TRANSMISSION TIMING MODULATION FOR INFORMATION CODING IN ENERGY-CONSTRAINED WIRELESS NETWORKS

By

Dezhi Feng

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Electrical Engineering—Doctor of Philosophy

2020

ABSTRACT

TRANSMISSION TIMING MODULATION FOR INFORMATION CODING IN ENERGY-CONSTRAINED WIRELESS NETWORKS

By

Dezhi Feng

The objective of this thesis is to develop a framework of transmission timing-based modulation framework for improving energy efficiency, security, and information transfer capacity in embedded wireless networks with very thin energy budgets. The key idea is to modulate both intra-PDU (Protocol Data Unit) and inter-PDU timing for addressing energy, security, and information transfer capacity in wireless embedded networks. As for energy efficiency, we developed a novel pulse position-coded PDU (PPCP) paradigm. The core idea is to encode a protocol data unit (PDU) in terms of the silence duration between two sets of delimiter pulses, whose positions are modulated based on the value of the PDU. This PPCP architecture achieves significant energy savings by using a lesser amount of bit/pulse transmissions, and by eliminating long multi-bit preambles and headers, which are normally used in traditional packets. The proposed multi-access pulse-based PDU scheme enables medium sharing among many sensor nodes without requiring per-PDU frame synchronization. As for security, we developed the concept of a novel chaotic pulse position coded protocol data unit (CPPCP) for secure embedded networking. The core idea of CPPCP is to encode a protocol data unit (PDU) with a wideband pulse train with chaotically-varied inter-pulse intervals. The architecture ensures communication security by introducing randomness between data symbols, noise-like frequency spectrum, and significant energy savings by using a smaller number of pulse transmissions compared to existing secure coding schemes such as Bluetooth Low Energy (BLE). Compared with the traditional key-based cryptographic techniques, CPPCP suppresses decipherable information by eliminating

symbol periodicity. The mechanism can also be piggy-backed on traditional cryptography solutions to achieve higher levels of security. Finally, for enhancing the information transfer capacity, we developed a data packet position modulation (DPPM) paradigm. Packet transmissions in low duty cycle networks are often scheduled as TDMA slots, whose periodicity is determined based on application sampling requirements and the energy in-flow, often in the form of energy harvesting. The key idea of DPPM is to modulate the inter-packet spacing for coding additional information without incurring additional transmission energy expenditures. We first developed a have a DPPM based networking solution for single-hop transmit-only networks in which a number of low-energy nodes transmit data to an aggregator. The architecture is developed for a two-node point-to-point link, followed by a multipoint-to-point multi-access network. Detailed analytical and simulation models are developed to demonstrate the performance of a symmetric and an asymmetric version of DPPM.

Dedicated to my Mother and Father.
Thanks for all your patience, love and inspiration.

ACKNOWLEDGEMENTS

I would like to acknowledge all the members of my committee for their contributions to the development and writing of my dissertation: Dr. Subir Biswas, Dr. Wen Li, Dr. Jian Ren, and Dr. Richard Enbody. I would like to show my gratitude to everyone for your support, knowledge, and expertise.

First and foremost, I would like to recognize my committee chair and my supervisor, Dr. Subir Biswas, who has my deepest appreciation. You have been persistently caring, supportive, encouraging, and patient. I really appreciate your expertise and generous guidance, which assisted me to achieve every single step of my professional and personal growth through this journey. I view you as my advisor not only in my doctoral training, but also through my entire life. Most importantly, you demonstrated to me what a professional researcher, educator, and good advisor is. You showed me how to be a successful scientist in life.

Thanks must be given to my lab mates Bo Dong, Qiong Huo, Faezeh Hajiaghajani, Yan Shi, Saptarshi, Tianyi Wu, Henry Griffith, Rui, and Brandon Harrington for all the brainstorming and implementation discussions, and for all your input and contributions. I would also like to give thanks to my friends Dennis LeBlanc, Althea LeBlanc, Ronald Fritz, Yanfen Zhai, Tina Qin, Yu Cheng, Tina Qin and Kelly Bartlett for your support, help and your continual friendships with me in life. It would not have been possible to stand where I am now without them.

I am forever grateful to my family, give thanks to my beloved wife, Boyang Tong, my son, Junhao (Leo) Feng, and my daughter Halia Feng, for their unconditional love and support. Special thanks to my grandmother, Yawen Dong and Yajing Wang and my grandfather, Shiming Han and Chang Feng, for raising me up with your endless and selfless love. I also want to say thanks to my

lovely mom, Suyan Han, and my dad, Zhenming Feng, for your unconditional love and encouragement throughout my life. Thanks for your hard work, your insights, and your support for providing me all kinds of opportunities to expand my horizon with new experiences in education and in my life. Thanks for giving me the freedom to explore and reach my goals, but at the same time always back me up when my steps faltered. Your kindness, integrity, and perseverance have shaped my character and have made me who I am. I would also like to thank my parents-in-law, Aiguo Tong and Shuqin Xu, for supporting me in my career and my life. Thanks for entrusting me to marry their daughter.

Finally, I want to thank all the people love me and the people I love in my life, for the things you have taught me, which have motivated me to always be the best of myself. This project would not have been possible without yours.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1. Motivation

Wireless Sensor Networks (WSN) are an important component in the emerging Internet of Things (IoT) ecosystem. WSNs also instituted a rich domain of active research involving hardware and system design, networking, distributed algorithms, data management, security, and social factors. A sensor network consists of numerous sensor nodes (SNs) with integrated capabilities such as data sensing, data gathering, data processing, and limited storage space.

Often, the goal of a sensor network is to collect the data from the environment and to deliver the sensing data to a Base Station (BS). The resources of sensor nodes in WSNs are limited in terms of energy, computational capability, communication range, and memory storage. The improvement of information transfer capacity under the constraint of limited energy is an important research topic in the study of WSNs. The SNs operate on battery power or harvested energy and are often deployed in rough environments. Due to the environmental constraints, it is usually cost-prohibitive or even impossible to replace depleted batteries. Furthermore, the data obtained from the sensors must be transmitted to the target in a secure manner. Wireless sensor networks have many attack types (Sybil, Wormhole, Sinkhole, etc.) that threaten data flow. Therefore, energy efficiency, security, and information transfer capacity enhancement are critical design goals to improve the performance of a WSN.

Research concerning energy efficiency, security, and information transfer capacity has attracted considerable attention from researchers during the past few years [1, 2, 3, 4]. The literature related to WSNs recognizes that the radio communication component of a sensor node is the most energy consuming part of a node [5]. Various energy-aware protocols are proposed at

various communication protocol layers. However, the application of these protocols leads to the high complexity of implementation and energy costs that are unaffordable for sensor nodes powered by batteries or energy harvesting system. The research about WSNs is still far from fully-fledged in both theory and application. More specifically, there are many open issues in developing better energy efficient, secure and information transfer capacity enhanced WSN protocols.

Our research centers around three goals that attempt to improve the energy efficiency, security, and information capacity of WSNs, which we will subsequently highlight. The first goal is to design a new pulse-based link layer architecture that replaces traditional packets for energy-efficient sensor networking. The second goal is to develop a novel chaotic pulse position coded protocol data unit for secure networking with very thin energy budgets. The third goal is to develop a Data Packet Position Modulation (DPPM) mechanism to enhance information transfer capacity of ultra-low-bandwidth communication links used by energy-constrained sensors and IoTs.

1.2. Key Concept of Transmission Timing Modulation for information Coding

The core concept of the thesis is inspired by the concept of timing modulation in relation to neural coding and communication in the brain. The massive information-processing capacity of the brain requires it to be extremely energy efficient. Human brains evolved to be powerful in neural communication, computation, and cognition. Neurons in the brain are remarkable in their ability to realize the above operations [6]. Neurons achieve this by generating characteristic electrical pulses called action potential: voltage spikes that can travel down nerve fibers as shown in Figure 1.1. Sensory neurons change their activities by firing sequences of spikes in various temporal patterns, with the presence of external sensory stimuli, such as light, sound, taste, smell,

etc. It is known that information about the stimulus is encoded in the pattern of spikes and transmitted around the brain.

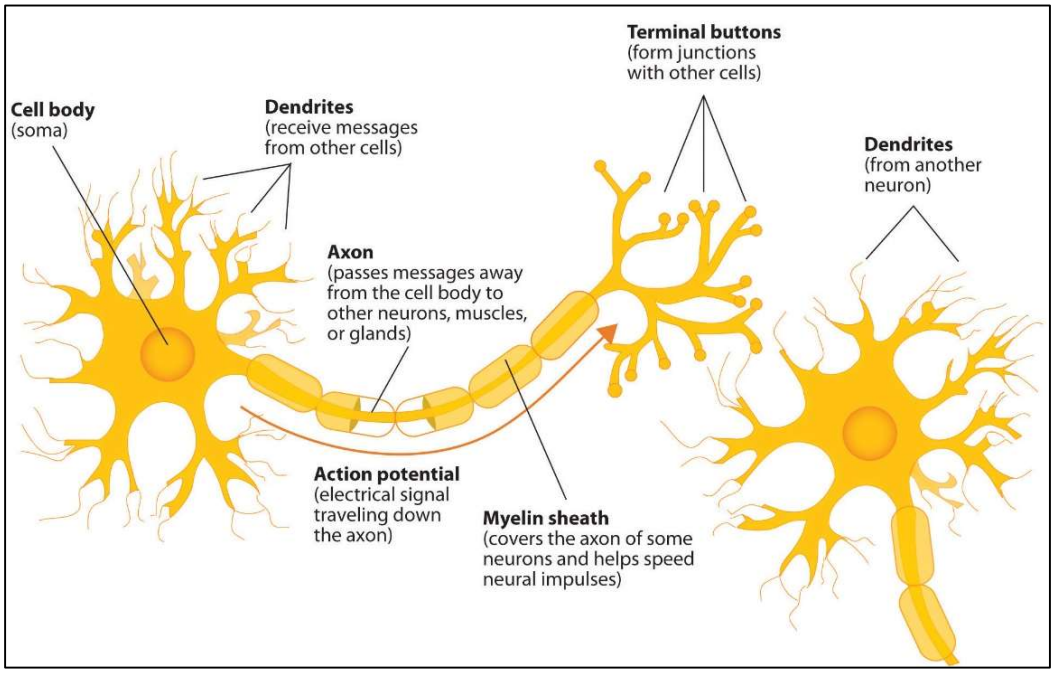


Figure 1.1: Neuron communication **[7]**

When precise spike timing or high-frequency firing-rate fluctuations are found to carry information, the neural code is often identified as a temporal code. Studies [8, 9] have found that the temporal resolution of the neural code is on a millisecond time scale, indicating that precise spike timing is a significant element in neural coding. Such codes, that communicate via the time between spikes, are referred to as inter-pulse interval codes.

The research in [10] demonstrated that there is a probability of firing rate, the neural communication based on the spatiotemporal coding leads to the fact the capacity to represent sensory information is maximized while energy expenditure is minimized. The studies conducted by the authors have linked the energy efficiency of spiking with the research on energy-efficiency and information transfer capacity of wireless sensor networking. Understanding the mechanisms

underlying the energy-efficient operation of neural coding in the brain can have wide implications for the design of the energy-efficient information coding in WSNs.

In this thesis, we aim to develop transmission timing-based modulation techniques for information coding to improve energy efficiency, security and information capacity in wireless sensor networking and Internet of Things (IoT) applications. The primary purpose is to leverage both the silence duration of the intra-protocol data unit (intra-PDU) and the silence duration of the inter-protocol data unit (inter-PDU) for data modulation. Inspired by the neural coding feature, we design transmission timing modulation-based architectures to offer a radically energy-lean link layer for data transmission in WSNs. The proposed architectures are then extended by combining the chaotically nonlinear function and inter-PDU modulation to further achieve security and capacity enhancement towards WSN and IoT applications.

1.3. Dissertation Objectives

1.3.1. Energy-Efficiency

The first objective of this thesis is to achieve energy-efficiency in WSNs. A new pulse-based link layer architecture is developed instead of traditional packets for wireless sensor networking and IoT applications with thin energy budget. In traditional packet transmission, the binary packet is transmitted with a synchronization preamble and packet header. Typical packet preamble size is few tens of bytes [11, 12, 13]. The transmission of such overheads can be prohibitively energy-inefficient, and that is irrespective of the employed modulation mechanisms. In this thesis, an energy-efficient communication model of pulse-based PDUs is proposed based on an inter-pulse silence-based data encoding and modulation mechanism, *Communication through Silence* (CtS), to achieve energy saving.

The primary design challenge stems from the fact that transmission time for a data value δ using CtS is $O(\delta)$ compared to $O(log_2\delta)$ for packets. This results in higher transmission delay and lower effective link capacity compared to packets. The second challenge is an intra-PDU idle listening at the receiver. After a receiver obtains the start delimiter pulse-set, its network interface needs to remain awake until the end delimiter pulse-set is received. Idle listening occurs during this period. This intra-PDU idle listening never happens for packets, thus posing a major architectural challenge for pulse-based PDUs. The third challenge is to transmit and receive a single pulse without synchronization overhead. Finally, all traditional packet-based abstractions such as error management, routing, reliable transport, compression, and security will need to be ported using pulse-based position modulation.

This thesis develops architectural solutions to a subset of the challenges mentioned above. The key idea is to encode a data value δ in pulse position modulation using multiple sets of delimiter pulses. Irrespective of the data value being sent, this new architecture requires fewer pulses compared to $O\big(log_2(\delta)\big)$ bits needed for packets in terms of base- β. Leveraging this feature, coupled with energy savings from not having to send per-PDU synchronization preambles and the packet header, our abstraction can offer a radically energy-lean link layer. When protocol syntaxes for managing idle listening are added, the proposed framework can offer a suitable networking technique for severely energy-starved networks.

1.3.2. Secure Communication

The security issues are yet to receive extensive focus for mission-critical application such as monitoring environmental pollutants, measuring traffic flows on roads, and tracking the location of personnel in a building. The major challenge for employing any efficient security scheme in

WSNs is posed by the size of sensors, consequently the limited energy, processing power, and the onboard memory.

Many key-based cryptography techniques with light-weight computational needs [14, 15, 16, 17, 18, 19] have been proposed in the literature for WSN security. Lately, an alternative to key-based schemes, namely, *chaos-based security*, is receiving significant attention due to its potentials for low-power communication privacy in industrial, human health monitoring, and military applications [20, 21, 22]. The main advantage of the chaotic secure communication systems is that they can generate a very complex set of chaotic signals, but be realized by very simple electronic circuits [23], which are especially suitable for WSNs. Compared with conventional pseudo-random-based cryptosystems which generate periodic signals, chaotic communication system eliminates the periodicity within the signal, thus providing better privacy and security in general.

The second objective of this thesis is to leverage chaotic security abstractions for energy-harvesting-based WSNs in the context of a pulse-based communication paradigm. A novel chaos-based communication scheme is proposed in the form of pulse trains where the inter-pulse intervals are determined by chaotic dynamics of a pulse generator. The multi-data symbols are used based on a new non-binary coding, which achieves higher randomness by increasing the overlapping area between the inter-pulse intervals for different data symbols in the time domain, as well as noise-like spectral characteristics in the frequency domain. Simultaneously, the proposed architecture demonstrates significant energy-saving by sending fewer pulses with a shorter transmission delay, which is better suited for thin energy-based IoT sensor networking applications.

1.3.3. Information Transfer Capacity Enhancements

The last objective of this thesis is to improve information transfer capacity by making the best use of the limited battery or harvested energy. Unlike prior coding methods for improving information transfer capacity, the proposed method and the corresponding MAC protocol in this thesis are differentiated in terms of zero extra energy consumption and without the need of additional complexity of the receiving circuit on sensor nodes. The mechanism can be implemented into application-specific low-power sensor networks and IoT systems for significant gains in the information transfer capacity, especially in sensor networks powered with slow energy-harvesting sources.

The major challenge towards capacity enhancement of WSNs is to improve the information transfer capacity and throughput under the limited energy. Another major challenge faced is the packet collision [24]. Due to the difficulty of synchronization and coordination between sensor nodes, there is a high probability of collision in a multi-access environment. A high collision rate will have a significant impact on the information transfer capacity of the system. It is therefore important to consider the chances of collision for maximizing the capacity.

Towards the above challenges, this thesis presents the study of a novel packet position modulation mechanism based on the modulation of inter-packet intervals for zero-energy data transmission in Tx-only sensor networks and IoT applications driven with thin energy budget. Taking advantage of the inter-packet spacing to encode additional data information in terms of the time interval between consecutive packets, such an architecture does not incur any extra energy expenses.

1.4. Pulse Position Coded PDUs (PPCP)

The first architecture proposed in this thesis is a new link layer architecture that uses *Pulse Position Coded Protocol Data Units* (*PPCP*s) instead of traditional packet *protocol data unit (PDU)* for energy-efficient wireless networking. The key idea is to send a data value δ using two pulses that are sent $\delta + 1$ time units apart (i.e., the one-time unit represents the value zero). Irrespective of the data value being sent, PPCP requires only two pulses, compared to $O\left(log_2(\delta)\right)$ bits needed for packets. This reduction, however, is achieved at the expense of a transmission delay of $\delta + 1$ pulse durations, which can be larger compared to the packet transmission delay of $O\left(log_2(\delta)\right)$ bit durations. The architecture employs mechanisms for reducing such transmission delay from $\delta + 1$ to $O(\beta log_\beta(\delta))$ by using a novel Flexible Base Digit Separation (FBDS) mechanism, which separately sends the digits of a base-β representation of the data value δ. The new pulse count is $O\left(log_\beta(\delta)\right)$, which can still be smaller than the packet bit-count $O\left(log_2(\delta)\right)$ for appropriately chosen β values.

First, our research team develops PPCP-based solutions for a Transmit-only (Tx-only) Network [2], in which low-energy sensors operate only in transmitter mode for sending data to access points. Through analytical modeling, simulation, and a prototype network implementation, we show the effectiveness of a PPCP Tx-only network in comparison with legacy packet-based networks. Building on the above work, we extend PPCP architecture to achieve collision-avoidance characteristics for the multi-access multi-hop networking. Specific contributions of PPCP architecture are as follows. First, a comprehensive link layer architecture is presented with detailed designs of PPCP-control PDUs and protocol components that are needed for multi-access operation. Second, experimental details and protocol performance are presented for a prototype

PPCP hardware platform powered by solar harvested energy. Using low-level operational parameters gleaned from the prototype deployment, a systematic simulation study is presented regarding the multi-access PPCP architecture's inherent ability to detect channel errors in terms of pulse loss, false positives, and collisions in realistic settings. Finally, we include a detailed energy consumption comparison of PPCP vs BLE (i.e., low energy Bluetooth as a comparable state-of-the-art low power protocol) when used in similar hardware and operational settings.

1.5. Chaotic Pulse Position Coded PDUs (CPPCP)

The concept of a novel chaotic pulse position coded protocol data unit (CPPCP) is developed for secure networking with very thin energy budgets. The core idea of CPPCP is to encode a protocol data unit (PDU) in terms of a wideband pulse train with chaotically-varied inter-pulse intervals. The architecture ensures communication security by introducing randomness between data symbols, noise-like frequency spectrum, and significant energy savings by using a smaller quantity of pulse transmissions compared to existing secure coding schemes such as Bluetooth Low Energy (BLE). Compared with the traditional key-based cryptographic techniques, CPPCP suppresses decipherable information by eliminating symbol periodicity. It can also be piggy-backed on top of traditional cryptography solutions to achieve higher levels of security. This thesis presents a detailed analysis of the CPPCP implementation in the presence of pulse shape and position fluctuations caused by hardware and channel variabilities. Additionally, this thesis offers a detailed analysis of CPPCP's abilities to detect errors without a traditional link layer. Finally, this thesis reports a prototype sensor platform and a wideband pulse transmission channel simulator used for demonstrating the efficacy of CPPCP in terms of energy-savings, communication security, and increased data transmission rates.

In this research design, the proposed CPPCP architecture incorporates chaos-based modulation of the inter-pulse time intervals in PPCP in order to provide security for light-weight networking in wireless sensor and IoT networks. A protocol data unit (PDU) is modulated in terms of the silence duration between two sets of wideband delimiter pulses, whose positions are modulated based on the value of the PDU and chaotically nonlinear function. The inter-pulse interval is set with chaotic alterations, which remove the periodicity from the signal. Compared with the existing binary-based chaotic communication, the multi-data symbols are used to achieve higher randomness by increasing the overlapping area between the inter-pulse intervals for different data symbols in the time domain, as well as noise-like spectral characteristics in the frequency domain. Simultaneously, CPPCP inherits the property of energy-saving from PPCP by sending fewer pulses with a shorter transmission delay. An architecture-based error detection mechanism is designed without adding the link layer and additional energy overhead. Based on hardware experiments, such energy-efficiency characteristic of CPPCP is better suited for thin energy-based IoT sensor networking applications than comparable state-of-the-art solutions such as BLE.

This thesis offers several contributions to improve energy efficiency and security in WSNs. First, a new chaos-based communication scheme, Chaotic Pulse Position Coded PDU, is designed for sensor networks with thin energy budget. Second, a methodology for Pulse Slot technique is developed for compensating the effect of pulse fluctuations and for achieving chaotic signal synchronization. Third, a CPPCP architecture-based error detection scheme is developed for the reliability of transmission without adding the link layer and additional energy overhead. Finally, an energy-harvesting-based sensor platform is specifically designed for CPPCP implementation.

1.6. Data Packet Position Modulation (DPPM)

The third goal of this research is to use a Data Packet Position Modulation (DPPM) mechanism to enhance information transfer capacity of ultra-low-bandwidth communication links used by energy-constrained sensors and IoTs. Packets from an energy-constrained sensor (or IoT) over a low-bandwidth link are often transmitted periodically based on the limited energy budget available to the sensor. For example, if transmission of a packet requires 0.5mJ of energy, and a sensor running on harvested solar energy requires 5 minutes to harvest 0.5mJ, then the sensor will periodically transmit one packet every 5 minutes. In such scenarios, there may be large time gaps between channel usage.

The core idea of the proposed DPPM is to leverage such large inter-packet spacing for coding additional information without incurring any additional transmission energy expenses for the transmitting node. Such additional information is coded by time-shifting packet transmissions with respect to the baseline periodicity determined by available energy harvesting rate as motioned above. Specifically, a packet's transmission time is shifted from the baseline periodic position based on some additional information to be transferred from the transmitter to the receiver. Consider a situation in which the base periodicity is T, so that a sensor, run by harvested energy, transmits one packet every T duration to a base station. Meaning, after receiving a packet, the base station knows when to expect the next packet. Now, if the sensor decides to send an additional data value v, it shifts a packet's transmission time by an amount that is computed based on v. The base station can decode the value v by observing the packet's timing with respect to when it was expected based on the baseline periodicity. This DPPM mechanism allows the sensor to send the value v in addition to the information content of the usual packet. In other words, the information transfer capacity is enhanced without any additional energy expenses.

In this thesis, we develop detailed system level protocols and algorithms for enabling such DPPM based information transfer capacity enhancements in the presence of multiple energy-constrained/harvested sensors and/or IoT nodes and low-bandwidth wireless communication links.

1.7. Thesis Organization

The rest of the thesis is organized as follows. Chapter 2 reviews the existing body of research on energy-efficiency, security, and information capacity of WSNs and IoT applications. Chapter 3 describes the concept PPCP and analyzes its performance in Tx-only network. Chapter 4 extends the idea of PPCP to multi-access and multi-hop sensor networking and further compare PPCP with start-of-the-art BLE on energy consumption. Chapter 5 develops CPPCP architecture and further analyzes the performance of CPPCP on security and energy-savings. Chapter 6 develops DPPM architecture and further analyzes the performance of DPPM on information transfer capacity. The future works on this topic are presented in Chapter 7.

CHAPTER 2: RELATED WORKS

2.1. Energy-Efficiency in WSNs

Energy conservation in wireless sensor and IoT networks has been extensively studied in recent years [25, 26, 27, 28, 29]. The battery on the SNs are usually irreplaceable or harvesting-based, thus have limited energy [1, 26], which makes energy-saving techniques a big requirement in WSNs . The research efforts to reduce energy consumption spanned from reducing the payload of the network by intelligent data aggregation schemes [30, 31] to optimizing the protocols of data transmissions [32, 33].

There are efforts on Medium Access Control (MAC) layer design to accommodate the sensor and IoT requirements for improving energy-efficiency. In reservation-based MAC protocols, such as Time Division Multiple Access (TDMA) [34, 26], a duty cycle is scheduled in order to achieve synchronization between transmitters and receivers and to put nodes in inactive mode until their allocated time slots. Time Slotted Channel Hopping (TSCH) [35] has been proposed as an amendment (IEEE 802.15.4e) to MAC portion of the IEEE 802.15.4 standard. TSCH is a combination of Time Division Multiple Access and Frequency-Division Multiple Access mechanisms as it uses diversity in time and frequency to enable the use of reliable low-power wireless networks. There is a huge body of work on synchronized access for low power devices with applications based on TSCH [35], ZigBee [36], BLE [27], etc., which are part of many commercial deployments. On the other hand, contention-based MAC protocols perform better on the scalability of the networks and collision avoidance between multi-transmitters compared to reservation-based MAC protocols. S-MAC [37] is a well-known contention-based protocol that uses a fixed sleep/listen cycle to conserve energy. Another example of a contention-based protocol is T-MAC [38], in which the fixed sleep/listen cycle of S-MAC is adjusted to be

adaptive based on traffic conditions and nodes' energy reserves. There are other protocols, which have been developed based on this core idea of sleep/listen cycle in recent decades, such as ADV-MAC [39] and R-MAC [40]. These efforts, however, are based on the conventional communication technique of sending information as binary strings of bits, called Energy-based Transmission (EbT) [41]. Such conventional binary packet suffers from the overhead of a large number of bits in the form of headers and preambles. The transmission of such overheads can be prohibitively energy-inefficient, and that is irrespective of the employed modulation mechanisms.

An energy-efficient communication model of pulse-based packets is proposed in [41]. The authors developed a silence-based data encoding and transmission mechanism, *Communication through Silence* (CtS), to achieve energy saving, but it comes along with undesirably long delay. The authors do not offer solutions in the key areas of 1) silence compression for handling large data values and 2) multi-field pulse PDUs. Building on [41], a *Variable-Base Tacit Communication* (VarBaTac) mechanism [28] is proposed to mitigate the transmission delay. Another pulse- and silence-based communication model is proposed in [25] for computing a function of data from multiple nodes for a wireless sensor network. The authors present a mechanism for integrating pulse position-based data aggregation and single-hop transmissions to a base station from multiple sensor nodes. These CtS architectures, however, do not consider intra-PDU and inter-PDU idle-listening energy consumption, which account for 50% to 85% of total communication energy consumption. Moreover, without a robust clock-synchronization mechanism and an error-detection technique, such CtS-based benefits for energy-saving cannot be achieved in implementations. The reliability issues of the communication network prevent precise measurements of silence duration.

Besides, pulse-based coding methods, such as Pulse Position Modulation (PPM) [42],

Multi-Pulse Position Modulation (MPPM) [43], Differential Pulse Position modulation (DPPM) [44], etc., have been applied in radio frequency (RF) and optical communications in recent decades because of their low energy expenditures. The work on pulse position modulation can be categorized as data encoding using: 1) pulse pattern signatures, and 2) inter-pulse silence duration. While the first category of solutions achieves enhanced security, error tolerance, and other link level performance, they do not cater to the energy needs. The second category has the potential for addressing energy issues. These inter-pulse silence duration modulation schemes can achieve energy-saving by sending a lower number of pulses, but longer transmission delays can occur, which leads to extra idle-listening energy consumption at receivers.

To mitigate the limitations demonstrated in the above related works, we develop a pulse-based PPCP architecture for transmit-only networks to achieve energy savings in [45]. However, the results in [45] does not consider idle-listening energy consumption at receivers and can only be used for one-hop scenarios. In multi-access networking, a significant amount of energy is consumed during idle-listening, overhearing, and collision-related retransmission, which turns out to be a critical challenge. To address that, this thesis further develops a multi-access PPCP PDU framework. The new architecture offers the key architectural concepts such as silence compression using *Flexible Base Digit Separation (FBDS)* and generalized multi-field pulse PDUs that enable all packet-based protocol operations including ARQ-based error management, and other higher layer abstractions used with packets. A comprehensive and implementable framework is provided in this thesis. Experimentally, it has been proved that our proposed PPCP framework can achieve higher energy-efficiency than a comparable state-of-the-art BLE.

2.2. Security in WSNs

WSNs are used for many applications in diverse forms from indoor deployment to outdoor deployment [18, 46, 14, 16]. The basic requirement of every application is to use the secured network [17]. The major challenge for employing any efficient security scheme in WSNs is posed by the size of sensors, consequently the limited energy, processing power, and the onboard memory.

Among the techniques for the secure transmission over WSNs, key-based cryptography is a well-known technique towards address security where the sender node encrypts the original data and the receiver node decrypts the received data to obtain an original data. Many key-based cryptography techniques with light-weight computational needs [14, 15, 16, 17, 18, 19] have been proposed in the literature for WSN security. In [14], different types of keys are used in the process of cryptography for solving the security issue in WSNs. Sensor Protocols for Information via Negotiation (SPIN) [15] is a key-based cryptographic technique. It consists of two secure building blocks named as Timed Efficient Stream Loss-tolerant Authentication (μTESLA) and Sensor Network Encryption Protocol (SNEP). However, SPIN performs best in small size networks because of its efficiency and high latency properties [16]. Localized Encryption and Authentication Protocol (LEAP) [17] is a protocol with a key management scheme that is very efficient with its security mechanisms used for large scale distributed sensor networks. LEAP satisfies several security and performance requirements of WSN to defend against HELLO Floods Attack, Sybil Attack and Wormhole Attack [18]. TinySec [19] is link layer security architecture for WSNs. To achieve confidentiality, encryption is done by using CBC (Cipher-block chaining) mode with ciphertext stealing, and authentication is done using CBC-MAC to support integrity, confidentiality, and authentication. ZigBee [36] is typical wireless communication technology and

can also support data confidentiality and integrity. A trust center is used in ZigBee which authenticates and allows other devices/nodes to join the network and to distribute the 128-bit keys. There are various cryptographic key-based protocols [16, 18] proposed by different authors for solving the security issue in WSNs. However, Cryptography entails a performance cost for extra computation that often increases packet size. Cryptographic hardware support increases efficiency but also increases the financial cost of implementing a network.

Lately, an alternative to key-based schemes, namely, *chaos-based security*, has been receiving significant attention due to its potentials for low-power communication privacy [20, 21, 22]. The main advantage of chaotic secure communication is that it can generate a complex set of chaotic signals using very simple electronic circuits [23], which are especially suitable for WSNs. Compared with the traditionally key-based cryptographic schemes, the chaos-based digital communication system can effectively eliminate the spectral characteristics of the signal, thus providing better privacy and security in general. Moreover, the chaotic communication system can remove the periodicity within the transmitted signal, which cannot be avoided in conventional pseudo-random-based cryptosystems.

Due to the nonperiodic characteristic, the chaotic signal cannot be stored in receivers as a reference. To overcome this problem, in some of the proposed communication schemes, the unmodulated chaotic waveform [47] is transmitted along with the modulated signal (transmitted reference scheme) either using a separate channel or using time division [48] to achieve coherent detection of the transmitted signal. Thus, a reliable detection can be achieved but at the expense of decreasing in the signal-to-noise ratio [49]. Some other chaos-based coding schemes have been proposed using different modulation schemes [50, 51]. A chaotic carrier, which resembles band-limited noise with a continuous non-periodic waveform and a naturally wideband spectrum, is

modulated by signal pulses. Such systems are sensitive to distortion and noise that can strongly affect the synchronization and cause errors in recovering information [52, 49].

A chaotic pulse position modulation (CPPM) [53, 54] is proposed using chaos synchronization to reduce the impact of channel distortion and noise on chaos-based communications. The information is encoded in the pulse train by alteration of time position of the pulse with respect to the chaotic carrier. A secure synchronization is established between the receiver and the transmitter based on the same chaotic function with the same parameter setup. Since binary information is modulated onto the inter-pulse intervals, the impact of distortion and noise on the pulse shape does not seriously affect the synchronization process. The principal advantage of CPPM is the automatic synchronization with the noncoherent demodulation type and without the need for specific hand-shaking protocols. However, CPPM sends one pulse for each binary bit, and a large number of pulses causes significant energy consumption. This leads to high energy storage requirement for energy-starved or energy-harvesting-based sensor nodes. Based on CPPM, a scheme of chaotic pulse width-position modulation (CPWPM) is proposed [55]. In CPWPM, the binary information is modulated onto both chaotically-varied intervals of position and width of output pulses. Since both the rising and the falling edge of pulses are used for data coding, the falling edge of pulses cannot be used for the functions of error detection, data recovery, and channel noise detection, etc. The nonlinear characteristics of the modulator/demodulator component (capacitor, amplifier, etc.) can cause fluctuations of pulse width and pulse position, which is not considered in [55]. A wider pulse used in CPWPM incurs extra energy consumption and leaves the spectral characteristics of the signal at risk of jamming or interception.

Given the limitations demonstrated in the previous related work, this thesis develops CPPCP architecture toward IoT energy-efficiently secure communication. In which, a value δ is

represented as a sum of information-bearing inter-pulse intervals with chaotically varying spacing. The time intervals between narrow pulses are chaotical alterations which remove the periodic property from the signal. The architecture ensures communication security by introducing randomness between data symbols, noise-like frequency spectrum, and significant energy savings by using a smaller number of pulse transmissions compared to existing secure coding schemes such as BLE. The mechanism can also be piggy-backed on top of traditional cryptography solutions to achieve higher levels of security. The thesis presents a detailed analysis of CPPCP's abilities to detect errors without a traditional link layer overhead.

2.3. Information Transfer Capacity in WSNs

The research towards improving information transfer capacity in WSNs [1, 56, 57, 58, 37] attracts a lot of attention in recent decades. Extensive work and protocols have been proposed to develop effective mechanisms for utilizing the available capacity in a communication medium. Protocols ranging from ALOHA [59] to CSMA [60] to various flavors of CSMA/CA [61] (i.e., WiFi, Bluetooth, ZigBee, etc.) indicate how the available information transfer capacity of a multiaccess channel is progressively better utilized by avoiding unused channel time as well as inter-node collisions. Various efforts [58, 62] towards improving channel utilization performance of those protocols were proposed.

In scenarios where per-node transmission slots can be allocated, either *a priori* [63] or in a dynamic manner in run-time [64], an upper bound of channel utilization can be achieved by completely avoiding collisions. For a single-channel system, no further mechanisms are found in the literature for enhancing the information transfer capacity farther than what TDMA can achieve. The proposed Data Packet Position Modulation mechanism proposed and explored in this thesis

sets out to achieve such enhancements for an increasingly popular class of embedded Transmit-only [3, 65] Sensor and IoT networks with limited energy budgets.

Multiple-Input-Multiple-Output (MIMO) based techniques [1] have been proposed for multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation. It is extensively used in many different communication standards including IEEE 802.11n (WiFi), IEEE 802.11ac (WiFi), HSPA+(3G), WiMax (4G), and Long-Term Evolution (4G LTE). The works in [66] improve the performance of baseline single-channel MIMO by extending it for multiple channels. While being able to enhance capacity, the biggest impediment for using MIMO for low-power embedded sensor nodes is that it requires multiple antennae and sophisticated signal processing hardware and software. These components are often too energy-heavy to be applied for embedded sensors. Moreover, the MIMO paradigm is fundamentally unsuitable for the low-cost transmit-only nodes [3, 65] that are aimed in this specific work.

Another fundamental way of improving information transfer capacity without commensurate number of additional transmissions is by using network coding [57]. In network coding, which usually applies to multipoint-to-multipoint communication. Data from multiple sources are cleverly combined and uncombined using bit-wise Boolean operations at the intermediate router nodes. It is done in such a way that the total number of needed transmissions can be smaller than what is needed for without-coding baseline operation. Such reductions in the required transmissions free up network capacity for sending more information, thus increasing the effective information transfer capacity. Since the functions of network coding involve multiple protocol layers, cross-layer protocol design and optimization are necessary. Moreover, protocol adaptations are needed for minimizing the interference due to the difference in power levels at

which neighbor nodes receive the same transmission in a broadcasting mode. All these add complexity that is not desirable for embedded sensor nodes. Also, there is no network-coding solution for transmit-only one-hop sensor networks that the proposed DPPM mechanism is aimed towards.

Tx-only sensor nodes have been analyzed by [67] on maximizing data throughput by means of data admission policies on the receiver end. However, the collision in a Tx-only system is not covered in [67], Due to the asynchronous and uncoordinated transmission nature of a Tx-only sensor node, there is a high probability of collision in a multi-user environment. In [2], it investigates packet admission policies for a network of Tx-only nodes. Cluster heads manage policies such as selecting the strongest of several incoming signals in order to optimize different performance criteria. The research only considers the packet admission policy used by receiver nodes, and the authors note that optimizing other parameters such as sensor density, transmit power, packet coding and frequency of transmissions is future work. In [68] it analyzed an asymmetric physical layer design in which a transmitter's encoder is much simpler than its receiver's decoder. For this setting, it is shown that single-hop networks have lower overall power consumption than multi-hop. The relative costs of forward error correction codes are measured by [69]. Different forward error correction codes from simple repetition to convolutional and turbo codes are investigated. The authors note that the optimal trade-off between coding strength and coding overhead will vary strongly from one node to another depending on channel quality and distance to the base station and has to be adapted at run time [69]. However, the above methods achieve the improvement of information transfer capacity based on the complex coding and design overhead. The optimal setup of parameters for maximum capacity is changing from node to node, which brings the difficulty for the implementation in a WSN with a relatively large number of

sensor nodes. Such coding strategies incur extra energy consumption except for the energy consumption on packet transmissions.

This thesis develops packet position modulation solutions to the challenges mentioned above. The DPPM architecture is designed based on the modulation of inter-packet silence duration. An algorithm is developed to obtain the maximum information transfer capacity of the networks based on the consideration of multi-parameters, such as sensor density, energy utilization rate, hardware parameters, and packet length, etc. Unlike prior coding methods for improving information transfer capacity, the proposed architecture and the corresponding MAC protocol are differentiated in terms of zero extra energy consumption and without without any new physical layer or hardware enhancements, thus making DPPM much simpler than the above existing solutions and suitable for ultra-low-cost embedded sensor nodes. The primary requirement for DPPM to work is the need for periodic transmissions in terms of TDMA, either with pre-allocated explicit slots or dynamically chosen implicit slots, both of which are explored in this thesis. The mechanism can be implemented into application-specific low-power sensor networks and IoT systems for significant gains in the information transfer capacity, especially in sensor networks powered with slow energy-harvesting sources.

