 mph, the energy consumption is 87.1 mJ and 87.4 mJ at 100 m and 900 m, respectively. The average energy consumption is 87.8 mJ and 87.9 mJ at 100 m and 900 m for 40 mph. These results are similar to the indoor scenario where the node is moving at walking speed. In Figure 3.16, the average latency for all nodes, regardless of the distance, is 1.735s. This result shows that the energy and latency for all nodes are similar except for the energy consumption at a 40 mph speed and a distance of 900 m where the results slightly vary due to higher PER.

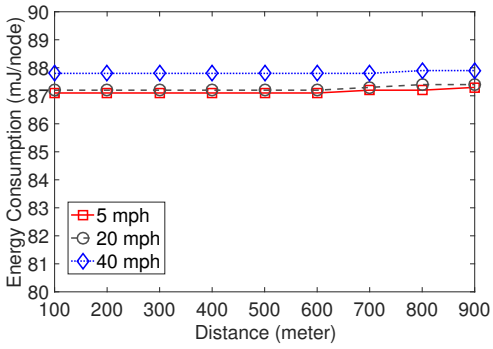


Figure 3.15: CC1310 Outdoor energy consumption

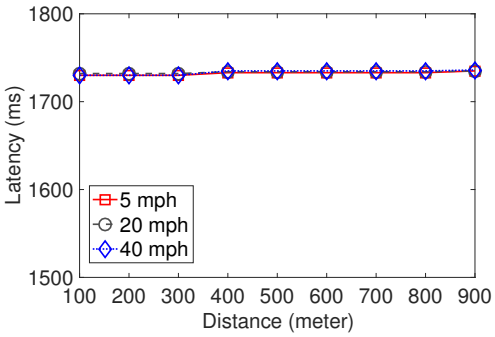


Figure 3.16: CC1310 Outdoor latency

3.6.3 Experiments with USRP: Deployment in a Metropolitan City

Figure 3.17 shows the distances in a metropolitan city where the mobility data were collected from nodes placed inside a moving car. Streets names and the locations in the map are blurred to hide the identity of the authors. The BSs are kept stationary. The vehicle is continuously moving at varying speeds (up to 40 mph) from one BS to the other in the mobile scenario. The antenna height was kept at 2 meters above the ground in all the experiments. We used the default setting in all the experiments.

Reliability over Distance. To observe the effect of distance on the reliability of SNOW in

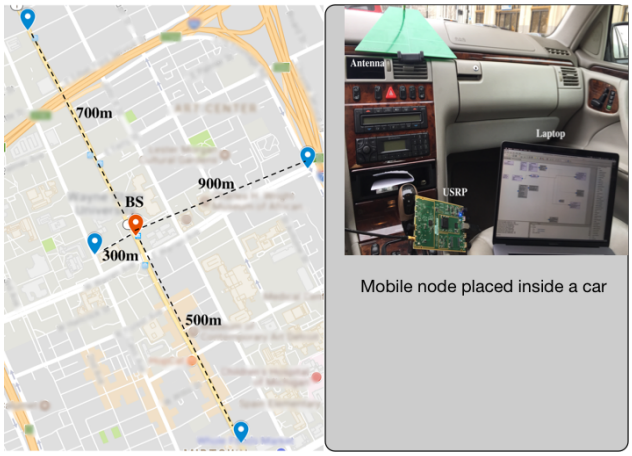


Figure 3.17: USRP experimental setup

mobile scenarios, we collect the data at 300m, 500m, 700m, and 900m from the BS, respectively. Each node transmits 5000 packets. To measure the reliability, we chose Correctly Decoding Rate (CDR), which is the ratio of the number of correctly decoded packets at the BS to the total number of transmitted packets [107]. Figure 3.18 shows the reliability over various distances from the BS when the node is moving from one BS to the other. At 300 meters, the BSs can decode on average 96.6% of the packets from the mobile node compared to 100% for the stationary node. Furthermore, at 500 meters away, the mobile node's reliability reduces to 96%, while the stationary node achieves 99.99% reliability. At 900 meters, the reliability is 80% for the mobile node compared to 99.95% at the stationary node. These results show that the distance between the mobile node and BS has a significant impact on decoding reliability. However, Even for the stationary node, its' performance is slightly impacted by the distance from the BS.

Performance of SNOW with CFO. In this experiment, we observe the performance of SNOW to demonstrate the effect of CFO estimation and compensation in mobile environments. We compare the CDR of a mobile SNOW node in two cases, with CFO estimation and compensation and

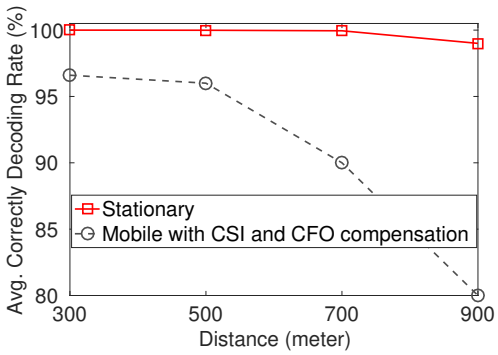


Figure 3.18: Reliability over distances

without CFO compensation. Also, we compare the performance of each case to the performance of a stationary SNOW node. All the nodes were 500m away from the BS. The mobile nodes were placed in a car moving at varying speeds. Each node transmits 5000 packets asynchronously to the BSs. For mobile nodes, each node transmits 2500 packets to BS1 and 2500 to BS2. Figure 3.19 demonstrates the effect of CFO under mobility. For stationary nodes, the average CDR is around 99.97% for all the transmitted packets. Without compensation for CFO, the average CDR is around 80% for all the nodes. However, we compensate for CFO; the average CDR increases to 96%, which is significant. This result demonstrates that in mobile environments, CFO could severely impact the transmission reliability. Thus, CFO estimation and compensation could significantly increase the reliability of the transmission in inter-SNOW communication.

Maximum Achievable Throughput. In this experiment, we compare the maximum achievable throughput in mobile inter-SNOW with the stationarySNOW. For both scenarios, each node transmits 100 40-byte packets. We calculate the combined throughput at the BSs. Figure 4.12 shows that when 8 nodes are transmitting, the maximum achievable throughput is 298 kbps and 393 kbps for mobile and stationary SNOWs, respectively. During mobility when 10 nodes transmit

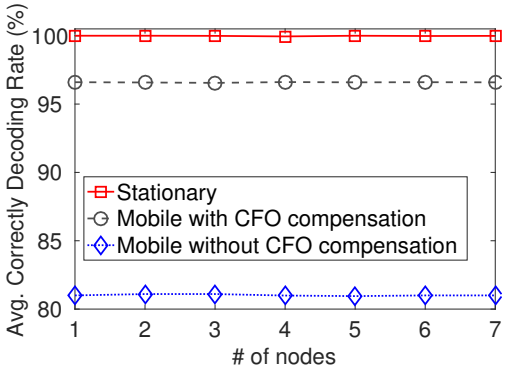


Figure 3.19: Performance under mobility with CFO

simultaneously. Due to the increased packet loss rate during mobility, stationary SNOW achieves better throughput.

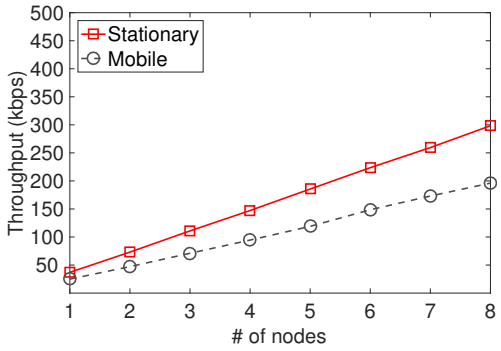


Figure 3.20: Throughput vs # of node

Energy Consumption and Latency. In this experiment, we demonstrate the efficiency of our mobility approach for USRP in terms of energy consumption and latency. Specifically, we compare the efficiency of mobile SNOW with stationary SNOW. We observed that the performance of SNOW under mobility is affected by the distance from the BS. Hence, for a fair comparison with stationary SNOW, we place 7 mobile node 900m away from the BS2 while continuously moving at approximately 20mph towards BS1. Furthermore, since USRP devices allow for bidirectional

communication, each node transmits 100 packets (50 to BS1 and 50 to BS2 during mobility) during the upward duration (1s) and waits until the end of the upward duration to receive an acknowledgment (ACK) from the BSs. We then calculate the average energy consumption per node and the time needed to collect all the packets at the BS.

Figure 3.21 shows that the average energy consumed at the mobile nodes is around 47.4mJ compared to 47.32% in stationary nodes when 7 nodes transmit. This shows that mobility has a minimal impact on the energy efficiency of the node. Similar to the average energy consumption, Figure 3.22 shows that the latency of collecting all packets in mobile SNOW is comparable to the stationary SNOW. These results demonstrate that the efficiency of SNOW is not affected by mobility.

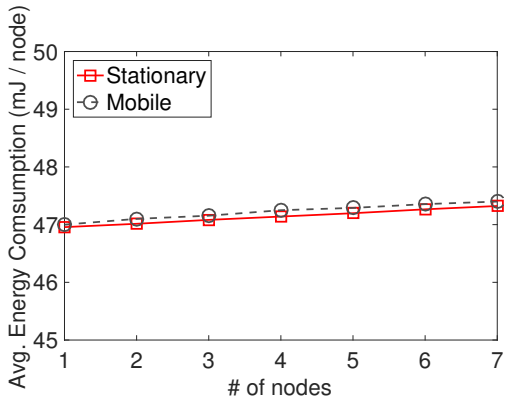


Figure 3.21: Energy consumption

3.7 Summary

In this chapter, we propose to handle mobility in SNOW (Sensor Network Over White spaces), an LPWAN that is designed based on D-OFDM and that operates in the TV white spaces. SNOW supports massive concurrent communication between a base station (BS) and numerous nodes. We

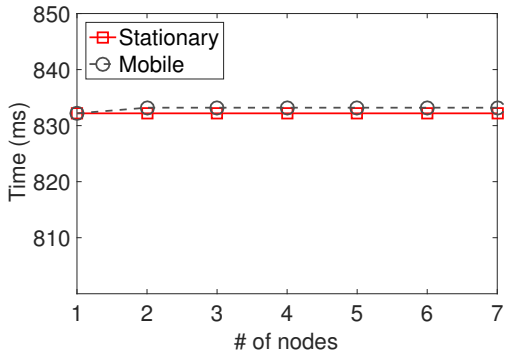


Figure 3.22: Latency

have proposed a dynamic CFO estimation and compensation technique to handle mobility impacts on ICI. We have also proposed to circumvent the mobility impacts on geospatial variation of white space through a mobility-aware spectrum assignment to nodes. To enable mobility of the nodes across different SNOWs, we have proposed an efficient handoff management through a fast and energy-efficient BS discovery and quick association with the BS by combining time and frequency domain energy-sensing. Experiments through SNOW deployments in a large metropolitan city and indoors have shown that our proposed approaches enable mobility across multiple different SNOWs and provide robustness in terms of reliability, latency, and energy consumption under mobility.