CHAPTER 3: PULSE POSITION CODED PUDS

3.1. Motivation

Wireless Sensor Networks (WSNs) consist of a large number of constrained wireless sensor nodes for the purpose of data gathering. The energy-efficient data transmission is very important in WSNs due to the limited amount of available energy. A data packet is typically transmitted in binary format with a synchronization preamble and packet header. The packet preamble size is a few tens of bytes [11, 12, 13]. The transmission of such overheads can be prohibitively energy-inefficient, and that is irrespective of the employed modulation mechanisms. In this chapter, an energy-efficient communication model of pulse-based PDUs is proposed based on an inter-pulse silence-based data encoding and modulation mechanism, Communication through Silence (CtS), to achieve energy saving.

When pulse-based CtS mechanism is used in the formatting of PDU, the primary design challenge stems from the fact that transmission time for a data value δ is $O(\delta)$ compared to $O(log_2\delta)$ for packets. This results in higher access delay and lower effective link capacity compared to packets. The second challenge is an intra-PDU idle listening at the receiver. After a receiver receives the start delimiter pulse-set, its network interface needs to remain awake till the end delimiter pulse-set is received. Idle listening occurs during this period. This intra-PDU idle listening never happens for packets, thus posing a major architectural challenge for the pulse-based PDU. The third challenge is to transmit and receive a single pulse without synchronization overhead. Finally, all traditional packet-based abstractions such as error management, routing, reliable transport, compression, and security will need to be ported using pulse position modulation in an energy-efficient way.

We offer the key architectural concepts such as silence compression using Flexible Base Digit Separation (FBDS) and generalized multi-field pulse PDUs that enable all packet-based protocol operations including ARQ-based error management, and other higher layer abstractions used with packets.

3.2. Our approach and contribution

The contribution of this chapter is to develop architectural solutions to a subset of the challenges mentioned above. Specifically, as a first step, it develops PPCP based solutions for a Transmit-only (Tx-only) network [2] architecture, in which low-energy sensors operate only in transmitter mode for sending data to access points. Through analytical modeling, simulation, and a prototype network implementation, we show the effectiveness of a PPCP Tx-only network in comparison with legacy packet-based networks.

3.3. Design Objectives

The objective of this thesis is to develop a new link layer architecture that uses Pulse Position Coded PDUs (PPCPs) instead of traditional packets for energy-efficient networking. The key idea is to encode a data value δ in pulse position modulation using two sets of delimiter pulses. Irrespective of the data value being sent, PPCP requires a constant number of pulses compared to $O(log_2(\delta))$ bits needed for packets. Leveraging this feature, coupled with energy savings from not having to send per-PDU synchronization preambles, PPCP can offer a radically energy-lean link layer. When protocol syntaxes for managing idle listening are added, the proposed framework can offer a suitable networking technique for severely energy-starved networks.

3.4. PPCP Architecture

3.4.1. Baseline Coding

Figure 3.1 depicts how a data value can be coded using packet and PPCP abstractions. In packet mode, a value $\delta(\delta \geq 0)$ is coded using a $log_2(\delta)$ bit packet, preceded by a ρ bit of preamble needed for physical layer synchronization. The resulting transmission energy consumption is $\rho + log_2(\delta)$ times bit transmission budget, and the corresponding reception energy consumption is $\rho + log_2(\delta)$ times bit reception budget. The transmission duration is $\rho + log_2(\delta)$ times bit duration. Over a half-duplex point-to-point (P2P) channel with capacity C Bits/s, packets can transport information at an effective rate of $\frac{C}{\rho + log_2(\delta)}$ data values per second. Although the exact energy and delay budgets are determined by physical layer coding mechanisms (e.g., Manchester coding, etc.), the above expressions are generally valid for a high-level comparison.

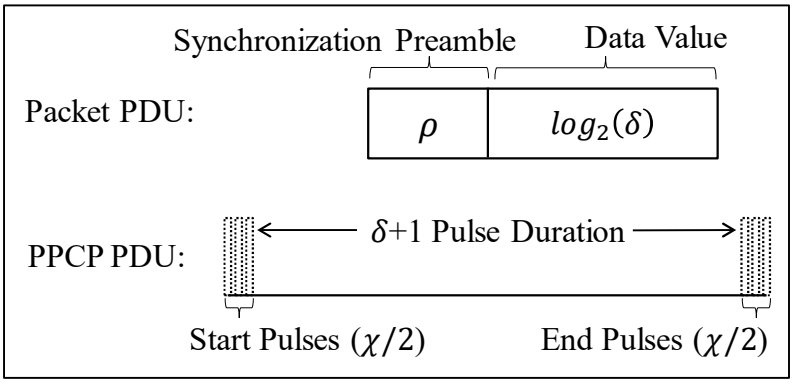


Figure 3.1: Packet and PPCP coding of a data value δ

PPCP coding starts with $\frac{\chi}{2}$ start-pulses, followed by a silence of $\delta + 1$ pulse duration, indicating the value to be transmitted, and finally $\frac{\chi}{2}$ end-pulses. The transmission energy consumption is χ times pulse transmission budget, and the reception energy consumption is χ

times pulse reception budget. The transmission duration is $\chi + \delta + 1$ pulse durations, resulting in an effective transmission rate of $\frac{C}{\chi+\delta+1}$ data values per second.

Note that the start pulse sequence and the end pulse sequence do not have to be of same length or format. They will be designed based on considerations including energy overhead and error-resilience in the presence of pulse losses and false positive detection.

The above expressions for PPCP and packet point that for typical packet preamble size of few tens of bytes [13] PPCP architecture has the potential to 1) bring significant savings in terms of transmission and reception energy expenditure, and 2) provide lower transmission delay and subsequently better transmission rates for small data values. However, it can suffer from the following two shortcomings. The first one is intra-PDU idling consumption, which is not present for packets and can offset the above two architectural gains. Intra-PDU idling happens during the time when a receiver waits for the end-pulses without being able to perform intra-PDU sleep. This can cause additional energy overhead for PPCP, especially for large data value δ. Note that Inter-PDU idling, which is different from intra-PDU idling, is well understood in the literature [70] and applies to both packets and PPCPs. The second notable shortcoming is that for large data, transmission delay can be prohibitively large. The following Flexible Base Digit Separation (FBDS) method is proposed next for mitigating both of these adverse effects.

3.4.2. Flexible Base Digit Separation (FBDS)

FBDS, as a silence compression mechanism, is introduced for mitigating intra-PDU idle listening and long PPCP transmission times for large data values. With FBDS compression, a value δ is first represented as a multi-digit number in a number system of base β. Then the resulting digits are separately sent using the PPCP format. For example, the data value 723 can be

represented in base-6 number system as 3203. With FBDS enabled, a transmitter sends the digits "3", "2", "0", and "3" separately ("4", "3", "1" and "4" pulse durations respectively) with a single pulse delimiting between the digits. The situation is illustrated in Figure 3.2. FBDS, in this example, drastically shrinks the PDU transmission time from 730-pulse duration to only 21-pulse durations. It assumes start and end patterns of 3 pulses each.

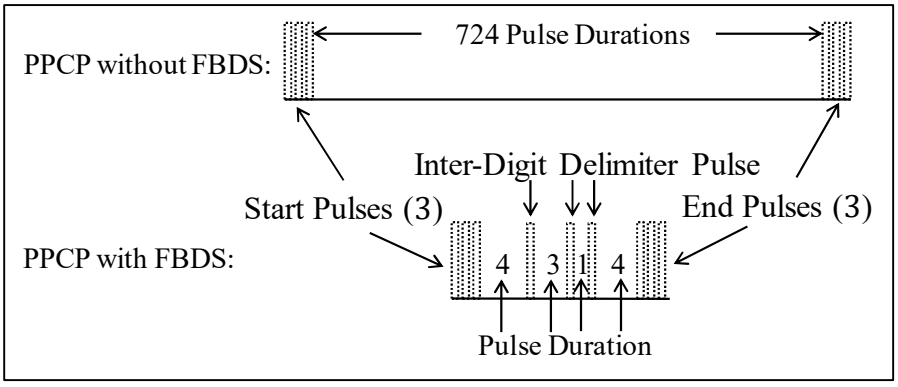


Figure 3.2: Coding of the value (δ) 723 using FBDS with base (β) 6

Formally stated, FBDS brings the transmission duration down from $\chi + \delta + 1$ (i.e., in Figure 3.2 (top)) to the upper bound of $\chi + \left(log_\beta \delta - 1\right) + \beta log_\beta \delta$. The first term is for the start and end-pulses, the second term is for inter-digit delimiters, and the final term is the worst-case cumulative duration of all the digits. Notably, FBDS also brings down the intra-PDU idling duration from δ (i.e., in Figure 3.2 (bottom)) to the worst-case of $log_\beta \delta$. These drastic reductions from O(δ) to worst case O($log_\beta \delta$) for both transmission and intra-PDU idling are achieved with an additional transmission/reception energy cost for only $log_\beta \delta - 1$ pulses for inter-digit delimiters.

Compared to packets, PPCP with FBDS can: 1) bring significant savings in terms of Tx/Rx expenditure, 2) provide lower transmission delay and better transmission rates for up to much larger data values, and 3) limit intra-PDU idling to logarithmic complexity.

It should be noted that for given transceiver hardware with known Tx, Rx, and Idling energy budgets, the FBDS base β should be chosen such that the difference between Tx/Rx energy savings over packets and the intra-PDU idling expenditure is maximized.

3.4.3. Multi-field PDUs

Like for packets, a PPCP protocol stack will be required to support control information such as header and trailer containing type, node identifiers, sequence numbers, CRC, etc. The proposed architecture is general in that an arbitrary number of fields can be included within a PDU using pre-agreed inter-field delimiters.

Figure 3.3 depicts the representation of an example PDU containing Number of Fields (F), Tx. Id, Type Indicator and two data fields ($i.e., 161$ and 723). The top part of the figure shows the values of different fields and the corresponding base-6 FBDS digits. Number of Fields is defined as the number of fields inside a PDU excluding F itself. Each field represents any arbitrary value. The Tx. Id. 38, is converted to base-6 FBDS of 102 as shown in the figure. Type indicator indicates the type of PDU. In the diagram, PPCP pulses are represented by the "1"s and the silence durations are represented by "0"s. The following delimiters are used: "1111" for PDU start, "111" for PDU end, "1" for inter-digit separation, and finally "11" as inter-field separation. Note that these are not the only possible choices of delimiter pulse patterns, but these provide reasonable error resilience as will be discussed later. It should be noted that an FBDS digit 'n' is represented

by a silence of '$n + 1$' pulse durations. An arbitrary number of fields can be incorporated in a PDU using the example delimiter formats in Figure 3.3.

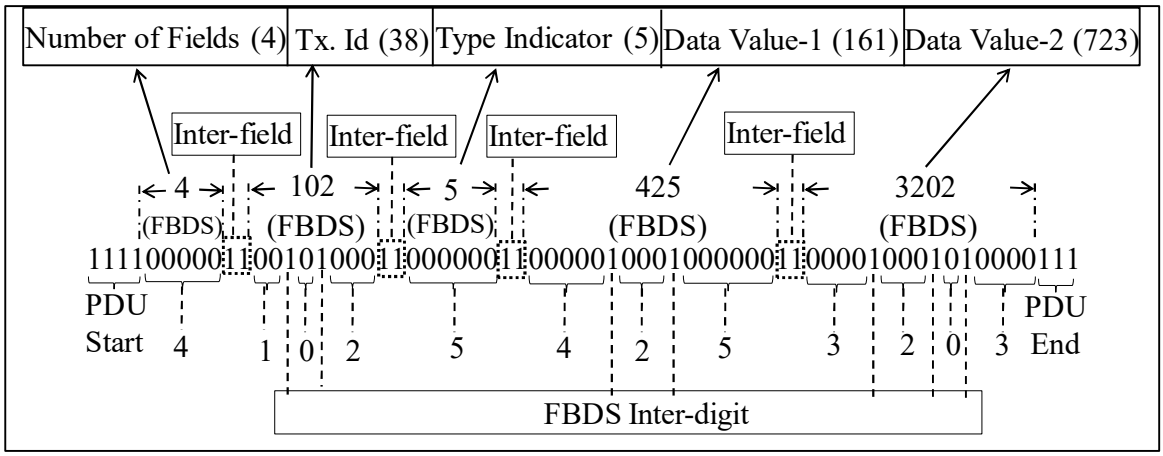


Figure 3.3: Example multi-field PDU with FBDS silence compression

3.4.4. Error Detection

Channel errors can affect PPCP's operation when its different delimiters (i.e., PDU-start, PDU-end, inter-FBDS, and inter-field) are distorted due to pulse losses or false pulse detection. Unlike packets, in PPCP such errors in many situations can be detected from the framing context. For example, the sequence number is sent as "0000010001000000", where the 1s represent pulses and 0s represent silence. Now think about a loss situation in which the pulse indicated by the underlined 1 is lost, resulting in the sequence: "0000000001000000". A '0' replaces the '1'. With an FBDS base of 6, which is known by the receiver, an FBDS digit cannot ever be larger than 6; meaning there can never be a contiguous silence period longer than 6 pulse durations. But in this case, the pulse loss created a contiguous silence of nine pulse durations (i.e., nine zeros). The receiver can detect that a pulse loss error has happened. For a given delimiter set, a comprehensive set of error detection rules can be developed for detecting possible errors based on such framing context. For example, for the default PPCP design FBDS with base-6, if any received

signal does not follow the following set of formatting rules, the error can be detected during PPCP PDU transmission. 1) Start Symbol: four consecutive pulses; 2) Trailer: three consecutive pulses; 3) Digit Range: each received digit $d_i \in [0, 5]$; 4) Field Value Range: the maximum pre-defined value of each field; 5) Number of Fields: The number of received fields should be equal to F.

3.5. Dimensioning Pulse Slot Size

A concept of pulse slot is used for accommodating pulse shifts during a PPCP transmission. A relative pulse shift can happen due to 1) mismatch of clocks between transmitter and receiver, and 2) variations in the received analog signal shape and the subsequent conversion to a digital pulse.

A node transmits a pulse at the start of a pulse slot of size τ. The transmitter can send the next pulse only after the pulse slot duration τ such that it is guaranteed that only one pulse's rising edge can appear within a pulse slot duration at the receiver, even if the pulse is shifted. Since pulse shifts can be variable, τ needs to be dimensioned such that a receiver can unambiguously retrieve the correct number of silence durations between the start and end pulses encompassing a data value d_i ($d_i = n - 1$), where n is the number of silence durations.

Figure 3.4 shows an example in which d_i, the data value to be sent, is 3, which is shown with 4 units of silence pulse durations between the start and end pulse. Let S_i refer to the pulse shift with range $[S_{min}, S_{max}]$, which usually depends on the hardware characteristics including transceiver operating range, supply voltage, detection voltage threshold, etc., and can be computed experimentally for a target transceiver. In the absence of any shift, or if $S_{max} \ll B$ (B is raw bit duration), a pulse slot can be chosen equal to the pulse width (i.e., $\tau = B$). In the presence of pulse shift, however, τ needs to be larger than B.

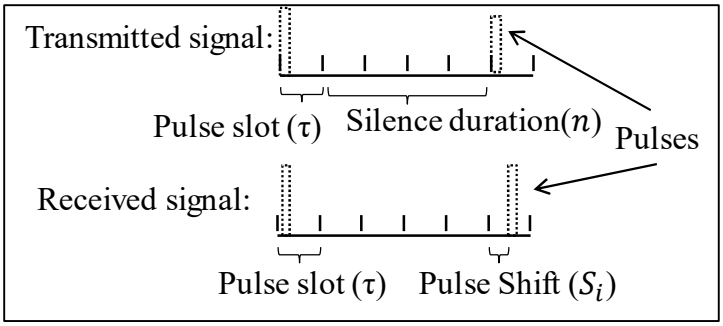


Figure 3.4: Pulse Slotting with $n = 4$

The temporal separation between the rising edges of start and end pulses of a PPCP depends on the range of pulse shifts and where the pulses are received within a defined pulse slot. Let D^n_{max} and D^n_{min} define the maximum and minimum of such separations for n ($0 \leq n \leq \beta$). They can be expressed as:

$$\begin{cases} D^n_{max} = (n+1)\tau + S_{max} - S_{min} \\ D^n_{min} = (n+1)\tau - S_{max} + S_{min} \end{cases} \tag{3.1}$$

In order to distinguish n silence durations from $(n+1)$ silence durations, a pulse slot duration τ is selected for transmitter and receiver such that the following Ineq. 3.2 hold true:

$$D^n_{min} < D^n_{max} < D^{n+1}_{min} < D^{n+1}_{max} \tag{3.2}$$

From the above conditions, the width of the slot can be selected as:

$$\tau > 2(S_{max} - S_{min}) \tag{3.3}$$

If a slot is chosen according to Eq. 3.3, the receiver can distinguish the number of silence pulse durations (n) (and thus the value $n-1$) unambiguously, irrespective of how the pulse shifts (within $[S_{min}, S_{max}]$) alter the arrival time of the start and end pulses encompassing n.

3.6. Optimal FBDS Base Selection

Table 3.1: Baseline System Parameters

System Parameters	Symbol	Representation
Traffic Variables	λ (PDU/sec/node)	data generation rate per node
	δ	maximum data value per field
Network Variables	N	number of nodes
	C (bps)	channel capacity
PDU variables	ρ (bit)	size of the preamble and start symbol for a packet
	θ (bit)	payload (including F, Tx. ID, PDU Type Indicator, Sensor data) for a packet
	B (second)	raw bit/pulse duration for a packet/PPCP
	β	FBDS base for a PPCP
	τ (second)	PPCP pulse slot duration
Energy Model Variables	P_{Tx}^{High} (watt)	power consumption for transmitting logical high $P_{Tx}^{High} = V_{Tx} * I_{Tx}^{High}$ (I_{Tx}^{High}: current for logical high Tx.)
	P_{Tx}^{Low} (watt)	power consumption for transmitting logical low $P_{Tx}^{Low} = V_{Tx} * I_{Tx}^{Low}$($I_{Tx}^{Low}$: current for logical low Tx.)

For a set of given system parameters, there is a specific base value in FBDS that can minimize the energy consumed by the PPCP protocol. In what follows, using the system parameters in Table 3.1, we develop a model for choosing the optimal FBDS base value.

For different maximum data value δ, there is a finite k that meets inequality $1 \leq \frac{\delta}{\beta^k} < \beta$ ($k \geq 0$). Each of the $k+1$ digits (with respect to base β) are marked as R_m ($m = k+1, k, \cdots, 1$). When the field value V ($V \in [0, \delta]$) follows a uniform distribution, the average number of pulses for one field (not including Start pulses and End pulses), N_{PPCP}, can be computed as follows.

$$N_{PPCP} = [2\beta + (\beta - 1)\sum_{n=2}^{k}(n-1)\beta^{n-1} + (k+2)(R_{k+1} - 1)\beta^k + (k + \sum_{n=2}^{k} R_n\beta^{n-1}$$

$$+(k+2)(R_1 + 1)]/(\beta + 1) \quad (3.4)$$

The average duration of PPCP (also, the average transmission delay) L_{PPCP} can be computed as follows:

$$L_{PPCP} = \tau\{\frac{k}{2}\beta^{k+1} + \frac{3k+2}{2}\beta^{k} - \sum_{n=1}^{k-1} 2\,\beta^{n} + (R_{k+1} - 1)\left(\frac{R_{k+1}+4}{2}\beta^{k} + \frac{k}{2}\beta^{k+1} + \frac{3k+2}{2}\beta^{k}\right)$$

$$+ \sum_{m=2}^{k+1}[(R_m + 2)(1 + \sum_{n=1}^{m-1} R_n\,\beta^{n-1})]$$

$$+ \sum_{n=2}^{k}\left[\frac{R_n+3}{2}R_n\beta^{n-1} + R_n\left(\frac{n-1}{2}\beta^{n} + \frac{3n-1}{2}\beta^{n-1}\right)\right]$$

$$+ \frac{(R_1+1)(R_1+6)}{2}]/(\beta + 1) - B \tag{3.5}$$

Then, the average energy expenditure for transmitting a PPCP PDU, E_{PPCP}, can be deduced based on the above equations:

$$E_{PPCP} = N_{PPCP}BP_{Tx}^{High} + (L_{PPCP} - N_{PPCP}B)P_{Tx}^{Low} \tag{3.6}$$

For given transceiver hardware with power model parameters P_{Tx}^{High} and P_{Tx}^{Low} and pulse duration B, the optimal FBDS base (β) that can minimize the average energy (E_{PPCP}) can be found from Eq. 3.6.

3.7. Performance in Transmit-only Network

Performance of PPCP and a legacy packet-based PDUs are evaluated using simulations from error detection, energy consumption, transmission delay, and network throughput perspectives.

3.7.1. Network Model

As the first step of evaluation for the new PPCP framework, a Tx-only network [2] is evaluated. 20 Nodes collect sensor data and send PPCP PDUs to an access point (AP). The nodes

are not capable of reception, thus only 1-hop ALOHA based operation is permitted. Nodes operate in a low-duty-cycle mode [37] in order to reduce idle power consumption. A node wakes up only when sensor data is generated based on an exponentially distributed data generation process. Even though they lack multi-hop routing, simplicity and better energy economy (i.e., no idling) makes Tx-only networks attractive for sensor-based data collection [2], especially where multi-hop is not needed.

Increasing node-count and data rate in a PPCP network has collision effects that are very similar to those in packet-based networks. Those effects were consistently observed in larger PPCP networks with higher traffic rates.

3.7.2. Simulation Results

The baseline transceiver parameters are chosen based on a simple On-Off-Keying modulated 434MHz transceiver [71]. Based on the implementation reported in the VirtualWire library [72], raw bit duration of $250\ \mu s$ is used for packet transmissions. An $\frac{8b}{12}$ coding scheme is for packet coding in order to maintain the physical layer DC balance. 48-bits preambles are used for packets as reported in [72]. For the sake of comparability with the packet, pulse duration of $250\ \mu s$ is chosen for PPCP. A pulse slot duration of $500\mu s$ for PPCP transmission is chosen based on Eq. 3.3.

In terms of traffic, both PPCPs and Packet PDUs are generated by each node following a Poisson distribution. Each PDU includes Number of Fields (F), Transmitter ID ($\in [0,19]$), Type Indicator (equal to 0, indicating there is one type of PDU in Tx-only networks), and data fields (each data value is generated using a uniformly distributed distribution in the range $[0, \delta]$). The

Start and End of a PPCP PDU follow Figure 3.3. Finally, unless stated otherwise, the FBDS base is set to 6.

A. Error Detection Accuracy

Effects of pulse loss and false positive detection on PPCP's performance are analyzed in this part. Since the impacts of such errors are well understood for packets, they are skipped here.

Figure 3.5 shows the error detection accuracy in PPCP for a different number of fields (F). The x-axis shows the error probability, either pulse loss or false positive pulse detection. Y-axis shows the Detection Accuracy, which does not rely on any link layer checksum. Detection Accuracy is defined as the number of correct PDUs delivered to the upper layer as a fraction of the ones received at the receiver. PPCP PDU format follows the one in Figure 3.3. Type indicator is set to 0 because there is only one type of PDU sent to the AP in the Tx-only network. Errors in Figure 3.5 are those due to pulse loss and false positives instead of those due to ALOHA collisions. Collisions are excluded by conducting the experiment on a point-to-point link.

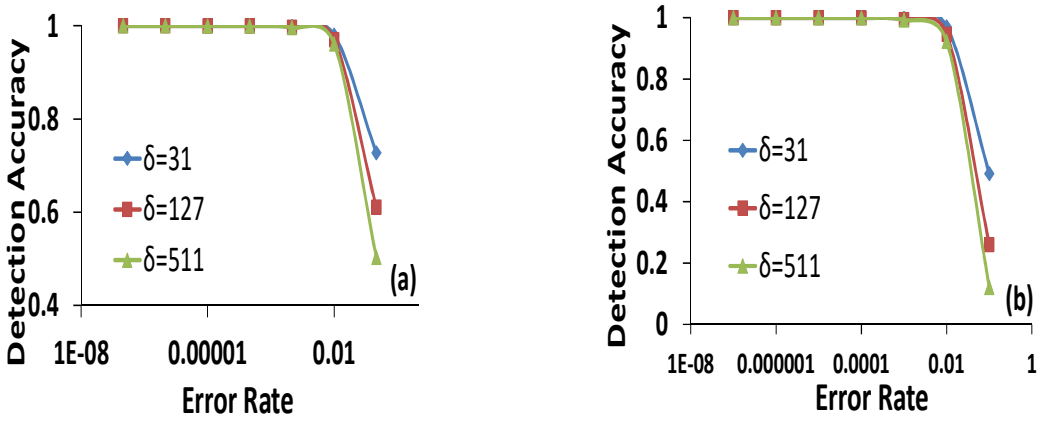


Figure 3.5: PPCP error detection accuracy for (a) $F = 3$, (b) $F = 5$

The Pulse Loss Rate (PLR) and False Positive Rate (FPR) vary in range 10^{-7} to 10^{-1}. It can be seen that for any value of F in Figure 3.5(a) and Figure 3.5(b), the detection accuracy is close to 100% when the error rate is less than 10^{-1}. That is true for all maximum data values ($\delta = 31, 127$ and 511). Increasing δ to 10^{-1} leads to a reduction in detection accuracy. Also, for such a high error rate, the detection accuracy is smaller for larger F ($F = 5$ in Figure 3.5(b)). The reason is that a longer PPCP PDU with more number of fields or larger data values has a higher probability of getting corrupted.

To summarize, the internal pulse dependencies within the PPCP structure alone can be used for reasonable error detection without using a link layer checksum. This is especially true for low pulse loss and false positive detection rates. Note that an additional link layer checksum field can also be added just the same way it is done for packets.

B. Energy Consumption

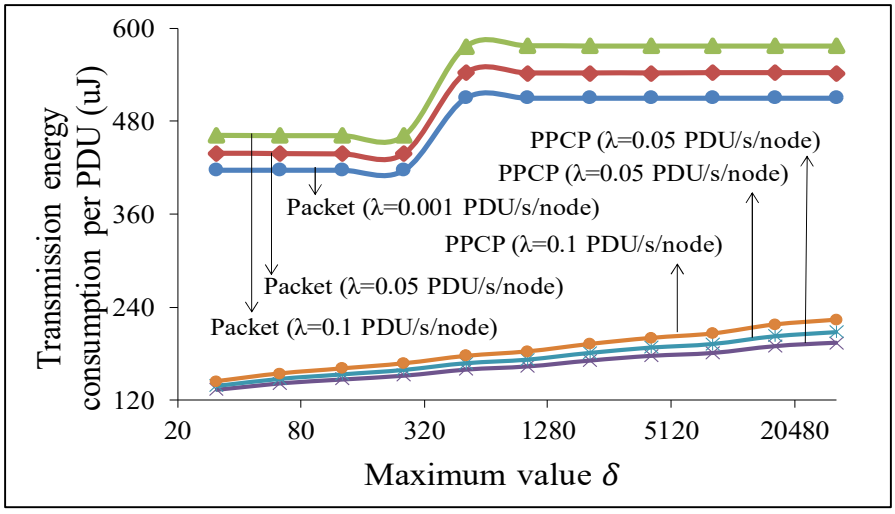


Figure 3.6: Average transmission energy consumption per PDU

In all experiments, the power consumption for transmitting one bit/pulse is 30.85 mW. The idling/silence power expenditure is 0.15 mW. Since the raw bit/pulse duration is 250 µs, the

energy consumption per bit/pulse is $7.71\mu J$. The simulation examines the energy and delay performance of PPCP and traditional packet under different data generation rates (λ), Number of Fields (F) and maximum data values (δ). The number of sensor nodes in an AP backbone cluster is $N = 20$.

Figure 3.6 shows the average transmission energy consumption per PDU. This value is computed using the average number of pulses in a transmitted PDU multiples the individual pulse transmission budget. Because PPCP uses less number of raw bits/pulses in the physical layer compared to the packets, PPCP transmission is more energy-economic for all λ (PDU generation rate) values. When $\lambda = 0.001$ PDU/s/node, on an average, PPCP saves 65.41% of transmission energy compared to the packets for any value size $\delta \in [31,\ 32767]$. On average, $475.94\ \mu J$ is consumed for the successful transmission of one packet PDU, which is almost four times the average energy needed to transmit a PPCP PDU.

For a fixed data generation rate, PPCP transmission energy shows a linearly increasing trend with an increase in maximum data value δ. That is because larger δ imposes the use of more number of digits with a fixed FBDS base. One extra digit requires an extra pulse delimiter to be transmitted for PPCP. Figure 3.6 shows a sudden increase in transmission energy for a packet when $\delta > 255$. The reason is as follows. Packet PDU uses an 8b/12b DC balance coding method. With such coding, the encoded packet length is 12 bits when the data value δ is in the range $[1, 255]$. For larger δ in the range $[256, 131071]$, the final encoded packet length consists of 24 bits. The extra 12 bits padding into each data field of the packet results in a drastic increase in transmission energy. The steady trend of energy beyond that point $(\delta = 256)$ is because the encoded packet length does not change and remains at 24 bits.

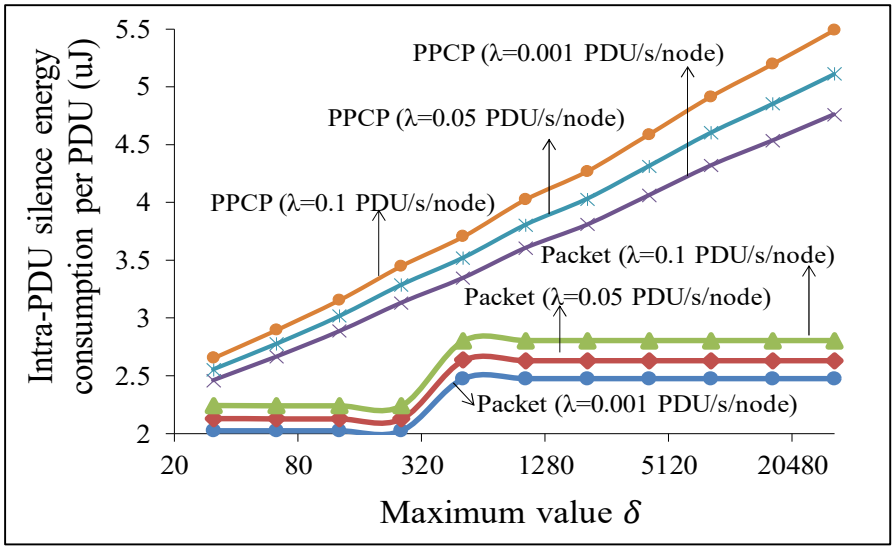


Figure 3.7: Intra-PDU energy consumption per PDU

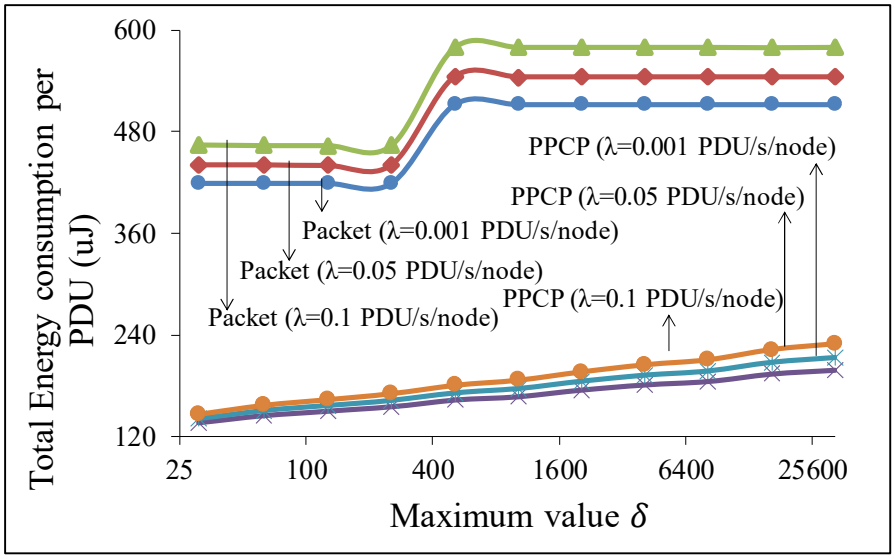


Figure 3.8: Total energy consumption per PDU

PPCP's significant savings on transmission energy comes at the expense of higher intra-PDU idling/silence energy consumption. This idling expenditure occurs during the silence period at a transmitter in transmitting logical low. Figure 3.7 shows intra-PDU energy consumption per PDU for PPCP and conventional packet. It can be seen that PPCP consumes more energy on intra-

PDU silence duration than a packet. This consumption load of PPCP, however, is much smaller compared to its transmission energy savings over packets as shown in Figure 3.6. The lower energy expenditure during idling compared to transmitting is due to the (200 times) lower current needed for transmitting a logical low (zero) compared to transmitting a logical high (one). This also leads to 200 times lower power expenditure during the idling. Figure 3.8 shows the total energy consumption per PDU with different data values δ and PDU generation rates λ. Observe that the total energy consumption for packet PDU transmission is always greater than that for PPCP transmission. In addition to PPCP's architectural advantages, the energy overheads of the packet preamble bits contribute to this consistent difference.

C. Delay

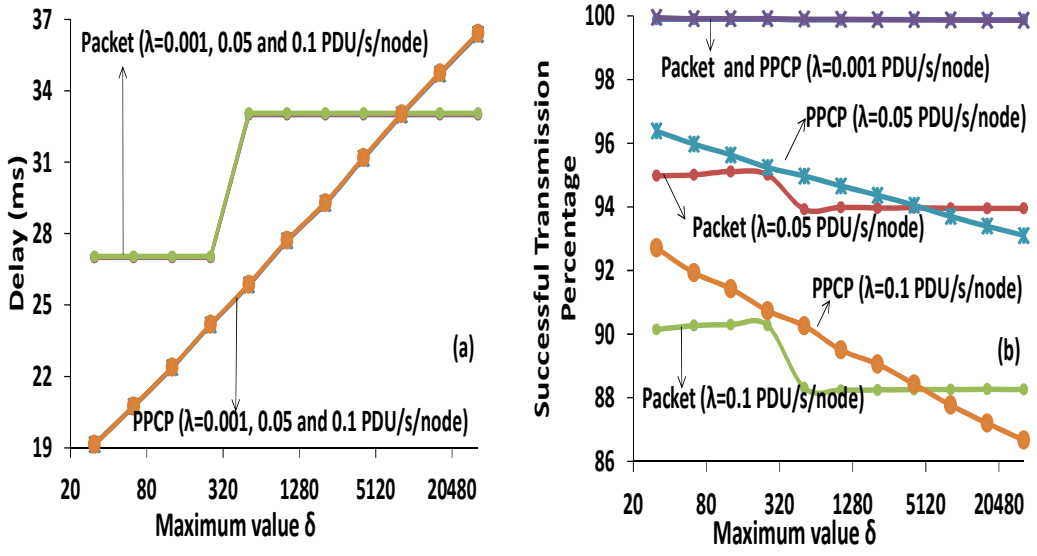


Figure 3.9: Comparison of (a) delay and (b) successful transmission rates

Per-PDU (both for PPCP and packets) delay as a function of data value size δ is depicted in Figure 3.9(a). The results are presented for multiple PDU generation rate λ. While this delay figure does not include propagation and processing delays, it does include PDU queuing delays in

the Tx-only network nodes. However, as can be seen in the figure, the queuing delay is almost negligible compared to the total delay, which is dominated by the PDU transmission duration. This is apparent from the fact that the delay numbers are almost the same for all PDU generation rates (λ's), indicating almost no queuing.

It is also apparent in Figure 3.9(a) that for PPCP, the total delay, which is mainly the PDU transmission delay, is smaller than that for the packets for smaller PDU data values. Until the PDU value size $\delta \leq 4095$, the duration of PPCP PDU with four fields ($F = 4$, one Transmitter ID (ID$\in$ $[0,19]$), one Type Indicator (0), and two data fields) is less than or equal to the duration of packet PDU with the same number of fields. That is why PPCP incurs a smaller delay compared to the packet before this point. The sudden increase of delay for a packet for when $\delta > 255$ is due to the larger packet duration and the extra 12 bits padding for each data field as mentioned in Chapter 3.7.2.

The effects of relative PDU size difference also shows up in successful transmission rates as shown in Figure 3.9(b). For very low PDU generation rate (e.g., $\lambda \leq 0.001$ PDU/s/node), almost all transmitted PDUs, both packet and PPCP, are successfully received at the AP with no collision. For larger λ values, sending PPCP PDUs involves fewer collisions because of PPCP's smaller PDU duration compared to packet's. Therefore, PPCP PDU maintains a higher successful transmission percentage for any maximum data value $\delta \leq 4095$ when $\lambda = 0.05$ and 0.1 PDU/s/node. When $\delta > 4095$, PPCP PDU duration and transmission delay (Figure 3.9(a)) is larger than that for packet PDU. As a result, the successful transmission rate for PPCP is lower than the packet's (Figure 3.9(b)).

D. Throughput

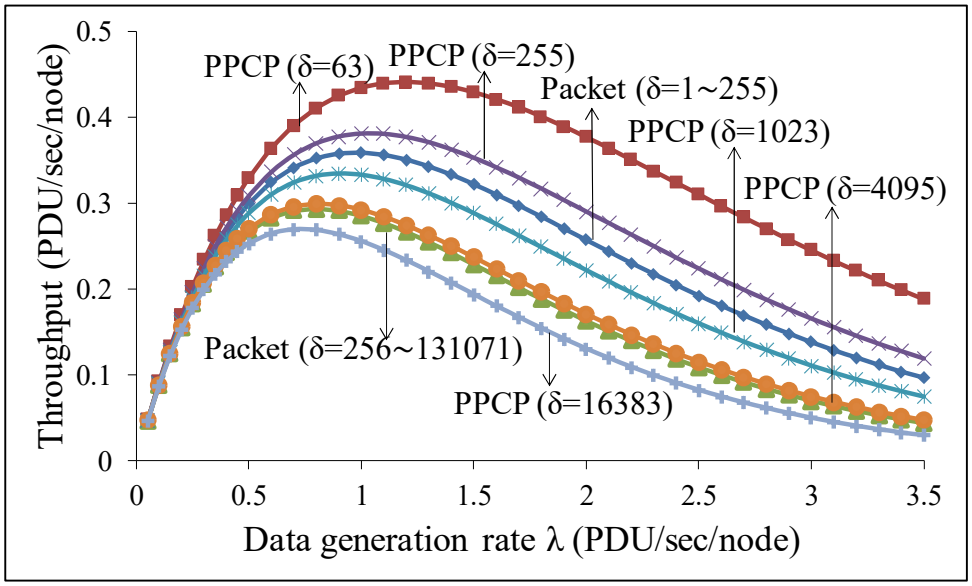


Figure 3.10: Throughput comparison between PPCP and packet

Figure 3.10 shows per-node throughput for different PDU generation rate λ when $F = 4$. Observe that for $\delta \in [1, 131071]$, the packet's throughput is shown in two curves corresponding to two different PDU durations. When $\delta \geq 256$, the extra 12 bits are padded to each data field of the packet. However, the duration of PPCP PDU linearly increases with increasing of maximum data value δ, leading to a decrease in maximum throughput for PPCP PDU as shown in Figure 3.10. When the maximum data value (δ) is less than 4095, the maximum throughput for PPCP is always larger than that for traditional packet due to the smaller duration of each PPCP PDU compared to packet PDU. However, when $\delta \in [4095, 131071]$, maximum throughput for PPCP is smaller than that of the packet due to the faster increase of PPCP PDU duration. In summary, using PPCP leads to a higher throughput as long as maximum data value $\delta \leq 4095$. It should be noted in Figure 3.10 that the general throughput behavior with increasing λ follows the usual

ALOHA throughput trend. It increases initially until it maximizes at the optimal data load. Beyond that point, for higher data load, throughput decreases due to excessive collisions.

Figure 3.11 shows the maximum throughput for a different number of fields in PDU, and the corresponding optimal data generation rate λ. The largest throughput difference between packet and PPCP happens when $F = 1$. This large difference is due to a large number of bits embedded within a packet's header and the preamble needed for synchronization. For larger F, the duration of PPCP increases faster than the duration of the packet. Longer PDU size/duration results in higher collision rates, and therefore, slightly lower (maximum) throughput for when $F \geq 7$. This difference is small since the packet's longer duration corresponding to $\lambda \geq 0.6$ PDU/s/node, results in frequent collisions, thus, resulting in throughputs almost as low as that of PPCP.

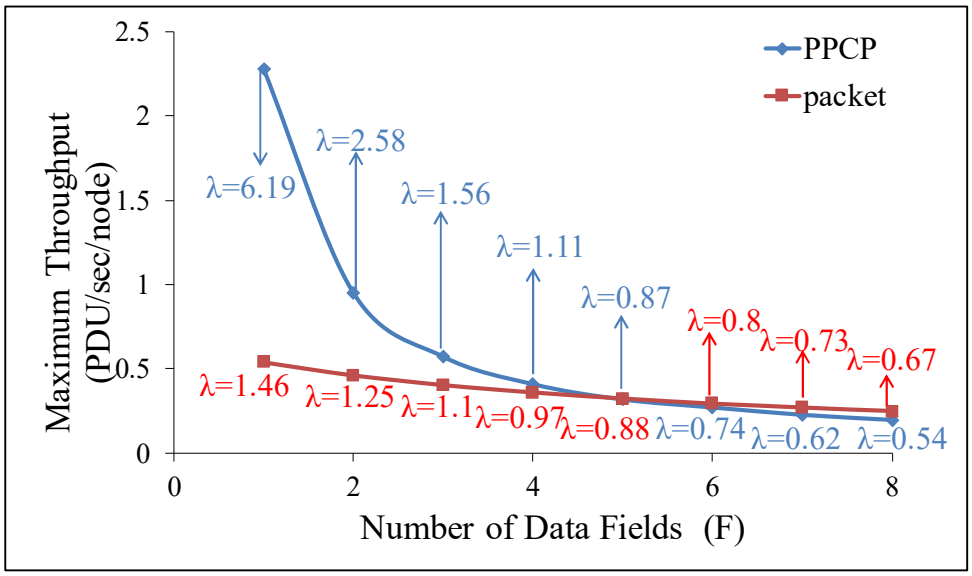


Figure 3.11: Maximum throughput of PPCP and packet

E. Detection of Errors Due to Collisions

Errors in PPCP can occur due to the collision between PPCP received except pulse losses and/or false positives. The PPCP frame-based error detection can be used for both types of errors.

Figure 3.12 presents the performance of detection of errors caused only due to collisions. Experiments are performed for a different number of fields F and the maximum data value δ.

It can be seen in Figure 3.12 that the error detection accuracy is maintained above 91% for any data generation rate approximately smaller than 1.0 PDU/s/node. This means that error detection rules which are based on a PPCP's architectural format can successfully detect more than 91% of the collided PPCP PDUs. When the data generation rate (λ) is less than 0.05 PDU/s/node, it can be guaranteed that among all the PPCP PDUs which are delivered to the upper layer, more than 96% of them are correct.

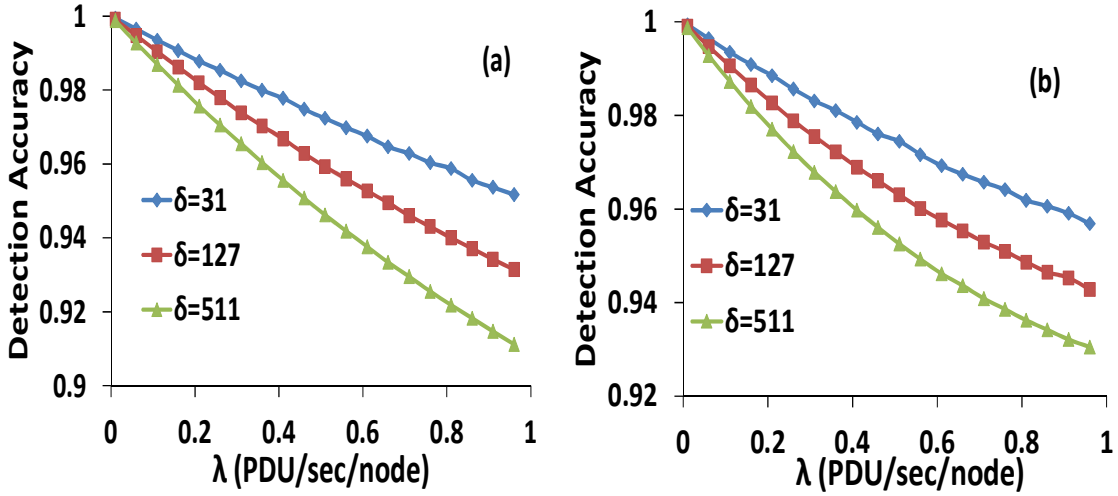


Figure 3.12: Detection accuracy (PPCP errors due to collisions); (a) $F = 3$, (b) $F = 5$

In summary, the error detection accuracy is higher than 93% for any combination of data generation rate λ (PDU/s/node), maximum value δ and number of fields, F. To achieve even higher error detection accuracy rates, a link layer checksum can be added the same way it is added for packets.

3.8. Summary and Conclusion

A new concept, namely, Pulse Position Coded PDU (PPCP) has been developed in this thesis mainly to provide energy-economical data transport compared to traditional packet-based mechanisms. A code compression method called Flexible Base Digit Separation (FBDS) has been developed and shown to solve several architectural challenges in PPCP to achieve superior energy economy while retaining most of the benefits (e.g., throughput, structure, reliability) of the conventional packet-based architecture. Through analytical modeling and simulation-based experiments, it is shown that the proposed PPCP architecture can be an effective means for data transmission in energy-constrained wireless sensor networks.

CHAPTER 4: PPCP FOR MULTI-ACCESS SENSOR NETWORKS

4.1. Motivation

In the previous chapter, we developed a pulse-based PPCP architecture for transmit-only networks to achieve energy-savings. However, the results in [45] did not consider idle-listening energy consumption at receivers and can only be used for one-hop wireless transmission. In multi-hop multi-access networking, a significant amount of energy is consumed during idle-listening, overhearing, and collision-related retransmission, which turns out to be a critical challenge. To address that, this chapter develops a multi-hop multi-access PPCP PDU framework. It also experimentally compares the proposed PPCP framework with a comparable state-of-the-art time-based protocol, namely BLE [73].

4.2. Our approach and contribution

Specific contributions of this chapter are as follows. First, a comprehensive link layer architecture is presented with detailed designs of PPCP-control PDUs and protocol components that are needed for multi-access operation. Second, experimental details and protocol performance are presented for a prototype PPCP hardware platform powered by solar harvested energy. Using low-level operational parameters gleaned from the prototype deployment, a systematic simulation study is presented regarding the multi-access PPCP architecture's inherent ability to detect channel errors in terms of pulse loss, false positives, and collisions in realistic settings. Finally, we include a detailed energy consumption comparison of PPCP vs BLE when used in similar hardware and operational settings.

4.3. Design Objectives

The objective of this chapter is to introduce the multi-access operation of a new link layer architecture [45] that uses Pulse Position Coded Protocol Data Units (PPCPs) instead of traditional packet protocol data unit (PDU) for energy-efficient wireless networking. The key idea is to send a data value δ using two pulses that are sent $\delta + 1$ time units apart (i.e., the one-time unit represents the value zero). Irrespective of the data value being sent, PPCP requires only two pulses, compared to $O(log_2(\delta))$ bits needed for packets. This reduction, however, is achieved at the expense of a transmission delay of $\delta + 1$ pulse durations, which can be larger compared to the packet transmission delay of $O(log_2(\delta))$ bit durations. The architecture employs mechanisms for reducing such transmission delay from $\delta + 1$ to $O(\beta log_\beta(\delta))$ by using a novel Flexible Base Digit Separation (FBDS) mechanism, which separately sends the digits of a base-β representation of the data value δ. The new pulse count is $O(log_\beta(\delta))$, which can still be smaller than the packet bit-count $O(log_2(\delta))$ for appropriately chosen β values.

4.4. Multi-Access PPCP Architecture

4.4.1. Baseline PDU Formation

The previous chapter depicts how a data value can be coded using packet and PPCP abstractions in Chapter 3. In packet mode, a value δ ($\delta \geq 0$) is coded using $\log_2(\delta)$ bits, preceded by ρ bits of preamble needed for physical layer synchronization. Typical packet preamble size is few tens of bytes [12, 13, 11]. The resulting number of transmitted bits is $\rho+\log_2(\delta)$. Although the exact number of bits is determined by the physical layer coding (e.g., unipolar, polar, Manchester coding, etc.), the above expression is generally valid for a high-level comparison.

However, PPCP can introduce a new source of energy drainage, namely, Intra-PDU idle-listening, which can offset the savings in transmission energy as stated above. Intra-PDU idling happens between the transmissions of the start and the end pulses. Energy wastage for Intra-PDU idling on the transmitter side can be mitigated by intra-PDU sleep. On the receiver side, however, such sleep is not feasible since the receiver needs to remain awake for receiving the end-pulses for which the time is not known. We introduce a mechanism called Flexible Base Digit Separation (FBDS) for mitigating the effects of intra-PDU idling.

With FBDS [45], which is a silence compression technique, a value δ is first represented as a multi-digit number in a number system of base β. Then the resulting digits are separately sent using the PPCP format. It should be noted that an FBDS digit 'n' is transmitted as a silence of '$n+1$' pulse durations. For example, the data value 723 can be represented in base-6 number system as 3203. As shown in Figure 3.2, with FBDS enabled, in order to communicate the value 723, a transmitter sends "4", "3", "1" and "4" silent pulse durations separately (representing digits "3", "2", "0", and "3" respectively) with a single pulse delimiting between the silence duration. FBDS effectively reduces the PPCP transmission time from $O(\delta)$ to $O(\beta log_{\beta}(\delta))$, which can be a substantial reduction, especially for large data value δ. This reduction in transmission time also reduces the energy expenditure of intra-PDU idling by the same proportion.

4.4.2. Supporting Multiple Fields Using Pulse Delimitation

Building on the baseline single-field PDU concept, in this chapter we develop a multi-field version in order to support access control and data-link operations. Each field can be used to represent an arbitrary value. Unlike binary coding using a fixed number of bits to represent a value, this design of PPCP benefits the applications in which users can flexibly adjust the resolution of a

field in a PDU. Figure 3.3 depicts an example of PPCP PDU containing four fields. The top part of the figure shows the values of different fields and the corresponding base-6 FBDS digits. In the figure, PPCP pulses are represented by the "1"s and the silence durations are represented by "0"s. The following delimiters are used: "1111" for PDU start, "111" for PDU end, "1" for inter-digit separation, and finally "11" as inter-field separation. Note that these choices of delimiter pulse patterns provide reasonable error resilience as it is discussed previously in Chapter 3. An arbitrary number of fields can be incorporated in a PPCP PDU using the example delimiter formats.

4.4.3. PDU Types for Medium Access Control

RTS/CTS (Request to Send / Clear to Send is the contention avoiding mechanism used by the 802.11 families of multi-access protocols [29]. This traditional protocol can be supported using the above multi-field PPCP PDUs. Figure 4.1 shows an example implementation of RTS, CTS, and EOT (End of Transmission) control PDUs and Data PDU used for the experiments presented in this chapter.

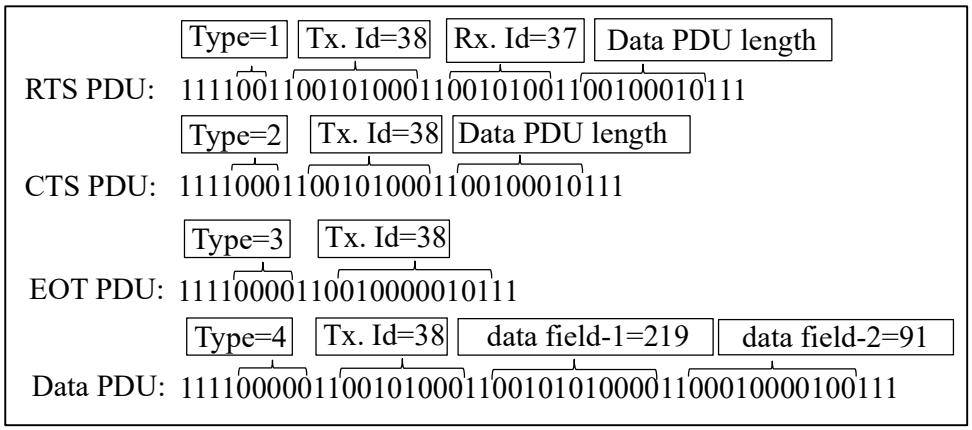


Figure 4.1: Example RTS, CTS, EOT Control PDUs and Data PDU with FBDS silence compression

The access protocol using RTS/CTS/EOT and Data PDU transmission are briefly summarized as follows. When a node wants to transmit, it sends a PPCP RTS with the length of the intended Data PDU and the receiver Id. If the receiver is ready to receive, it replies to the sender with a PPCP CTS, containing the length of the Data PDU. Meanwhile, any other node that hears RTS or CTS should remain silent to avoid conflict until the sender successfully receives EOT from the receiver. The entire procedure is shown in Figure 4.2.

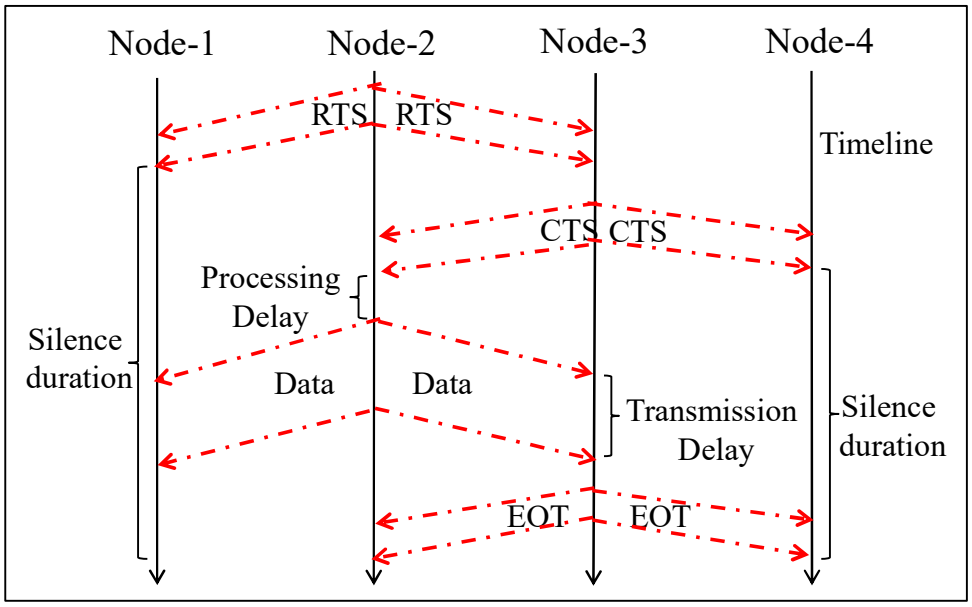


Figure 4.2: PPCP-based multi-access Data transmission

4.4.4. Compatibility with Lower- and Upper-layer Protocols

PPCP is a link layer coding scheme designed for low energy budget networks. The architecture itself possesses reasonable error detection ability. As a link layer mechanism, PPCP is compatible with the usual lower- and upper-layer protocols used for traditional packet-based communication. For example, PPCP can be implemented with both reservation- and contention-based MAC protocols. More advanced techniques such as channel hopping in TSCH [35] and BLE, can also be used by PPCP to increase robustness against external interference and persistent

multi-path fading. Simultaneously, energy-efficient routing protocols or the well-known protocol stacks designed for sensor networks (6LoWPAN, WirelessHART, etc.) can be implemented using the PPCP architecture. To summarize, with suitable adaptations, most of the existing packet-based MAC and routing layer protocols can be used in conjunction with the PPCP framework.

4.5. Prototype PPCP Implementation

A prototype system has been developed for experimental functional validation and performance evaluation of the proposed PPCP architecture, and to compare it with BLE and traditional packets.

4.5.1. Protocols Transceiver Hardware

Table 4.1: Current input under different working modes

Mode	Transmitting logical high	Transmitting logical low	Receiving	Idle listening
Current (mA)	6.17	0.03	3.78	3.77

We have chosen a simple 434MHz transceiver [74], which is capable of sending pulses using on-off-keying at a very low energy budget. The transmitter has two operating modes of transmitting logical high (a pulse or a bit "1") and logical low (silence or a bit "0"). The receiver also has two operating modes: idle-listening and reception of a pulse. Table 4.1Table 4.1: Current input under different working modesshows the current consumption for the above four modes. It can be seen that idle-listening and receiving have almost the same current consumption, thus further indicating the need for designing a link layer with minimum idle-listening.

For all the presented experiments, $5V$ power supply was used for maintaining a practical transmission range of at least 18 meters. The corresponding power expenditures for transmitting

logical high, transmitting logical low, and receiving (or idle-listening) are 30.85mW, 0.15mW, and 18.9mW, respectively. Note that PPCP can be implemented using any standard transceivers using their native modulation mechanisms for sending individual pulses. The modulation mechanism may influence the specific energy expenditure profile and its relative benefits in comparison to packets.

4.5.2. Pulse Loss and False Positives

As outlined in Chapter 3, pulse losses and false positive detection can significantly influence the efficacy of the proposed PPCP framework. Table 4.2 reports such errors measured experimentally using the transceiver described above.

Table 4.2: Pulse Error Rate (pulse loss rate and false positive rate)

Duty cycle	Pulse width	150 μs	200 μs	250 μs	300 μs
50%	PLR	$3.5{\cdot}10^{-4}$	$9.3{\cdot}10^{-5}$	$6{\cdot}10^{-7}$	$3.2{\cdot}10^{-7}$
	FPR	$5{\cdot}10^{-6}$	$2.25{\cdot}10^{-6}$	$8{\cdot}10^{-6}$	$5.9{\cdot}10^{-6}$
1%	PLR	$4.7{\cdot}10^{-5}$	$3.6{\cdot}10^{-5}$	$8{\cdot}10^{-7}$	$2.7{\cdot}10^{-8}$
	FPR	$2{\cdot}10^{-4}$	$9{\cdot}10^{-5}$	$7{\cdot}10^{-6}$	$5.3{\cdot}10^{-6}$

The width of a PPCP pulse turns out to be a key design parameter. While a wider pulse can improve transmission reliability (i.e., fewer pulse losses), it leads to more transmission energy consumption. Table 4.2 reports the average Pulse Loss Rate (PLR) and False Positive Rate (FPR) measured for different pulse widths with 10 pairs of transmitters and receivers. The distance between the transmitter and the receiver was set to 20 meters during all these experiments. We have also varied the duty cycle, which affects the pulse repetition period, in the range from 1% to 50%. This range reflects the expected separation between pulses in typical PPCP PDUs. From the reported numbers in Table 4.2, it can be seen that pulse width with 250 μs can give acceptably

low PLR and FPR, both below 10^{-5}. Based on these findings, a pulse width of 250 μs is chosen for all our subsequent protocol implementation.

4.5.3. Received Pulse Distortion

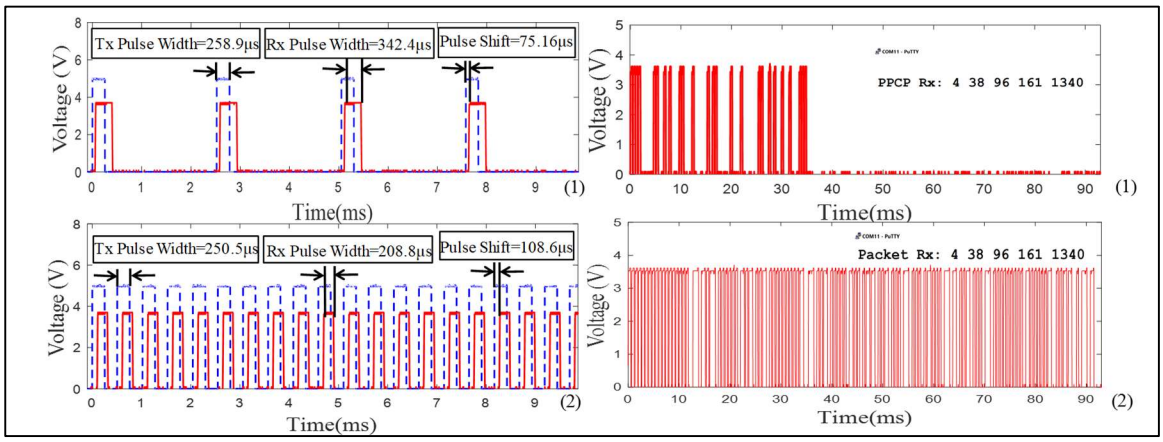


Figure 4.3: Oscilloscope plots for pulses and PDU reception with 250 µs pulse width.

Figure 4.3 depicts transmitted and received pulses as well as packet and PPCP PDUs formed using such pulses. During our experiments, Oscilloscope MSO 2024B is used to capture all the plots and data. As shown in Figure 4.3(a.1) with pulse transmission and reception with 10% duty cycle and Figure 4.3(a.2) pulse transmission and reception with 50% duty cycle. It can be seen that a received pulse can differ from the corresponding transmitted pulse both in terms of its width and position. Such drifts in position and width generally result from the shape of the demodulated analog signal and its impacts on the digital comparator that eventually produces the received digital pulse. One way to mitigate the impacts of those drifts is to use a local slot structure as follows.

A node transmits a pulse at the start of a Pulse Slot with size τ. The transmitter can send the next pulse only after the pulse slot duration τ such that it is guaranteed that only one pulse's rising edge can appear at the receiver within a pulse-slot duration, even if the pulse is shifted. Since

pulse shifts can be variable, τ needs to be dimensioned such that a receiver can unambiguously retrieve the correct number of silence durations between the start and end pulses within a PPCP PDU. Let S_{min} and S_{max} are the minimum and maximum pulse shifts respectively. These quantities depend on the hardware characteristics including transceiver operating range, supply voltage, detection voltage threshold, and can be computed experimentally for a target transceiver. In the absence of any shift, or if $S_{max} \ll B$ (B is raw pulse duration), a pulse slot can be chosen equal to the pulse width (i.e., $\tau \approx B$). In the presence of pulse shift, however, a pulse slot τ is determined according to Eq. 4.1.

$$\tau > 2(S_{max} - S_{min}) \tag{4.1}$$

If a slot is chosen according to Eq. 4.1, the receiver can distinguish the number of silence pulse durations (n), irrespective of how the pulse shifts (within the range $[S_{min}, S_{max}]$) alter the arrival time of the start and end pulses encompassing n. The detailed pulse slot dimensioning procedure has been presented in our previous work [45].

Figure 4.3(b) shows the conventional packet and PPCP signal formats implemented on Zero-energy IoT sensor platform (Figure 4.4) and the corresponding receiver serial port outputs, wherein the same information "4 38 96 161 1340" is coded in both PPCP format (Figure 4.3(b.1)) and traditional packet (Figure 4.3(b.2)) format, where "4" indicates the type of the PDU (see Figure 4.1), "38" is Tx id, and the rest of Data PDU $96, 161$, and 1340 are three random field values. For packet implementation, VirtualWire1 library is used in which each message is transmitted as 36 bits training preamble consisting of $0-1$ bit pairs, 12 bit start symbol $0xb38$, 1 byte of

1 VirtualWire is an Arduino library that provides features to send short messages, without addressing, retransmit or acknowledgement, using amplitude shift keying. Supports a number of inexpensive radio transmitters and receivers.

message length byte count n message bytes, and 2 bytes CRC. In PPCP implementation, pulse slot duration of $500\mu s$ and FBDS base (i.e., β) of 6 were chosen. It can be seen in Figure 4.3(b) that under the same pulse/bit width ($250\ \mu s$), for the same data value, PPCPs use only one fourth of the number of pulses that packets use. This provides a pictorial indication of the transmit energy savings of PPCP as compared to the packets. Figure 4.3(b) also shows that the duration of a PPCP PDU is only one-third of the length of the packet PDU. This indicates potentially higher channel utilization efficiency and overall lower energy expenditure.

4.5.4. Solar PPCP Platform

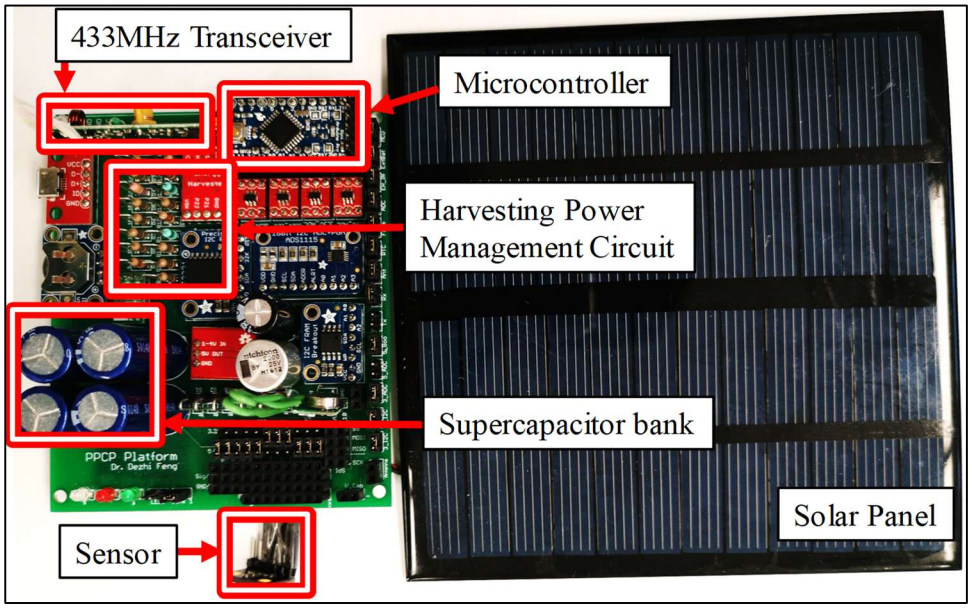


Figure 4.4: Solar Powered Zero-Energy IoT device

In order to demonstrate the above PPCP link layer functions, we developed a prototype Zero-energy IoT device as shown in Figure 4.4. The device is equipped with a modified Arduino Pro Mini [75] for protocol processing and a 433 MHz transceiver [74]. An energy harvesting management circuit is specifically designed for eliminating the noise and spikes during the process of solar energy harvesting. The key components of the IoT device are marked in the picture.

Two such PPCP-enabled Zero-energy IoT platforms have been deployed in Michigan State University Greenhouses (with the size of 20×50 square meters) for agricultural parameter sensing. Each of the two installed units senses and sends data to a PPCP base station which uploads the data in a google firebase server. It should be noted that in this deployment, only point-to-point link layers are used. Multi-access operations are not yet supported. For this specific installation, each IoT module is equipped with a 1.5 Watts solar panel and a 10 volts 2.5 Farads supercapacitor bank.

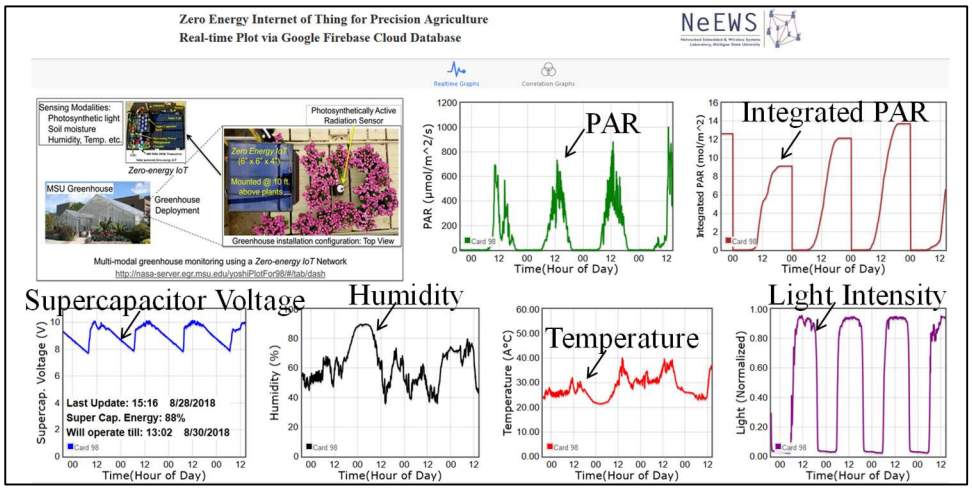


Figure 4.5: Plots of various sensor data from PPCP-enabled greenhouse monitoring

Figure 4.5 shows a snapshot (for a four-day time period) of the available Photosynthetically Active Radiation (PAR), light intensity, temperature, humidity, and the supercapacitor voltage level collected from one of the installed solar-powered IoT units once in every five minutes. The system is now operational for close to two years of uninterrupted greenhouse data monitoring.

Figure 4.6 shows the supercapacitor bank voltage evolution over a 15-day period from December 17, 2017 to December 31, 2017. December is chosen since in Michigan, it is typically a very low-light month. In spite of the low-light condition, the supercapacitor voltage was never

discharged below around 7.3 volts during December and the other winter months. For the PPCP-enabled IoT, the minimum required capacitor voltage was experimentally found to be around 3.61 volts. This explains the extended uninterrupted operation of the system during the low-light months.

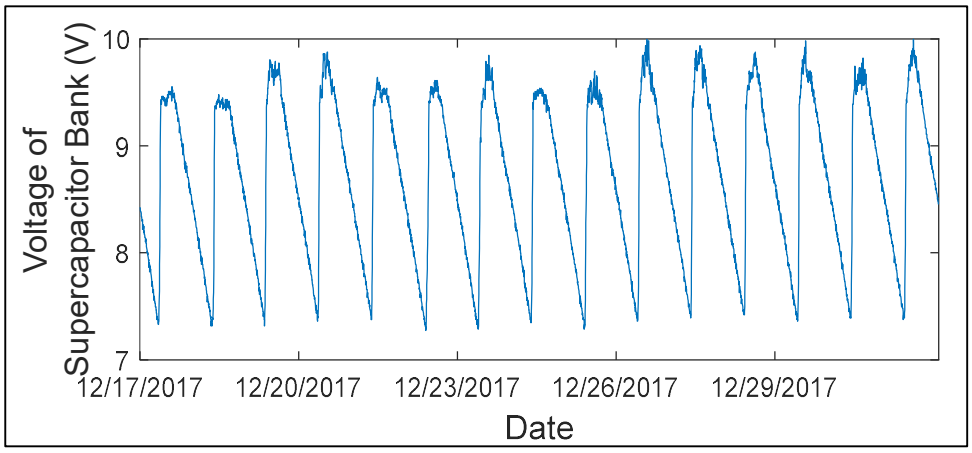


Figure 4.6: Supercapacitor bank voltage for the last 15 days in December 2017

4.6. Optimal FBDS Base Selection

For a given set of system parameters and transceiver energy budget, there is a specific base value for FBDS (see Chapter 3 for its definition) that can minimize the energy consumed by the PPCP protocol. In what follows, using the parameters in Table 4.1, we develop a mathematical model for choosing the optimal FBDS base value β. Note that compared to our previous work [45], this model is more comprehensive in terms of capturing all elements of the energy expenditures including transmission, reception, and idle-listening.

For different maximum value per field δ, there is a finite k that meets inequality $1 \leq \delta/\beta^k < \beta$ $(k \geq 0)$. Each of the $k+1$ digits (remainders with respect to base β) is marked as R_m $(m = k+1, k, \cdots, 1)$. Assuming that for any field value V, V follows a uniform distribution in

$[0, \delta]$, the average number of pulses for one field (including a start pulse and an end pulse) N_{PPCP}, can be computed as follows.

For $k = 0$, $N_{PPCP} = 2$.

For $k = 1$,

$$N_{PPCP} = [2\beta + 3(R_2 - 1)\beta + 3(R_1 + 1)]/(\delta + 1) \tag{4.2}$$

For $k \geq 2$,

$$N_{PPCP} = [2\beta + (\beta - 1)\sum_{n=2}^{k}(n-1)\beta^{n-1} + (k+2)(R_{k+1} - 1)\beta^k + (k+2)\sum_{n=2}^{k} R_n\beta^{n-1} + (k+2)(R_1 + 1)]/(\beta + 1) \tag{4.3}$$

The average duration of a PPCP PDU (i.e., the average transmission delay) L_{PPCP} can be computed as follows:

For $k = 0$,

$$L_{PPCP} = \tau(R_1 + 1)(R_1 + 6)/[2(\beta + 1)] - B \tag{4.4}$$

For $k = 1$,

$$L_{PPCP} = \tau[\frac{1}{2}\beta^2 + \frac{5}{2}\beta + \frac{(R_2-1)(R_2+4)}{2}\beta + \frac{(R_2-1)(\beta+5)}{2}\beta + (R_2 + 2)(R_1 + 1) + \frac{(R_1+1)(R_1+6)}{2}]/(\beta + 1) - B \tag{4.5}$$

For $k \geq 2$,

$$L_{PPCP} = \tau\{\frac{k}{2}\beta^{k+1} + \frac{3k+2}{2}\beta^{k} - \sum_{n=1}^{k-1} 2\,\beta^{n}$$

$$+(R_{k+1} - 1)(\frac{R_{k+1}+4}{2}\beta^{k} + \frac{k}{2}\beta^{k+1} + \frac{3k+2}{2}\beta^{k})$$

$$+ \sum_{m=2}^{k+1}[(R_m + 2)(1 + \sum_{n=1}^{m-1} R_n\,\beta^{n-1})]$$

$$+ \sum_{n=2}^{k}[\frac{R_n+3}{2}R_n\beta^{n-1} + R_n(\frac{n-1}{2}\beta^{n} + \frac{3n-1}{2}\beta^{n-1})]$$

$$+ \frac{(R_1+1)(R_1+6)}{2}\}/(\beta + 1) - B \tag{4.6}$$

The energy consumption for transmitting one PPCP field at the transmitter side is E_{Field}^{Tx}.

$$E_{Field}^{Tx} = N_{PPCP}BP_{Tx}^{High} + (L_{PPCP} - N_{PPCP}B)P_{Tx}^{Low}. \tag{4.7}$$

The power consumption values for pulse reception and idle-listening are almost equal to each other for most wireless sensor motes [37, 38]. Hence, we used the same power expenditure for both these situations in the thesis. Thus, if the energy consumption on pulses' reception and idle-listening during intra-PPCP silence at the receiver side is E_{Field}^{Rx}, then

$$E_{Field}^{Rx} = L_{PPCP}P_{Rx} \tag{4.8}$$

From Eq. 4.7 and Eq. 4.8, it can be calculated that the total energy consumption of transmitting and receiving one PPCP field is:

$$E_{PPCP} = E_{Field}^{Tx} + E_{Field}^{Rx}. \tag{4.9}$$

For given transceiver hardware with power model parameters P_{Tx}^{High}, P_{Tx}^{Low}, P_{Rx} and bandwidth, the optimal FBDS base (β) can be found from Eq. 4.9 for minimizing PDU energy consumption (E_{PPCP}). For instance, a representative transmitter and receiver [74] with $5V$ voltage supply. $B = 250\mu s$ and pulse slot duration $\tau = 500\mu s$ were chosen for PPCP hardware

implementation. The power consumption for pulse transmission, logical low transmission, and PDU reception can be calculated as $P_{Tx}^{High} = 30.85mW$, $P_{Tx}^{Low} = 0.15mW$, and $P_{Rx} = 18.9mW$, respectively. For any value $V \in [0, \delta]$, the average energy consumption of a PPCP field, with maximum value $\delta = 127, 511,$ and 2047, is shown in Figure 4.7 under different FBDS base β. The average energy consumption of a field can be minimized when base β is approximately equal to 6. This result has been used in our simulations.

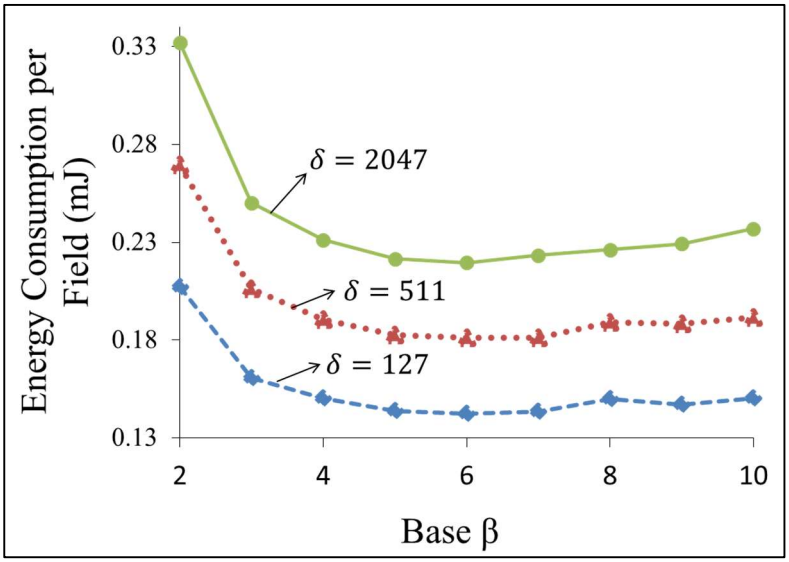


Figure 4.7: Energy consumption per field with different FPDS base β.