CHAPTER 4 RNR: REVERSE & REPLACE DECODING FOR COLLISION RECOVERY IN WIRELESS SENSOR NETWORKS

Interference between concurrent transmissions causes severe performance degradation in a wireless network. This work addresses interference cancellation to enable simultaneous packet receptions at a node with a single radio in WSN. Interference cancellation is particularly important for WSN as most of its applications rely on *convergecast* where all the traffic in the network is delivered to a base station leading to a lot of packet collisions. Existing solutions for collision recovery make simplified assumptions such as the availability of one of the collided packets, repeated collisions of the same packets, and the ability to identify the collided packets before recovering them which do not hold for WSNs and most wireless networks. In this chapter, we propose a novel collision recovery method called ***Reverse and Replace Decoding (RnR)*** for WSNs. RnR entails a physical-link layer design to exploit the raw samples of the colliding signals. It does not rely on the assumptions made in existing work, and can recover all packets from a ***single*** collision. To demonstrate its feasibility, we have implemented RnR using GNU Radio on USRP devices based on IEEE 802.15.4 network. Our experiments on a 6-node testbed demonstrate that RnR can successfully decode packets in 95% cases of collisions, and improves the correctly packet decoding rate up to 97.5% compared to standard decoders in the case of collisions. Also, our simulation based on GNU Radio simulator using 25 nodes shows that RnR achieves 4x higher throughput compared to the state-of-the-art collision recovery mechanisms.

4.1 Introduction

In a wireless network, concurrent transmissions from different devices sharing the same channel collide at the receiver, causing no successful packet reception. Such *interference* between concurrent transmissions is a well-known problem that causes severe performance degradation in a wireless network. Many networks (e.g., IEEE 802.11 [54], IEEE 802.1.5.4 [55]) adopt Carrier Sense Multiple Access (CSMA) to avoid collisions [15, 44, 111]. CSMA senses the channel before transmitting, and backs-off for some amount of time if it detects any traffic on the channel, and attempts to retransmit thereafter. However, in many cases, CSMA cannot avoid collisions, for example, in the presence of hidden terminals [66] which is quite common in most wireless networks. Such collisions in CSMA protocols severely reduce the throughput. While networks such as IEEE 802.11 have the option of adopting RTS/CTS [142] to reduce collisions, it introduces significant overhead to the network and reduces the effective throughput. In most 802.11 nodes, RTS/CTS is disabled by default. In low-power wireless networks such as IEEE 802.1.5.4 and WirelessHART [139], this method is impractical and is never adopted.

We address interference cancellation in WSNs such as those based on IEEE 802.15.4 and WirelessHART. Interference cancellation is particularly important for WSN as most of its applications rely on *convergecast* [109] where all the traffic in the network is delivered to a base station leading to a lot of packet collisions. Collision recovery has been studied in many early works. *Capture effect* [80] can recover at most one packet and only if its Received Signal Strength (RSS) is significantly higher (by 1-3dB) than that of the other colliding signal/s, and in cases (based on radio design) if it arrives before the others. A link layer solution cannot recover all collided packets as it

requires the raw signal sampled at the physical layer, thus making collision recovery **challenging** for network engineers. Existing physical layer solutions for collision recovery in wireless networks make simplified assumptions such as the availability of one of the collided packets [48, 61, 64, 65], and repeated collisions of the same packets and the ability to identify the collided packets before recovering them [47] that do not hold in WSN as well as in most wireless networks. The broadcast scheme proposed in [18] adopted a collision recovery technique for identical broadcast transmission only, thus limiting its applicability for packet collisions in WSNs. A recently proposed recovery technique [69] from a single collision for ZigBee [151] radio only leverages on discerning an exponential (in number of packets that collide) number of amplitude levels, thus being subject to high bit error that makes it less effective in practice even when just two packets collide. It cannot be used if more than four packets collide. In WSN convergecast, a large number of packets may collide, thus requiring a new collision recovery mechanism.

In this chapter, we propose a new collision recovery method called ***RnR*** for WSNs. RnR entails a physical-link layer design to exploit the raw samples of the colliding signals. It does not rely on the assumptions made in existing work, and can recover all packets from a ***single*** collision. It is bootstrapped only after a collision is detected, and starts by first extracting a collision-free chunk from the collided signal. This chunk is then subtracted from the collision to retrieve the collided ones. This iterative process continues until the collided packets are recovered. To decode all packets from a single collision, the key idea in the proposed physical-link layer design is to replace the CRC (Cyclic Redundancy Check) of a packet by a longer error correction code, thus requiring packet augmentation. Since WSN packets, in practice, are much shorter than their maximum

carriable size [18], augmenting a packet length is easily affordable in WSN without exceeding channel capacity. Hence, our RnR design is specifically focused on WSN. However, any network based on digital modulation that can afford such packet augmentation can adopt RnR for collision recovery.

To demonstrate the feasibility of recovering from collisions, we have implemented RnR in GNU Radio [46] on USRP [103] devices for IEEE 802.15.4 networks. We have experimented on a 6-node testbed and also through GNU Radio simulator for larger scale tests. The experiments demonstrate that RnR can successfully decode packets in $\geq 95\%$ cases. RnR also achieves 4x higher throughput over the state-of-the-art collision recovery mechanisms [69, 47]. Our extensive experiments also demonstrate that, in the case of collisions, RnR improves the correctly packet decoding rate up to 97.5% over standard decoders.

The rest of the chapter is organized as follows. Section 4.2 reviews related work. Section 4.3 provides a detailed description of the proposed RnR decoder. Section 4.4 describes our implementation of the RnR decoder. Section 4.5 describes the experimental results. Section 4.6 describes the simulation results. Section 4.7 concludes the chapter.

4.2 Related Work

Collision recovery was studied in various wireless domains under various simplified assumptions that do not hold for most wireless networks [48, 61, 64, 65, 47, 51, 96, 112]. Successive interference cancellation [51, 96, 112] works only if the radio's bit rate is significantly reduced from what its SNR (signal to noise ratio) allows and if the interfering senders have significantly different powers or pre-coded signatures. It also demands prior scheduling and known users, and

is basically designed for cellular networks. Analog network coding [64], XORs [65], interference alignment [48], and full duplex [61] require a receiver to have one of the two colliding packets. Hence, they are not applicable for WSNs where packets from different senders are unknown a priori. SNOW [106] base station receives multiple packets using an OFDM based physical layer design that is different from the traditional WSN devices and not yet adopted in the commercially available WSN devices.

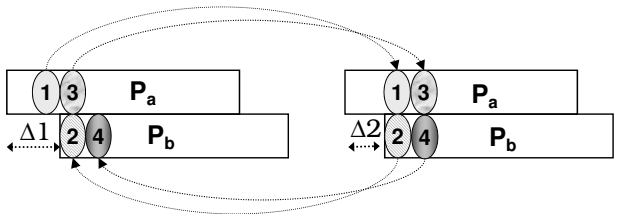


Figure 4.1: ZigZag decoding: first decodes interference free chunk 1 in first collision. It subtracts chunk 1 from second collision to decode chunk 2, which it then subtracts from first collision to decode chunk 3, so on [47].

Obviating most of the above assumptions, ZigZag [47] was designed as a modulation independent decoding for 802.11 networks. As shown in Fig. 4.1 for 2 packets P_a and P_b, ZigZag first decodes all interference-free samples using a standard decoder and then re-encodes those symbols and subtracts them from the collision that overlaps with those. It iteratively applies this technique to decode entire frames. However, to resolve one collision of m packets, it needs at least m repetitions of the collision, every time with different arrival time offsets between the packets (i.e. $\Delta_1 \neq \Delta_2$ must hold in Fig. 4.1). Depending on at least m collisions reduces throughput, consumes huge energy, and is not worth adopting in WSN where nodes are resource constrained. Even if it is adopted at the cost of energy, to merge the chunks of a packet from different collisions, the receiver

should correctly identify which packets the chunks across collisions belong to before recovering them. This assumption does not hold in WSN and most wireless networks. In fact, ZigZag would require to explore all possible combinations of the chunks which is exponential (in terms of the number of chunks as well as m) to recover a packet as its chunks cannot be identified from multiple collisions. In contrast, RnR is capable of recovering all packets from a single collision, and hence does not suffer from this problem.

While mZig [69] is designed to recover packets from a single collision in ZigBee networks, it depends on discerning 2^m amplitude levels if m packets collide, thereby being subject to high bit errors. Since amplitude of a signal is highly susceptible to noise and obstacle, it is difficult to distinguish many amplitude levels in practice even if the signals are received correctly. Thus, mZig is less effective in recovering even when just two packets collide. Also, mZig will not work when the two bits to be separated from the different packets have an equal amplitude as explained below. It exploits the half-sine pulse shape of baseband signal in ZigBee devices. Thus, when 2 packets collide, it has to discern 4 amplitude levels of the bits. Considering α and β as the amplitudes from the two packets, the 4 signal levels are $\alpha+\beta, \alpha-\beta, -\alpha+\beta, -\alpha-\beta$. Assuming $\alpha > \beta$, if the level $\alpha-\beta > 0$, then α is decoded as '1' and β is decoded as '0', and if the level $-\alpha+\beta < 0$, then α is decoded as '0' and β is decoded as '1'. Hence, when the bits from 2 packets have an equal amplitude, the signal levels $\alpha-\beta$ and $-\alpha+\beta$ will not allow us to determine which packet's bit is '0' and which packet's bit is '1'. Thus the decoding will fail. Most importantly, mZig does not work when $m > 4$. In WSN convergecast, a large number of packets may collide, thus requiring a new collision recovery mechanism. Finally, mZig is not applicable to any network

other than ZigBee [151]. In contrast, RnR does not suffer from the above limitations as it does not depend on discerning amplitude levels. Specifically, RnR is capable of recovering all packets successfully from a collision of any number of packets (with no limitation on m). Additionally, RnR is applicable to any physical layer of WSN.

4.3 Reverse & Replace Decoding

This section presents our proposed ***Reverse & Replace decoding*** for recovering collided packets in WSNs. We first present the underlying challenges in collision recovery and the key principle in RnR design. This is followed by a detailed technical description of RnR and the design considerations.

4.3.1 Key Design Principle

When two or more packets collide at a receiver's radio, the radio cannot recover any of those packets. Recovering the collided packets requires further decoding of the composite signal of the collision and is challenging. Also, for different modulation techniques, the decoding for collision resolution may be different. It is also impacted by the underlying radio design. As an example, we provide an overview of the off-the-shelf radios based on IEEE 802.15.4 [23] and WirelessHART [139]. During the synchronization header decoding mode while receiving a packet, its radio searches for preambles and start frame delimiter with the strongest RSS [7, 23, 139]. After this, the radio generates an interrupt and locks to payload reception mode, and no more searches for preambles. Therefore, ***capture effect*** [67, 80] can recover the stronger packet if it comes before the radio locks to a weaker packet's payload reception mode. If the stronger packet comes later, it may be possible to make the radio search for new preambles and resynchronize to it [137].