For simplicity, value V is assumed to follow a uniform distribution in $[0, \delta]$. FBDS representation of PPCP and the optimal FBDS base β can be calculated based on any distribution or random value in $[0, \delta]$. Similarly, the traditional packet-based data compression techniques can also be implemented on PPCP to shrink the PDU transmission delays. Further advantages of PPCP with FBDS over packets in terms of transmission delays are presented in this Chapter.

4.7. Performance of PPCP

Energy performance of PPCP is analyzed from two perspectives. First, through hardware experiments, state-of-the-art BLE is used as a benchmark to compare with PPCP about energy consumption at the link level due to BLE's outstandingly low energy consumption [27, 73]. Secondly, the multi-access networking performance of PPCP is compared with packets using simulations, in which the parameters are chosen based on the real-life link layer hardware. The performance of PPCP error detection is also deduced in this part.

4.7.1. Error Detection Accuracy

Errors on a PPCP-based link are caused by pulse loss (PL), false positive (FP) detection, and data collision. The performance of error detection is analyzed based on the PPCP architecture itself using a Detection Accuracy, which is defined as the number of correct PDUs delivered to the upper layer as a fraction of the ones decoded by a receiver. Since the impacts of such errors are well understood for packets, they are skipped here.

A. Pulse Loss and False Positive Error Detection

Figure 4.8 shows the effect of pulse loss and false positive on error detection accuracy of PPCP Data PDU with seven fields (Type + Node id + five data fields) using the detection rules. The X-axis shows pulse error rate (either PLR or FPR), which varies in the range from 10^{-4} to 10^{-1}. It shows that detection accuracy is close to 100% when the error rate is less than 10^{-2}. That is true for all maximum data values ($\delta = 31, 127 \text{ and } 511$). Increasing pulse error rate beyond 10^{-1} leads to a severe reduction in detection accuracy. Also, for such a high error rate, detection accuracy is smaller for larger values (δ). This is because, with the increase of the

maximum data value δ, both the silence duration in a PPCP and the duration of each data field increase, and this leads to a higher pulse loss and false positive probability.

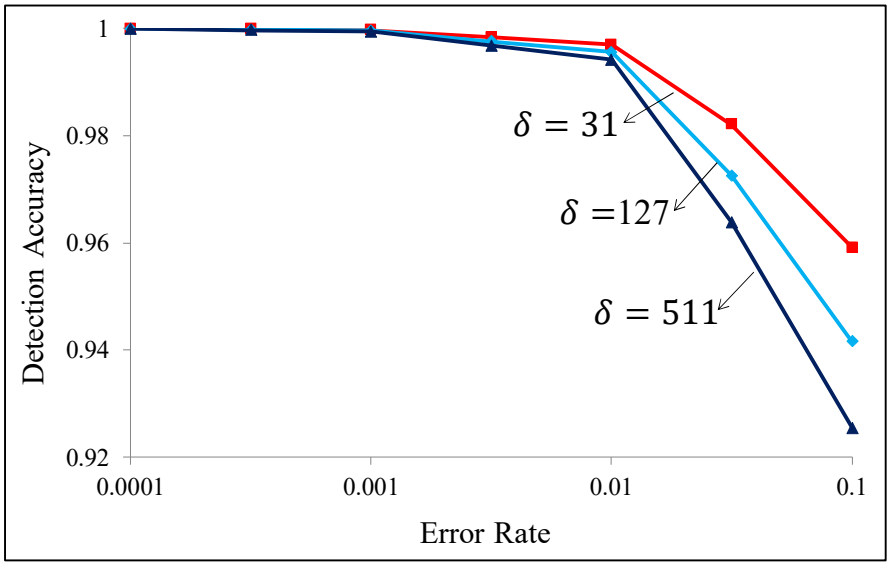


Figure 4.8: PPCP architecture-based error detection

Note that the data field range rule plays a less significant role in error detection with a relatively larger δ. Therefore, a longer PPCP PDU with a larger maximum value per field δ has a lower error detection rate. However, according to our hardware experiments, the probability of both pulse loss and false positive is on the order of 10^{-6} and PPCP error detection performance under this pulse error rate is near 100%.

B. Collision Error Detection

The PPCP architecture-based error detection rules can be also used for detecting errors caused due to collisions in a multi-access environment. Figure 4.9 presents the performance of the detection of such errors with varying Data PDU generation rates λ (Data PDU/s/node). ALOHA is used as the MAC protocol in a 20-node network.

It can be observed in Figure 4.9 that the error detection accuracy with Type-1 PPCP architecture is consistently maintained above 93% for Data PDU generation rates that are smaller than 1 PDU/s/node. This trend holds across a large range of maximum data values (i.e., δ). This indicates that the error detection rules in the PPCP architecture can guarantee that among all the PPCP PDUs which are delivered to the upper layer more than 93% of them are correct. Figure 4.9 also shows that the error detection accuracy decreases with the increase of Data PDU generation rate λ. This is because a relatively larger λ incurs a higher probability of collision, resulting in errors that are missed by the PPCP rules.

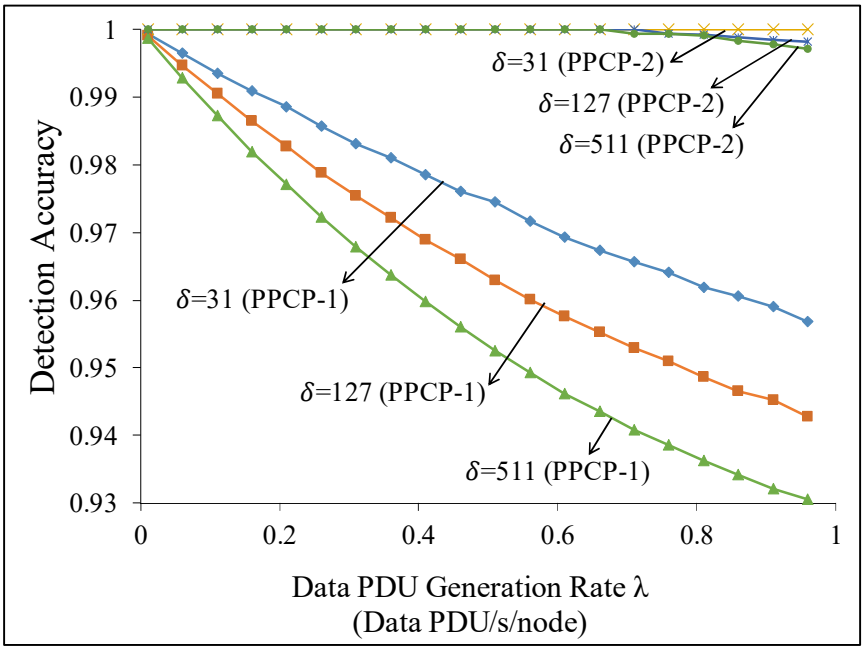


Figure 4.9: Detection accuracy of the PPCP errors caused due to collisions

It can be also observed that for a fixed Data PDU generation rate λ, an increase in maximum data value δ results in a decrease in the error detection accuracy. That is because, with larger δ, the inter-pulse duration between the last delimiter and the trailer (the last three consecutive pulses of a PPCP PDU) increases. That, in turn, increases the collision probability of multiple PPCPs in

a way such that the last FBDS digit of one PPCP gets corrupted by the start of another PPCP. This effect can be seen in Figure 4.10.

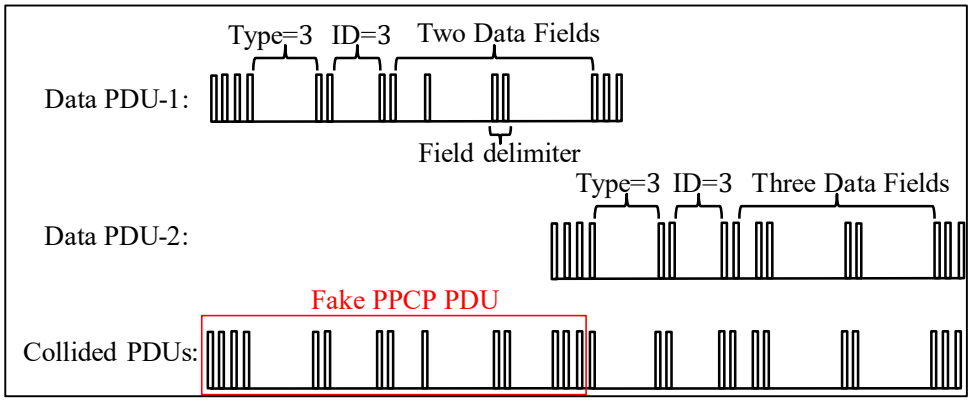


Figure 4.10: Failed detection scenario during PPCP collision

In Type-2 PPCP, however, an extra field, namely, Number of Fields (NoF) is added (see Figure 4.11) in order to enable the error detection rules to be capable of detecting errors shown in Figure 4.10. NoF indicates the number of fields inside a PPCP PDU, including the NoF itself. With NoF and the appropriate augmentation of error detection rules, Type-2 PPCP can achieve more than 99.78% error detection accuracy across δ values as large as 511.

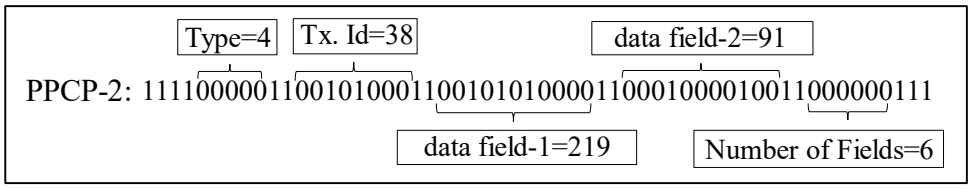


Figure 4.11: Type-2 PPCP (i.e., PPCP-2) with Number of Fields (NoF) information

In summary, PPCP should be able to provide reliable data transmission based on its architectural error detection capabilities alone. To achieve even higher error detection accuracy rates, a link layer checksum, such as a bit parity or Cyclic Redundancy Check (CRC) in the traditional packet, can also be utilized by PPCP.

4.7.2. Energy Consumption

A. Comparison with BLE at the Link Layer

We have used Bluetooth Low Energy (BLE) as the benchmark for energy consumption in order to compare with PPCP at the link layer. BLE is chosen as the benchmark since it brings state-of-the-art performance and power efficiency to typical IoT hardware [27, 73].

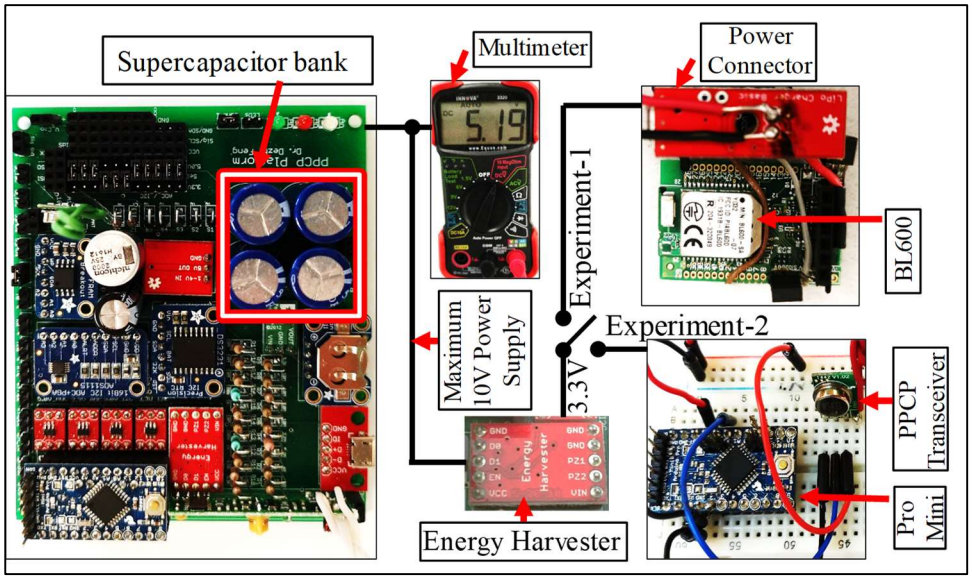


Figure 4.12: System setup for measuring the energy consumption of PPCP and BLE

Figure 4.12 shows the experimental hardware setup in which an energy harvesting and management circuit is used for driving either a PPCP transceiver (e.g., Experiment-1) or a BLE transceiver (e.g., Experiment-2). One of the transceivers is chosen at a time by using a switch. One PDU is transmitted once in every 250 microseconds in both cases. For BLE, we have used BL600 [76], which is a well-vetted and certified BLE module from Laird Technologies. PPCP is implemented in the transceiver [74]. Using the same power harvesting/management hardware [77], which consists of four 10F/10V supercapacitors [78] connected in series, provides a fair way of measuring energy consumption across the PPCP and the BLE cases.

In Experiment-1 (i.e., with BLE), the output 3.3V of energy harvester drives BL600 through a power connector. In Experiment-2 (i.e., with PPCP), a modified Arduino Pro Mini [75] is used as a microcontroller to manage the transmission of PPCP. The instantaneous voltage of the supercapacitor bank is measured by a multimeter for calculating the cumulative energy consumption in each experiment. The cumulative energy consumption ΔE can be calculated through the following formula:

$$\Delta E = \frac{1}{2} C {V_0}^2 - \frac{1}{2} C V^2 \tag{4.10}$$

where $C = 2.5$ Farads is the capacitance of the supercapacitor bank, V_0 is the initial voltage of the fully charged supercapacitors at the start of an experiment. V is the instantaneous voltage of the supercapacitors, which is read from multimeter every 60 seconds.

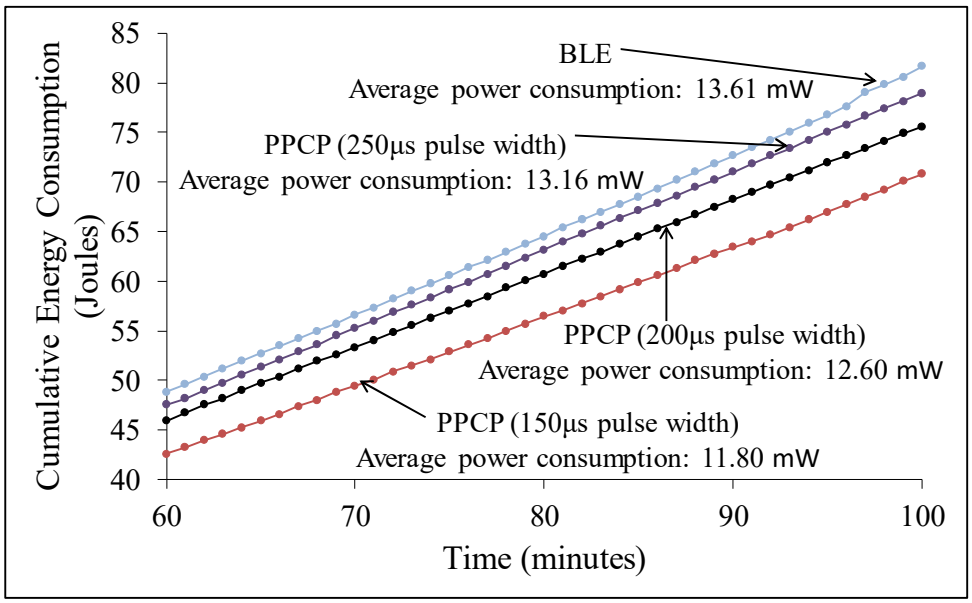


Figure 4.13: Cumulative energy consumption of PPCP and BLE at the link layer

The cumulative energy consumption of PPCP with different pulse widths and BLE are measured with 100 minutes of operation. Figure 4.13 shows the cumulative energy consumption

with the x-axis from the $60th$ minute to the $100th$ minute. The first 60 minutes is ignored because the major differences show up only with a relatively large value. It shows that the PPCP based system with a pulse width of 150 μs can save 13.3% of power consumption compared with BLE for 100 minutes operation. With a larger pulse widths of 200 μs and 250 μs, the corresponding savings are 7.44% and 3.34% compared to the BLE based system. Since BLE uses one-byte preamble and two-byte header in each packet and uses energy for every bit transmitted, such overhead cause it to consume more energy per PDU compared to PPCP. On the other hand, PPCP only transmits a limited number of pulses to represent the PDU and puts transmitters on silence mode (logical "0") for the most time to achieve power-saving.

Note that the energy consumption of PPCP is measured in these experiments based on the prototype hardware setup with a separate microcontroller and transceiver. The performance of energy-saving can be better when PPCP is implemented on a highly integrated hardware platform as used for the BL600 hardware unit. PPCP also provides users higher flexibility to assign arbitrary lengths of a PDU, which cannot be achieved on BLE due to the limitation of bit synchronization [27]. However, compared with BLE, the robustness and security of PPCP still needs to be studied, which will be part of future work.

B. Energy Consumption at the Network Level

Unlike the above experiments, this part of the evaluation is performed using simulation on an 8×8 grid network with 64 nodes (node id $\in [0, 63]$). The objective is to analyze the performance of PPCP and the traditional packet from a multi-access end-to-end networking perspective. From each node, Data PDUs as shown in Figure 5.1 are generated at an average rate of λ Data PDUs per second, following an exponential distribution. Each Data PDU consists of a

certain number of data fields, and the value of each data field is uniformly distributed within the range $[0,\ \delta]$. During the simulation, a various number of data fields are sent in a Data PDU using PPCP or traditional packet format to a receiver, which is randomly chosen from a transmitter's one-hop neighbors, to examine the energy consumption, delay, and throughput.

The energy budget from the baseline 434MHz transceiver is used. The three operational modes, namely, transmitting logical high, transmitting logical low, and receiving (or idle-listening), consume 30.85mW, 0.15mW, and 18.9mW, respectively. Raw bit duration of $250\mu s$ (i.e., a channel rate of 4 Kbps) is used for both packet and PPCP.

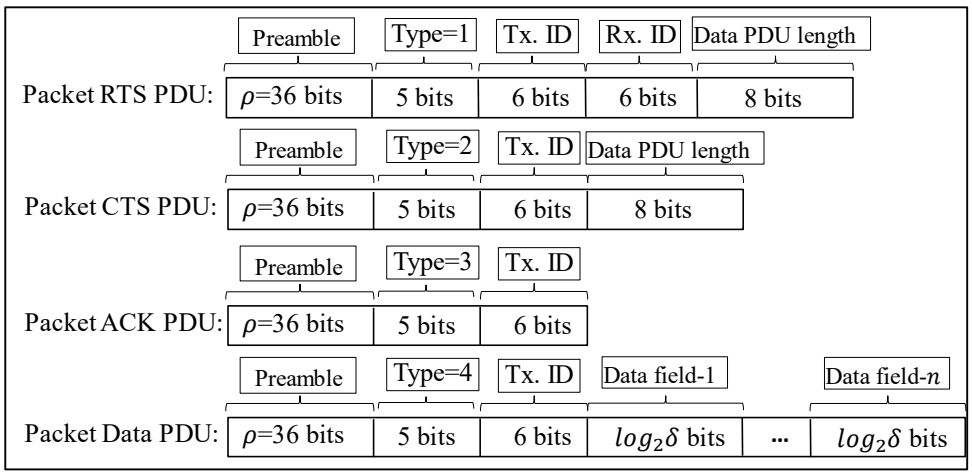


Figure 4.14: RTS, CTS, ACK and Data PDU formats in a multi-access packet protocol

During PPCP simulation, Pulse Slot duration of $500\mu s$ is chosen for each 1s and 0s. FBDS base is set to be 6 as shown in the hardware experiment. During packet simulation, a 36-bit long preamble consisting of alternating 0s and 1s is used for frame synchronization. The values (Type, node id and data values) in PDUs are encoded in the raw binary format as shown in Figure 4.14. The packet in this coding provides a reasonably compact format for performance comparison. A

standard RTS/CTS-based carrier-sense multiple access with collision avoidance (CSMA/CA) protocol is implemented for both the baseline PPCP mechanism and conventional packets.

On-off keying (OOK) modulation is used for both packet and PPCP when energy consumption is calculated. For relatively low energy budget sensor nodes, OOK is a good option because of lower energy consumption compared to PSK [79] or FSK [80] modulation.

Note that the packet implemented in the simulation uses a raw data coding format without considering header, field delimiter, and any binary encoding overheads. Neither parity bits nor cyclic redundancy checksum (CRC) is used during packet transmission. This means that the packet with the minimum energy cost and short transmission delay is used in our simulation to fairly compare with the PPCP's energy cost.

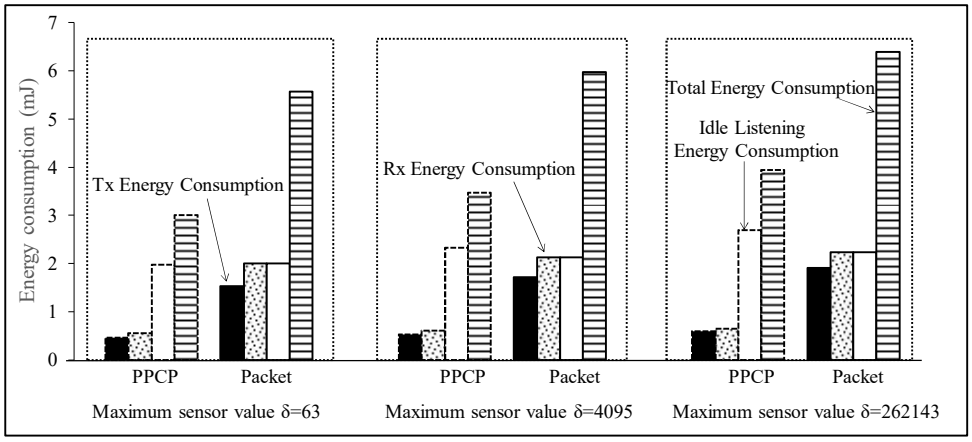


Figure 4.15: Average energy consumption for successfully transmitting one Data PDU

Figure 4.15 shows average energy consumption for successfully transmitting one Data PDU. Each Data PDU contains six fields (Type + Node id + four data fields). Total energy consumption per Data PDU is divided into three parts: transmission, reception and intra-PDU idle-listening. Each bar represents Transmission (Tx), reception (Rx), idle-listening or total energy consumption per Data PDU for successfully transmitting one PPCP or traditional packet Data

PDU. Transmission energy consumption contains the energy for transmitting logical high (“1”) and the energy for transmitting logical low (“0”). Since the energy for sending logical “0” is less than $1/200$ of energy for sending logical “1”, the PPCP architecture makes use of this large difference by transmitting less number of pulses (logical “1”) than silence duration (logical “0”) compared to traditional packet transmissions.

Therefore, it can be seen in Figure 4.15 that transmission and reception energy consumption of PPCP is less than 70% of transmission and reception energy consumption of traditional packet. Even though PPCP achieves the above energy saving at the expense of idle-listening, it does not use a synchronization preamble and its FBDS mechanism can significantly shrink the PDU length, as a result of which the idle-listening energy consumption for PPCP is lower than or equal to that for equivalent packet scenarios as shown in Figure 4.15. Overall, the total energy consumption of PPCP is less than 60% of the total energy consumption of raw binary coded packets.

Besides, packet RTS and CTS have a greater length than PPCP RTS and CTS due to preamble and header, and this causes the packet to have a greater collision probability than PPCP during RTS-CTS exchanges. In view of less number of pulses used in PPCP RTS/CTS than in packet RTS/CTS, retransmission of collided RTS and CTS leads packet into consuming more energy than PPCP.

Figure 4.16 shows the total energy consumption for successfully transmitting one Data PDU with a different number of data fields. It can be seen that with the increase of the maximum value of data field (δ) and the number of data fields per Data PDU, the total energy consumption for PPCP can be up to $2.3mJ$ lower than that of packets. Figure 4.17 shows the percentage of

overall energy saving. In summary, PPCP is shown to be able to provide up to 51% to 92% energy savings depending on the specific physical layer coding methods. Observe the abrupt increase of energy consumption for packet scenarios. This is because a packet PDU uses an 8b/12b DC balance coding [81] at the physical layer. An extra one-bit increase from 8 bits ($\delta = 255$) to 9 bits ($\delta = 256$) or from 16 bits ($\delta = 65535$) to 17 bits ($\delta = 65536$) at the application layer results in using extra 12 bits at the physical layer. Thus, causing the abrupt increase in total energy values. The DC balance coding is necessary for the traditional packet to prevent the cumulation of charge across the coupling capacitor in the receiver, which can prevent error-free reception.

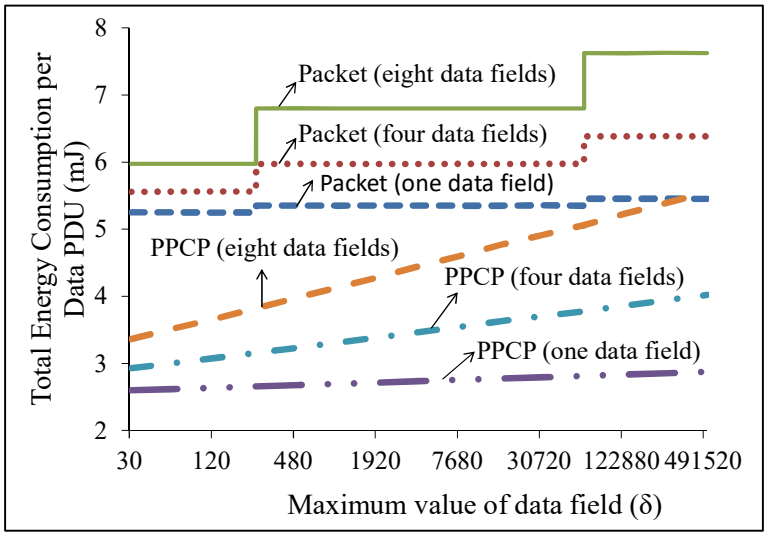


Figure 4.16: Average total energy consumption for transmitting one Data PDU

Figure 4.16 shows the energy consumption of PPCP catches up with that of the packet for a large PDU size. However, PPCP can still maintain an advantage on energy-saving over the traditional packet for a further increase of PDU size. Because a large amount of data incurs packet fragmentation [12, 13, 27] so that the data is transmitted through multiple PDUs. Each packet PDU is associated with the energy overhead of preamble, DC balance coding, header, and the error detection bits. On the contrary, PPCP fragmentation does not involve the overhead. Meanwhile,

users can flexibly adjust the length of a PPCP PDU, unlike the traditional packet which has the limitation of packet PDU size. According to our hardware experiment, PPCP can support up to 60 data fields with the maximum value of each field $\delta = 65535$ in a PDU without extra overhead, which provides PPCP a high energy-efficiency even in a longer PDU.

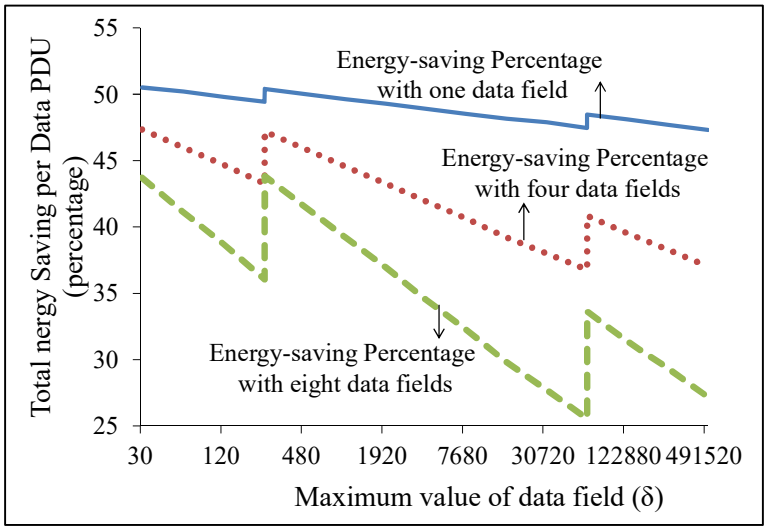


Figure 4.17: Total energy saving percentage of PPCP compared to traditional packet

C. Delay and Throughput

The performance of delay and throughput of PPCP and the traditional packet is analyzed here based on the previous 8×8 grid network simulation. Delay is defined as the time interval between the generation of a Data PDU at the transmitter, and the successful reception of the corresponding ACK or EOT by the transmitter. The delays consist of four components: propagation delay, processing delay, queuing delay, and transmission delay. The propagation and processing delay are negligible due to the high transmission speed of radio wave and high processing speed of the microcontroller.

Figure 4.18 depicts delay as a function of Data PDU (with six fields) generation rate λ in PDUs per second, and the maximum data value δ. Delay can be divided into three periods. 1) When λ is less than 0.39 PDUs/sec/node, the delay per PDU is smaller for PPCP than that for packets. This is because preamble-based packet RTS and CTS have longer transmission delays than PPCP-based RTS and CTS. Further, long packet PDU leads to higher collision probability. 2) When $\lambda \in [0.39, 0.43]$ PDUs/sec/node, the delay of PPCP increases dramatically compared to that of the packets. During this period, nodes have more PDUs waiting in the queue and each node tries to capture the channel to transmit its own PDU.

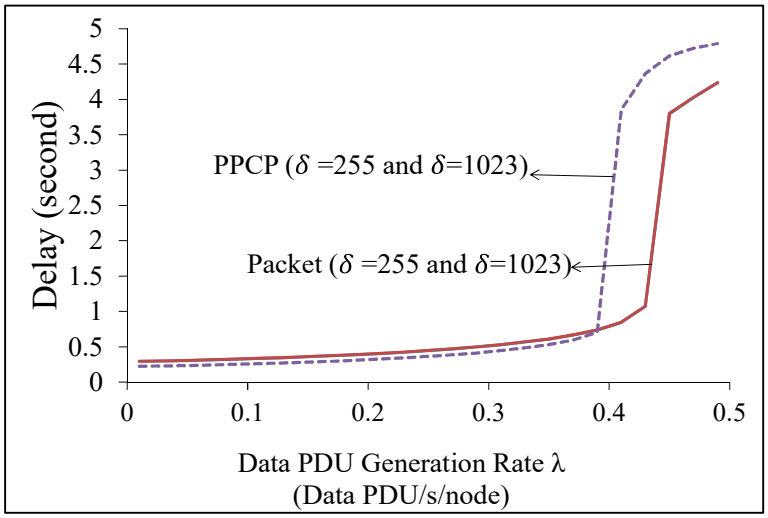


Figure 4.18: Delay Measurement with different Data PDU generation rate λ

It should be noted that the proposed PPCP mechanism is more susceptible to the exposed node problem [82] compared to packets. This is mainly due to PPCP's variable length design. Figure 4.19 depicts a scenario in which two transmitters, namely, Transmitter-1 and Transmitter-2, need to retransmit Data PDUs due to the corruption of their simultaneously transmitted EOTs. For packets, however, since they are coded in raw binary and can have the same Data PDU lengths, the packets can effectively avoid the exposed node problem during ACK transmission. 3) When

Data PDU generation rate λ is more than 0.43 PDUs/sec/node, more collisions kick in and collision-related retransmission brings a greater delay for both PPCP and packet. Still, the varying PPCP PDU length leads to more collisions for PPCP than for packets. The delay characteristics of the sensor nodes in these three periods can be explained by the throughput performance shown in Figure 4.20.

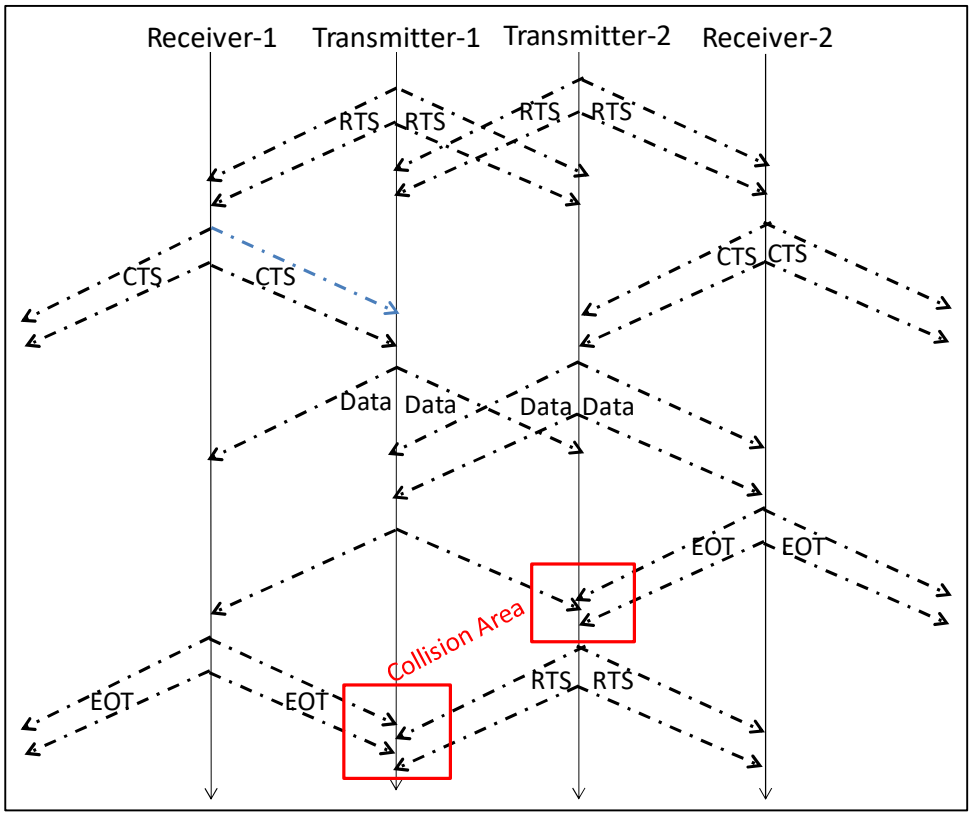


Figure 4.19: Susceptibility of PPCP to exposed node problem

Figure 4.20 shows the throughput performance of both PPCP and packet with the x-axis from 0.3 to 0.5 Data PDU/s/node. For lower Data PDU generation rates ($\lambda < 0.39$ PDUs per node per second), since the multi-access collisions are rare, both PPCP and packet deliver similar throughput (the four curves are overlapping). In the scenario where $\lambda \in [0.39, 0.43]$ and $\delta = 1023$, PPCP Data PDU generation rate greater than the maximum throughput of each node. The

collision can happen frequently during the EOT exchange process due to PPCP's variable Data PDU length as shown in Figure 4.19. However, the packet can avoid ACK collision due to its constant raw binary coding in the simulation. Therefore, the throughput of PPCP drops down abruptly, which is also the evidence for the delay as it goes up drastically in Figure 4.18. When $\lambda > 0.43$ Data PDU/sec/node for both $\delta = 255$ and $\delta = 1023$, packets show a slight advantage on throughput over PPCP due to packet's relatively uniform length.

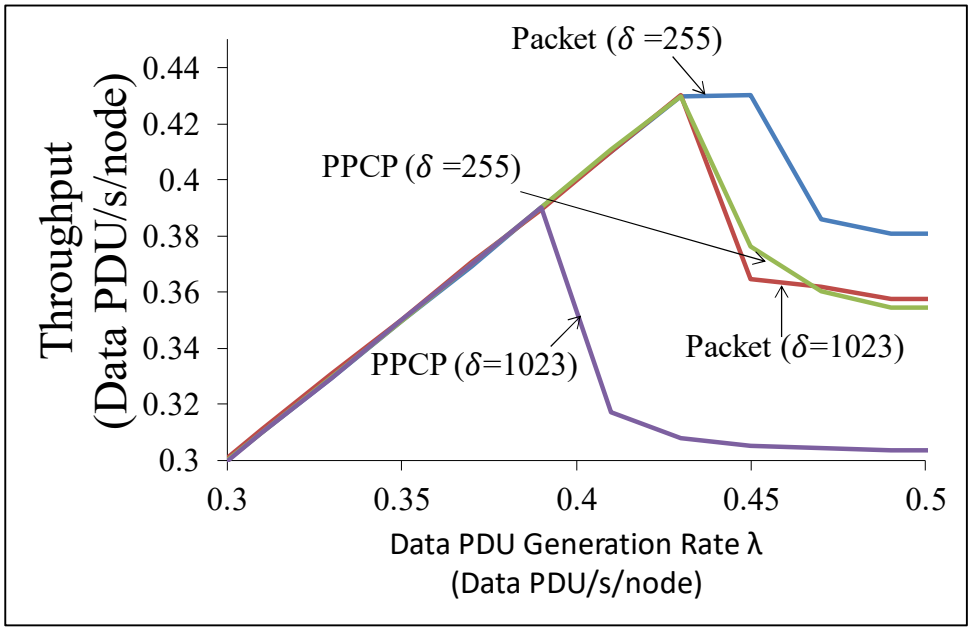


Figure 4.20: Measured throughput for both Packets and PPCP

It should be noted that Figure 4.20 shows the difference in throughput between $\delta = 255$ and $\delta = 1023$ for $\lambda \in [0.39, 0.43]$, but the difference cannot be seen in Figure 4.18 for the delay. This is because the transmission rate of Data PDU with $\delta = 255$ is less than or equal to Data PDU generation rates in this period, but the transmission rate of Data PDU with $\delta = 1023$ is slightly greater than Data PDU generation rates, which leads to a little more collision and the resulting retransmissions for $\delta = 1023$ compared to for $\delta = 255$. Such an increase in collisions cause

slightly more delay for $\delta = 1023$ compared to for $\delta = 255$. However, the caused delay is tens of milliseconds, it cannot be seen in Figure 4.18 when it is drawn at the scale of seconds.

Figure 4.21 shows how a different number of data fields in a Data PDU affects delay with relatively low data flow rate ($\lambda \leq 0.01$ Data PDU/s/node). Note that all the results for the packet are based on the raw binary formatting as shown in Figure 4.14 that does not consider headers, field delimiters, error detection bits, and binary encoding overhead. The packets have the same Data PDU length due to a raw binary coding, which effectively avoids the exposed node problem. For a relatively large maximum value per field (for example, $\delta = 16777215$), the packets can achieve a smaller transmission delay than PPCP. However, different mechanisms of DC balance and synchronization increase the energy consumption and transmission delay overheads of the packet-based protocol. The exposed node problem can cause the additional cost for energy consumption and transmission delay of the traditional variable-length packet.