However, in either case, only the strongest packet can be recovered and only if its RSS is significantly higher (by 1–3dB based on modulation) than the other signal/s. A link layer solution cannot recover all collided packets, as it requires the raw signal sampled at the physical layer. Hence, the proposed RnR decoder involves a physical-link layer design to recover packets from collisions.

As discussed in Section 3.2, existing physical layer solutions for collision recovery [64, 47, 69, 51, 96, 112] make simplified assumptions that do not hold for WSN and most wireless networks. As a quick recap, network coding [64, 65] requires a receiver to know one of the two colliding frames. mZig [69] depends on discerning 2^m amplitude levels if m packets collide, thereby being subject to high bit errors. It does not work when the two bits from the different packets have the same amplitude. Also, it does not work when $m > 4$. Finally, mZig is not applicable to any network other than ZigBee [151]. ZigZag [47] decodes frames in 802.11 networks by iteratively subtracting collision free chunks from multiple collisions. However, to resolve one collision of m packets, it needs at least m repetitions of the collision, every time with different arrival time offsets between the packets. This is not worth adopting in WSNs. Even if it is adopted at the cost of energy, to merge the chunks of a packet from different collisions the receiver should correctly identify which packet each chunk belongs to before recovering them. This assumption does not hold in WSNs. The dependence on multiple collisions is the root of this problem. This motivates a collision recovery mechanism that should depend on a single collision. Our proposed RnR decoding hence depends on a single collision while following the principle of ZigZag in that it also first finds a collision free chunk. But, unlike ZigZag, it exploits that chunk to decode all packets from a *single* collision. RnR is invoked only upon a collision, and is applicable to any physical layer of WSNs.

Now we review the structure of the composite signal of collided packets which will be exploited by RnR. A wireless signal is represented as discrete complex values [126]. A received signal is represented as a sequence of samples spaced by sampling interval T. If $X[n]$ is the complex value of the n-th sample at the transmitter, the received sample is given by

$$Y[n] = HX[n] + W[n]$$

where $H = he^{\gamma}$ is the channel parameter with channel attenuation h and phase shift γ, and $W[n]$ is the noise. If two senders a and b transmit concurrently, the received sample can be expressed as

$$Y[n] = H_a X_a[n] + H_b X_b[n] + W[n]$$

where H_a and H_b are the channel parameters; $X_a[n]$ and $X_b[n]$ are the transmitted samples of a and b, respectively. In RnR design, we exploit the above structure of collided signals which helps recover a chunk of one packet from a collision by subtracting an already recovered chunk of the other.

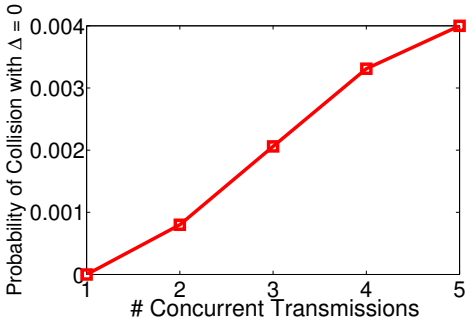


Figure 4.2: Fraction of collisions with $\Delta = 0$ in experiment.

4.3.2 Core Technique of RnR Decoding

We detail the RnR decoding technique first for 2 packets P_a (transmitted by a) and P_b (transmitted by b) with arrival time offset Δ. Two senders' processing, clock drifts, back-offs, and distances from the receiver cause $\Delta \neq 0$, allowing an interference-free chunk to exist. Our 10-day long experiments show that the probability of collisions with $\Delta = 0$ tends to be 0 as shown in Fig. 4.2. We performed an experiment based on 802.15.4 networks in an indoor environment. We used our 6-node testbed (5 transmitters and 1 receiver). All the transmitting and receiving nodes were fixed in different locations. Every transmitter (Tx) is at a distance of approximately 25 ft from the receiver and all 5 transmitters try to send to one receiver at 0 dBm transmission power. Each transmitter sends a 129-byte packet (32 bits preamble and 1000 bits payload) every 4ms consecutively. We record the data for 5 hours a day for a period of 10 days considering 500,000 packets (100,000 packets for each Tx). Fig. 4.2 shows the fraction of total collisions that experience $\Delta = 0$ under varied number of concurrent transmitters. As the figure shows, the probability of collisions with $\Delta = 0$ is very low. Making the senders do a small random back-off before transmitting can further reduce this probability. Thus a collision-free chunk is almost certain to exist. RnR exploits this collision-free chunk.

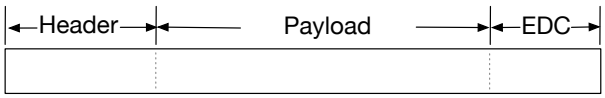


Figure 4.3: A WSN packet structure.

To exploit a collision-free chunk to decode all packets from a single collision, a packet needs a little preprocessing before transmission. As shown in Fig. 4.3 for WSN, a MAC layer packet

(frame) consists of three segments: header, payload, and EDC (error detection code). The EDC is usually 2-byte CRC. As preprocessing before transmission, we replace the CRC with a new and longer Error Correction Code (ECC) that is created by reversing the order of the bits of the entire packet and append it just after the original CRC. Thus, each packet P_a is ***augmented*** as a new packet P'_a whose first half is exactly P_a and the second half is its ***clone*** created by reversing the order of the bits of P_a. We take the advantage that WSN packets, in practice, are much shorter than their maximum carriable size [18]. For example, IEEE 802.15.4, a widely used standard for WSN, has a maximum allowable packet size of 128 bytes of which 104 bytes is payload. In practice, their payload (data) is very short and of several bytes only [18]. The same is true for WirelessHART which is predominantly being used worldwide for wireless process monitoring and control purposes [139]. Thus, augmenting a packet length is easily affordable within channel capacity in WSN, and hence our RnR decoder design is specifically focused on WSN. However, any network based on digital modulation that can afford such packet augmentation can use our RnR decoder for collision recovery.

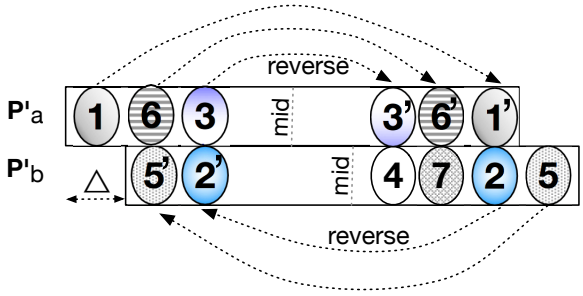


Figure 4.4: RnR: first decodes chunk 1 and 5. Chunk 1 is reversed and re-encoded as chunk 1' and then subtract from collision which gives chunk 2, and so on.

Fig. 4.4 illustrates the RnR decoding for P_a and P_b when they collide with arrival time offset Δ.

As the figure shows, chunk 1 of P'_a and chunk 5 of P'_b are interference free and hence are decoded using standard decoder. Any chunk in one half of a packet has a ***clone*** in the other half which is its reversed version, and is located at the same position from the other end. For example, chunk 1' is the clone of chunk 1. To recover all chunks of P_a and P_b, we iteratively do the following: An already decoded chunk is reversed and re-encoded as its clone, and then subtracted from the collision that overlaps with those symbols, giving a new chunk. That is, chunk 1 is reversed and re-encoded as chunk 1' and then subtracted from the collision that overlaps with those symbols, giving chunk 2. Chunk 2 is reversed and re-encoded as chunk 2' and then subtracted from the collision which gives chunk 3, and so on. We do the same for chunk 5 to get chunk 6, and so on. This re-encoding is done using a standard approach [126] as described in the next Section. Once all the chunks of a packet are decoded, they are merged and retrieved as the original packet. We can repeat the same for any number of packets to recover all packets involved in an m-packet collision, for any value of $m > 2$. In the general case when $m > 2$, we transform the decoding problem into system of linear equations problem. We consider each chunk in a packet as a variable, and each chunk-level collision yields an equation. We can decode all the packets only if number of equations $\geq$ number of unknown variable. Upon recovering, the link layer sends an acknowledgment (ACK) to all senders.

It can be noted that packet augmentation in our design may increase the chance of collision. Specifically, any collision that happens due to augmented packet length may be due to our design. As Fig. 4.5 illustrates, if a collision starts at the second half of a packet, there is no need to use our RnR decoder as each packet's non-colliding part contains the original packet or its clone and,

hence, is decoded using standard decoder. Thus, the increased collision probability due to packet augmentation does not increase decoding overhead.

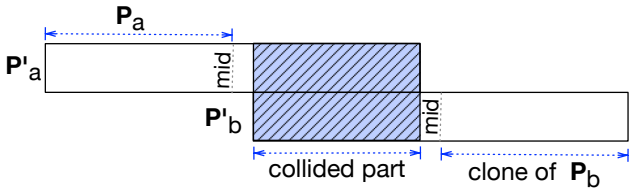


Figure 4.5: A collision that starts at the second half of P'_a: both packets are recoverable from the collision-free parts using a standard decoder.

Re-encoding of Chunks. Ideally, when transmitting a signal, we expect to receive identical signal. In practice, we always receive slightly different signal from the transmitted one, which complicates the signal processing at the receiver. Frequency offset, δf, usually exists between two radios due to the difficulty of manufacturing radios with the same center frequency. Due to such offset, the received signal will always be shifted in frequency. Most receivers estimate the frequency offset, δf, by tracking the phase and then compensate for it. When building a communication system, we must compensate for frequency offset in a received sample as follows.

$$Y[n] = H_a X_a[n] e^{j2\pi n \delta f T} + W[n]$$

In our decoding, we first need to reverse the bits of an already recovered chunk and then re-encode it to be subtracted from the collision to recover a new chunk. This re-encoding is done using a standard approach [126]. Considering δf_a as a's frequency shifting, its symbol $X_a[n]$ is received as $Y_a[n] = H_a X_a[n] e^{j2\pi\delta f_a T}$ at the receiver if it is sampled exactly at the same locations as a. Taking into account a sampling offset of μ_a seconds between a and the receiver, the sample at

time $n + \mu_a$ can be re-encoded through interpolation based on Nyquist criterion as follows.

$$Y_a[n + \mu_a] = \sum_{i=-\infty}^{\infty} Y_a[i]\text{sinc}(\pi(n + \mu_a - i))$$

which, in practice, is approximated by taking the summation over few symbols near n. Standard wireless receivers can estimate the system's parameters such as H_a and δf_a using the preamble in a's transmission. Note that preambles are detectable through correlation even during collision.

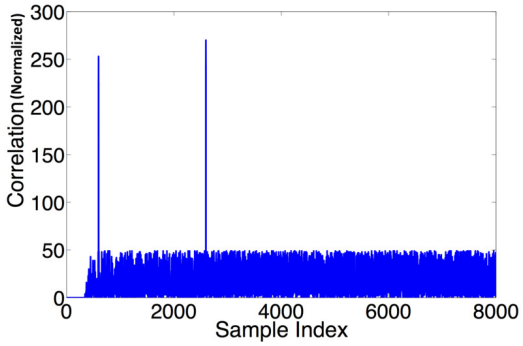


Figure 4.6: Time offset collision detection using correlation method.

Collision Detection. Collision Detection is a critical part in the RnR decoding. We adopt the preamble correlation based technique which is a well-known and commonly adopted technique [47, 69]. In a wireless network, every packet is preceded by a known preamble. RnR detects the collision using the correlation between the known preamble and the received signal. Correlation is a widely used technique in signal processing to measure the similarity between two signals [20]. To understand how this technique works, let L be the preamble length (in number of samples). When the receiver receives the first R samples of the packet, it aligns those with L preamble samples and calculates the correlation. It then shifts the alignment to the next R samples

and re-calculates the correlation. The receiver repeats this process until the end of the packet.

Fig. 4.6 shows an example of a 2-packet collision. The preamble is a pseudo-random sequence independent of transmitted data. Hence, the correlation value is always near zero, except when the preamble is perfectly aligned with the beginning of the packet. A value significantly greater than zero indicates a collision. In the figure, the spike at the beginning indicates the beginning of the first packet, while the position of the second spike indicates the beginning of the second packet. After collision detection, to detect the offset (Δ) between the packet arrival times in the same collision, which yields the collision-free chunks, let t_a be the arrival time of a's packet (P_a) and t_b be the arrival time of b's packet (P_b). To find Δ between P_a and P_b in the same collision, the receiver finds the distance between the position of the beginning of the first packet and the position of the beginning of the second packet. Mathematically, $\Delta = |t_a - t_b|$. Thus, in Fig. 4.6, the distance between the two spikes indicates Δ. Beyond two collisions, to detect m-packet collision, we detect if there are m spikes in the correlation results. The receiver must compensate for the frequency offset before applying correlation. However, the frequency offset between two communication ends does not change significantly over a long period of time [47]. Hence, the receiver maintains a coarse estimation for each active transmitter at the beginning of the transmission by tracking the frequency offset on the collision-free samples.

4.4 Implementation

We implemented RnR in GNU Radio [46] on Universal Software Radio Peripheral (USRP) devices [103]. Each USRP device is connected to a PC running GNU Radio. GNU Radio is a free development toolkit that provides signal processing tools for implementing Software Defined

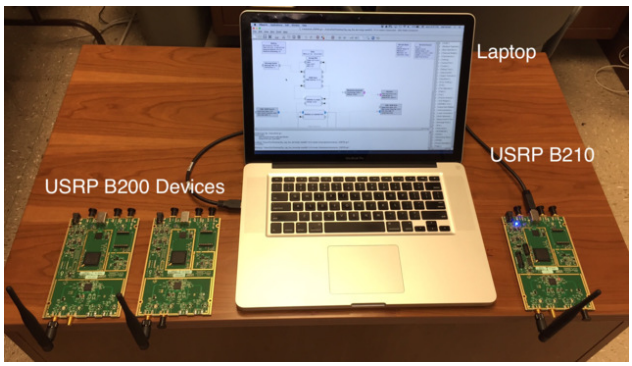


Figure 4.7: USRP connected to PC used in our experiment.

Radios (SDR). USRP devices act as a transmitter/receiver front-end of the SDR platform that help implementing RF applications in a wide range of frequencies. We incorporated RnR in IEEE 802.15.4 GNU Radio implementation [56]. Fig. 4.7 shows a USRP device connected to a laptop, which was used in our experiment.

On the transmitter (Tx) side, we used B200 USRP device as an RF front-end, which can operate in 70 MHz - 6 GHz coverage range. We used a custom packet generator to generate augmented packets in the IEEE 802.15.4 packet format. A packet is represented using the default GNU Radio vector. RnR can use any standard decoder/encoder as a black-box since it is modulation-independent. Finally, we send the packet to the USRP RF front-end for transmission.

On the receiver side (Rx), a USRP B210 device is used as a base station and acts as the receiver. We include new block to extract the collision-free samples to bootstrap the decoding process. After receiving the signal we apply the correlation method explained in Section 4.3.2 to detect collisions. If there is a collision, we detect how many packets collided together using the correlation values outputted from the correlation block. Next, we extract the collision-free samples and start the iterative RnR decoding process until all collided packets are recovered. Fig. 4.8 shows the flow

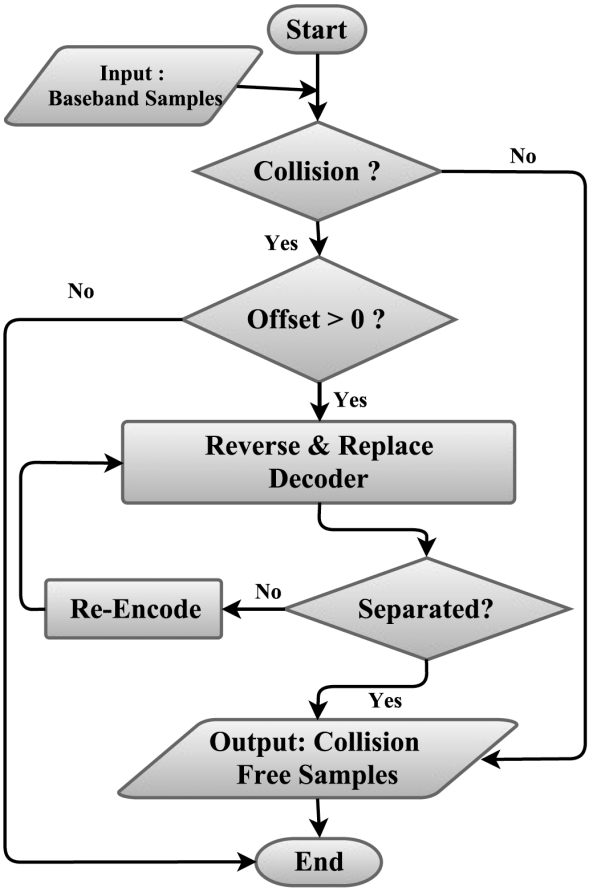


Figure 4.8: Reverse & Replace decoding flow chart.

chart for the RnR decoding process.

4.5 Experiment

To verify the feasibility of RnR, we perform experiments based on IEEE 802.15.4 networks. IEEE 802.15.4 is a widely adopted low power WSN technology. The experiments were performed using 6 USRP devices. Larger-scale evaluation is done in simulations (to be explained later).

4.5.1 Experimental Setup

We incorporated the RnR decoder in the GNU Radio implementation of 802.15.4 [56]. Our experiments are limited to indoor and non-mobile environment, where all the transmitting and

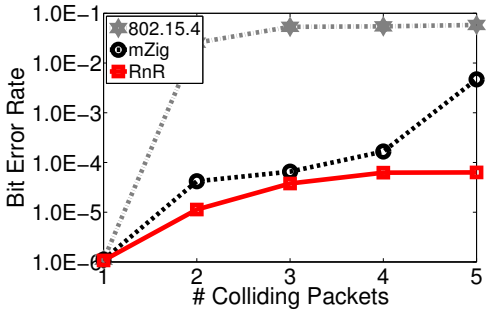
Figure 4.9: Node positions on building floor plan.

receiving nodes are fixed in different locations. Fig. 4.9 shows the positions of the nodes on the building floor plan where the experiments were conducted. We fixed the distance for each transmitter from the receiver to 25 ft. Five nodes are transmitters and one node is the receiver. Unless stated otherwise, each transmitter sends a 1032-bit packet (32 bits (preamble+header) and 1000 bits payload) every 4ms. We experimented in the 2.4GHz band. To avoid interference from the existing WiFi networks, we choose channel 26 as the operating channel for 802.15.4, which is non-overlapping with WiFi. The bandwidth for this channel is 2MHz. To meet the IEEE 802.15.4 standard transmission and reception power requirements (maximum 0dBm), we set Tx gain to 70 dB in GNU Radio, which allows the USRP devices to perform transmission/reception near 0dBm. We fixed the antenna height approximately 5 ft above the ground.

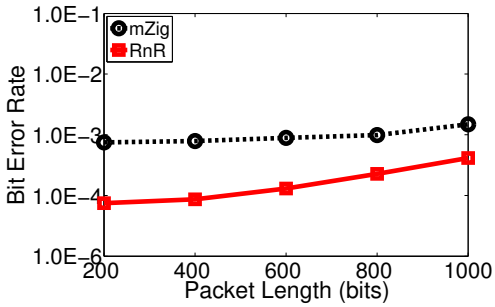
4.5.2 Evaluation Criteria and Baselines

We compare the performance of RnR against that of mZig, which is the state-of-the-art collision decoder for ZigBee networks. mZig exploits the physical layer of ZigBee to resolve collision. We also compare against ZigZag, which is the state-of-the-art collision recovery mechanism for IEEE 802.11 networks, by adapting it to 802.15.4 networks. Finally, we compare RnR against the

conventional IEEE 802.15.4 MAC protocol which handles collisions using CSMA/CA mechanism. For networks where few collision events occur, conventional IEEE 802.15.4 decoders would be sufficient.



(a) Under varying number of packets colliding



(b) Under varying packet sizes

Figure 4.10: Bit Error Rate under different decoding

We use the following metrics for performance evaluation.

- ***Bit Error Rate (BER)*** defined as the ratio of the number of incorrect bits to the total number of bits in the packet. We drop a packet if the BER $\geq 10^{-3}$. This setting complies with traditional wireless design [47].

- ***Correctly Decoding Rate (CDR)*** defined as the ratio of the number of packets that are correctly decoded at the receiver to the total number of transmitted packets. This is a key

metric to evaluate RnR's performance.

- ***Throughput*** defined as the total number of bits received per unit time.
- ***Energy Consumption***.
- ***Latency***.

4.5.3 Results

BER. First, we analyze the BER for different numbers of colliding packets. The node positions are shown in Fig. 4.9. We run the experiment for one hour. We vary the number of collided packets between 2 and 5 by turning off and on the Tx's. We compare the performance against mZig and the conventional 802.15.4 (we particularly considered ZigBee [55]). In this experiment, CSMA/CA is disabled for 802.15.4 to show the decoding capability from collisions. Fig. 4.10(a) shows that 802.15.4 has BER greater than 10^{-3} when 2 or more packets collide. Hence, it cannot decode packets from collisions. RnR has BER less than 10^{-3} when two or more packets collide. Analytical results from mZig [69] show that its BER exceeds 10^{-3} when more than 4 packets collide. RnR has much lower BER than mZig, and significantly lower than 802.15.4 as the number of colliding packets increases.