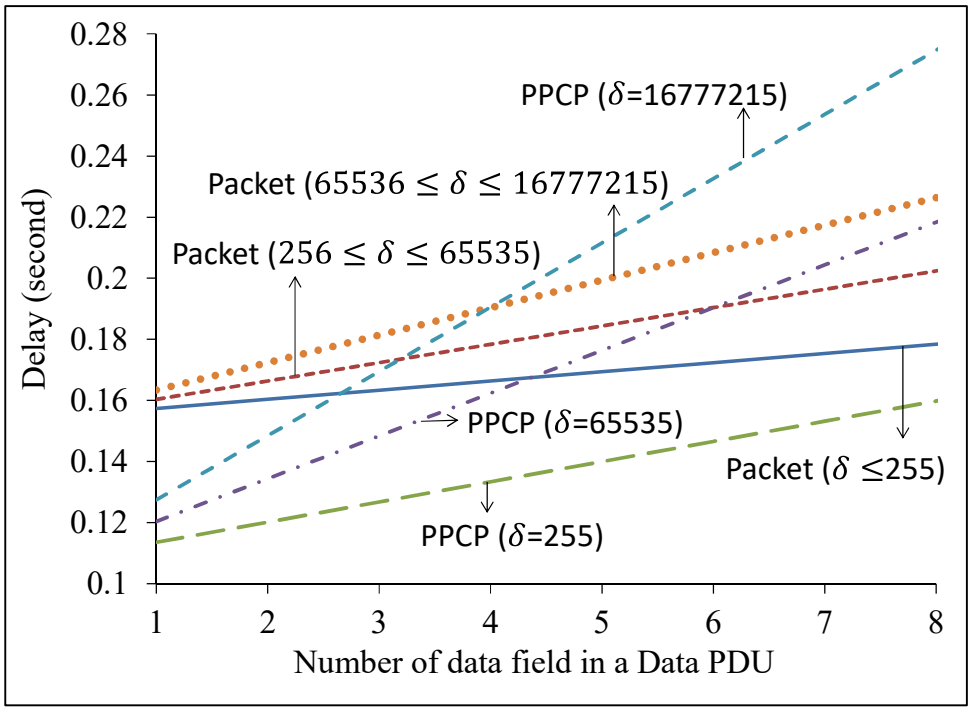


Figure 4.21: Delay with different number of data fields in a Data PDU

D. Architecture Reduction of Inter-PDU Idle-Listening in PPCP

Inter-PDU idle-listening, which is different from intra-PDU idle-listening, is another major source of inefficiency in many sensor network applications. Inter-PDU idle-listening happens when a receiver keeps the radio on during the interval between two PDUs. Few mechanisms [37, 38] have been proposed to periodically put nodes into sleep mode for reducing inter-PDU idle-listening energy consumption, namely, Sleep/Listen Duty Cycle Protocols. PPCP can be adapted to be used within any of the mentioned MAC protocols to save inter-PDU idle-listening energy expenditure. In this Chapter, the comparison of total energy expenditure between packet and PPCP is shown when S-MAC protocol [37] is used on the MAC layer. For sleep/listen scheduling, packet and PPCP use a SYNC PDU as shown in Figure 4.22. The same raw binary coding method is used for the packet as it is discussed in this Chapter.

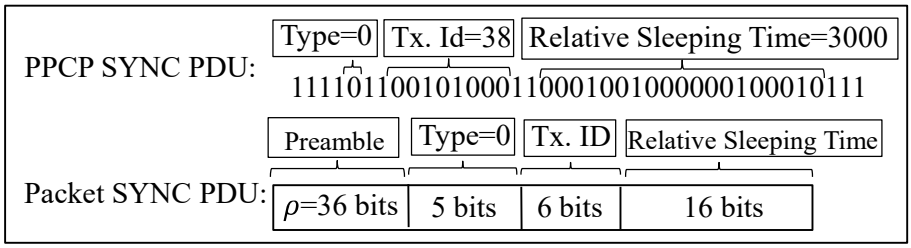


Figure 4.22: Example PPCP and packet synchronization PDU

Figure 4.23(a) shows the total energy expenditure of PPCP and packet with four data fields in a Data PDU, Data PDU generation rate $\lambda = 0.01$ Data PDU/s/node and under different duty cycles based on S-MAC protocol [37]. The number of contention windows for SYNC and RTS are three and five, respectively. The size of the contention window is assigned according to individual sizes of raw binary coding packet-based PDU and PPCP-based PDU, respectively. Such a parameter setup provides the same collision probability and running environment for both packet

and PPCP. Figure 4.3(b) shows energy saving percentage of PPCP compared to legacy packet situation.

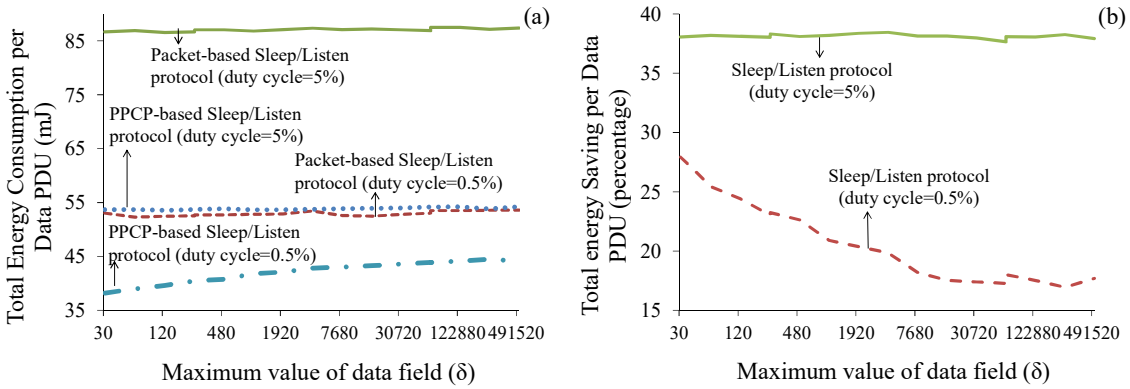


Figure 4.23: Total energy comparison between PPCP and packet in S-MAC

With a relatively small duty cycle 0.5% (large delay for both packet and PPCP), even though PPCP is affected easier by collision than packet due to the diversity of PPCP PDU duration, it can still achieve greater than 17% of total energy savings compared to the packet. For a relatively large duty cycle of 5% (small delay for both packet and PPCP), PPCP can save more than 37% of total energy consumption over the packet. This is because PPCP has shorter sized RTS and CTS, thus sensor nodes can go into sleep mode earlier than the packet in each cycle. It can be seen that PPCP energy saving percentage increases with the increase of duty cycle in Figure 4.23(b). Note that selecting the optimal duty cycle for shortening the delay is out of the scope of this thesis and can be adopted from existing techniques (e.g., [37, 38]).

Compared with traditional packets which are coded in raw binary coding, PPCP also shows an energy saving benefit after implementing a Sleep/Listen Duty Cycle Protocol. According to the hardware experiments, PPCP can save energy up to 65% or higher of the total packet energy consumption if the traditional packet is in standard ASCII coding.

4.8. Summary

A novel energy-efficient pulse position-coded protocol data unit (PPCP) paradigm has been developed in this chapter mainly to provide energy-economic data transport in a multi-access network. This mechanism achieves significant energy savings and shorter delay by using less amount of bits/pulse transmissions and eliminating the preamble and header. Moreover, multi-format PPCPs can effectively reduce idle-listening energy expenditure and allow a large number of sensor nodes to share the common medium without a hidden terminal problem. A concrete hardware implementation is presented which enables deployment of PPCP in IoT applications. Analytical modeling and experiment-based simulation prove that the proposed PPCP architecture can be an effective means for data transmission in energy-constrained wireless sensor networks.

CHAPTER 5: CHAOTIC PULSE POSITION CODED PDUS

5.1. Motivation

Among the techniques for the secure transmission over WSNs, key-based cryptography is a well-known technique towards address security where the sender node encrypts the original data and the receiver node decrypts the received data to obtain an original data. Different types of keys [14] are used in the process of cryptography for solving the security issue in WSNs. However, Cryptography entails a performance cost for extra computation that often increases packet size. Cryptographic hardware support increases efficiency but also increases the financial cost of implementing a network.

Compared with the traditionally key-based cryptographic schemes, chaos-based digital communication chaotic communication system can effectively eliminate the spectral characteristics of the signal by removing any periodicity which is ubiquitous in conventional pseudo-random-based cryptosystems. Chaotic nonlinear techniques are applied in encryption/decryption blocks of the system, which is only known to the desired receiver, significantly enhancing security [83]. Channel encoding/decoding functions with the chaotic technique are also beneficial for immunity to channel fading.

In this chapter, we design a novel concept Chaotic Pulse Position Coded PDU (CPPCP) based on chaotically nonlinear characteristics. The proposed architecture incorporates chaos-based modulation of the inter-pulse time intervals in PPCP in order to provide security for light-weight networking in wireless sensor and IoT networks. A protocol data unit (PDU) is modulated in terms of the silence duration between two sets of wideband delimiter pulses, whose positions are modulated based on the value of the PDU and chaotically nonlinear function. The inter-pulse

interval is set with chaotic alterations, which remove the periodicity from the signal. Compared with the existing binary-based chaotic communication, the multiple data symbols are used to achieve higher randomness by increasing the overlapping area between the inter-pulse intervals for different data symbols in the time domain, as well as noise-like spectral characteristics in the frequency domain. Simultaneously, CPPCP inherits the property of energy-saving from PPCP by sending fewer pulses with a shorter transmission delay. An architecture-based error detection mechanism is designed without adding the link layer and additional energy overhead. Based on hardware experiments, such energy-efficiency characteristic of CPPCP is better suited for thin energy-based IoT sensor networking applications than comparable state-of-the-art solutions such as BLE and legacy binary packet.

5.2. Our approach and contribution

The specific contributions of this chapter are as follows. First, a new chaos-based communication scheme, Chaotic Pulse Position Coded PDU [84], is designed for sensor networks with thin energy budget. Second, a methodology for Pulse Slot technique is developed for compensating the effect of pulse fluctuations and for achieving chaotic signal synchronization. Third, A CPPCP architecture-based error detection scheme for the reliability of transmission without adding the link layer and additional energy overhead. Finally, an energy-harvesting-based sensor platform is specifically designed for implementation.

5.3. Design Objectives

The objective of this chapter is to leverage these chaotic abstractions for implementing security and privacy for a packet-less communication paradigm. Based on our previous work [45], a new chaotic communication architecture is proposed to achieve communication security by

achieving higher randomness between data symbols, lower probability of unambiguity, and significant energy savings by using a smaller number of pulse transmissions than the existing chaotic coding schemes in the literature [54, 55, 83].

5.4. Chaotic Pulse Position Coded PDU Architecture

A new protocol data unit (PDU) architecture CPPCP is proposed towards secure communication in WSNs based on our previous work pulse position coded PDU (PPCP) structure.

5.4.1. Pulse Position Coded PDU (PPCP)

A PPCP PDU architecture was proposed and implemented in Chapter 3. *Flexible Base Digit Separation (FBDS)* was proposed for mitigating the effects of intra-PDU idling. FBDS is a silence compression technique, a value δ is first represented as a multi-digit number in a number system of base β. Then the resulting digits are separately sent using the PPCP format. Figure 5.2 shows an example of the data value 723 represented in base-6 number system as 3203. It shows that with FBDS enabled, the value 723 is transmitted as "4", "3", "1" and "4" silent pulse durations respectively with a single pulse delimiting between the silence duration.

In packet mode, a value δ ($\delta \geq 0$) is coded using $\log_2(\delta)$ bits, preceded by ten of bytes preamble needed for physical layer synchronization [11, 12]. FBDS effectively reduces the PPCP transmission time from $O(\delta)$ to $O(\beta log_\beta(\delta))$, which can be a substantial reduction, especially for large data value δ. This reduction in transmission time also reduces the energy expenditure of intra-PDU idling by the same proportion.

Building on the baseline single-field PDU concept from Figure 3.2, we developed a multi-field version in order to support access control and data-link operations in [45]. Each field can be used to represent an arbitrary value. Unlike binary coding using a fixed number of bits to represent

a value, this design of PPCP benefits the applications in which users can flexibly adjust the resolution of a field in a PDU. Figure 5.1 depicts the representation of an example PPCP PDU containing three fields ($\delta_1 = 161$, $\delta_2 = 3$ and $\delta_3 = 19$) and the corresponding base-6 FBDS digits.

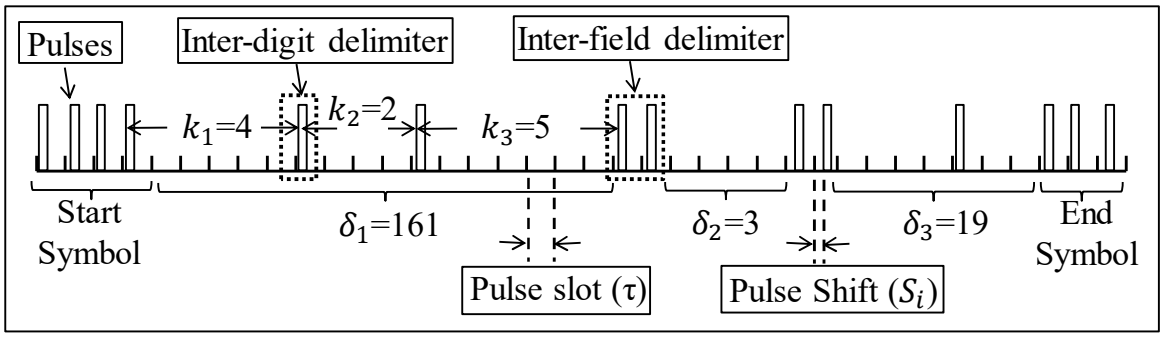


Figure 5.1: Example multi-field PPCP PDU with base $\beta = 6$

A standard PPCP PDU signal with n fields can be described as

$$U(t) = \sum_{j=1}^{n+1} \sum_{i=0}^{\{m_1, m_2, \ \dots, m_n\}} \omega\left(t - \left(k_i^j + 2\right)\tau\right) \tag{5.1}$$

where $\omega(t)$ represents the waveform of a pulse generated at the time $t = \left(k_i^j + 2\right)\tau$. τ is Pulse Slot (PS) to mitigate the impacts of the pulse fluctuations. The dimensioning of the Pulse Slot is developed in Chapter 4. k_0^j ($k_0^j = -1, j = 0,1, \dots, n+1$) is inserted between $\delta_1, \delta_2, \cdots, \delta_n$ as field delimiters.

Note that the Start Symbol and the End Symbol can be designed based on considerations including energy overhead and error-resilience in the presence of pulse losses and false positive detection [45]. In this chapter, the Start Symbol, the End Symbol, and the field delimiter are set as four, three and two consecutive pulses, respectively.

However, such a PPCP architecture cannot provide any security. Without robust security features not only users' information, for example, patients' privacy in health monitoring, can be breached but also adversaries can potentially manipulate/modify actual data resulting in inaccurate transmission and even interception. In the following, CPPCP is proposed based on the nonlinear chaotic function for data secure communication.

5.4.2. Chaotic Pulse Position Coded PDU (CPPCP)

A secure communication PDU format CPPCP is proposed based on the nonlinear chaotic function

$$U(t) = \sum_{j=1}^{n+1} \sum_{i=0}^{\{m_1, m_2, \ \ldots, m_n\}} \omega(t - \left(k_i^j + 2\right)\tau - \theta F(T_{k_i^j})) \tag{5.2}$$

where each pulse is generated at the time $\left(k_i^j + 2\right)\tau + \theta F(T_N)$, and T_N $(N = k_i^j)$ is the time interval between rising edges of the previous two pulses. The sequence of T_N represents iterations of a nonlinear chaotic function $F(\cdot)$, $T_N = F\left(\theta F\left(T_{k_{i-1}^j}\right) - \left(k_i^j + 2\right)\tau\right)$, where k_{i-1}^j is the previously coded digit of k_i^j. θ is a scaling parameter which is used for adjusting the randomness of CPPCP signal and for compensating the difference in charging rate of different receivers' capacitor.

A nonlinear iteration function $F(\cdot)$ can generate chaotic behavior of the map. Research on the design of the chaotic pulse generator can be found in [50, 51]. Tent map is a one-dimension nonlinearly chaotic function with such advantages as the simplified calculation and the robust regime of chaos generation for a broad range of modulation parameters. Here, the utilization of the tent map for the chaotic behavior of CPPCP is investigated:

$$F(X) = \alpha f(X) = \begin{cases} \alpha X & if\ X < \frac{T_{max}}{2} \\ \alpha(T_{max} - X) & if\ X \geq \frac{T_{max}}{2} \end{cases} \quad (5.3)$$

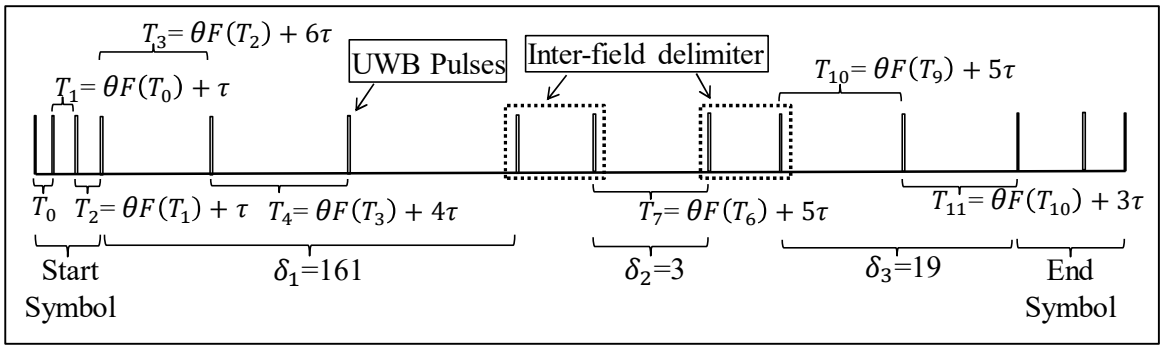


Figure 5.2: CPPCP Example with three-field 161, 3 and 19

Figure 5.2 shows an example of CPPCP architecture with three-field 161, 3 and 19 based on $\alpha = 1.1$, $\theta = 0.4$, base $\beta = 6$. Since chaotical time duration $\theta F(T_N)$ is introduced into the PPCP concept, the inter-pulse intervals in CPPCP are completely different from each other even though the same digit is coded in CPPCP. CPPCP removes any periodicity from the transmitted signal to reduce the spectral characteristics.

During the decoding process, when the chaotic function of the receiver is not matched to the function of the transmitter with enough precision, a decoding error can happen. Therefore, an unauthorized receiver who has no information about the chaotic system cannot determine how long a received pulse was delayed with respect to its original position.

CPPCP also has the advantage of energy efficiency. Compared with the conventional communication technique of sending information as binary strings of bits in Energy-based Transmission (EbT) [41], CPPCP architecture decreases the number of pulse transmission from $O(log_2(\delta))$ in the binary bit string to $O(log_\beta(\delta))$ in terms of base-β representation for an arbitrary data value δ. The energy-saving characteristic can give CPPCP a benefit for applications

with thin energy budget on IoT devices. The parameter, base β, can be carefully chosen for further minimizing energy consumption and transmission delay [45].

5.4.3. Architecture-based Error Detection Mechanism

Based on CPPCP architecture, an error detection mechanism is developed on the top of the physical layer, which is independent of link layer error detection mechanism. Unlike traditional binary packets, PPM [42], MPPM [43], or DPPM [44] which need extra bits or marker for error detection, CPPCP error detection mechanism is established based on the architecture itself without the overhead of extra bits. A comprehensive set of error detection rules is developed for detecting possible errors, due to pulse loss, false positive or collision, etc., based on CPPCP framing context. In summary, an error can be detected if any of the following patterns is violated:

- Format Rule: Start Symbol should consist of four consecutive pulses, and End Symbol should consist of three consecutive pulses. The minimum time interval between two consecutive rising edges is equal to or larger than Pulse Slot.
- Digit Range Rule: The value of each FBDS digit should be in the range between 0 and base β, namely, $\frac{T_n - \theta F(T_{n-1})}{\tau} - 2 \in [0, \beta]$, where T_n and T_{n-1} are the current and previous inter-pulse intervals, where pulse slot τ is specified in next Chapter.
- Inter-Pulse Interval Rule: The current pulse interval T_n should be larger than $\theta F(T_{n-1})$.
- Value Range Rule: Finally, the value of each field should belong to a certain range (i.e., the value of data field $\in [0,\ \delta]$, where δ is the maximum value of each field).

Any deviation from these rules will indicate an error within the CPPCP. Since CPPCP architecture establishes a connection between two consecutive digits through the chaotic system

T_n=$\left(k_i^j + 2\right)\tau + \theta F(T_{k_{i-1}^j})$, an error happening in the process of decoding k_{i-1}^j has a higher probability to be detected in the processing of decoding later digits if the measured inter-pulse duration $\widetilde{T_n} < \theta F(T_{k_{i-1}^j})$, because a small error or perturbation in a chaotic system can lead to a future drastic violation of the coding rules. The further performance of CPPCP error detection will be explained in Chapter 5.7.2.

5.5. Pulse Slot Dimensioning

In hardware implementation of the wideband or ultra-wideband pulse train [85], a received pulse can differ from the corresponding transmitted pulse both in terms of width and position. Such fluctuations in position and width generally result from inherent nonlinear characteristics of hardware and the impact of received analog signal on the digital comparator. Noise, channel distortion, multipath and inter-symbol interference, etc., also affect the position of received pulses [54]. The parameters of a circuit are never the same, and a chaotic analog system brings more difficulty for synchronization of the signals due to the nonperiodic characteristic compared to non-chaotic pulse position modulations. A methodology of *Pulse Slot (PS)* is proposed in this chapter to mitigate the impacts of wideband pulse fluctuations.

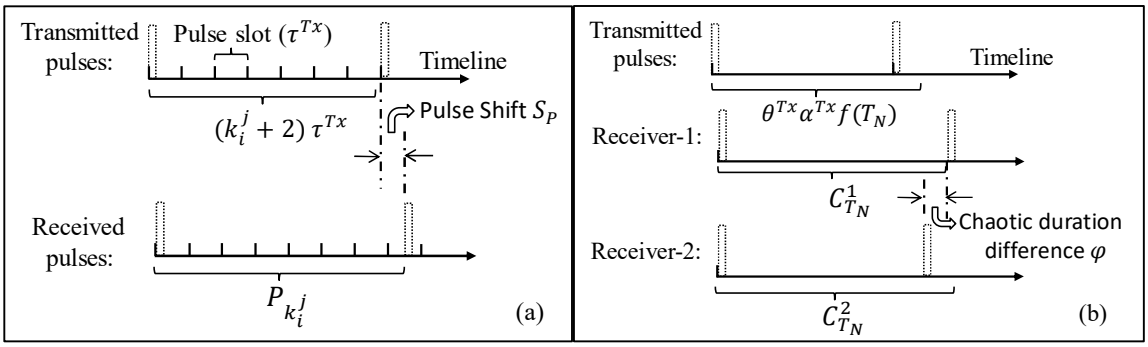


Figure 5.3: Dimensioning of Pulse Slot for chaotic signal synchronization

According to Eq. 5.2, the inter-pulse intervals in CPPCP can be divided into two parts, the deterministic digit time duration - $\left(k_i^j + 2\right)\tau$ and the nonlinear chaotic duration - $\theta F(T_N)$, the process of dimensioning Pulse Slot τ is divided into two stages accordingly. Assume that the receiver system was synchronized up to the $(n-1)th$ pulse in the signal.

1) Impact of Digit Time Duration on PS Dimensioning

A transmitter firstly sends digit time duration $\left(k_i^j + 2\right)\tau$ between two pulses without chaotic function. A receiver records the inter-pulse intervals as $P_{k_i^j}$, and $P_{k_i^j}$ can be given by

$$P_{k_i^j} = \left(k_i^j + 2\right)\tau + S_P \tag{5.4}$$

where $S_P \in [S_p^{min},\ S_P^{max}]$ is pulse shift. Figure 5.3(a) shows the measurement of pulse shift for digit value coding. S_p^{min} and S_P^{max} is the minimum and maximum pulse shift, respectively. S_p^{min} can a negative value.

2) Impact of Chaotic Time Duration on PS Dimensioning

During the qualifying of chaotic time duration, a transmitter sends chaotic time duration $\theta^{Tx}F(T_N) = \theta^{Tx}\alpha^{Tx}f(T_n)$. where θ^{Tx} and α^{Tx} represent the parameters for the transmitter's chaotic function. M $(M \geq 2)$ receivers are receiving the signal simultaneously to measure the inter-pulse intervals $C_{T_n}^L$ $(1 \leq L \leq M)$. Define φ as the chaotic time duration difference between different receivers for the same T_n. Figure 5.3(b) shows the measurement of chaotic function impact on pulse drift. The maximum value φ^{max} of chaotic duration difference between M receivers can be measured as

$$\varphi^{max} = \max_{\substack{i \neq j \\ 1 \leq i,j \leq M}} \left| C_{T_n}^i - C_{T_n}^j \right| \tag{5.5}$$

The dimensioning of the Pulse Slot for CPPCP can be deduced when combining 1) and 2). When an integral CPPCP is transmitted through the channel, the inter-time intervals are $D_{k_i^j}$

$$D_{k_i^j} = P_{k_i^j} + C_{T_n} \tag{5.6}$$

The minimum and maximum inter-pulse intervals are $D_{k_i^j}^{min} = \left(k_i^j + 2\right)\tau + S_p^{min} + \min_{1 \le i \le M} \left|C_{T_n}^i\right|$ and $D_{k_i^j}^{max} = \left(k_i^j + 2\right)\tau + S_p^{max} + \max_{1 \le i \le M} \left|C_{T_n}^i\right|$. If a receiver wants to decode the digit value k_i^j in the signal, it should have the ability to distinguish the time durations which represent different digit values when the chaotic function input T_n is the same. Therefore, the following inequalities should be given

$$\begin{cases} D_k^{max} < D_{k+1}^{min} \\ D_k^{min} > D_{k-1}^{max} \end{cases} \tag{5.7}$$

where k is the coded digit value. The dimension of Pulse Slot (τ) can be obtained from Eq. 5.7 that

$$\tau > |S_P^{max}| + \left|S_p^{min}\right| + \varphi^{max} \tag{5.8}$$

If pulse slot satisfies Ineq. 5.8, a receiver can unambiguously retrieve the value k_i^j in a chaotic signal. The value S_P^{max}, S_p^{min}, and φ^{max} can be easily measured through the experiment.

After the receiver successfully decodes the signal k_i^j in the signal using a measured inter-pulse duration T_n, it should adjust the measured inter-pulse interval $\widetilde{T_n}$ as an ideal value $T_n = \left(k_i^j + 2\right)\tau + \theta F(T_{k_{i-1}^j})$ based on the current k_i^j to avoid cumulation of error. The above procedure provides an efficient way of decoding a chaotic signal. Pulse Slot-based synchronization

can significantly reduce the sensitivity of the pulse train signal to the channel noise and distortions [50].

5.6. Randomness Analysis of CPPCP

In PPM, the raw data is encoded as the data symbols, which can be binary or M-ary or $(\beta + 1)$-ary (CPPCP/PPCP). The data symbols are modulated as the inter-pulse intervals through the communication channel. A specific range of inter-pulse intervals (due to drift of pulse position) represents a unique data symbol. Secure PPM communications achieve security by mixing the inter-time intervals of different data symbols, namely adding randomness (or uncertainties) into the time sequences of the pulse train. Therefore, Randomness can be used to measure the security level of different coding schemes.

Entropy [86, 87] has been used to measure randomness or ambiguities in coding, image processing, and modeling, etc. Specifically, entropy is of described as "amount of randomness" or regarded as a measure of unpredictability [88, 89, 90]. In this thesis, entropy is used to measure the randomness in coding schemes.

Assume that L number of data symbols are used in different PPM coding schemes. Each data symbol appears in the data stream with the probability $P = 1/L$. S represents the entire range of inter-pulse intervals. T_k $(k = 1,2,\cdots,n)$ is a small portion of S, namely $T_k \in S$ and $\sum_{k=1}^{n} T_k = S$. There is no overlapping between T_k and T_{k+1}. The integer parameter x $(x \in [0, L-1])$ is one of the data symbols and $p_{T_k}^{x}$ is the probability of data symbol x whose inter-pulse intervals are falling in T_k. Therefore, $\sum_{T_k\,(k=1,\cdots n)} \sum_{x=0}^{L-1} p_{T_k}^{x} = 1$. According to the definition of entropy, the randomness of x in T_k is:

$$H(x, T_k) = -\frac{p_{T_k}^x}{\sum_{x=1}^{L} p_{T_k}^x} \log_L \frac{p_{T_k}^x}{\sum_{x=1}^{L} p_{T_k}^x} \tag{5.9}$$

where $H(x, T_k)$ is the entropy of a data symbol x in T_k, and $\log_L$ is the logarithm of base L. Eq. 5.9 qualifies the randomness or ambiguities of a data symbol in a small range of inter-pulse intervals from a coding scheme.

Note that when there is no overlapping between inter-pulse intervals of different data symbols in T_k, this means that the inter-pulse interval which falls in T_k only represents one data symbol, Eq. 5.9 becomes $(T_k) = -\frac{p_{T_k}^x}{p_{T_k}^x} \log \frac{p_{T_k}^x}{p_{T_k}^x} = 0$. The randomness in T_k is zero. This is true for all the non-secure communication PPM schemes (BPPM, PPCP, M-ary PPM, and M-ary DPPM). For any inter-pulse intervals which fall in the range T_k, the receiver can correctly decode the symbol without ambiguity.

Based on the definition of entropy Eq. 5.9, the randomness of a coding scheme can be calculated as:

$$H(L, S) = -\sum_{T_k\,(k=1,\cdots n)} \sum_{x=1}^{L} p_{T_k}^x \sum_{x=1}^{L} \frac{p_{T_k}^x}{\sum_{x=1}^{L} p_{T_k}^x} \log \frac{p_{T_k}^x}{\sum_{x=1}^{L} p_{T_k}^x}$$

$$= -\sum_{T_k\,(k=1,\cdots n)} \sum_{x=1}^{L} p_{T_k}^x \log \frac{p_{T_k}^x}{\sum_{x=1}^{L} p_{T_k}^x} \tag{5.10}$$

Based on the different level of randomness in coding, the probability of unambiguity, which is defined as the probability for unauthorized receivers to correctly distinguish different data symbols is

$$Prob(L, S) = \sum_{T_k\,(k=1,\cdots n)} \frac{\sum_{x=1}^{L} p_{T_k}^x}{\left\| \left[p_{T_k}^1, p_{T_k}^x, \ldots, p_{T_k}^x \right] \right\|_0} \tag{5.11}$$

where $\|\cdot\|_0$ is ℓ_0-norm, that is a total number of non-zero elements in vector $[p_{T_k}^1, p_{T_k}^x, \ldots, p_{T_k}^x]$. Multiple data symbols, which have the same inter-pulse intervals, can lower the probability of unambiguity for unauthorized receivers. A further comparison of different coding schemes is given in Chapter 5.7 in detail.

5.7. Performance Analysis

The performance of CPPCP is compared with CPPM [53, 54], Pulse Position Modulation Time Hopping (PPM TH) [91] (key-based cryptographic coding), our previous work PPCP [45], BPPM [92, 93], M-ary PPM [94] and M-ary DPPM [44] using a wideband channel model and hardware experiments based on the prototype of the designed IoT sensor platform.

5.7.1. Channel Model and Network Model

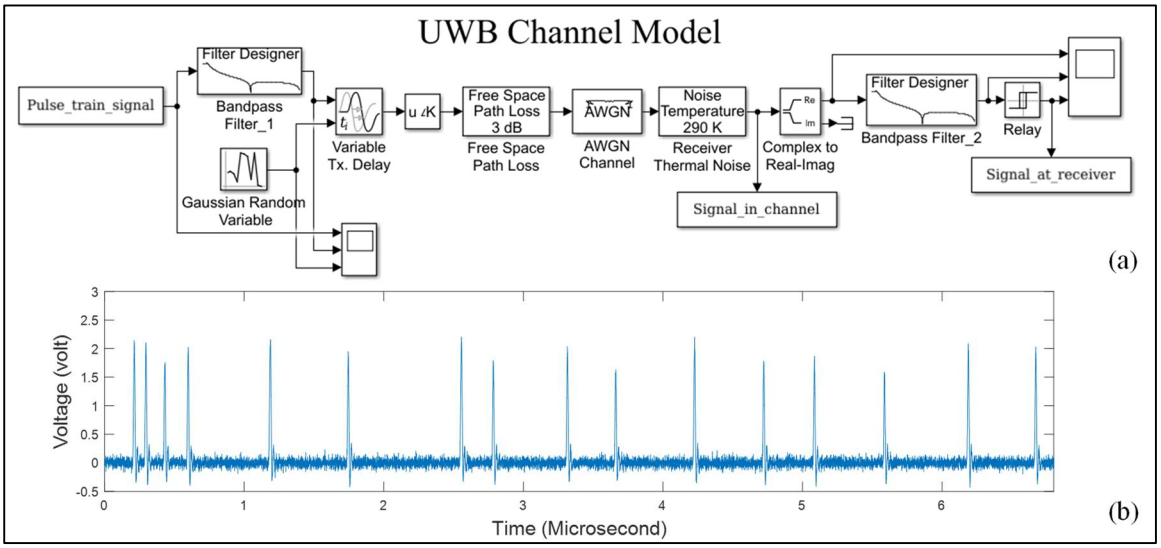


Figure 5.4: (a) Channel model for wideband pulse transmission.

(b) CPPCP with four fields, the field values being 161, 19, and 85 respectively.

A channel model for wideband pulse transmission is designed using MATLAB/Simulink for the performance simulation of all the pulse-based coding schemes. The wideband channel model in this thesis is based on the properties from the related wideband channel research [54, 95, 96, 61, 97, 98]. The parameter setup is from a prototype of sensor platform, which is specifically designed for CPPCP implementation. The channel consists of five components as shown in Figure 5.4(a). The simulated pulse signal in the channel is shown in Figure 5.4(b) with $10\ ns$ pulse width and $100\ ns$ pulse slot size to handle relevant pulse fluctuations which are designed in the model architecture to follow a normal distribution $\mathcal{N}(mean = 2.5 \times 10^{-8},\ std.dev = 0.0083)$.

The first component is a bandpass filter with the passband $1\ kHz$ - $50\ MHz$ to simulate the characteristics of the channel toward eliminating the low-frequency and high-frequency parts of the signal [54]. During the transmission of the wideband pulse train in the air, DC component (low frequency) of the signal cannot go through the channel, since the DC impedance of open-circuited transmission line of the antenna is infinite. The high-frequency part of the signal has greater attenuation due to water or oxygen molecules in the air.

The second component is a variable transmission delay module, which simulates the fluctuations of pulse position and width following a normal distribution [54]. The third component is a Free Space Path Loss module, which is proposed by IEEE 802.15.3a [12] based on average power loss. The last two components are Additive White Gaussian Noise (AWGN) and receiver thermal noise, respectively. Those are ubiquitous in impulse radio wideband communication. Note that since wideband signals are real, only the real part or in-phase component of the channel is considered in the channel model, and the imaginary or quadrature component is set to zero [98]. The parameters in the simulation are based on the implementation of pulse trains on the designed hardware sensor platform.

An 8×8 grid network with 64 nodes (node ID $\in [0, 63]$) is established. To ensure fairness in comparison, a standard RTS/CTS/ACK-based CSMA protocol with the same RTS, CTS and ACK control PDUs are used for all the coding schemes. A Data PDU bearing the same data information is coded using CPPCP, CPPM, PPCP, PPM TH, BPPM, M-ary PPM, M-ary DPPM, respectively. Each coded value δ in a Data PDU follows uniform distribution in $[0, \delta_{max}]$. A standard ASCII coding, without error detection bits, is used for binary-based Data PDU, which is a reasonably compact format for decoding and performance comparison.

5.7.2. Simulation Analysis

The performance of CPPCP, CPPM, PPM-TH, PPCP, BPPM, M-ary PPM, and M-ary DPPM are compared from the frequency domain, the time domain, and the energy efficiency perspectives to demonstrate the key distinctions among these strategies.

A. Frequency Domain Analysis

Spectral characteristics of the above-mentioned seven coding schemes are compared based on the transmitted signals captured by the receiver equipped with a simulated planar monopole receiving antenna. Power spectral density (PSD) is used to measure the strength of the variations (energy) as a function of frequency. The frequency spectrum is expected to show distinct peaks corresponding to any periodic components in the signal.

Figure 5.5 shows the PSDs of channel noise and other seven coding methods. It can be seen that PSDs of PPCP, BPPM, 4-ary PPM, and 4-ary DPPM show peaks due to the periodic repetition of the pulses with the characteristic frequency $\sim 3\ MHz$, $\sim 10\ MHz$, $\sim 2.5\ MHZ$ and $\sim 4\ MHz$, respectively. Each peak corresponds to a unique data symbol in terms of inter-pulse intervals.