In addition to our chosen 1000-bit payload length, we vary the packet length and observe the BER. In this experiment, we vary the payload length from 200 to 1000 bits, and the number of colliding packets is limited to 2. Fig. 4.10(b) shows a negligible increase in BER under RnR as we increase the packet length. In contrast, the BER under mZig significantly increases as the packet length increases. This happens because mZig decodes by discerning amplitude levels of

the colliding packets (as we discussed in Section 3.2). It has serious limitations in decoding as it experiences a BER greater than 10^{-3} when the payload length approaches 1000 bits. Our results (Fig. 4.10) as well as that in [69] show that mZig can decode packets with a maximum length of ≈ 1032 bits, with up to 4 concurrent transmissions, while RnR shows the capability of decoding any number of concurrent transmissions.

CDR. We measure the CDR, we use 2 transmitters. Every transmitter attempts to send a packet in a random time between 50-100ms of frame gap for 5 hours. Once the receiver receives the packets, we record the data. We recorded reception of nearly 100,000 packets and analyzed the CDR offline. In this experiment, we disabled CSMA/CA for 802.15.4 to show its decoding capability from collisions. Fig. 4.11 plots the Cumulative Distribution Function (CDF) of the CDR values of RnR and that of 802.15.4. It shows that RnR can correctly decode packets from almost all collisions. RnR has a CDR of nearly 97.5% in more than 95% cases of collisions. On the other hand, conventional 802.15.4 has CDR less than 0.05% for 85% cases of collisions. This is because 802.15.4 physical layer is inherently not capable of recovering packets from collision. The results demonstrate RnR as a highly effective approach for collision recovery.

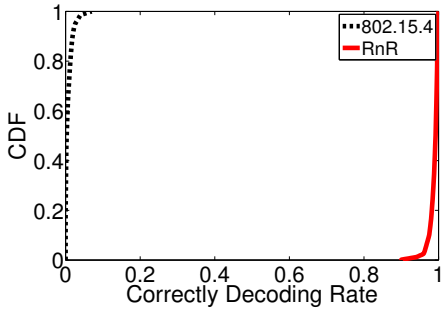


Figure 4.11: Distribution of CDR in RnR.

Throughput. We now observe throughput under varying number of transmitters. In each 4ms time window, each transmitter sends one packet at some random time in the window (maintaining exactly one transmission per window). Fig. 4.12 compares the throughput of RnR against that of the default 802.15.4, mZig, and ZigZag. While all schemes achieve almost the same throughput under one transmitter (no collision), RnR outperforms others as the number (m) of concurrent transmissions increases. Although the throughput under mZig looks competitive against that under RnR as long as $m \leq 4$, it sharply decreases when $m > 4$ as mZig cannot decode packets in the latter case. It decodes some of those packets later if 4 or less of these packets re-collide. For larger values of m, we will show later in simulation that RnR significantly outperforms mZig. RnR also outperform ZigZag. Since ZigZag needs m repetitions to decode packets from m-collisions, its throughput never exceeds that achieved with a single transmitter. Also, it requires to explore all possible (exponential number) combinations of the chunks to recover a packet as we cannot identify the packets across multiple collisions before they are recovered. On the other hand, RnR requires a single collision to decode all m packets. Hence, RnR's throughput increases gradually with the increase in m, and remains nearly m times that of ZigZag.

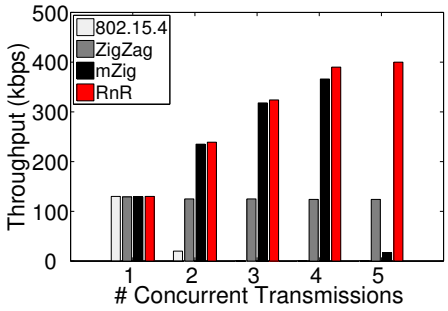


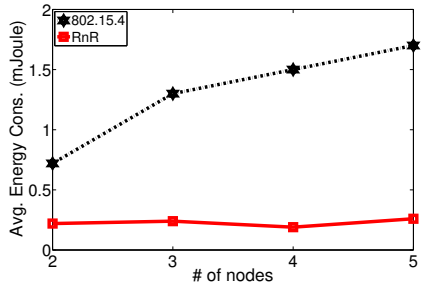
Figure 4.12: Throughput comparisons among RnR, mZig, ZigZag, and 802.15.4.

Device mode	**Current Consumption (Supply voltage 3 v)**
Tx	17.5 mA
Rx	18.8 mA
Idle	0.5 mA
Sleep	0.1 μA

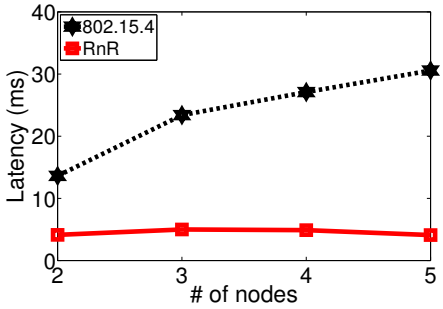
Table 4.1: Current Consumption in CC2420

Energy Consumption and Latency. We measure the energy consumption in RnR and compare with that in the conventional 802.15.4. Here we enable CSMA/CA of 802.15.4 to measure the energy efficiency of the protocol. In 802.15.4 each transmitter uses CSMA/CA to sense the channel before transmitting. If the channel is busy, it performs a random back-off between 0.32ms and 4.8ms, and then attempts to retransmit. In this experiment, we collect packets from 5 transmitters all of which try to send to one receiver. Every transmitter is 25 ft apart from the receiver and sends a 1032-bit packet every 4ms. We calculate energy consumption to collect 100 packets from each node. We model the energy consumption based on CC2420 radio [23] which is based on IEEE 802.15.4 in 2.4 GHz. Table 4.1 show the energy model for CC2420. We assume the receiver is always connected to a power source, and do not consider its energy consumption. Fig. 4.13(a) shows the average energy in each node per packet. RnR has almost a fixed energy consumption of 0.013mJ. On the other hand, 802.15.4 consumes an average of 0.7mJ considering 2 transmitters. Its average energy consumption increases linearly with the number of transmitters due to retransmissions and the 802.15.4 MAC overhead (back-off, ACKs). This shows that RnR is highly energy efficient.

Fig. 4.13(b) demonstrates the latency improvement for using RnR under the same previous



(a) Average Energy Consumption



(b) Latency

Figure 4.13: Energy consumption and latency under varying # of nodes.

setting. We measured the latency to deliver each packet at the receiver under varying numbers of concurrent transmissions. RnR takes approximately 4ms on average to deliver a packet, while the 802.15.4 takes approximately 13ms for 2 transmitters. As expected, with the increase in the number of concurrent transmissions, the latency in 802.15.4 increases due to its MAC overhead while, in RnR, it remains almost constant.

4.6 Simulation

To evaluate RnR in larger scale, we have performed simulations using the GNU Radio simulation environment [46]. GNU Radio includes a simulation environment that provides signal processing blocks to simulate signal processing systems on the host. For evaluation in simulations, we consider the same metrics and baselines used in our testbed experiment.

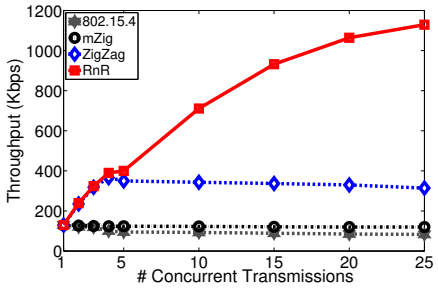


Figure 4.14: Throughput comparison in simuation.

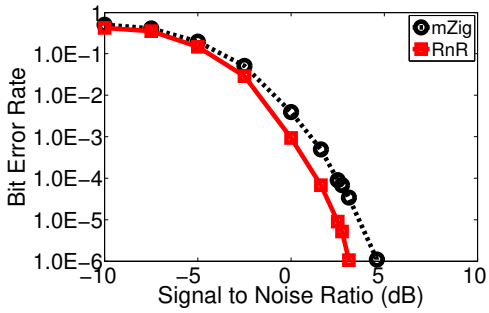


Figure 4.15: Bit error rate under different SNR conditions in simulation.

4.6.1 Simulation Setup

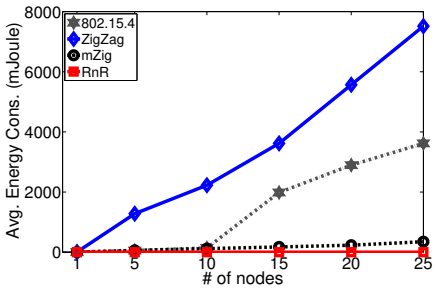
In simulations, we consider the number transmitters up to 25 all of which try to send to one receiver. Once the receiver receives 100 packets for each value of m between 2 and 25, we record the data. Every transmitter attempts to send a packet in a sliding window of 4ms, then remains idle for 100 ms. Every packet has a fixed length of 1032 bits. We record the data for 10 hours a day for 5 days, and analyze the results offline. During the simulation, every transmitter has a fixed gain of 70 dBi. A 3 dBm of Additive white Gaussian noise (AWGN) noise was added to the channel.

4.6.2 Simulation Results

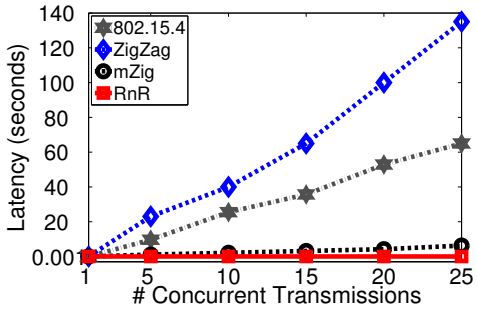
Throughput. We compare the RnR throughput against the conventional 802.15.4, mZig, and ZigZag. In this simulation, the MACs were enabled for both 802.15.4 and mZig. As Fig. 4.14 shows, when $m > 2$, RnR's throughput increases linearly while 802.15.4 maintains the same throughput of approximately 120 kbps with a small decrease as m increases. As ZigZag requires m retransmissions to recover m collided packets, it maintains a constant throughput of around 121 kbps with the increase of m. RnR achieves much higher throughput compared to mZig, and continues to outperform mZig as m increases. When $m > 4$, the throughput of mZig starts decreasing due to its decoding limitation. When $m = 25$, RnR has an average throughput of 1.2 mbps which is approximately 4x higher than mZig's average throughput.

BER. Fig. 4.15 shows the BER comparison among different schemes under varying SNR conditions when $m = 2$. The conventional 802.15.4 is not considered in this simulation since its BER exceeds the threshold for even 2-packet collision. The BER in RnR is much lower than that in mZig. Since mZig uses amplitude estimation to determine certain bits, the impact of SNR is

higher in mZig. However, both schemes are still within the range of reference (3dB) line for $m = 2$.