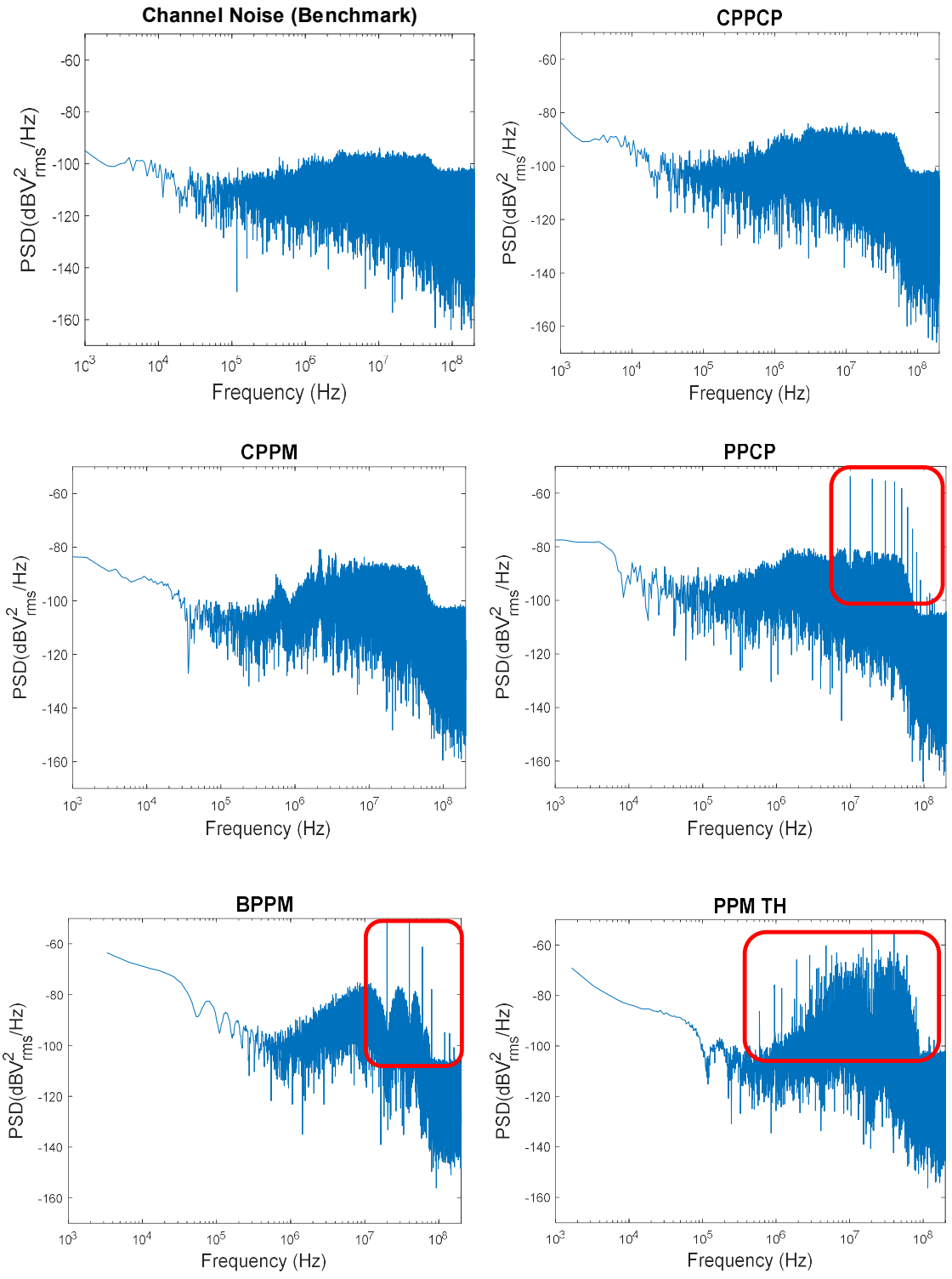
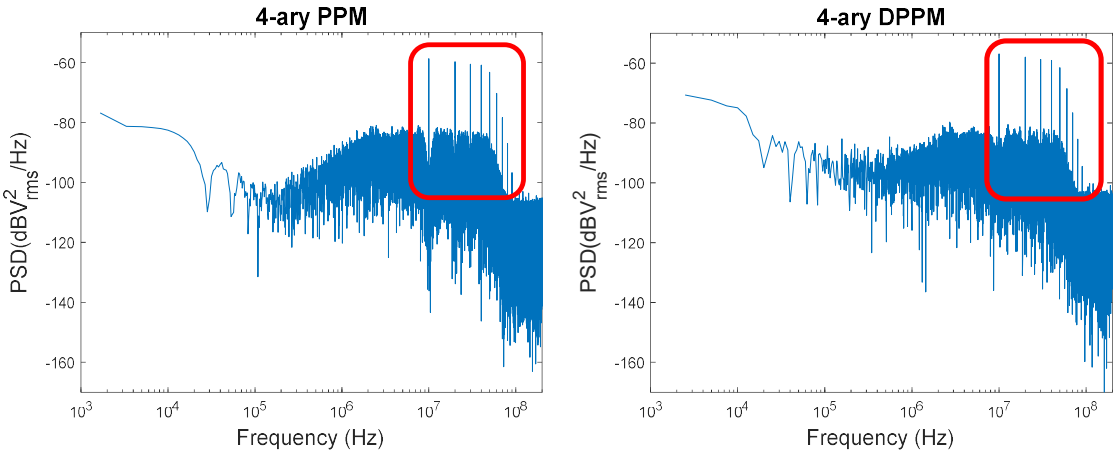


Figure 5.5: Power spectral density of CPPCP, CPPM, Channel noise, PPCP, BPPM, PPM TH, 4-ary PPM and 4-ary DPPM.

Figure 5.5 (cont'd)



Traditional key-based cryptographic communication schemes rely on changing the inter-pulse interval sequences according to the shared key between transmit and receiver to add ambiguities into the data symbols, this method is also called as pseudo-random-based cryptography. However, the pseudo-random sequences eventually repeat, and the digital character of the algorithm in traditional pseudo-random-based schemes is introduced into the signal features associated with the corresponding quantization [54]. PPM TH, as a pseudo-random security scheme, is implemented, and the peaks of PPM TH PSD shows periodicity due to the quantization in the pseudo-random time interval sequences at $\sim 8\ MHZ$. Since PPM TH introduces randomness between different data symbols to achieve security, the spectral plot of PPM-TH shows more peaks. Unauthorized receivers can still exploit these spectral features to intercept such pseudo-random-based pulse train transmission.

The PSD of the channel noise is used as a benchmark due to its characteristic of the frequency spectrum. Chaos-based security schemes, CPPCP, and CPPM, avoid the above-mentioned and shows almost the same spectral characteristics as channel noise as shown in Figure 5.5. This is because the inter-pulse intervals are chaotically changing in these cases, and the

periodicity in the signal is eliminated from the pulse train. This illustrates the advantage of a chaotic system on achieving a low probability of intercept (LPI) over conventional pseudo-random secure schemes in the frequency domain.

B. Time Domain Analysis

When a data-bearing signal is transmitted in the air, the energy level of the transmitted pulse is always higher than the energy level of noise so that the receiver can detect the existence of the signal. This leads to the risk of interception i.e. unauthorized receivers can measure the energy level of the signal in the time domain to detect the existence of the pulse train. Therefore, the security of code in the time domain is very important to ensure covert communication.

Figure 5.6 shows the distribution of inter-pulse intervals for different data symbols across various mechanisms. (a), (b), (c) and (d) in Figure 5.6 are the distribution diagrams for non-secure coding schemes BPPM, PPCP, 4-ary PPM, and 4-ary DPPM, respectively. It shows that 4-ary DPPM and PPCP shows the clear boundaries between inter-pulse intervals for each data symbol. Unauthorized receivers can easily distinguish the data symbols using the measured inter-pulse intervals. BPPM and 4-ary PPM show the overlapping inter-pulse intervals between multiple data symbols. However, this ambiguity can be eliminated from the previously coded data symbol. For example, in 4-ary PPM, if a receiver gets an inter-pulse interval which falls in the range of $[300ns,\ 350ns]$, this can be coded as three kinds of data symbols $(0, 1, \text{or } 2)$. If the previously coded symbol is 2, then the current symbol should be 1 (eliminating the possibility of 0 and 2) without ambiguity. Therefore, 4-ary DPPM, PPCP, BPPM, and 4-ary PPM do not provide randomness between the data symbols, namely, $H_{4-ar\ \ DPPM} = H_{4-ary\,PPM} = H_{BPPM} = H_{PPCP} =$ 0 (i.e. the randomness is zero) as shown in Table 5.1.

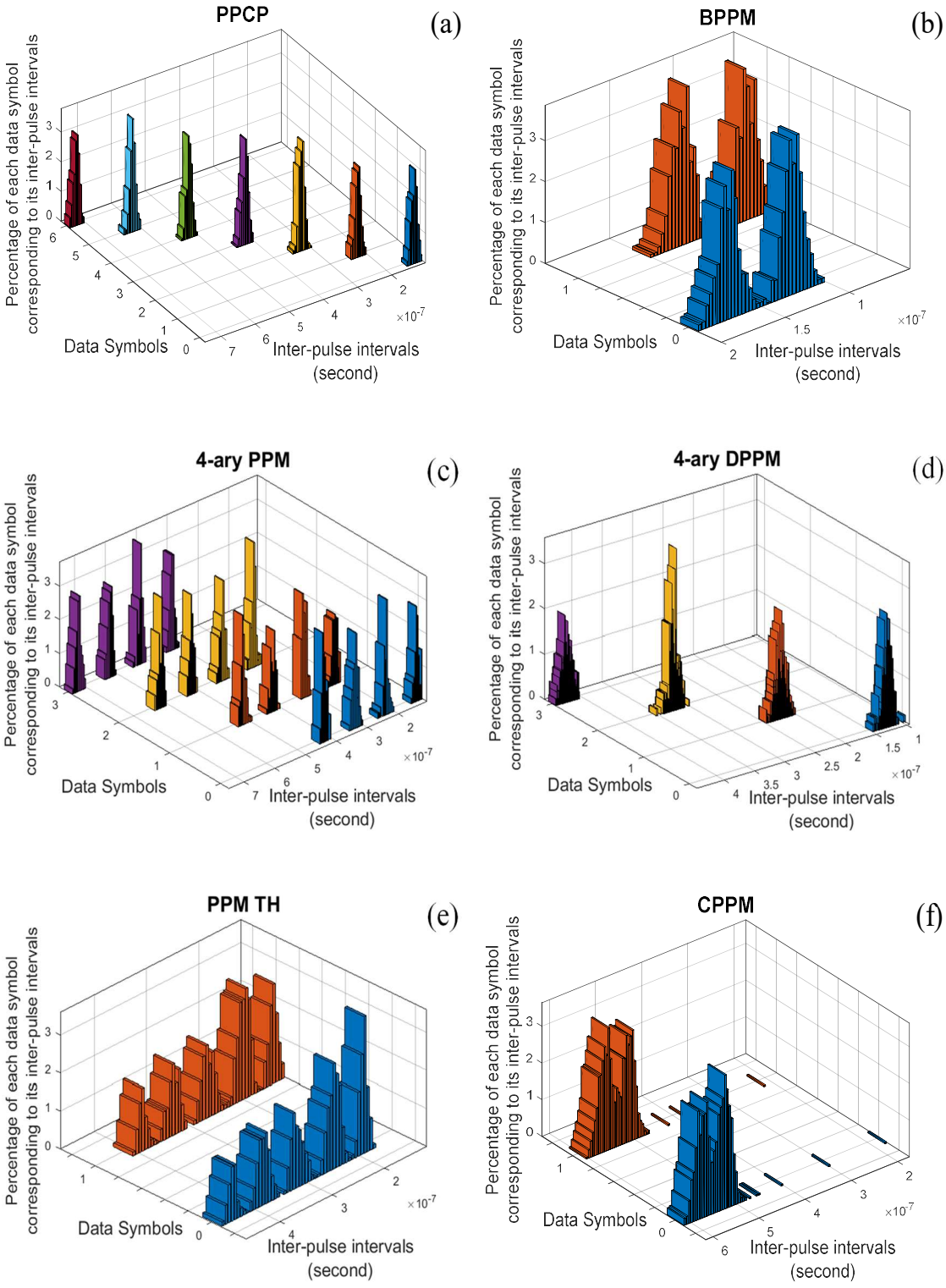


Figure 5.6: The distribution of inter-pulse intervals for different data symbols across various mechanisms

Figure 5.6 (cont'd)

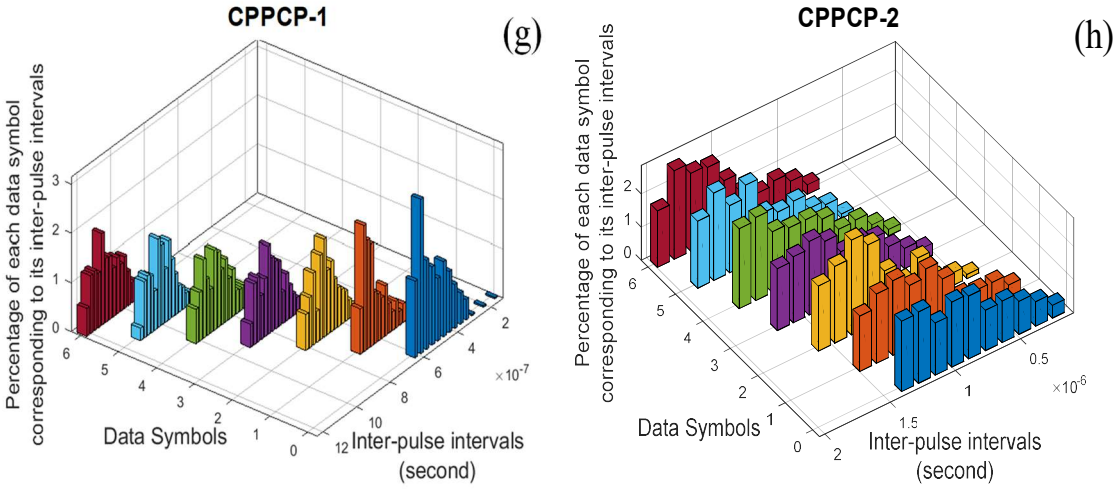


Table 5.1: The randomness (entropy) and the probability of unambiguity

	Randomness (entropy)	Probability of unambiguity
PPCP (Figure 5.6(a))	$H_{PPCP} = 0$	$Prob_{PPCP} = 1$
BPPM (Figure 5.6(b))	$H_{BPPM} = 0$	$Prob_{BPPM} = 1$
4-ary PPM (Figure 5.6(c))	$H_{4-ary\ PPM} = 0$	$Prob_{4-ary\ PPM} = 1$
DPPM (Figure 5.6(d))	$H_{DPPM} = 0$	$Prob_{DPPM} = 1$
PPM TH (Figure 5.6(e))	$H_{PPM\ TH} = 0.812$	$Prob_{PPM\ TH} = 0.426$
CPPM (Figure 5.6(f))	$H_{CPPM} = 0.897$	$Prob_{CPPM} = 0.483$
CPPCP-1(Figure 5.6(g)) with chaotic parameters $\alpha = 1.1, \theta = 0.2, T_{max} = 1.5$	$H_{CPPCP-1} = 0.609$	$Prob_{CPPCP-1} = 0.392$
CPPCP-2 (Figure 5.6(f)) with chaotic parameter $\alpha = 1.1, \theta = 0.6, T_{max} = 1.5$	$H_{CPPCP-2} = 0.934$	$Prob_{CPPCP-2} = 0.193$

(e), (f), (g) and (h) in Figure 5.6 shows the distribution of secure communication schemes – CPPM, PPM TH, CPPCP-1 and CPPCP-2 (with different chaotic parameters and base $\beta = 6$). It is seen that these three secure coding schemes generate overlap between the L data symbols. As a result, unauthorized receivers cannot unambiguously predict the data symbols by measuring the

inter-pulse intervals. By appropriately choosing chaotic parameters as shown in (g) and (h) of Figure 5.6, CPPCP shows the seven overlapped data symbols (six digit symbols and one function symbols) in term of inter-pulse intervals compared to PPM TH and CPPM which only have two overlapped data symbols, CPPCP obtains more randomness between data symbols. Therefore, a relatively low probability of unambiguity is achieved between the seven data symbols in CPPCP as shown in Table 5.1.

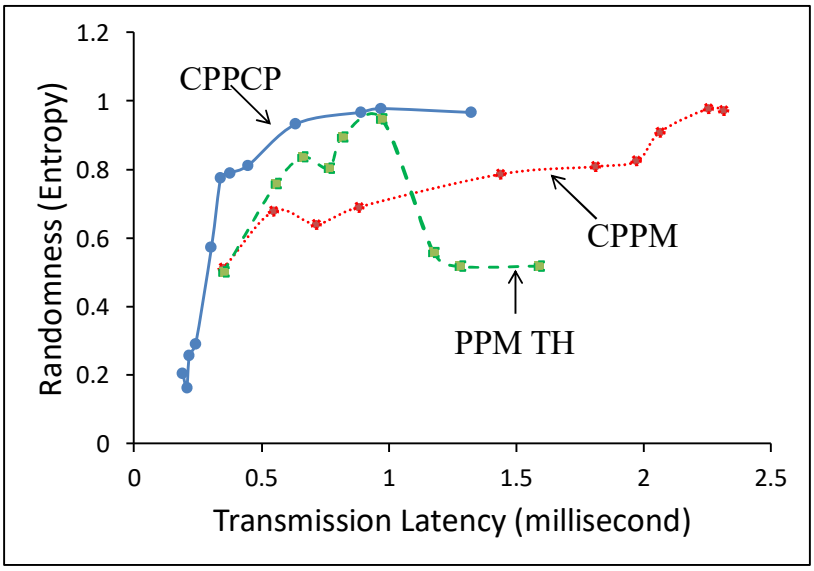


Figure 5.7: Randomness of CPPCP, CPPM and PPM TH corresponding to delay.

Since all the PPM schemes achieve security by rearranging the position of pulses, which is at the expense of long transmission delay, Figure 5.7 shows the randomness of these three coding schemes and the corresponding transmission delay of 100 fields in a Data PDU based on different hopping width or chaotic parameters. The maximum value for each field $\delta_{max} = 255$. When hopping width T_c of PPM TH is close to zero, or chaotic parameter α and β of CPPM is equal to 1, PPM TH and CPPM have the minimum overlapping area. The randomness of these two coding schemes is 0.5. With the increasing of T_c, the inter-pulse intervals representing different data

symbols can have a maximum overlapping area. Therefore, the randomness of PPM TH reaches maximum value of 0.928. If T_c keeps increasing, pseudo-random hopping interval overtakes the size of pulse slot, and the overlapping area between data symbol 0 and 1 is decreasing. The randomness of PPM TH returns to 0.5. However, chaotic-based security schemes, CPPCP and CPPM, achieve more randomness by increasing time duration i.e. transmission latency of chaotic system $F(X)$. It can be seen in Figure 5.7 that with the increasing of $F(X)$, the randomness of each scheme increases and plateaus at a maximum value of randomness. It is shown in Figure 5.7 that compared with CPPM, CPPCP can achieve larger randomness with a shorter transmission delay.

C. Energy Expenditure and Data Transmission Rate

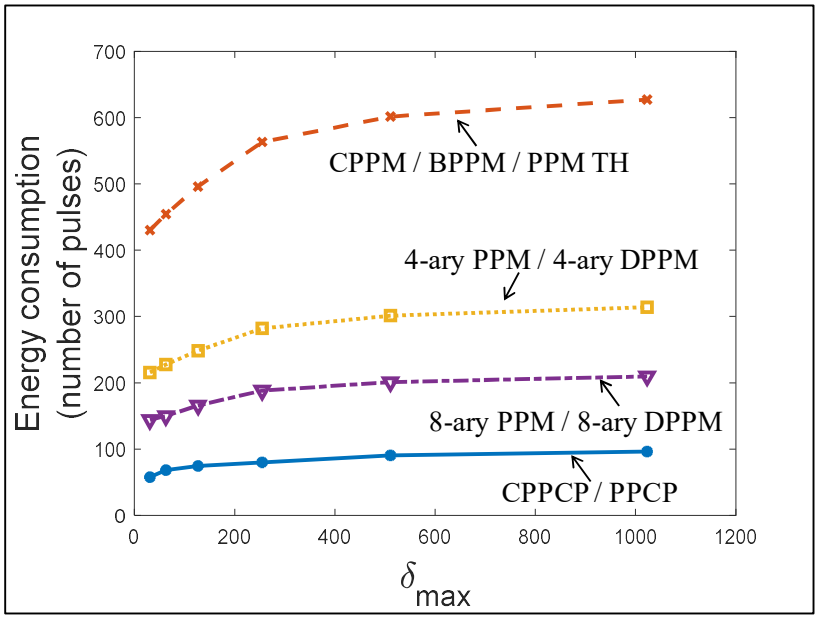


Figure 5.8: Comparison of (a) delay and (b) successful transmission rates

Pulse-based wideband transmission consumes most of the energy on sending pulses compared with the energy consumption during inter-pulse intervals. For the comparison of the

energy comparison between different coding schemes, the energy expenditure on pulse sending is considered here.

Figure 5.8 shows the energy consumption (pulse count) per Data PDU with the increasing of the maximum value δ_{max}. Each Data PDU consists of 20 fields. The three secure coding schemes (CPPCP, CPPM and PPM TH) chosen are assumed to achieve maximum randomness. CPPCP shows the advantage of low energy expenditure due to a smaller number of pulses used to code the same information compared with BPPM, CPPM and PPM TH which require one pulse per bit. M-ary PPM and DPPM save energy at the expense of large inter-pulse intervals, but still not as much as PPCP / CPPCP.

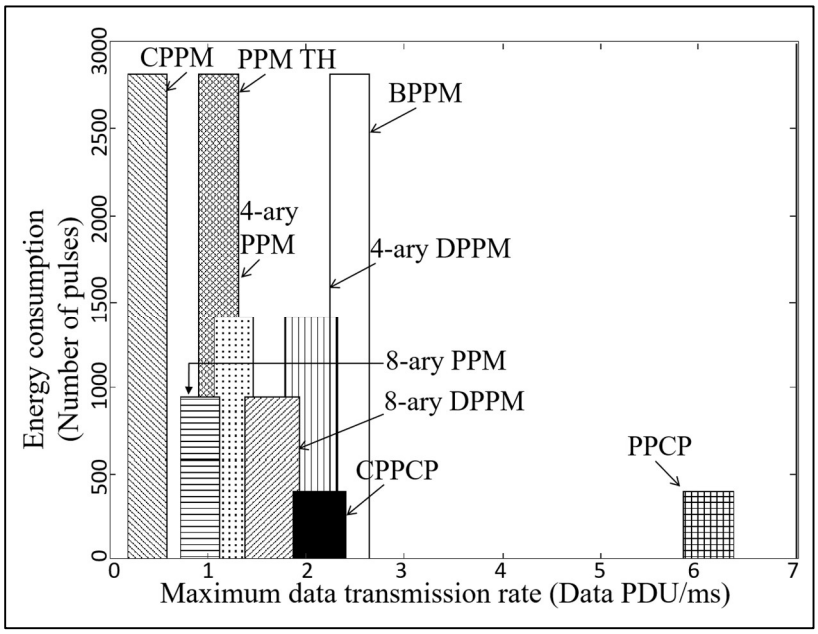


Figure 5.9: Maximum data transmission rate in a network

Figure 5.9 shows the relationship between energy consumption and the maximum data transmission rate in the grid sensor network. The width of each bar represents the fluctuation of the maximum data transmission rate. Since the only factor which affects the Data PDU

transmission rate is the length of Data PDU. Among the three secure coding schemes (CPPM, CPPCP, and PPM TH), CPPCP can have a greater maximum data transmission rate due to the short length of CPPCP. It should also be noted that CPPCP has larger fluctuation of the maximum data transmission rate compared to CPPM and PPM TH due to variations of the CPPCP Data PDU length. CPPM and PPM TH show more regular Data PDU length.

D. CPPCP Architecture-based Error Detection

Errors on a link can be caused by pulse loss (PL), false positive (FP) and transmission collision, etc. Since error detection of CPPM, TH-PPM, BPPM, M-ary PPM, and M-ary DPPM are implemented through extra bits (CRC or parity bit, etc.) and is well understood, they are skipped here. CPPCP architecture-based error detection is developed based on architecture error detection rules without the overhead of any extra bits. The performance of CPPCP error detection is analyzed using a *Detection Accuracy* measurement, which is defined as the number of correctly detected PDUs (including true negative detection and true positive detection) as a fraction of the ones received by a receiver.

A different number of fields are encoded in a CPPCP PDU, and the value of each data field follows a uniform distribution in $[0, \delta]$. Note that the error detection process is only based on the error detection rules and the values of all the three data fields cannot be used for error detection purpose.

A. Detection Accuracy for Pulse Loss Error and False Positive Error

Figure 5.10 shows the effect of pulse loss and false positives on error detection accuracy of CPPCP Data PDU with two data fields. The X-axis shows error rate (either pulse loss or false positive), which varies in the range from 10^{-4} to 10^{-1}. It shows that detection accuracy is above

98% when the error rate is less than 10^{-3}. That is true for all maximum data values ($\delta = 31, 127$ and 511). Increasing pulse error rate beyond 10^{-1} leads to a reduction in detection accuracy. During this stage, most of the undetected errors occur at the end of the CPPCP, as there are no fields left in a CPPCP for the error detection digit rule ($\frac{T_n - \theta F(T_{n-1})}{\tau} - 2 \in [0, \beta]$) to kick in. A relatively large δ has a higher error detection accuracy. Because a large δ can lead to more data fields in a PDU, and the probability is increasing that the errors can be detected by Inter-Pulse Interval Rule.

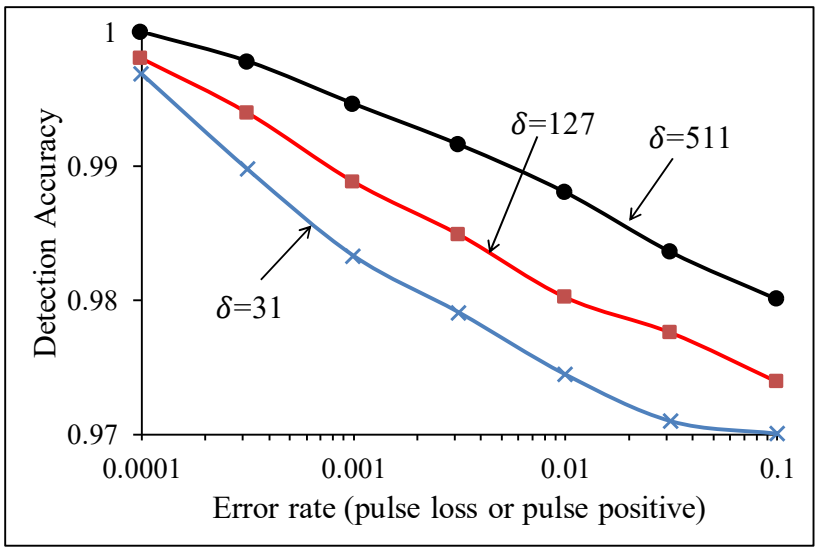


Figure 5.10: PPCP architecture-based error detection for bit error

Figure 5.11 shows the detection accuracy of CPPCP PDU with one, two and three fields, respectively, and the corresponding maximum data value δ. It shows that a relatively longer CPPCP PDU with multiple data fields benefits from the error detection performance based on the fact that the later fields are dependent on the previous inter-pulse interval through chaotic dynamics. According to the experiments based on hardware platform with pulse width 5 μs and pulse slot 25 μs, the probability of both pulse loss and false positive is on the order of 10^{-6} and

CPPCP can provide a reliable wireless transmission under this pulse error rate.

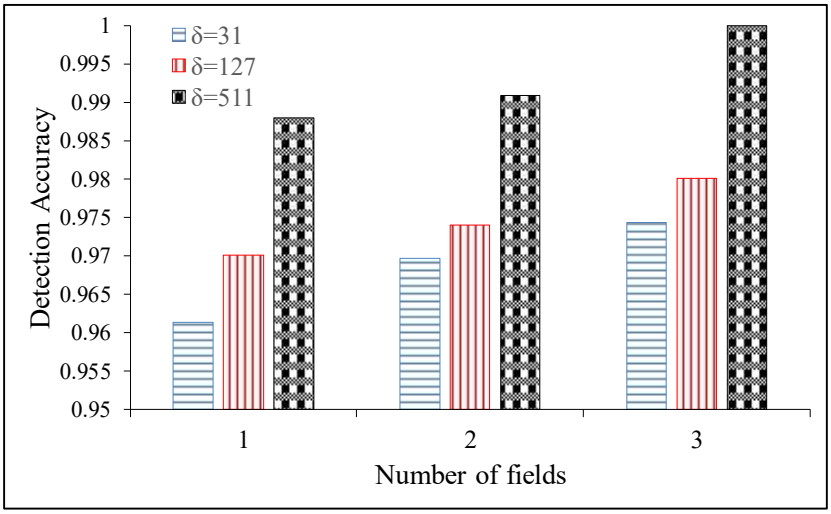


Figure 5.11: PPCP architecture-based error detection

B. Detection Accuracy for Collision Error

The CPPCP architecture-based error detection rules can be also used for detecting errors caused due to collisions in a multi-access networking scenario. ALOHA is used as the MAC protocol in a 20-node sensor network to create the communication collision scenario. Each node sends PDU with more than two fields and with varying PDU generation rates λ (PDU/s/node).

Figure 5.12 shows the performance of four error detection rules. during the collision error detection. When the four detection rules work together, detection accuracy can be achieved more than 0.9996. Herein, Inter-Pulse Interval Rule can detect more than 75% of all the corrupted PDUs. Because most of the collision violate the internal relationship between consecutive digits. The red bars demonstrate the detection accuracy of each rule when the rules work individually in a busy channel where some of collided PDUs can be detected by more than one rule. All four rules provide a reliable error detection mechanism, and CPPCP architecture-based error detection can

guarantee that among all the CPPCP PDUs which are delivered to the upper layer more than 99.96% of them are correct.

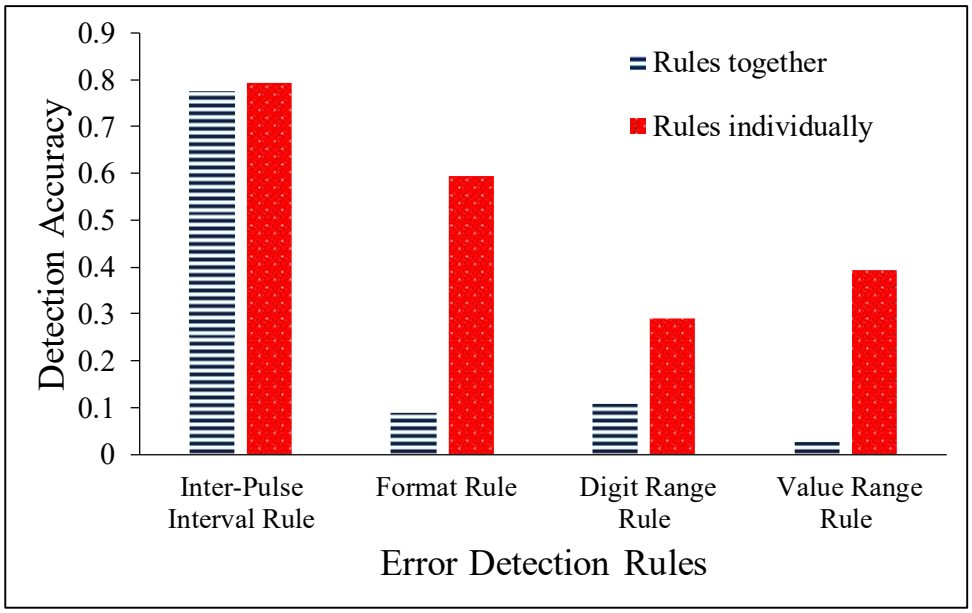


Figure 5.12: PPCP architecture-based error detection

In summary, PPCP should be able to provide reliable data transmission based on its architectural error detection capabilities alone. A higher detection accuracy can be achieved by encoding a relatively large number of data fields in a CPPCP PDU due to the inter-connection between digits through the chaotic system $T_n - \theta F(T_{n-1})$. To achieve even higher error detection accuracy rates, a link layer checksum, such as a bit parity or Cyclic Redundancy Check (CRC) in the traditional packet, can also be utilized by CPPCP.

5.7.3. Experimental Analysis

A prototype of sensor and IoT platform is designed for the implementation of CPPCP. The state-of-the-art BLE is used as a benchmark to compare with CPPCP at the link level due to BLE's outstanding performance of low energy consumption [27, 73]

A. CPPCP Sensor Platform

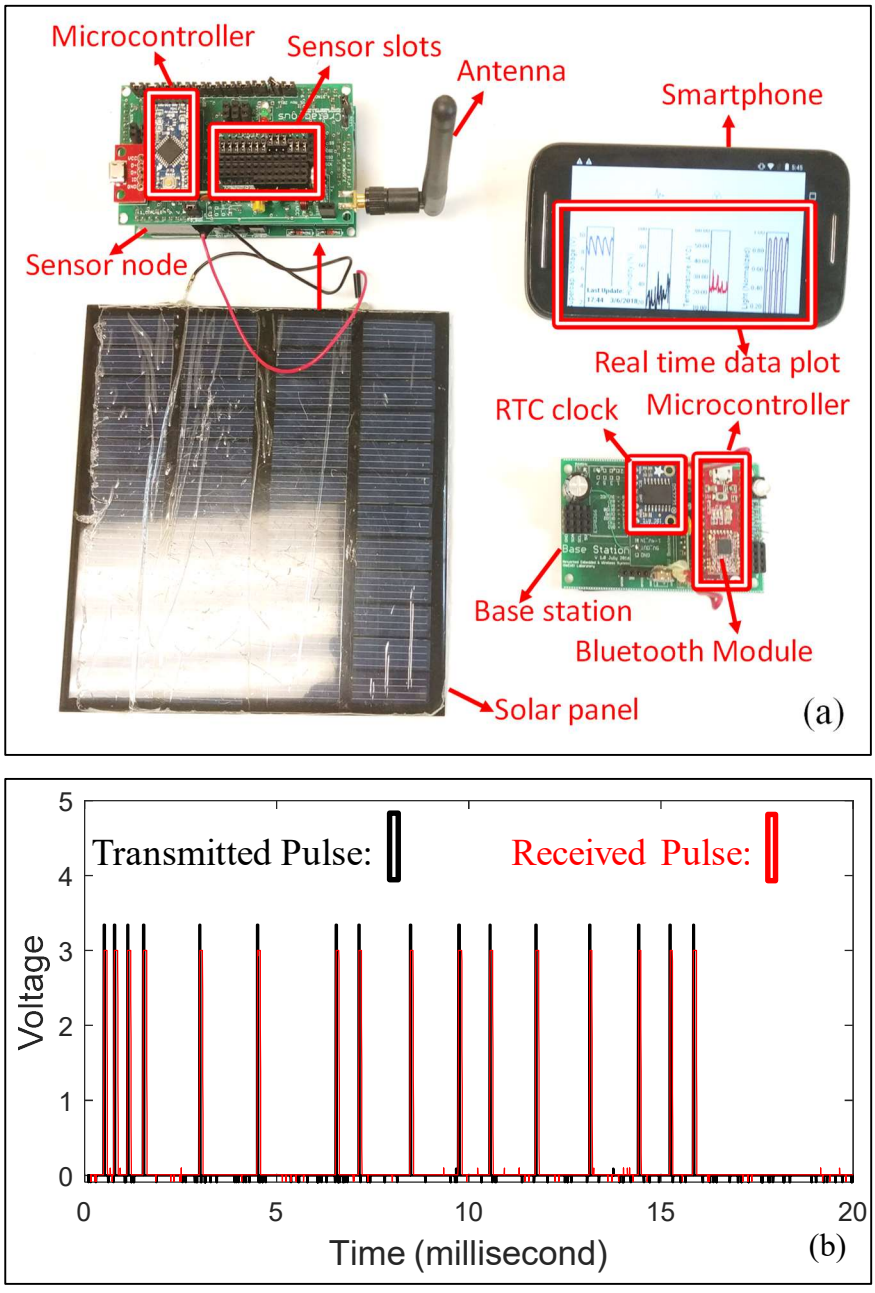


Figure 5.13: (a) CPPCP platform and IoT network. (b) Screenshot of CPPCP

A prototype of sensor platform and IoT network are designed as shown in Figure 5.13(a) for IoT application. 20 μs pulse duration and 200 μs pulse slot are chosen based on the consideration of the tradeoff between pulse error rate and energy consumption.

According to the hardware experiment, the sensor platform based on the above parameters can provide reliable pulse transmission with pulse loss rate 5.9×10^{-4} and false positive rate 3.6×10^{-5} on average for $1\% \sim 50\%$ duty cycle, respectively. The Picoscope screenshot of a CPPCP with three data fields $(161, 19$ and $85)$ is shown in Figure 5.13(b). The signals are transmitted to a Base Station. The Base Station forwards the data collected from IoT sensor platform to user's smartphone for real-time monitoring.

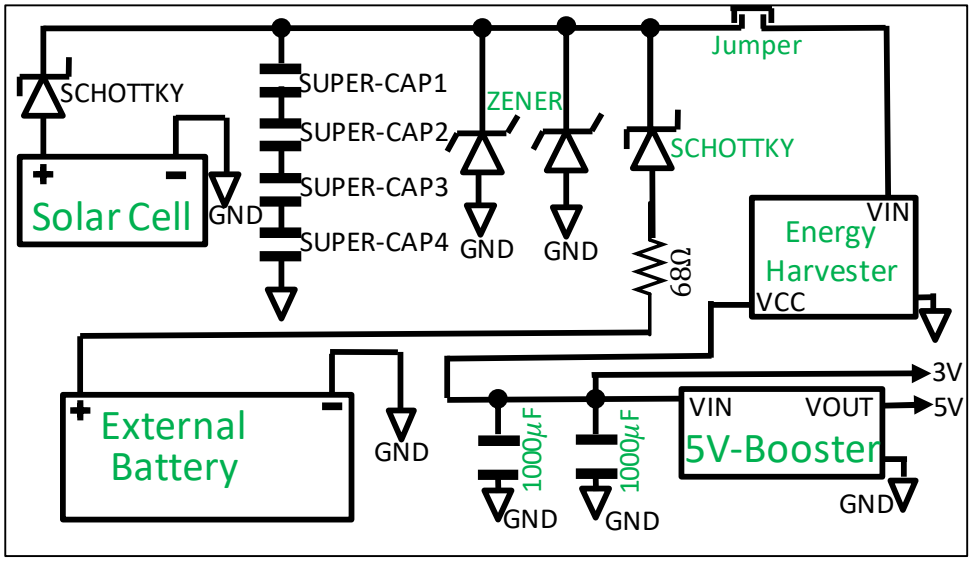


Figure 5.14: Energy harvesting management circuit

The hardware platform is based on a solar energy harvesting system and provides multiple sensor slots, which has the flexibility to meet the requirements of different applications. An energy harvesting management circuit in Figure 5.14 is specifically designed for eliminating the sudden spikes (surge or reduction) during the process of solar energy harvesting. The management circuit can provide a reliable $3v$ and $5v$ power supply. Energy consumption experiments are implemented for CPPCP and BLE based on the above circuit and energy harvesting system.