(a) Average energy consumption per node



(b) Latency

Figure 4.16: Energy consumption and latency in simulation.

Energy Consumption and Latency. To measure the energy consumption and latency, we use a sliding window of 1 second. Fig 4.16(a) shows the average energy consumption per packet at each node for all four schemes. For all the values of m, RnR maintains an average energy of 0.2 mJoules per packet. For 5 nodes, mZig consumes an average of 60 mJoules per packet to deliver 100 packets. For 25 nodes, it consumes approximately 349 mJoules. For mZig, the energy consumption increases due to the MAC protocol overhead as it allows only 4 concurrent transmissions. ZigZag consumes even higher energy. For 5 nodes it consumes approximately 1280 mJoules, and the average energy consumption increases sharply with the increase in m. This is because ZigZag depends on m retransmission to resolve an m-packet collision. Thus, an exponential time is needed

in calculating different chunk combinations to resolve the collision. For 802.14.5, the average energy consumed for 5 nodes is 53 mJoules. Also in 802.15.4, the increase in m leads to an increase in the average energy consumed due to the MAC overhead (back-off, ACKs, and retransmissions).

Fig. 4.16(b) shows the per packet latency for delivering 100 packets for each value of m. RnR takes approximately 5ms on average for the different values of m. For 5 nodes, mZig takes 1 second on average to deliver the packets, and for 25 nodes it takes approximately 6 seconds. In mZig, the BER constraints the number of concurrent transmissions, and mZig experimental result shows that up to 4 concurrent transmission must be decoded before transmitting again. Hence, mZig suffers from an increased latency. ZigZag on the other hand takes around 23 seconds to deliver the packets for 5 nodes. Its latency increases with the increase in the value of m due to the exponential waiting time and the retransmission. While the latency in RnR is 8 ms for 25 concurrent packets, traditional 802.15.4 takes around 65 seconds. This time increases with the increase of m in 802.15.4 because it suffers from collisions, random back-off waiting time, and retransmissions.

4.7 Summary

In this chapter, we have presented *Reverse and Replace decoding (RnR)*, a novel interference cancellation method for wireless sensor network (WSN). Because interference poses a serious problem in wireless network, the mechanisms for recovering from collisions have been studied in many early works [48, 61, 64, 65, 47, 51]. However, these existing solutions for collision recovery make simplified assumptions such as the availability of one of the collided packets, repeated collisions of the same packets, and the ability to identify the collided packets before recovering them which do not hold for WSNs and most wireless networks. RnR does not rely on the assump-

tions made in the existing works, and can recover all packets from a single collision. It entails a physical-link layer design that exploits the raw signal samples from a collision to recover the collided packets. RnR is bootstrapped only when a collision is detected, and involves no decoding overhead in the absence of collision. We have also implemented RnR in GNU Radio for USRP devices considering IEEE 802.15.4 based networks. Our experiments using 6 USRP devices and also simulation results using GNU Radio simulator demonstrate that RnR can successfully decode packet in 95% cases of collisions, and improves the correctly packet decoding rate of up to 97.5% compared to standard decoders in case of collisions, providing 4x higher throughput compared to the state-of-the-art collision recovery mechanisms. The results demonstrate RnR as a practical choice for collision recovery in WSNs.

CHAPTER 5 FUTURE WORK

With several competing LPWAN technologies supporting various requirements for different IoT applications, there are still many limitations and challenges that need to be addressed. In this chapter, we are particularly interested in future research to address handling burst transmission over LPWAN and localization in mobile LPWAN.

5.1 Handling Burst Transmission over LPWAN

LPWAN design suffers from two key drawbacks relating to burst/bulk data transmission. First, to achieve low-power operations, LPWANs are designed to support low data rate communication. Such design limits the adoption of LPWAN in several IoT applications that require high data rates (e.g., volcano monitoring, infrastructural health monitoring, and video monitoring) [102, 152, 125]. Second, to the best of our knowledge, the MAC layer design of LPWANs is unresponsive to the changes in link/channel quality, resulting in degradation in the overall network performance.

To enable burst communication over LPWAN, we will design an energy-efficient approach that combines data compression and dynamic transmission parameter selection. We will exploit LoRa capabilities by adjusting its transmission parameter (spreading factor, coding rate, TX power) to ensure reliable and energy-efficient communication.

5.2 Localization in Mobile LPWAN

Localization has been widely studied in the context of cellular networks [72, 122], Wi-Fi networks [71, 131, 140], and Bluetooth [13, 63, 73]. Outdoor localization relies on GPS to provide meter-level accuracy. Using GPS is energy-consuming as LPWAN devices are powered by constraint and unreliable sources (e.g., small batteries, energy harvesters). In LPWAN, the expected

battery life of a device is around 10 years [102]. Thus, relying on GPS is not practical in LPWAN.

As already studied in [50, 26, 41, 75], RSSI-based, fingerprinting, and TDoA-based localization approaches are not practical for LPWAN localization. These approaches suffer from several issues including strong signal attenuation, high energy consumption, and high localization errors.

Recent work on LoRa localization [11] achieved meter-level localization accuracy by utilizing the TV white spaces spectrum to emulate a wider band necessary for accurate localization. However, their approach is limited to stationary LoRa nodes and considers the presence of line-of-sight between the nodes and the gateways. In the future, we will investigate new approaches to enable practical localization in LPWANs

CHAPTER 6 CONCLUSION

With the increasing number of connected devices and the variety of applications supported by the Internet-of-Things (IoT), efficient and reliable communication technologies are needed. Low-Power Wide-Area Network (LPWAN) offers long-range and low-power connectivity for a large number of devices at a low cost to realize the IoT vision. In this dissertation, we have proposed to enable applications that involve mobility in LPWAN.

To enable mobility in LPWAN, we have proposed an efficient approach to handle mobility in Sensor Network Over White spaces (SNOW), a highly scalable LPWAN operating over TV white spaces. We proposed a dynamic Carrier Frequency Offset (CFO) estimation and compensation technique that considers the Doppler shift impact. Along with a fast and energy-efficient Base Station (BS) discovery approach, we presented a novel subcarrier alignment technique that combines time and frequency domain energy-sensing. We have implemented our approach in USRP and Texas Instruments (TI) CC1310 devices. Our experimental results in two deployments (indoor and outdoor) show that our approach is reliable, energy-efficient, and time-efficient.

We presented RnR, a collision detection and recovery technique designed for Wireless Sensor Network (WSN) and adaptable in LPWANs.

Finally, we discussed the future research directions, which include handling burst transmission over LPWAN and enabling localization in mobile LPWAN.

REFERENCES

[1] I. 802.15.4, 2018. http://standards.ieee.org/about/get/802/802.15.html.

[2] N. Abramson. The aloha system: another alternative for computer communications. In *Proceedings of the November 17-19, 1970, fall joint computer conference*, pages 281–285. ACM, 1970.

[3] D. Acharjya and M. K. Geetha. Internet of things: Novel advances and envisioned applications, 2017.

[4] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne. Understanding the limits of loRaWAN. *IEEE Communications Magazine*, January 2017.

[5] M. Ali, T. Suleman, and Z. A. Uzmi. Mmac: A mobility-adaptive, collision-free mac protocol for wireless sensor networks. In *Performance, Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International*, pages 401–407. IEEE, 2005.

[6] https://amsterdamsmartcity.com.

[7] Atmel. http://www.atmel.com/images/doc8111.pdf.

[8] Att. https://m2x.att.com/iot/industry-solutions/iot-data/agriculture/.

[9] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley. A study of lora: Long range and amp; low power networks for the internet of things. *Sensors*, 16(9), 2016.

[10] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh. White space networking with wi-fi like connectivity. *ACM SIGCOMM Computer Communication Review*, 39(4):27–38, 2009.

[11] A. Bansal, A. Gadre, V. Singh, A. Rowe, B. Iannucci, and S. Kumar. Owll: Accurate lora localization using the tv whitespaces. In *Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)*, pages 148–162, 2021.

[12] J. P. Bardyn, T. Melly, O. Seller, and N. Sornin. Iot: The era of lpwan is starting now. In *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, pages 25–30, 2016.

[13] M. S. Bargh and R. de Groote. Indoor localization based on response rate of bluetooth inquiries. In *Proceedings of the First ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments*, MELT '08, pages 49–54, 2008.

[14] K. Bian and J. M. Park. Asynchronous channel hopping for establishing rendezvous in cognitive radio networks. In *2011 Proceedings IEEE INFOCOM*, pages 236–240, 2011.

[15] G. Bianchi, L. Fratta, and M. Oliveri. Performance evaluation and enhancement of the CSMA/CA MAC protocol for 802.11 wireless LANs. In *PIMRC*, 1996.

[16] Bluetooth, 2018. http://www.bluetooth.com.

[17] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso. Do LoRa low-power wide-area networks scale? In *Proceedings of the 19th ACM Intl. Conf. on Modeling, Analysis and Simulation of Wireless and Mobile Syst.*, pages 59–67, 2016.

[18] E. H. Callaway Jr. *Wireless sensor networks: architectures and protocols*. CRC press, 2003.

[19] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communication and Mobile Computing*, 2:483–502, 2002.

[20] P. Castoldi. *Multiuser detection in CDMA mobile terminals*. Artech House, 2002.

[21] M. Cattani, C. A. Boano, and K. Romer. An experimental evaluation of the reliability of lora long-range low-power wireless communication. *Journal of Sensor and Actuator Networks*, 6(2), 2017.

[22] Ti CC1310. http://www.ti.com/product/CC1310.

[23] Texas instruments. http://www.ti.com/product/cc2420.

[24] C.-T. Chen. *System and Signal Analysis*. Thomson, 1988.

[25] X. Chen and J. Huang. Game theoretic analysis of distributed spectrum sharing with database. In *Proceedings of the 2012 IEEE 32Nd International Conference on Distributed Computing Systems*, ICDCS '12, pages 255–264, 2012.

[26] W. Choi, Y.-S. Chang, Y. Jung, and J. Song. Low-power lora signal-based outdoor positioning using fingerprint algorithm. *ISPRS International Journal of Geo-Information*, 7(11):440, 2018.

[27] Climate. https://www.climate.com.

[28] Smart and connected communities framework. https://www.nitrd.gov/sccc/.

[29] C. Cormio and K. R. Chowdhury. A survey on mac protocols for cognitive radio networks. *Ad Hoc Networks*, 7(7):1315–1329, sep 2009.

[30] C. Cormio and K. R. Chowdhury. An adaptive multiple rendezvous control channel for cognitive radio wireless ad hoc networks. In *2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pages 346–351, 2010.

[31] L. Da Xu, W. He, and S. Li. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics*, 10(4):2233–2243, 2014.

[32] DASH7. http://www.dash7-alliance.org.