B. Energy Expenditure Vs. BLE

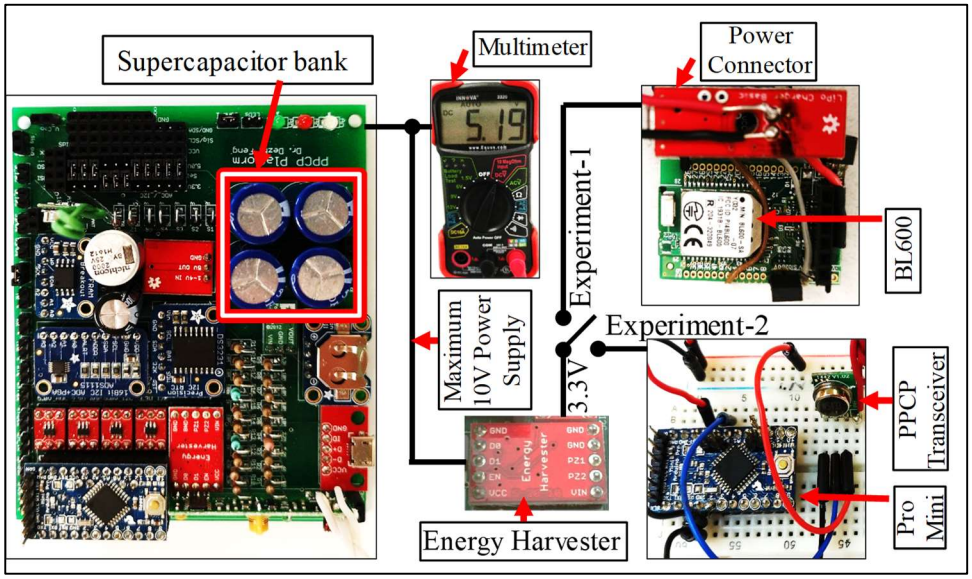


Figure 5.15: System setup for measuring the energy consumption of PPCP and BLE

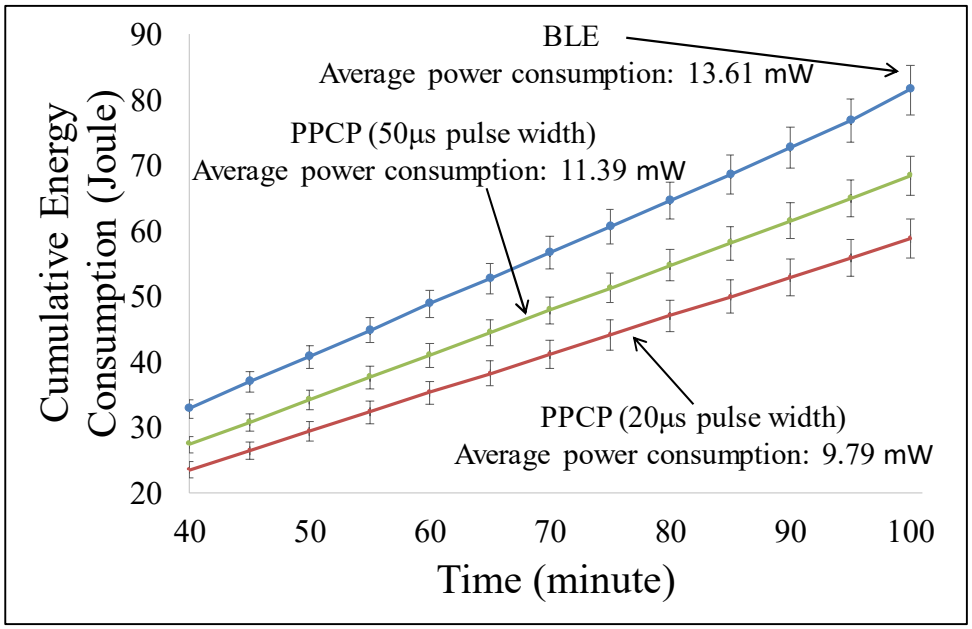


Figure 5.16: Cumulative energy consumption of PPCP and BLE at the link layer

Figure 5.15 shows experimental hardware setup for driving either a PPCP transceiver (e.g., Experiment-1) or a BLE transceiver (e.g., Experiment-2). One of the transceivers is chosen at a

time by using a switch. The same data information (eight fields: 7, 10, 94, 77, 748, 44926, 28 and 1) is coded as one PDU and transmitted once in every 250 microseconds in both cases. For BLE, we have used BL600 [76], which is a well-vetted and certified BLE module from Laird Technologies. *PPCP is implemented in the transceiver* [74]. Using the same power harvesting/management hardware [77], which consists of four 10F/10V supercapacitors [78] connected in series, provides a fair way of measuring energy consumption across the PPCP and the BLE cases.

In Experiment-1 (i.e., with BLE), the output 3.3V of energy harvester drives BL600 through a power connector. In Experiment-2 (i.e., with CPPCP), a modified Arduino Pro Mini [75] is used as a microcontroller to manage the transmission of CPPCP. The instantaneous voltage of the supercapacitor bank is measured by a multimeter for calculating the cumulative energy consumption in each experiment. The cumulative energy consumption ΔE can be calculated through the following formula:

$$\Delta E = \frac{1}{2} C {V_0}^2 - \frac{1}{2} C V^2 \tag{5.12}$$

where $C = 2.5$ *Farads is the capacitance of the supercapacitor bank,* V_0 is the initial voltage *of the fully charged supercapacitors at the start of an experiment.* V is the instantaneous voltage of the supercapacitors, which is read from multimeter every 60 seconds.

The cumulative energy consumption of CPPCP with different pulse widths and BLE are measured with 100 minutes of operation. Figure 5.16 shows the cumulative energy consumption with the x-axis from the $40th$ minute to the $100th$ minute. The first 40 minutes is ignored because the major differences show up only with a relatively long operation. It shows that the CPPCP based system with a pulse width of 20 μs can save 28.034% of power consumption

compared with BLE for 100 minutes of operation. With a larger pulse width of 50 μs, the corresponding savings are 16.285% compared to the BLE based system. Since BLE uses one-byte preamble and two-byte header in each packet and uses energy for every bit transmitted, such overhead causes it to consume more energy per PDU compared to CPPCP. On the other hand, CPPCP only transmits a limited number of pulses to represent the PDU and puts transmitters on silence mode (logical "0") for the most time to achieve power-saving.

Note that the energy consumption of CPPCP is measured in these experiments based on the prototype hardware setup with a separate microcontroller and transceiver. The performance of energy-saving can be better when PPCP is implemented on a highly integrated hardware platform as used for the BL600 hardware unit. CPPCP also provides users higher flexibility to assign arbitrary lengths of a PDU, which cannot be achieved on BLE due to the limitation of bit synchronization [27]. During the real implementation, users can change the base β in each transmission based on the requirement of security level. Simultaneously, CPPCP can also run on the top of a traditional cryptographic security mechanism to achieve higher security in wireless sensor networks.

5.8. Summary and Conclusion

A chaotic pulse position coded PDU (CPPCP) is developed for digital communication in wireless sensor networks toward IoT. CPPCP is to encode a PDU in terms of wideband pulse train with chaotically-varied inter-pulse intervals. The architecture achieves communication security by more randomness and lower probability of unambiguity, and meanwhile, shows significant energy savings compared to the state-of-the-art BLE. A prototype sensor platform is designed for hardware experiment and implementation.

CHAPTER 6: PACKET POSITION MODULATION TOWARD INFORMATION CAPACITY ENHANCEMENTS

6.1. Motivation

Low duty cycle networks have been extensively studied in the sensor network literature [99, 100] for their ability to provide energy-constrained data transport. Access control in such networks can be TDMA [101] or asynchronous non-TDMA [59, 60] based. While the asynchronous approaches can operate in the absence of a centralized scheduling entity, they can suffer from energy wastage due to packet collisions which cannot be afforded in such energy-constrained networks. A TDMA-based approach, on the other hand, provides a collision-free solution for medium access for low-cost embedded transceivers. For both cases, the transmission duty cycle is very large when the energy inflow rate for a harvesting sensor is low.

The proposed DPPM system works by shifting the position of a packet over time such that the amount of shift encodes additional information to be sent. Consider a scenario in which a sensor node sends packets to a base station at a regular interval *T*, which is the TDMA frame duration. Now consider an example implementation in Figure 6.1, in which instead of transmitting packets at T intervals, each packet is postponed by $\tau.\delta_i$ durations, where τ is the bit duration and δ_i $(i = 1, 2, \cdots)$ is the DPPM-coded data value. Since the base station expects a packet after T duration since the last received packet, it interprets the shift $\tau.\delta_i$ as the additional DPPM-coded information. With *L*-bit packets, the baseline information transfer capacity is *L/T* bits per second. With DPPM as shown in Figure 6.1, in addition to that baseline capacity, the node is able to send additional information values δ_1 and δ_2 by modulating the positions of the second and the third packets respectively. This increases the node's *effective information transfer capacity (EITC)* by

at no additional transmission energy costs. Formally stated, the capacity is enhanced from L bits in T duration to $L + log_2^{\delta_i}$ bits in $T + \tau\delta_i$ duration.

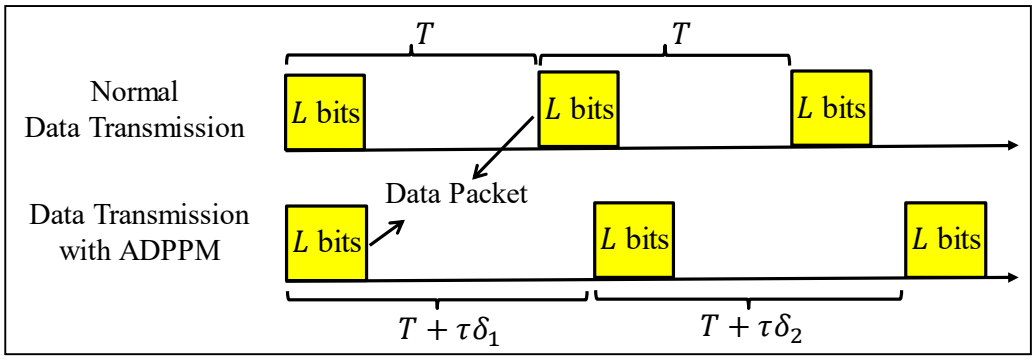


Figure 6.1: DPPM-enabled zero-energy information transfer

One key assumption in DPPM is that there exists sufficient inter-packet spacing so that the transmitting node has enough room for shifting packets. This requires the operating duty cycle (i.e., τ/T) to be low, which is the case for many energy-harvested sensor nodes [102]. Another assumption is that the sensor nodes are transmit-only and they themselves do not receive data from other sensors. Not receiving allows them to sleep in between transmissions and conserve idling energy. Such transmit-only arrangements [3, 65] are simpler, low-cost, and getting increasingly popular for small-scale networks used in human health, smart home, process monitoring, and many other embedded sensing applications.

Scaling the simple point-to-point DPPM in Figure 6.1 to a deployable system would require a number of design questions to be addressed. First, since the additional information encoding can be done by both right-shift (i.e., deferring) or left-shift (i.e., preponing) of packet transmissions, which one of them to be used in which situations. A comprehensive set of protocol rules would be required to choose the appropriate shift directions in a packet-by-packet manner. Second, in the presence of multi-node TDMA, those DPPM-induced time shifts would be susceptible to inter-

node packet collisions and its resulting wastage of energy and information transfer capacity. To mitigate that, protocol syntaxes along with appropriate parameter dimensioning would be needed. Finally, the impacts of transmission errors on DPPM would have to be understood. This chapter sets out to address these issues regarding DPPM.

6.2. Our approach and contribution

The specific contributions of this chapter are as follows. First, a baseline protocol, Asymmetric DPPM (ADPPM) [103], which always defers transmission for information encoding is developed and explored using analytical and simulation models. Second, an improved scheme, symmetric DPPM (SDPPM), is developed to further augment the information transfer capacity and to eliminate the latency of ADPPM. In SDPPM, transmissions are preponed or deferred on a packet by packet basis based on the current energy availability. Third, the SDPPM protocol is enhanced to support multi-node multiaccess while minimizing the energy wastage and capacity loss due to inter-node packet collisions. Finally, a formal methodology is developed for achieving maximum information transfer capacity for a given set of system parameters.

6.3. Design Objectives

The objective of this chapter is to present a data packet position modulation (DPPM) paradigm to enhance information transfer capacity of communication links used by energy-constrained devices. Packet transmissions in low duty cycle networks are often scheduled as TDMA slots, whose periodicity is determined based on application sampling requirements and the energy in-flow, often in the form of energy harvesting. The key idea of DPPM is to modulate the inter-packet spacing for coding additional information without incurring additional transmission energy expenditures. This chapter presents a DPPM based solution for single-hop transmit-only

networks in which a number of low-energy nodes transmit data to an aggregator. The architecture is first developed for a two-node point-to-point link, followed by a multipoint-to-point multi-access network. Detailed analytical and simulation models are developed to demonstrate the performance of a symmetric and an asymmetric version DPPM. It is shown that by carefully choosing the protocol parameters, DPPM can enhance the effective information transfer capacity of an ultra-low duty cycle network by up to 65% in certain scenarios.

6.4. Asymmetric DPPM (ADPPM) Architecture

The example in Figure 6.1 is asymmetric DPPM, or ADPPM. It is asymmetric because the additional information in this case is always encoded by deferring as opposed to a preponing and deferring on a packet by packet basis (i.e., symmetric).

Analytical Representation: Let Δ be the maximum allowed packet deferral in bit durations. The additional information value δ_i ($\delta_i \in [0, \Delta - 1]$) is encoded by deferring packet transmission by $(\delta_i + 1)$ bit durations. We develop a capacity model assuming that the additional information to be sent takes a random value in the range $[0, \Delta - 1]$ following a uniform distribution. Information capacity enhancement for other distributions can be similarly computed. In Figure 6.1, the average time interval between the previous and the current packet is $T_{avg} = T + (1 + \Delta) \cdot \tau/2$.

For a sensor node, let E and W denote the energy consumption per bit transmission (Joule/bit) and the energy harvesting rate (Joule/sec) respectively. The baseline inter-packet interval T (i.e., without ADPPM) is dimensioned such that the node should be able to harvest enough energy in T duration to send an L-bit packet. Meaning $T = \frac{L \cdot E}{W}$. This leads to:

$$T_{avg} = \frac{L \cdot E}{W} + \frac{1+\Delta}{2} \cdot \tau \tag{6.1}$$

With ADPPM, two separate parts of information are sent to the base station. The first and main part is what is contained in the L-bit data packet itself. The second is what is coded by ADPPM by transmission time shift. Therefore, the average amount of information per packet transmission can be expressed as:

$$D_{avg} = L + \frac{\log_2 1 + \log_2 2 \cdots + \log_2 \Delta}{\Delta} = L + \frac{\log_2(\Delta!)}{\Delta} \tag{6.2}$$

From Eqns. (1) and (2), the expected information transfer capacity of ADPPM can be written as:

$$C_{ADPPM} = \frac{L + \frac{\log_2(\Delta!)}{\Delta}}{\frac{L \cdot E}{W} + \frac{1+\Delta}{2} \cdot \tau} \tag{6.3}$$

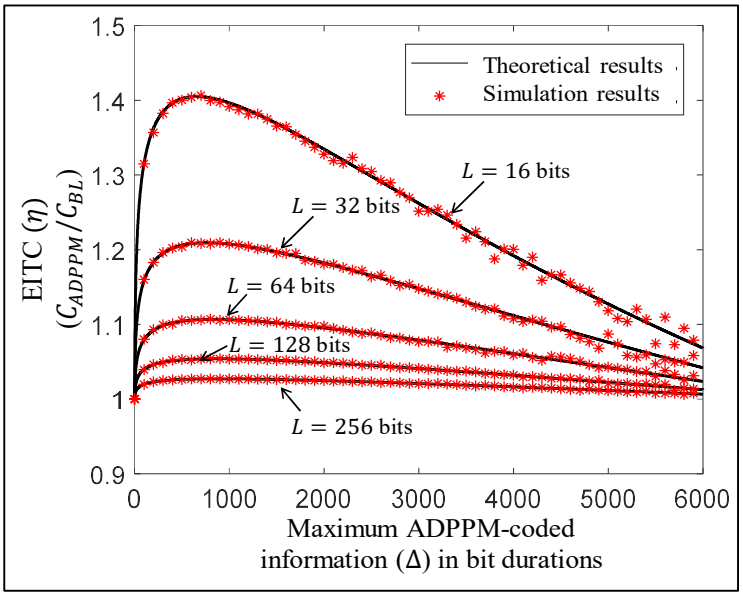


Figure 6.2: EITC of ADPPM with different packet lengths

The ratio of C_{ADPPM} to the baseline information transfer capacity (i.e., without ADPPM) C_{BL} ($C_{BL} = \frac{L}{T}$) is defined as the *Effective Information Transfer Capacity* (EITC) $\eta = \frac{C_{ADPPM}}{C_{BL}}$. Figure 6.2 shows the EITC of ADPPM when a single node sends packets to a base station. For

these experiments, the values of E and τ were chosen as $8\,\mathrm{mJ/bit}$ and $250\,\mu s$ based on a representative embedded transceiver (CC1000). The energy harvesting rate W for the sensor node was chosen to be $0.1\,mW$.

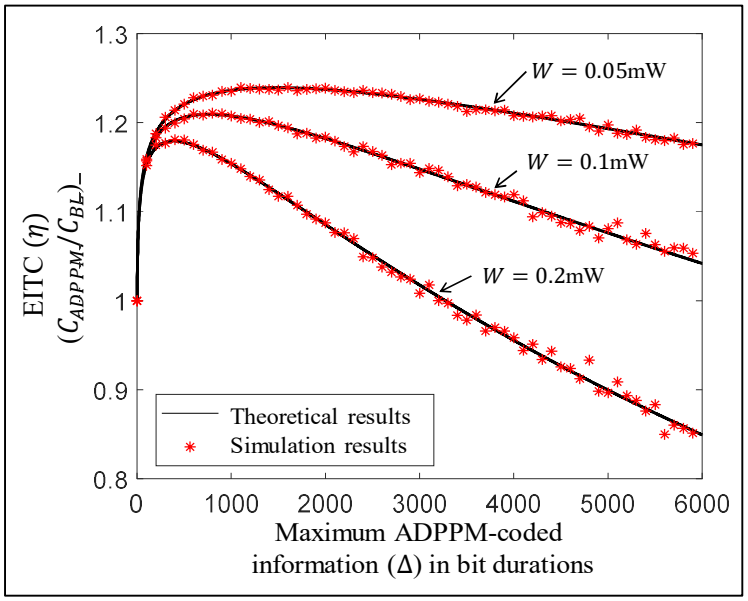


Figure 6.3: EITC under different energy harvesting rates

Figure 6.2 shows that for any given packet length, the EITC value first increases with time shift Δ, but then start falling. This is because initially the increase of time shift Δ can increase the amount of extra information ($\frac{\log_2(\Delta!)}{\Delta}$) sent with each packet transmission. However, any further increase of time shift Δ increases the average inter-packet interval ($\frac{L\cdot E}{W}+\frac{1+\Delta}{2}\cdot\tau$), which leads to the decrease of the overall information transfer capacity. Figure 6.2 also shows that with larger packets, the advantages of ADPPM shrinks. This is because with increasing packet size L, the amount of ADPPM-coded information ($\frac{\log_2(\Delta!)}{\Delta}$) as a fraction of the total information amount ($L+\frac{\log_2(\Delta!)}{\Delta}$) reduces for each packet transmission. Overall, it is evident, that depending on the packet length and the time shift, the ADPPM scheme can enhance the information transfer capacity of a

single sensor point-to-point link by 20% to 40%. It is worth noting that this additional capacity is achieved with no additional transmission energy whatsoever.

Figure 6.3 shows the simulated and the theoretical EITC values under different energy harvesting rates when the packet length is set to $L = 32$ bits. The overall trend of EITC is similar to those observed in Figure 6.2 for similar reasons as explained above. The performance is better for smaller energy harvesting rates. This is because, a smaller harvesting rate leads to a larger inter-packet time interval T (i.e., $T = L \cdot E/W$), and a larger T allows more room for packet shifting, thus helping ADPPM in terms of higher information transfer capacity.

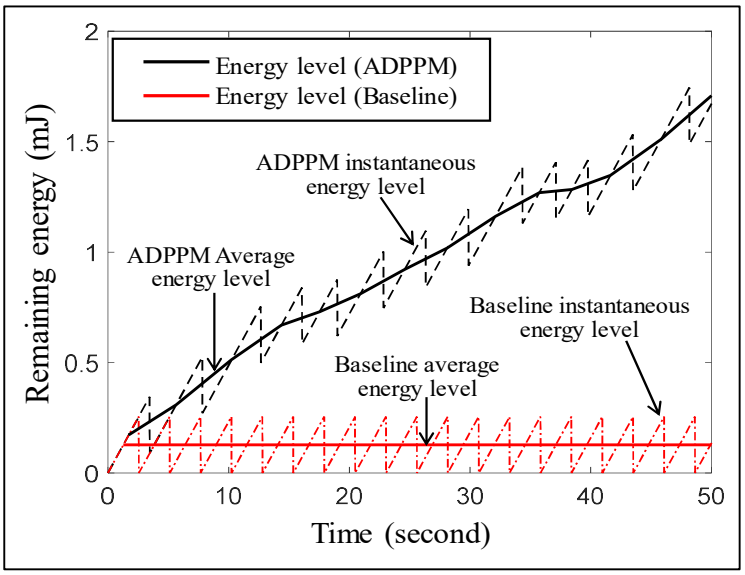


Figure 6.4: Instantaneous and average energy levels

ADPPM suffers from two shortcomings. First, the right shift of transmission adds additional latency, which can be represented by the quantity $t_{APPM} = (1 + \Delta)\tau/2$. Second, such latency can cause a mismatch between the incoming harvested energy and the energy expenditure, leading to cumulative unused energy, which is an indirect loss of capacity over time.

Figure 6.4 shows the evolution of instantaneous and the average energy level within a node with $L = 16\ bits$ and $W = 0.2\ mW$. For the baseline case (i.e., without ADPPM) the harvested energy is periodically spent on packet transmissions at a rate such that the remaining energy remains stable. For ADPPM, however, the remaining energy keeps increasing. This indicates that ADPPM does not take full advantage of the harvested energy for capacity enhancement. We address this issue in the symmetric version of DPPM presented in the next chapter.

6.5. Symmetric DPPM (SDPPM) Architecture

6.5.1. Protocol Architecture

The key idea of SDPPM is that a node can code additional information by either preponing or postponing a transmission depending on its current energy availability. If there is sufficient remaining energy for sending a packet early, then the information is coded by preponing. If there is not sufficient energy to send a packet then the information is coded by deferring the transmission as done in ADPPM in Figure 6.1.

The specific process for SDPPM is as follows. First, a reference inter-packet interval T' (i.e., $T' \geq T = L \cdot E/W$) is chosen based on the system parameters. Optimal dimensioning of T' is presented later in this chapter. At run-time, the transmitting node prepones or postpones its packet transmissions as follows. Based on the energy harvesting rate W, if enough energy can be accumulated during the period $T' - \tau\delta_i$ (where δ_i is the next additional information to be sent) for sending a packet, the sensor node sends the next packet at time $T' - \tau\delta_i$. This amounts to preponing a transmission. Otherwise, the next packet is postponed by sending it at the time $T' + \tau\delta_i$. Since the base station knows the reference inter-packet interval T', upon receiving a packet it can detect if the transmission was preponed or postponed with respect to the last packet. It can

then decode the additional information δ_i from the reception timing. For a chosen reference interval T', the maximum allowed packet deferral Δ (in bit duration) is bounded as $\Delta \leq T'/\tau$.

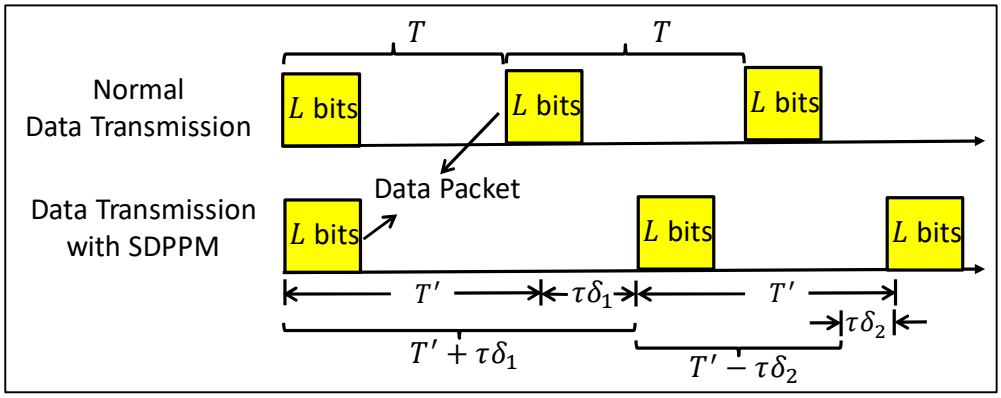


Figure 6.5: Information coding mechanism in SDPPM

An example coding instance is shown in Figure 6.5, in which for the first SDPPM information value δ_1, the sensor node does not have enough time to accumulate enough energy for preponing the packet. Thus, the packet is postponed for a time duration $\tau\delta_1$. However, for the second packet transmission with information value δ_2, the energy for a packet transmission can be attained for a preponed transmission. With this symmetric operation of SDPPM, a postponed transmission produces surplus energy, which in turn allows subsequent transmission preponing, thus leading to a much better utilization of harvested energy compared to the asymmetric operation of ADPPM.

It should be noted that the shift time duration $\tau\delta_i$ for a packet is scheduled corresponding to the previous packet's position, and not with respect to any absolute timing. This provides a mechanism for implicit transmitter-receiver synchronization and minimizes the impacts of clock drift which is prevalent in low-cost embedded sensors. Such implicit mechanism also makes the

system immune to loss of synchronization in the event of packet losses due to channel errors or collisions.

6.5.2. Analysis of SDPPM

The first step is to analyze the information transfer capacity enhancements of SDPPM for different values of the reference inter-packet interval T' (i.e., $T' \geq T = L \cdot E/W$). Like in ADPPM analysis, we assume that the maximum allowed packet shift (i.e., in either direction) is Δ bit durations. The DPPM-coded information value δ_i ($\delta_i \in [0, \Delta - 1]$) is encoded via shifting packet transmissions by $(\delta_i + 1)$ bit durations. With this parameterization, the Effective Information Transfer Capacity (EITC) for SDPPM is computed for different ranges of the reference inter-packet interval T' as follows.

1) When $T \leq T' \leq (2L \cdot E/W/\tau - 2L + 1)\tau$: Since the reference interval T' is greater than or equal to the minimum required interval T, the energy accumulated after the time period T' is guaranteed to be greater than or equal to the energy required for sending a packet. Thus, a sensor node in this scenario is more likely to prepone transmissions than postponing them. In the extreme case when $T' = (2L \cdot E/W/\tau - 2L + 1)\tau$, it is large enough so that all packet transmissions can be preponed. As a result, the long-term average inter-packet interval T_{avg} will be less than T'. However, to maintain the energy balance, T_{avg} will be equal to the baseline inter-transmission interval T (i.e., $T = L \cdot E/W$). Therefore, the information transfer capacity is:

$$C_{SDPPM} = \frac{L + \frac{\log_2(\Delta!)}{\Delta}}{\frac{L \cdot E}{W}} \tag{6.4}$$

This capacity expression, which is valid for $\Delta \leq \frac{T'}{\tau}$, is larger than that for ADPPM as expressed by Eqn. (3). The additional term $\frac{1+\Delta}{2} \cdot \tau$ in the denominator of Eqn. (3) is eliminated here in SDPPM because of its preponed transmission opportunities.

2) When $\mathrm{T}' > (2L \cdot E/W/\tau - 2\mathrm{L} + 1)\tau$: The reference interval T' in this case is large enough for all transmissions to be preponed. The average inter-packet interval in this case turns out to be $\mathrm{T_{avg}} = \mathrm{T}' - ((\mathrm{T}'/\tau + 1)/2 - \mathrm{L})$, which is smaller than the reference interval T', but larger than the baseline interval T. So the information transfer capacity can be expressed as:

$$C_{SDPPM} = \frac{\mathrm{L} + \frac{\log_2(\Delta!)}{\Delta}}{\mathrm{T}' - \left(\frac{\frac{\mathrm{T}'}{\tau} + 1}{2} - \mathrm{L}\right)} \tag{6.5}$$

It can be seen in the above equation that for any value of T', the capacity can be maximized when Δ (i.e., the maximum allowed packet preponing or deferral) is equal to its upbound, which is T'/τ (i.e., $\Delta \leq \mathrm{T}'/\tau$). Therefore, the expression for the upper bound of C_{SDPPM} as a function of only Δ (i.e., not T') can be expressed as:

$$C_{SDPPM}^{Upper} = \frac{\mathrm{L} + \frac{\log_2(\Delta!)}{\Delta}}{\Delta\tau - \left(\frac{\Delta+1}{2} - \mathrm{L}\right)} \tag{6.6}$$

It can be observed that in Eqn. (4), the capacity is an increasing function of Δ, and in Eqn. (6), it is a decreasing function. These lead to the fact that the capacity is maximum when the value of Δ is at the boundary between the two scenarios, which is $\Delta = 2L \cdot E/W/\tau - 2\mathrm{L} + 1$.

Using Eqns. (4) and (6), Figure 6.6 shows the EITC (i.e., defined as $\eta = \frac{C_{SDPPM}}{C_{BL}}$) of SDPPM for a single node to base station link over the entire range of allowable Δ values. As in Figure 6.2 for ADPPM, an energy harvesting rate of $W = 0.1\ mW$ has been used for these results. It can be

observed that for each graph, the first increasing part is from Eqn. (4) and the decreasing part is from Eqn. (6). As expected, a higher maximum EITC is achieved for shorter packets. This is because a smaller packet (L) can cause the increase of the proportion of extra coded information ($\log_2(\Delta!)\ /\Delta$)When compared to the equivalent results in Figure 6.2 for ADPPM, it is evident that SDPPM can achieve higher effective information transfer capacity. For instance, with 16-bit packets, while the maximum EITC for ADPPM was around 1.4, it is around 1.7 for SDPPM. The latter is able to achieve this by judiciously utilizing all available energy via preponing and postponing transmissions.

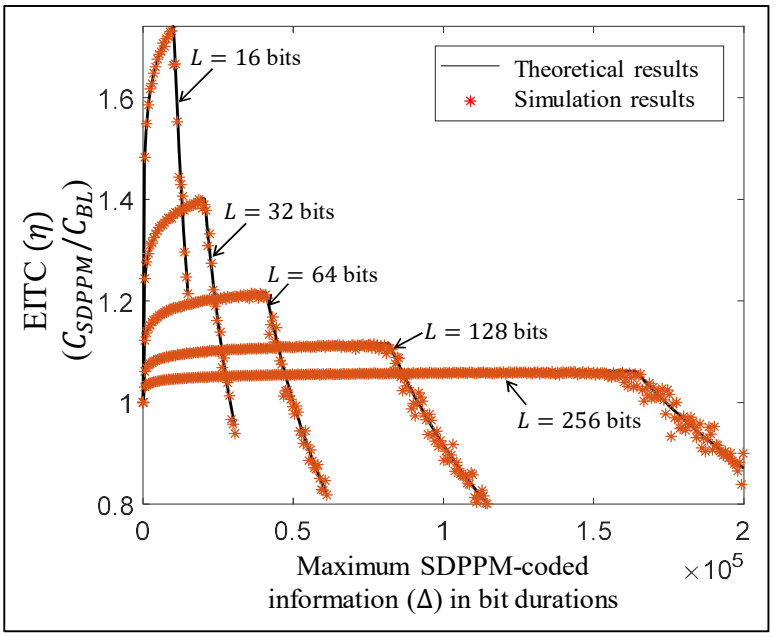


Figure 6.6: EITC of SDPPM under different packet lengths

Figure 6.7 demonstrates the impacts of energy harvesting rates for a given packet length $L = 32\ bits$. When compared to the equivalent graphs in Figure 6.3 for ADPPM, the effective capacities for SDPPM in Figure 6.7 are better for all the energy harvesting rates. The reasons for this are the same as those for Figure 6.6.

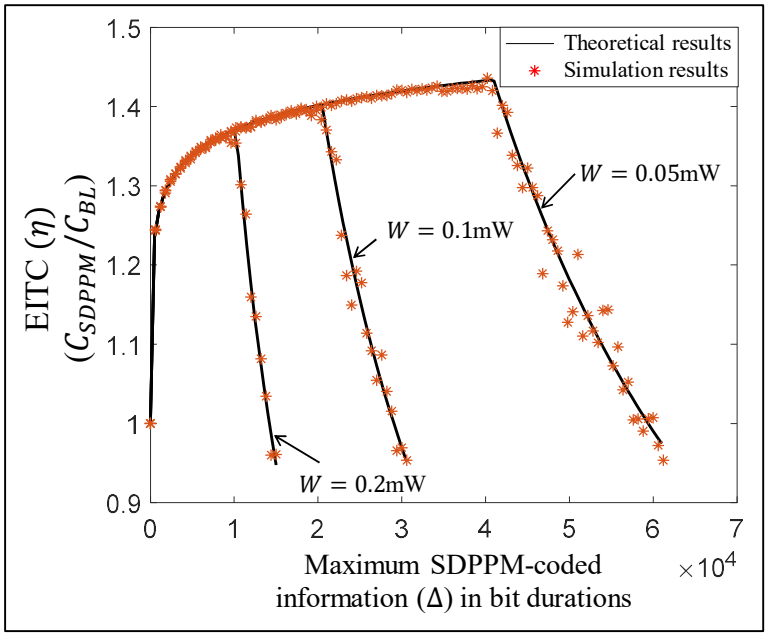


Figure 6.7: EITC under different energy harvesting rates

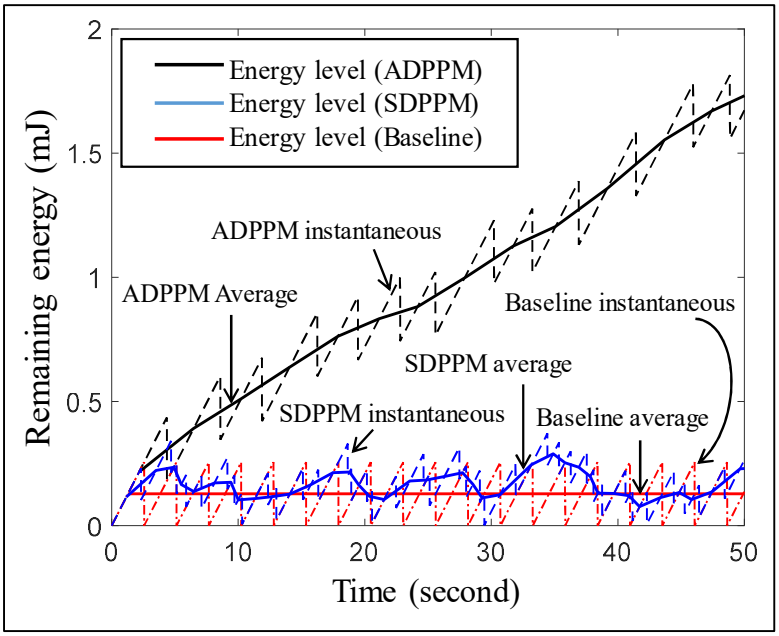


Figure 6.8: Instantaneous and average energy levels

Figure 6.8 shows the instantaneous and average energy levels within a transmitting node with packet length $L = 16\ bits$ and energy harvesting rate $W = 0.2\ mW$. Observe how unlike

ADPPM, the SDPPM mechanism can maintain the energy balance by dynamically preponing and postponing packet transmissions. As a result, the latter's remaining energy hovers around the baseline system without any DPPM.

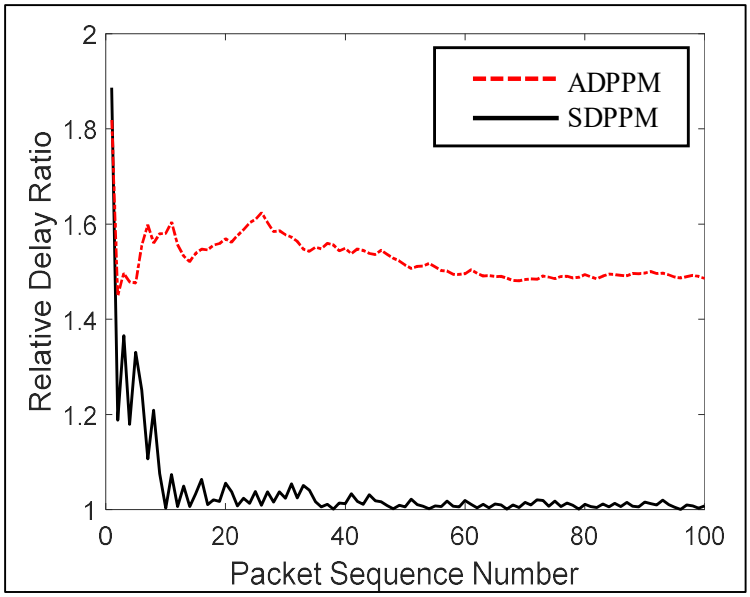


Figure 6.9: Relative delay ratio of ADPPM and SDPPM

Finally, to evaluate the delay performance we define a Relative Delay Ratio $R_t = \frac{t_i}{i \cdot T}$. Here t_i is the transmission time of the ith packet since the start time t = 0. In the baseline case without any versions of DPPM, this quantity should always be 1, since packets in this case are sent every T second without any preponing or postponing. With ADPPM or SDPPM, the values can be larger than one depending on their shift dynamics.

Figure 6.9 shows the relative delay ratio for both ADPPM and SDPPM. Since ADPPM incurs an average time delay $(\Delta + 1)\tau/2$ after each packet transmission, R_t settles down to a steady state value that is much larger than 1. For SDPPM, on the other hand, it converges to almost

1, indicating no additional delay over baseline DPPM. This low delay of SDPPM is achieved by preponing and postponing on a packet by packet basis.

6.6. Multiaccess SDPPM

The single-node point-to-point SDPPM protocol from the previous chapter is extended for multiaccess in this chapter.

6.6.1. SDPPM over Pre-allocated TDMA Slots (SDPPM-PAD)

Consider a TDMA [101] network in which N Tx-only nodes send data to a base station. The inter-packet interval T (i.e., $T = L \cdot E/W$) constitutes the TDMA frame which is divided into N packet-sized slots, each one assigned to a node. In baseline TDMA operation, without SDPPM, a node transmits its packets in its allocated slot. With SDPPM, the additional information is coded by the amount of shift in transmission time with respect to the allocated slot timing.