[33] E. De Poorter, J. Hoebeke, M. Strobbe, I. Moerman, S. Latré, M. Weyn, B. Lannoo, and J. Famaey. Sub-ghz lpwan network coexistence, management and virtualization: an overview and open research challenges. *Wireless Personal Communications*, 95(1):187–213, 2017.

[34] E. De Poorter, J. Hoebeke, M. Strobbe, I. Moerman, S. Latr, M. Weyn, B. Lannoo, and J. Famaey. Sub-ghz lpwan network coexistence, management and virtualization: An overview and open research challenges. *Wirel. Pers. Commun.*, 95(1):187–213, July 2017.

[35] A. D. Domenico, E. C. Strinati, and M. G. D. Benedetto. A survey on mac strategies for cognitive radio networks. *IEEE Communications Surveys Tutorials*, 14(1):21–44, 2012.

[36] Q. Dong and W. Dargie. A survey on mobility and mobility-aware mac protocols in wireless sensor networks. *IEEE communications surveys and tutorials*, 15(1):88–100, 2013.

[37] P. Dutta and D. Culler. Practical asynchronous neighbor discovery and rendezvous for mobile sensing applications. In *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems*, SenSys '08, 2008.

[38] E. Ekici, Y. Gu, and D. Bozdag. Mobility-based communication in wireless sensor networks. *IEEE Communications Magazine*, 44(7):56–62, 2006.

[39] N. Ekiz, T. Salih, S. Kuukoner, and K. Fidanboylu. An overview of handoff techniques in cellular networks. *International Journal of Information Technology*, 2, 2007.

[40] Ericsson, 2016. https://www.ericsson.com/assets/local/publications/white-papers/wp_iot.pdf.

[41] B. C. Fargas and M. N. Petersen. Gps-free geolocation using lora in low-power wans. In *2017 Global Internet of Things Summit (GIoTS)*, pages 1–6, 2017.

[42] FarmBeats: IoT for agriculture, 2015. https://www.microsoft.com/en-us/research/project/farmbeats-iot-agriculture/.

[43] D. Floreano and R. J. Wood. Science, technology and the future of small autonomous drones. *Nature*, 521(7553):460–466, 2015.

[44] M. Garetto, T. Salonidis, and E. W. Knightly. Modeling per-flow throughput and capturing starvation in csma multi-hop wireless networks. *IEEE/ACM TON*, 16:864–877, 2008.

[45] O. Georgiou and U. Raza. Low power wide area network analysis: Can lora scale? *IEEE Wireless Communications Letters*, 6(2):162–165, 2017.

[46] GNU Radio. http://gnuradio.org.

[47] S. Gollakota and D. Katabi. Zigzag decoding: Combating hidden terminals in wireless networks. In *Proceedings of the ACM SIGCOMM 2008 conference on Data communication*, pages 159–170, 2008.

[48] S. Gollakota, S. D. Perli, and D. Katabi. Interference alignment and cancellation. In *Proceedings of the ACM SIGCOMM 2009 conference on Data communication*, pages 159–170, 2009.

[49] gsma. https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf.

[50] C. Gu, L. Jiang, and R. Tan. Lora-based localization: Opportunities and challenges. *CoRR*, abs/1812.11481, 2018.

[51] D. Halperin, T. Anderson, and D. Wetherall. Taking the sting out of carrier sense: interference cancellation for wireless LANs. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 339–350, 2008.

[52] J. Harri, F. Filali, and C. Bonnet. Mobility models for vehicular ad hoc networks: a survey and taxonomy. *IEEE Communications Surveys and Tutorials*, 11(4):19–41, 2009.

[53] IEEE 802.11, 2018. http://www.ieee802.org/11.

[54] IEEE 802.11 standards. http://standards.ieee.org/about/get/802/802.11.html.

[55] IEEE 802.15 standards. http://standards.ieee.org/about/get/802/802.15.html.

[56] GNU Radio IEEE 802.15.4 implementation.

[57] Ingenu. https://www.ingenu.com/technology/rpma.

[58] IQRF. http://www.iqrf.org/technology.

[59] Iscoop. https://www.i-scoop.eu/internet-of-things-guide/iot-network-lora-lorawan/.

[60] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak. The internet of things for health care: a comprehensive survey. *IEEE Access*, 3:678–708, 2015.

[61] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha. Practical, real-time, full duplex wireless. In *Proceedings of the 17th annual international conference on Mobile computing and networking*, pages 301–312, 2011.

[62] A. Jhumka and S. Kulkarni. On the design of mobility-tolerant tdma-based media access control (mac) protocol for mobile sensor networks. In *International Conference on Distributed Computing and Internet Technology*, pages 42–53. Springer, 2007.

[63] K. Kalliola, K. Doppler, H. Kauppinen, J. Jantunen, J. Ollikainen, T. Lehtiniemi, A. Kainulainen, and J. Juntunen. System and methods for direction finding using a handheld device, aug 2007. US Patent App. 11/357,165.

[64] S. Katti, S. Gollakota, and D. Katabi. Embracing wireless interference: Analog network coding. In *ACM SIGCOMM Computer Communication Review*, pages 397–408. ACM New York, NY, USA, 2007.

[65] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft. Xors in the air: Practical wireless network coding. In *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 243–254, 2006.

[66] S. Khurana, A. Kahol, and A. P. Jayasumana. Effect of hidden terminals on the performance of IEEE 802.11 MAC protocol. In *LCN*, 1998.

[67] J. H. Kim and J. K. Lee. Capture effects of wireless CSMA/CA protocols in rayleigh and shadow fading channels. *IEEE Trans. Vehicular Technology*, 48(4):1277–1286, 1999.

[68] S. M. Kim and T. He. Freebee: Cross-technology communication via free side-channel. In *MobiCom*. ACM, 2015.

[69] L. Kong and X. Liu. mzig: Enabling multi-packet reception in zigbee. In *Proceedings of the 21st annual international conference on mobile computing and networking*, pages 552–565, 2015.

[70] L. Krupka, L. Vojtech, and M. Neruda. The issue of lpwan technology coexistence in IoT environment. In *2016 17th International Conference on Mechatronics - Mechatronika (ME)*, pages 1–8, 2016.

[71] S. Kumar, S. Gil, D. Katabi, and D. Rus. Accurate indoor localization with zero start-up cost. In *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking*, MobiCom '14, pages 483–494, 2014.

[72] S. Kumar, E. Hamed, D. Katabi, and L. Erran Li. Lte radio analytics made easy and accessible. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, pages 211–222, 2014.

[73] P. Lazik, N. Rajagopal, O. Shih, B. Sinopoli, and A. Rowe. Alps: A bluetooth and ultrasound platform for mapping and localization. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, SenSys '15, pages 73–84, 2015.

[74] https://www.link-labs.com.

[75] Link labs localization. https://www.link-labs.com/blog/lora-localization.

[76] J. Lloret, M. Garcia-Pineda, D. Bri, and S. Sendra. A wireless sensor network deployment for rural and forest fire detection and verification. *Sensors (Basel, Switzerland)*, 9:8722–47, 11 2009.

[77] LoRaWAN. https://www.lora-alliance.org.

[78] LTE Advanced Pro, 2017. https://www.qualcomm.com/invention/technologies/lte/advanced-pro.

[79] Lte-cat-m1. https://www.u-blox.com/en/lte-cat-m1.

[80] J. Lu and K. Whitehouse. Exploiting the capture effect for low-latency flooding in wireless sensor networks. In *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pages 409–410, 2008.

[81] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark. Connected vehicles: Solutions and challenges. *IEEE Internet of Things Journal*, 1(4):289–299, 2014.

[82] G. Mao, B. Fidan, and B. D. O. Anderson. Wireless sensor network localization techniques. *Computer networks*, 51(10):2529–2553, 2007.

[83] P. Marcelis, V. S. Rao, and R. V. Prasad. DaRe: Data recovery through application layer coding for loRaWANs. *IoTDI '17*, 2017.

[84] Monsanto. https://www.rcrwireless.com/20151111/internet-of-things/agricultural-internet-of-things-promises-to-reshape-farming-tag15.

[85] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl. Senseless: A database-driven white spaces network. In *DySpan '11*. IEEE, 2011.

[86] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl. Senseless: A database-driven white spaces network. *IEEE Transactions on Mobile Computing*, 11(2):189–203, 2012.

[87] M. Nabi, M. Blagojevic, M. Geilen, T. Basten, and T. Hendriks. Mcmac: An optimized medium access control protocol for mobile clusters in wireless sensor networks. In *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*, pages 1–9. IEEE, 2010.

[88] NBIoT, 2017. http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete.

[89] M. D. Nellis, K. Lulla, and J. John. Interfacing geographic information systems and remote sensing for rural land use analysis. *Photogrammetric Engineering and Remote Sensing (ISSN 0099-1112)*, 56:329–331, 1990.

[90] ngmn, 2018. http://www.ngmn.org.

[91] T. Nuortio, J. Kytöjoki, H. Niska, and O. Bräysy. Improved route planning and scheduling of waste collection and transport. *Expert systems with applications*, 30(2):223–232, 2006.

[92] Oil field. http://petrocloud.com/solutions/oilfield-monitoring/.

[93] F. F. Order, 2008. FCC, ET Docket No FCC 08-260, November 2008.

[94] F. S. Order, 2010. FCC, Second Memorandum Opinion and Order, ET Docket No FCC 10-174, September 2010.

[95] D. Patel and M. Won. Experimental study on low power wide area networks (LPWAN) for mobile internet of things. In *2017 IEEE 85th Vehicular Technology Conference (VTC'17 Spring)*, 2017.

[96] P. Patel and J. Holtzman. Analysis of a simple successive interference cancellation scheme in a DS/CDMA system. *Selected Areas in Communications, IEEE Journal on*, 12:796–807, 1994.

[97] J. PetArvi, K. Mikhaylov, M. Pettissalo, J. Janhunen, and J. Iinatti. Performance of a low-power wide-area network based on lora technology: Doppler robustness, scalability, and coverage. *International Journal of Distributed Sensor Networks*, 13(3):1550147717699412, 2017.

[98] H. Pham and S. Jha. An adaptive mobility-aware mac protocol for sensor networks (ms-mac). In *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on*, pages 558–560. IEEE, 2004.

[99] http://hit.psy.unipd.it/padova-smart-city.

[100] R. Prasad and F. J. Velez. Ofdma wimax physical layer. In *WiMAX networks*, pages 63–135. Springer, 2010.

[101] M. Rahman, D. Ismail, V. P. Modekurthy, and A. Saifullah. Implementation of lpwan over white spaces for practical deployment. In *Proceedings of the International Conference on Internet of Things Design and Implementation (IoTDI '19)*, pages 178–189, 2019.

[102] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low power wide area networks: An overview. *IEEE Communications Surveys Tutorials*, 19(2):855–873, 2017.

[103] E. Research, 2017. http://www.ettus.com/product/details/UB210-KIT.

[104] RPMA - a technical drill-down into ingenu's LPWAN technology. https://www.leverege.com/blogpost/rpma-technical-drill-down-ingenus-lpwan-technology.

[105] A. Saeed, K. A. Harras, E. Zegura, and M. Ammar. Local and low-cost white space detection. In *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*, pages 503–516. IEEE, 2017.

[106] A. Saifullah, M. Rahman, D. Ismail, C. Lu, R. Chandra, and J. Liu. SNOW: Sensor network over white spaces. In *SenSys '16 (Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems)*, pages 272–285. ACM, 2016.

[107] A. Saifullah, M. Rahman, D. Ismail, C. Lu, J. Liu, and R. Chandra. Enabling reliable, asynchronous, and bidirectional communication in sensor networks over white spaces. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, pages 1–14, 2017.

[108] A. Saifullah, M. Rahman, D. Ismail, C. Lu, J. Liu, and R. Chandra. Low-power wide-area networks over white spaces. *ACM/IEEE Transactions on Networking*, 26(4):1893–1906, 2018.

[109] A. Saifullah, S. Sankar, J. Liu, C. Lu, R. Chandra, and B. Priyantha. Capnet: A real-time wireless management network for data center power capping. In *2014 IEEE Real-Time Systems Symposium*, pages 334–345. IEEE, 2014.

[110] LoRa modem design guide. http://www.semtech.com/images/datasheet/LoraDesignGuide_STD.pdf.

[111] S. Sen, R. R. Choudhury, and S. Nelakuditi. CSMA/CN: carrier sense multiple access with collision notification. *IEEE/ACM TON*, 20:544–556, 2012.

[112] S. Sen, N. Santhapuri, R. R. Choudhury, and S. Nelakuditi. Successive interference cancellation: Carving out mac layer opportunities. *IEEE Trans. Mobile Computing*, 12:346–357, 2013.

[113] Z. Shelby and C. Bormann. *A: IPv6 Ref.* John Wiley and Sons, 2009.

[114] J. Shin, D. Yang, and C. Kim. A channel rendezvous scheme for cognitive radio networks. *IEEE Communications Letters*, 14(10):954–956, 2010.

[115] SIGFOX. http://sigfox.com.

[116] A. Sikora and V. F. Groza. Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band. In *2005 IEEE Instrumentationand Measurement Technology Conference Proceedings*, volume 3, pages 1786–1791, 2005.

[117] Smart city. https://transmitter.ieee.org/smart-connected-communities/.

[118] Snow implementation. https://github.com/snowlab12/gr-snow.

[119] Y. Song and J. Xie. Prospect: A proactive spectrum handoff framework for cognitive radio ad hoc networks without common control channel. *IEEE Transactions on Mobile Computing*, 11(7):1127–1139, 2012.

[120] E. Sourour, H. El-Ghoroury, and D. McNeill. Frequency offset estimation and correction in the ieee 802.11 a wlan. In *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, volume 7, pages 4923–4927. IEEE, 2004.

[121] L. Standard. The LTE standard, 2014. https://www.qualcomm.com/media/documents/files/the-lte-standard.pdf.

[122] G. Sun, J. Chen, W. Guo, and K. J. R. Liu. Signal processing techniques in network-aided positioning: a survey of state-of-the-art positioning designs. *IEEE Signal Processing Magazine*, 22(4):12–23, 2005.

[123] Telensa, 2017. https://www.telensa.com.

[124] TinyOS. http://www.tinyos.net.

[125] I. Tomić, L. Bhatia, M. J. Breza, and J. A. McCann. The limits of lorawan in event-triggered wireless networked control systems. In *2018 UKACC 12th International Conference on Control (CONTROL)*, pages 101–106. IEEE, 2018.

[126] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[127] U-blox. https://www.u-blox.com/en/narrowband-iot-nb-iot.

[128] USDA, 2007. http://www.nrcs.usda.gov/Internet/FSE_DOCUMENTS/stelprdb1043474.pdf.

[129] D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra, S. Sinha, A. Kapoor, M. Sudarshan, and S. Stratman. Farmbeats: An iot platform for data-driven agriculture. In *14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17)*, pages 515–529, 2017.

[130] D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra, S. Sinha, A. Kapoor, M. Sudarshan, and S. Stratman. Farmbeats: An iot platform for data-driven agriculture. In *14th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 17)*, pages 515–529, 2017.

[131] D. Vasisht, S. Kumar, and D. Katabi. Decimeter-level localization with a single wifi access point. In *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, NSDI'16, pages 165–178, 2016.

[132] N. Vatcharatiansakul, P. Tuwanut, and C. Pornavalai. Experimental performance evaluation of LoRaWAN: A case study in Bangkok. In *2017 14th International Joint Conference on Computer Sc. and Software Engg. (JCSSE)*, pages 1–4, 2017.

[133] A. J. Viterbi. *CDMA: principles of spread spectrum communication*. Addison Wesley Longman Publishing Co., Inc., 1995.

[134] T. Voigt, M. Bor, U. Roedig, and J. Alonso. Mitigating inter-network interference in lora networks. In *Proceedings of the 2017 International Conference on Embedded Wireless Systems and Networks*, EWSN '17, pages 323–328, 2017.

[135] WeightLess. http://www.weightless.org.

[136] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, and Y. Tabakov. Dash7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication. In *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 54–59. IEEE, 2015.

[137] K. Whitehouse, A. Woo, F. Jiang, J. Polastre, and D. Culler. Exploiting the capture effect for collision detection and recovery. In *The Second IEEE Workshop on Embedded Networked Sensors, 2005. EmNetS-II.*, pages 45–52. IEEE, 2005.

[138] WiMAX, 2018. http://wimaxforum.org.

[139] WirelessHart. http://www.hartcomm2.org.

[140] J. Xiong and K. Jamieson. Arraytrack: A fine-grained indoor location system. In *Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation*, NSDI '13, pages 71–84, 2013.

[141] X. Xiong, K. Zheng, R. Xu, W. Xiang, and P. Chatzimisios. Low power wide area machine-to-machine networks: key techniques and prototype. *IEEE Communications Magazine*, 53(9):64–71, 2015.

[142] K. Xu, M. Gerla, and S. Bae. Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. *Ad Hoc Networks*, 1:107–123, 2003.

[143] D. Yang, Y. Xu, and M. Gidlund. Coexistence of ieee802.15.4 based networks: A survey. In *IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society*, pages 2107–2113, 2010.

[144] D. Yang, Y. Xu, and M. Gidlund. Wireless coexistence between ieee 802.11- and ieee 802.15.4-based networks: A survey. *International Journal of Distributed Sensor Networks*, 7(1):912152, 2011.

[145] W. Ye, J. Heidemann, and D. Estrin. An energy-efficient mac protocol for wireless sensor networks. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1567–1576. IEEE, 2002.

[146] B. Yin and J. R. Cavallaro. LTE uplink MIMO receiver with low complexity interference cancellation. *Analog Integr Circ Sig Process*, 73:5443 – 450, 2012.

[147] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE IoT journal*, 1(1):22–32, 2014.

[148] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32, 2014.

[149] M. Zareei, A. K. M. Muzahidul Islam, N. Mansoor, S. Baharun, E. M. Mohamed, and S. Sampei. Cmcs: a cross-layer mobility-aware mac protocol for cognitive radio sensor

networks. *EURASIP Journal on Wireless Communications and Networking*, 2016(1):1–15, 2016.

[150] Y. Zhang, G. Yu, Q. Li, H. Wang, X. Zhu, and B. Wang. Channel-hopping-based communication rendezvous in cognitive radio networks. *IEEE/ACM Transactions on networking*, 22(3):889–902, 2013.

[151] Zigbee alliance. http://www.zigbee.org.

[152] D. Zorbas, K. Q. Abdelfadeel, V. Cionca, D. Pesch, and B. OFlynn. Offline scheduling algorithms for time-slotted lora-based bulk data transmission. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 949–954. IEEE, 2019.

ABSTRACT

VERSATILITY OF LOW-POWER WIDE-AREA NETWORK APPLICATIONS

by

DALI ISMAIL

August 2021

Advisor: Dr. Abusayeed Saifullah

Co-Advisor: Dr. Sanjay Madria

Major: Computer Science

Degree: Doctor of Philosophy

Low-Power Wide-Area Network (LPWAN) is regarded as the leading communication technology for wide-area Internet-of-Things (IoT) applications. It offers low-power, long-range, and low-cost communication. With different communication requirements for varying IoT applications, many competing LPWAN technologies operating in both licensed (e.g., NB-IoT, LTE-M, and 5G) and unlicensed (e.g., LoRa and SigFox) bands have emerged. LPWANs are designed to support applications with low-power and low data rate operations. They are not well-designed to host applications that involve high mobility, high traffic, or real-time communication (e.g., volcano monitoring and control applications). With the increasing number of mobile devices in many IoT domains (e.g., agricultural IoT and smart city), mobility support is not well-addressed in LPWAN. Cellular-based/licensed LPWAN relies on the wired infrastructure to enable mobility. On the other hand, most unlicensed LPWANs operate on the crowded ISM band or are required to duty cycle,

making handling mobility a challenge.

In this dissertation, we first identify the key opportunities of LPWAN, highlight the challenges, and show potential directions for future research. We then enable the versatility of LPWAN applications first by enabling applications involving mobility over LPWAN. Specifically, we propose to handle mobility in LPWAN over white space considering Sensor Network Over White Space (SNOW). SNOW is a highly scalable and energy-efficient LPWAN operating over the TV white spaces. TV white spaces are the allocated but locally unused available TV channels (54 - 698 MHz in the US). We proposed a dynamic Carrier Frequency Offset (CFO) estimation and compensation technique that considers the impact of the Doppler shift due to mobility. Also, we design energy-efficient and fast BS discovery and association approaches. Finally, we demonstrate the feasibility of our approach through experiments in different deployments.

Finally, we present a collision detection and recovery technique called RnR (Reverse & Replace Decoding) that applies to LPWANs. Additionally, we discuss future work to enable handling burst transmission over LPWAN and localization in mobile LPWAN.

AUTOBIOGRAPHICAL STATEMENT

Dali Ismail is a Ph.D. candidate in the Department of Computer Science at Wayne State University under the supervision of Dr. Abusayeed Saifullah. He received his MS in Computer Science and Engineering at Washington University in St. Louis. His research concerns Internet-of-Things, mobile and wireless networks, and embedded and real-time systems. He published papers in leading conferences and journals including ACM SenSys, ACM IoTDI, ACM EWSN, ACM/IEEE Transaction on Networking, and ACM TECS. He served as a TPC member of ACM/IEEE IoTDI poster/demo track and as a reviewer for several conferences and journals including IEEE INFOCOM, ACM SenSys, ACM EWSN, IEEE RTSS, ACM/IEEE IoTDI, IEEE/ACM TON, and ACM TOSN.