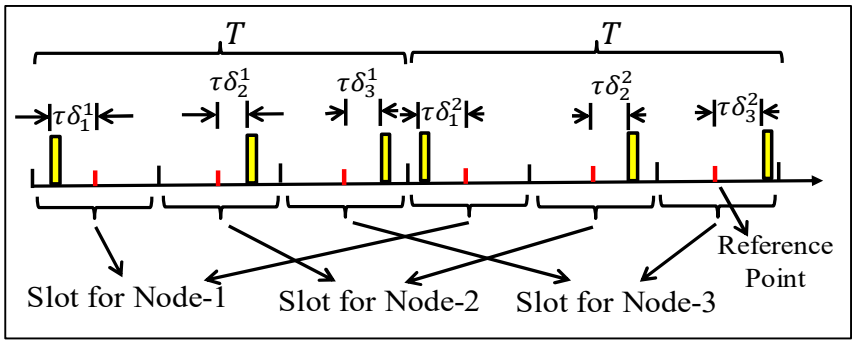


Figure 6.10: SDPPM over pre-allocated TDMA slots

An example 3-node operation is shown in Figure 6.10. A reference point is chosen for each node right in the middle of its allocated slot. Any transmission that is shifted by $\tau\delta_i$ amount from that reference point is interpreted by the receiver base station as the additional information δ_i, where τ is the known bit duration. Collisions between two nodes with adjacent slots are

avoided by limiting the amount of shift to half the slot duration. The maximum time shifts that a node can use is $\lfloor (T/N/\tau - L) \rfloor /2$ in bit durations in either direction with respect to the reference point. The resulting information transfer capacity for each node is:

$$C_{SDPPM}^{TDMA} = (L + \log_2 \left(\left\lfloor \frac{\left(\frac{T}{N \cdot \tau} - L\right)}{2} \right\rfloor ! \right) / \Delta) / \frac{L \cdot E}{W} \tag{6.7}$$

The primary limitation of SDPPM-PAD is that the amount of allowed shift is bounded to only half the slot duration in each direction, which limits the maximum possible information transfer capacity, especially at small node population. Also, the mechanism requires all nodes to be tightly absolute time-synchronized among each other and the base station. This is particularly challenging due to: a) high clock drifts in inexpensive embedded nodes, and b) lack of reception ability of the Tx-only nodes by periodically synchronizing with the base station. The following protocol addresses these.

6.6.2. SDPPM with Implicit Slotting (SDPPM-WIS)

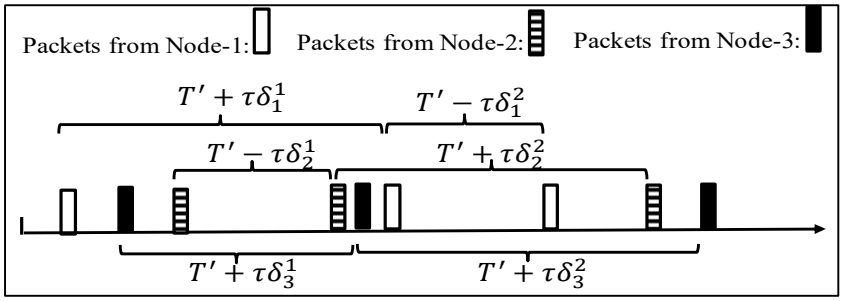


Figure 6.11: SDPPM with implicit slotting

There is no explicit slot allocated to a node in this version. Rather, once a node picks a transmission time, it keeps sending packets periodically with the baseline interval $T = L \cdot E/W$, which depends on energy harvesting rate, packet length, and transmission energy budget. With

this strategy, the nodes do not have to be absolute time synchronized with other nodes. It is sufficient to self-synchronize in a relative sense so that the receiver is able to measure any transmission time shift in order to decode the additional information coded by SDPPM-WIS.

A node is allowed to shift (i.e., left or right depending on the energy availability) a transmission with respect to its last transmission time by up to the reference duration T' as defined and dimensioned in Chapter 6.5.1. The preponing and postponing of transmissions based on available energy is performed the same way as presented in Chapter 6.5. An example operation of SDPPM-WIS is shown in Figure 6.11.

Unlike in SDPPM-PAD, there can be collisions in SDPPM-WIS. However, since the range of encoded data value is $(T'/\tau - L)$, which is larger than that in SDPPM-PAD, this version can achieve a higher information transfer capacity, especially at smaller node populations. This advantage diminishes due to frequent collisions in larger networks.

A detailed analytical model for the collision probability and performance of SDPPM-WIS, along with an algorithm for choosing the optimal time shifts for the maximum information transfer capacity, are developed in Appendix-A.

6.7. Performance of Multiaccess SDPPM

6.7.1. Impacts of Maximum Allowed Time Shift

Figure 6.12 shows the effective information transfer capacity (EITC) with varying Δ and network size. For the simulation results presented here, the energy harvesting rate $W = 0.08\,mW$, and the corresponding baseline inter-packet interval is $1.6\,seconds$. The Δ values in the x-axis of these graphs are normalized by the inter-packet spacing for the baseline case (i.e., without any DPPM), which is $\Delta_T = L \cdot E/W/\tau - L$. The y-axis is the Effective Information Transfer Capacity

(EITC) η, which represents the information transfer capacity of the multiaccess SDPPM protocols normalized by that of the baseline case without any DPPM. To facilitate a comprehensive understanding of the performance numbers, a part of Figure 6.12 for lower Δ/Δ_T values is zoomed in Figure 6.13.

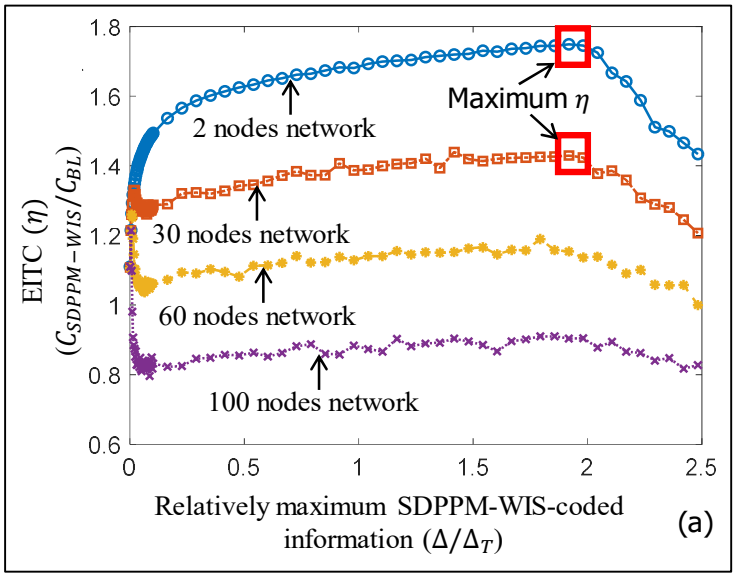


Figure 6.12: EITC with varying Δ and network size

Let us examine the EITC of the SDPPM-WIS protocol for a moderate size network with 30 nodes. Figure 6.13 shows that the EITC value first increases with increasing Δ (i.e., Δ_T in Δ/Δ_T is a constant). This is because with higher allowable shift more SDPPM-WIS-coded information can be sent. For higher Δ values, packets from different nodes start colliding due to the unrestricted shifts allowed by the SDPPM-WIS strategy. Such collisions cause EITC to start coming down. This initial increase in the collision probability with increasing Δ values is shown in the experimental graphs in Figure 6.14. Note that a packet lost due to collision reduces information transfer not only due to the loss of information in the packet, but also due to the loss of SDPPM-

WIS-coded additional information represented by the two packets (i.e., the lost one and the one after that).

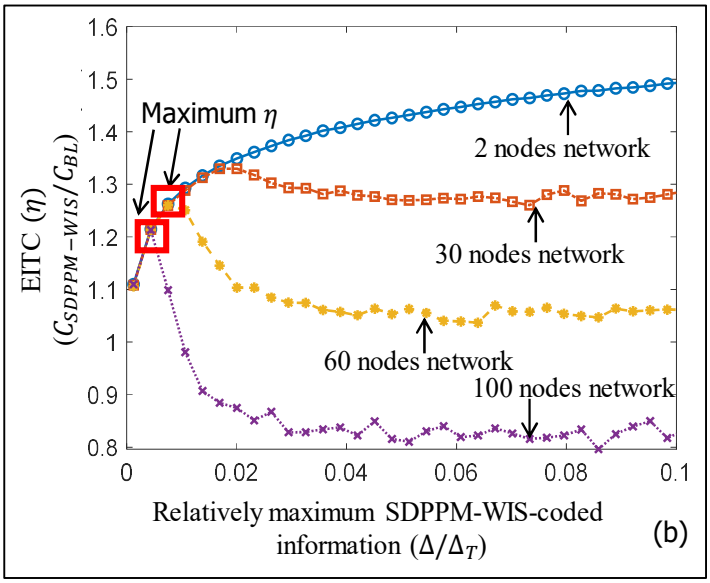


Figure 6.13: Zoomed in EITC for a smaller range of Δ/Δ_T

As shown in Figure 6.14, when the shift amount Δ is increased further, the collision probability remains more or less constant with a small decreasing trend. In this region (i.e., Δ/Δ_T ranges approximately from 0.03 to 2 for the 30-node network) the EITC in Figure 6.12 monotonically increases due to non-increasing collisions, but more SDPPM-WIS-coded information allowed by larger Δ values. As Δ keeps increasing, at some point (i.e., Δ/Δ_T to be 2), the condition $T' > (2L \cdot E/W/\tau - 2L + 1)$ is reached, which causes the EITC to steadily decrease, as explained by Eqns. (4) and (6) and demonstrated in Figure 6.6 and Figure 6.7.

In summary, Figure 6.12 and Figure 6.13 show that the EITC for a given network size has two maxima for the reasons explained above. For instance, the absolute maximum is around 1.75 for the 30-node network. Meaning, with SDPPM-WIS, the network can have almost 75% more information transfer capacity for very low duty cycle (i.e., very large T) networks.

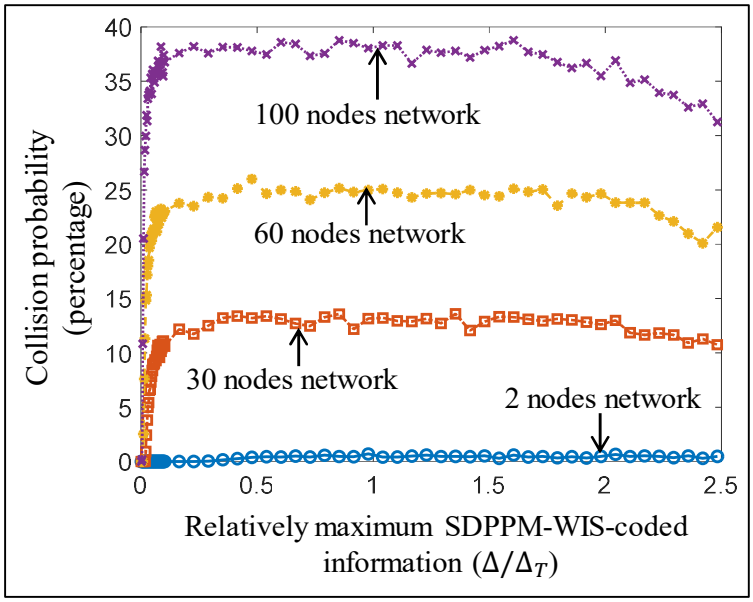


Figure 6.14: Collision probability with different amounts of transmission shifts

6.7.2. Impacts of Duty cycle

The baseline interval between two transmissions (i.e., T) determines the amount of free channel space available for the SDPPM-WIS protocol to encode additional information by time-shifting the transmissions. The operating duty cycle is $L\tau/T$. Since $T = L \cdot E/W$, duty cycle can be expressed as $W \cdot \tau/E$. In other words, for a given bit duration, and per-bit transmission energy budget E, duty cycle is determined by the energy harvesting rate W. Lower harvesting rates would cause lower duty cycles.

Figure 6.15 shows how the maximum Effective Information Transfer Capacity (EITC) reduces with higher duty cycles for different network size. For each point in the graph, the value of time shifts for which the EITC is maximized is marked. This is because with higher duty cycles, lesser amount of shifting space is available coupled with more frequent inter-node collision. Also, for larger networks, the maximum EITC is smaller due to more frequent collisions.

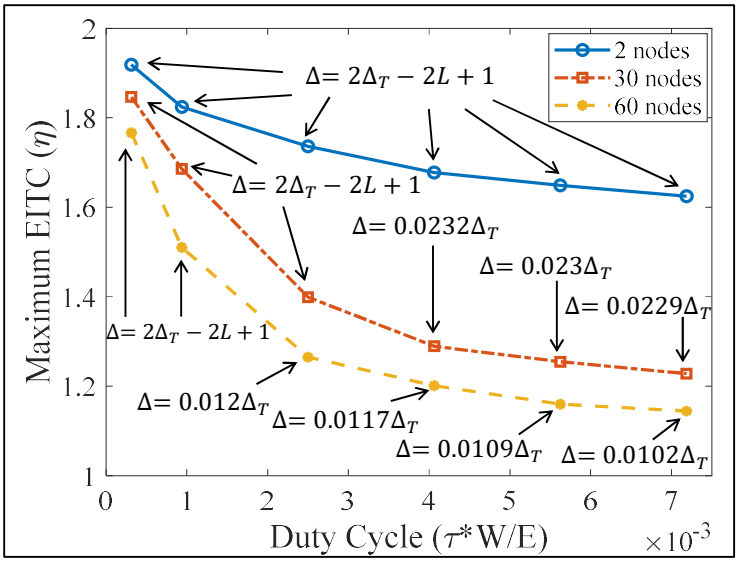


Figure 6.15: Duty cycle versus information transfer capacity

6.7.3. Impacts of Network Size

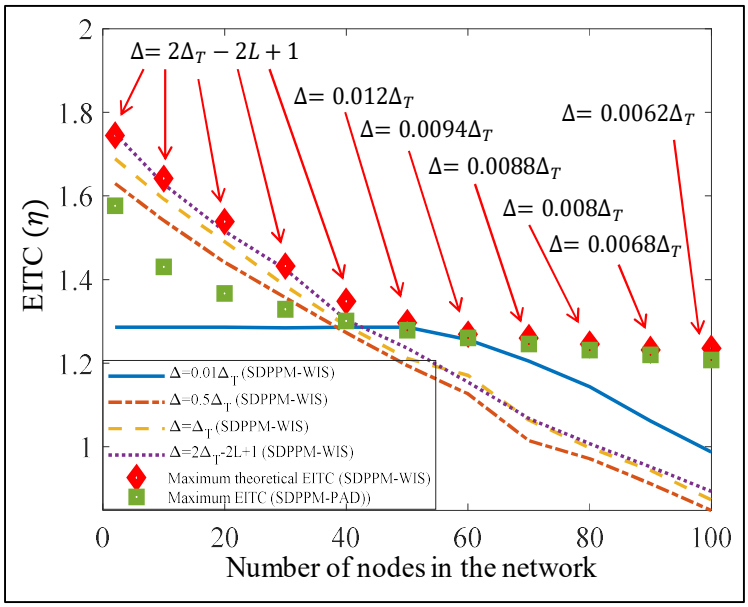


Figure 6.16: EITC for different network size

Figure 6.12, Figure 6.13, and Figure 6.14 also show that networks of all sizes yield similar performance trends, while smaller networks enjoy better effective information transfer capacity

due to fewer collisions. Also, for larger networks, SDPPM-WIS makes sense for limited shift values to achieve EITC values larger than 1.

Figure 6.16 shows more insight into the impacts of network size on the performance of SDPPM-PAD and SDPPM-WIS with different maximum allowed shift values (i.e., Δ). Observe that for SDPPM-WIS, for all Δ values, the effective information transfer capacity (EITC) drops with increasing network size. This is expected since the total amount of capacity gets distributed among all nodes in the fully connected network. It can be also observed that for all shift vales except $\Delta = 0.01\Delta_T$, EITC of SDPPM-WIS decreases for larger networks.

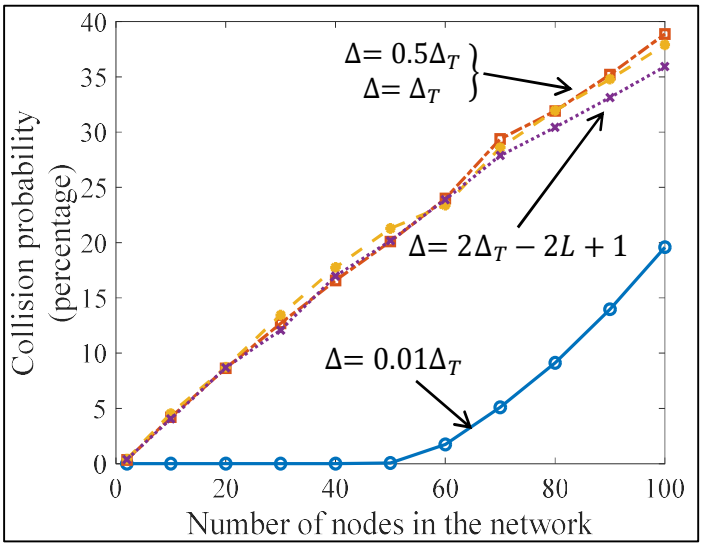


Figure 6.17: Collision probability for different network size

This is due to increasing collisions as shown in Figure 6.17. Except when $\Delta = 0.01\Delta_T$, due to the very small allowed shift, there is virtually no collisions for networks with less than approximately 50 nodes. Beyond that, collisions start increasing monotonically. The impacts of such collision profile are visible in Figure 6.16 in which the EITC for the $\Delta = 0.01\Delta_T$ remains

steady at approximately 1.3 till the network grows bigger than around 50 nodes, which is when EITC starts falling monotonically.

The diamond points in Figure 6.16 represent the upper envelope of EITC of SDPPM-WIS across all Δ values. The square points show the EITC values for SDPPM-PAD. Note that for smaller node-counts, the WIS version is able to achieve better overall information transfer capacity because unlike in the PAD version, the amount of maximum allowed shift is not restricted. With larger networks (i.e., larger than about 50 nodes), however, the collisions in SDPPM-WIS offset its benefits over the PAD version. This results in very similar performance for both the protocols.

6.7.4. Impacts of Packet Loss Due to Channel Errors

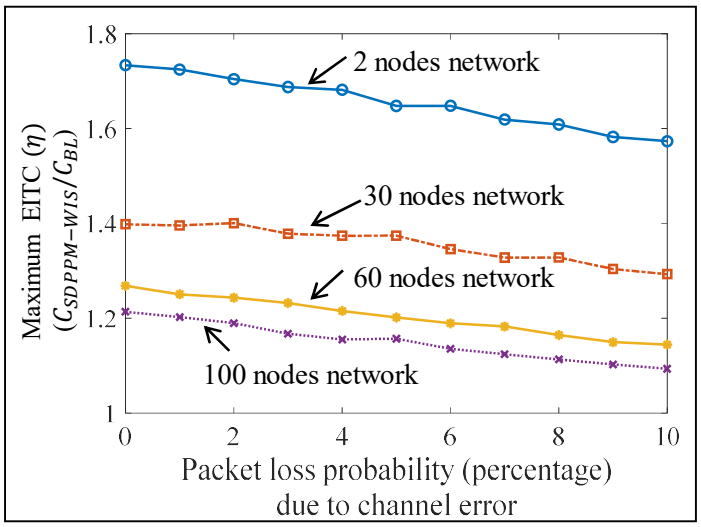


Figure 6.18: Impacts of channel errors on EITC

A lost packet has two distinct effects on the effective information transfer capacity. First, the raw information contained within the packet is lost. Additionally, two separate pieces of the SDPPM-coded information data is lost. One represented by the interval between the transmission times of the last packet and the lost packet, and the other represented by the interval between

timings of the lost packet and the next packet. Figure 6.18 reports the maximum attainable effective information transfer capacity (EITC) of SDPPM-WIS as a result of different packet loss probabilities due to channel errors. The experiments for these results are run such that for a given network size, the shift value (i.e., Δ) that provides the maximum EITC is chosen.

As expected, the capacity diminishes monotonically with higher packet losses, although the values remain larger than one for up to 10% packet losses. Meaning SDPPM-WIS still works better than the baseline case for up to 10% packet losses. It is notable that the decrease rate of EITC with higher packet losses are very similar for all network sizes. In summary, these results show that SDPPM-WIS is deployable in networks with reasonable packet losses due to channel errors.

6.8. Optical Time Shift for Maximizing Capacity

6.8.1. Computing Packet Position

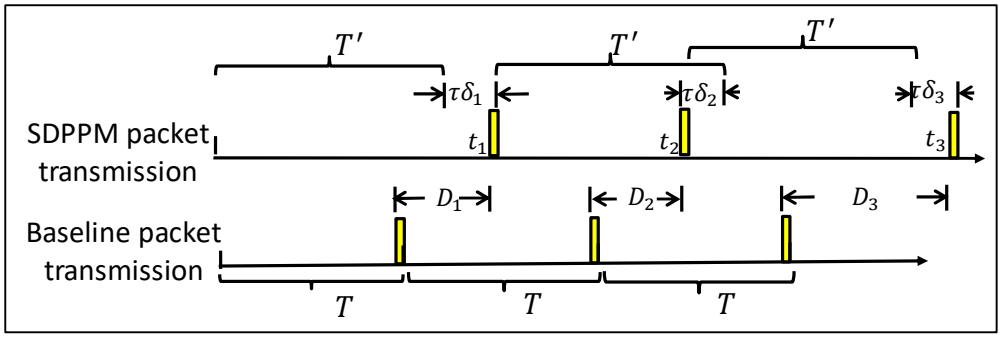


Figure 6.19: Packet position D in different scenarios

We define packet distance D as the time interval (in bit duration) between the baseline transmission time without SDPPM-WIS and the transmission time with SDPPM-WIS. This is illustrated in Figure 6.19, in which starting from zero energy reserve at time $t_1 = 0$, a sensor node postpones the first packet and sends at the time $t_1 = T' + \tau\beta_1$. The distance for the first packet is

$D_1 = \frac{t_1 - T}{\tau} + L$ in bit durations, and the instantaneous energy level at the node is $D_1 \tau W$. Similarly, the distances for the second packet (which is preponed) is $D_2 = \frac{t_2 - 2T}{\tau} + L$ bit durations, and the corresponding energy level is $D_2 \tau W$.

Since the baseline interval T is the minimum average inter-packet interval, the value of D_i in SDPPM-WIS is always larger than or equal to zero. The maximum possible distance is $D_i = 2\Delta - 1$, which can be obtained in the scenario when distances for three consecutive packets are $D_{i-2} = 0$, $D_{i-1} = \Delta - 1$ with the remaining energy level $(\Delta - 1)\tau W$ (i.e., postponing $\Delta - 1$ bit durations), and $D_i = 2\Delta - 1$ with the cumulative energy level $(2\Delta - 1)\tau W$ (i.e., postponing Δ bit durations), respectively.

We model the dynamics of the D values (i.e., in the range 0 to $2\Delta - 1$) in a node on packet by packet transmissions as a Markov Process with state transitions that depend on the available energy level and the time shift Δ. State is defined as the current value of D in bit duration τ. On every new packet transmission, a node's state changes, which is represented by its new D value corresponding to the new transmission. The process is Markovian since a state change depends only on the previous state and nothing beyond that. The resulting Markov chain is irreducible and aperiodic with a unique solution for the steady state probability of finding it at any of the possible states.

When $T' = T$, meaning the maximum allowed packet deferral $\Delta = \frac{T}{\tau}$, the initial timing of a node's transmission corresponds to $D = 0$. Meaning, the initial state $D_0 = 0$. The possible next state space can be represented by the vector $[0, 1, \cdots, 2\Delta - 1]$. The corresponding transition probability vector from D_0 is:

$$V_0 = \left[0, \overbrace{\frac{1}{\Delta}, \frac{1}{\Delta}, \cdots, \frac{1}{\Delta}}^{\Delta}, 0, 0, \cdots, 0\right] \tag{6.8}$$

Meaning that from the state D_0, a node can transit to the states $1, 2, \cdots, \Delta$ with individual probability $\frac{1}{\Delta}$, and it cannot transit to any other states. Similarly, when the current packet position is $D_i = 1$, the transition probability vector can be written as:

$$V_1 = \left[\overbrace{\frac{1}{\Delta}, 0, 0, \frac{1}{\Delta}, \cdots, \frac{1}{\Delta}}^{\Delta+2}, 0, 0, \cdots, 0\right] \tag{6.9}$$

This expression is obtained as follows. When the current state $D = 1$, it can be interpreted as a postponed transmission by one-bit duration from the previous state representing the state $D = 0$. Therefore, the maximum time distance where the next packet can be transmitted will represent the state $\Delta + 2$. As a result, the elements of V1 beyond that distance are all zero.

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ \vdots \\ \Delta{-}1 \\ \Delta \\ \Delta{+}1 \\ \vdots \\ 2\Delta{-}1 \end{array}
\begin{array}{c}
\begin{array}{ccccccccccc} 0 & 1 & 2 & 3 & \cdots & \Delta{-}1 & \Delta & \Delta{+}1 & \Delta{+}2 & \cdots & 2\Delta{-}2 & 2\Delta{-}1 \end{array} \\
\left[\begin{array}{ccccccccccc}
0 & 1/\Delta & 1/\Delta & 1/\Delta & \cdots & 1/\Delta & 1/\Delta & 0 & 0 & \cdots & 0 & 0 \\
1/\Delta & 0 & 0 & 1/\Delta & \cdots & 1/\Delta & 1/\Delta & 1/\Delta & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1/\Delta & 1/\Delta & 1/\Delta & 1/\Delta & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 1/\Delta \\
1/\Delta & 1/\Delta & 1/\Delta & 1/\Delta & \cdots & 1/\Delta & 0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1/\Delta & 1/\Delta & 1/\Delta & \cdots & 1/\Delta & 1/\Delta & 0 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1/\Delta & 1/\Delta & 1/\Delta & 1/\Delta & \cdots & 1/\Delta & 0
\end{array}\right]
\end{array}
= P \tag{6.10}$$

After combining the transition probability vectors for all possible states $D = 0$ to $D = 2\Delta - 1$, the complete transition probability matrix can be written as shown in Eqn. (10). This matrix can be used for computing the packet position distribution, and subsequently, the steady state probability of inter-node collisions induced by SDPPM-WIS. Figure 6.20 shows an example

probability mass function (PMF) for the positions of packets from two nodes. These represent an energy harvesting rate of $W = 2\ mW$ and packet length of $L = 16\ bits$. The time shift parameter $\Delta = 240$ in bit durations is used by each node.

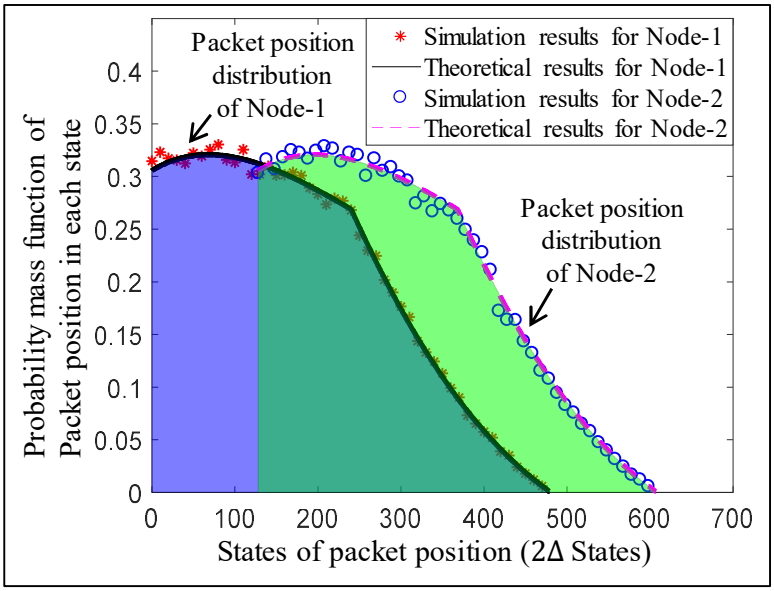


Figure 6.20: Packet position distributions in a network

Note that since SDPPM-WIS does not perform carrier sensing, the packet position distributions at each node is independent of that for the other nodes. The black solid and pink dash line in Figure 6.20 represent theoretical values of steady state packet position distributions computed using the probability matrix in Eqn. (10). The discrete points indicate PMF obtained through simulation experiments. Results show excellent agreements among the analytical and experimental values.

6.8.2. Computing Collision Probability

In Figure 6.19, even though the nodal packet position PMFs are mutually independent, the overlapping of the two PMF graphs represent inter-node collisions. In fact, the area under the

overlapping part is a measure of collision probability as presented below. As derived earlier in Chapter 6.5, the maximum information transfer capacity in SDPPM-WIS for a single node scenario can be achieved when $\Delta = \frac{2L \cdot E}{W \cdot \tau} - 2L + 1$. Let us consider an N-node network with the node Ids $\in [1, N]$, in which the initial state for each node is randomly placed within the baseline time interval T. Such states are formally defined as $[D_0^{(1)}, D_1^{(1)}, \cdots, D_{2\Delta-1}^{(1)}]$ for Node-1, $[D_{\frac{T}{\tau N}}^{(2)}, D_{\frac{T}{\tau N}+1}^{(2)}, \cdots, D_{\frac{T}{\tau N}+2\Delta-1}^{(2)}]$ for Node-2, and so on, and $[D_{\frac{T(N-1)}{\tau N}}^{(N)}, D_{\frac{T(N-1)}{\tau N}+1}^{(N)}, \cdots, D_{\frac{T(N-1)}{\tau N}+2\Delta-1}^{(N)}]$ for Node-N. The probability of packet position at each state is defined as $P_{D_i}^{(j)}$ ($j = 0,1,\cdots,N$ and $i = 0,1,\cdots,T(N-1)/\tau/N + 2\Delta - 1$).

We compute the collision probability for Node-1 at any state D_i ($i = 0, 1, \cdots, \frac{T(N-1)}{\tau N} + 2\Delta - 1$). First, calculate the probability that the packets from Node-1 at state D_i collides with the packets from Node-2. When the packet from Node-1 appears at state D_i, collision happens when the packet from Node-2 appear at states between D_{i-L+1} and D_{i+L-1}, but Node-3, Node-4, ⋯, Node-N should not appear between D_{i-L+1} and D_{i+L-1}. The collision probability for the packets at state D_i from Node-1 with the packets from Node-2 can be expressed as:

$$P_{D_i}^{(1)} \left(\sum_{D_j \in [D_{i-L+1},\ D_{i+L-1}]} P_{D_j}^{(2)} \right) \cdot \left(\prod_{a \in [1,N] \backslash \{1,2\}} \left(\sum_{D_k \in [0, \frac{T(N-1)}{\tau N} + 2\Delta - 1] \backslash [D_{i-L+1},\ D_{i+L-1}]} P_{D_k}^{(a)} \right) \right) \quad (6.11)$$

where the notation $a \in [1,\ N] \backslash \{1,2\}$ indicates $a \in [1,\ N]$ and $a \notin \{1,2\}$. The next step is to compute the probability that packets from Node-1 collide with the packets from Node-3, Node-4, ⋯, Node-$(N-1)$. These probabilities are denoted as $P_4^{(1)}, P_5^{(1)}, \cdots, P_N^{(1)}$. When M number of packets are sent by N number of nodes, each node sends $\frac{M}{N}$ packets due to their same energy harvesting rate. The collision probability for an N-node network can be expressed as:

$$\left(\frac{M}{N}\left(P_2^{(1)} + P_3^{(1)} + \cdots + P_N^{(1)}\right) + \frac{M}{N}\left(P_2^{(2)} + P_3^{(2)} + \cdots + P_N^{(2)}\right) + \cdots\right.$$

$$\left. + \frac{M}{N}\left(P_2^{(N)} + P_3^{(N)} + \cdots + P_N^{(N)}\right)\right) \cdot \frac{1}{M} = \frac{1}{N}\sum_{x=1}^{N}\sum_{y=2}^{N} P_y^{(x)} \quad (6.12)$$

6.8.3. Computing Optimal Time Shift for Maximizing Capacity

Building on the above models, the question addressed here is how to choose the optimal time shift amount in SDPPM-WIS for maximizing the information transfer capacity for a given set of system parameters including E, τ, W, N and L.

Initialize the time shift as the baseline inter-packet interval, which is $\Delta = \Delta_T$. For this shift value, the EITC $\eta_{\Delta=\Delta_T}$ can be calculated using Eqns. (10), (11), and (12), and can be expressed as:

$$\eta_{\Delta=\Delta_T} = \frac{1}{N}\sum_{x=1}^{N}\sum_{y=2}^{N} P_y^{(x)} \cdot \frac{L + \frac{\log_2(\Delta!)}{\Delta}}{L} \quad (6.13)$$

If the value $\eta_{\Delta=\Delta_T}$ is less than one, this means that collision significantly reduces the capacity due to a large Δ. The value of optimum shift Δ_0 for maximum capacity in this case falls in the range of $[\frac{T}{2\tau N}, \frac{T}{\tau N}]$, which can be found through the calculation of EITC η_Δ using Eqns. (10), (11), and (12). However, if the value $\eta_{\Delta=\Delta_T}$ is equal to or greater than one, the value of Δ_0 either falls in the range of $[\frac{T}{\tau N}, \frac{T}{\tau}]$ or is equal to $\frac{2L \cdot E}{W \cdot \tau} - 2L + 1$. The comparison of EITC for those Δ values can provide the optimal shift amount. The following algorithm defines the overall search process for the optimal shift values.

1) Calculate EITC $\eta_{\Delta=\Delta_T}$ when $\Delta = \Delta_T$ using Eqn. (13); If $\eta_{\Delta=\Delta_T} < 1$, go to (4). Otherwise, go to (2);

2) Calculate EITC η_{Δ} when $\Delta \in [\frac{T}{\tau N}, \frac{T}{\tau}]$ using Eqn. (13), and find the maximum η_{Δ_1} and the corresponding time shift value Δ_1. Then go to (3).
3) Calculate EITC η_{Δ_2} when $\Delta_2 = 2L \cdot E/W/\tau - 2L + 1$. Compare the two values of effective channel capacity η_{Δ_1} and η_{Δ_2}. If $\eta_{\Delta_1} \geq \eta_{\Delta_2}$, then the time shift for maximum channel capacity $\Delta_0 = \Delta_1$. If $\eta_{\Delta_1} < \eta_{\Delta_2}$, the time shift parameter $\Delta_0 = \Delta_2 = 2L \cdot E/W/\tau - 2L + 1$. Go to (5).
4) Calculate EITC η_{Δ} when $\Delta \in [\frac{T}{2\tau N}, \frac{T}{\tau N}]$ using Eqn. (13), and find the maximum η_{Δ_0} and the corresponding time shift value Δ_0. The time shift Δ_0 is obtained. Go to (5).
5) Output the time shift parameter Δ_0 and the corresponding maximum effective information transfer η_{Δ_0}.

The above analytical model and algorithm for choosing optimal time shift in SDPPM-WIS can be used for determining the correct operating points of a deployable SDPPM-WIS based energy-constrained network with low duty cycle.

6.9. Summary

This chapter presents a novel packet position modulation concept for enabling additional information transfer without incurring additional energy expenditure. The key concept is to encode the additional information by modulating the time of packet transmissions. The chapter developed an asymmetric and a symmetric version of the protocol to demonstrate how they can pack in more information using the proposed technique. It then extends the symmetric mechanism for multiaccess networks with large number of transmit-only sensor and/or IoT nodes. A methodology is developed for calculating the time shift parameter in packet position modulation for maximizing the achievable information transfer capacity. A concrete mathematical analysis is also developed for getting insight to the method.

CHAPTER 7: FUTURE WORKS

7.1. Introduction

Results from this thesis demonstrate that transmission timing modulation can effectively increase energy efficiency, security, and transfer information capacity of WSNs. In Chapter 3, we proposed a PPCP architecture to achieve significant energy-saving in Tx-only networks. In Chapter 4, we extended the PPCP architecture to a multi-access sensor network and developed multi-format PDUs for collision avoidance. In Chapter 5, we combined the PPCP concept with chaotic function and designed a chaos-based secure communication for WSNs. In Chapter 6, we designed a DPPM paradigm to enhance information transfer capacity of communication links used by energy-constrained devices. Building on the above work, the following research works can be conducted.

7.2. Joint Pulse Position and Pulse Width Modulation (PPnPWM)

PPnPWM uses a further compact architecture to reduce the number of bits to be transmitted in a PDU transmission, which has the potential to drastically reduce communication energy costs and to increase network lifetime. A data value δ can be represented as the limited number of digits based on a base-β. For example, value $\delta = 192$ can be represent as $5, 3,$ and 0 based on base-6 ($\beta = 6$). Instead of transmitting the real digit number, a compression mechanism is used to shrink the value of the digit number. If a digit $d > \frac{\beta}{2}$, the transmitted digit becomes $(\beta - d)$. An wider pulse is inserted in front of the digit to indicate that the incoming digit is a compressed one. As shown in Figure 7.1: Example of PPnPWM architecture, the first data value $\delta_1 = 192$ is represent as $5, 3,$ and 0 when base $\beta = 6$. However, δ_1 is transmitted as $1, 3,$ and 0 in order to reduce the transmission delay.

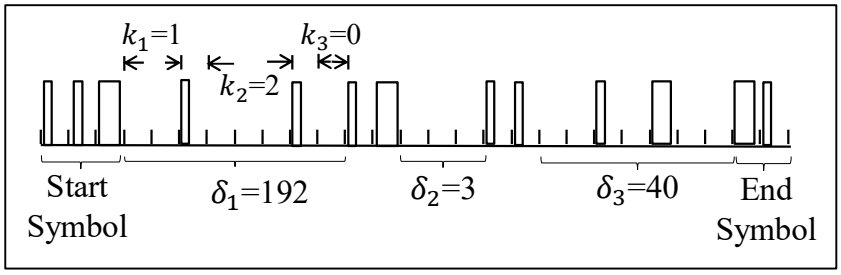


Figure 7.1: Example of PPnPWM architecture

Such a PDU architecture combines pulse position and pulse width modulation for the compression of transmitted data and puts transceivers into sleep mode earlier compared to the traditional packet modulation and our previous work PPCP. The transmission delay can be significantly decreased in terms of PPnPWM representation during the communication in WSNs.

7.3. Robustness and Error Correction of Packet Position Coded PDU

There has been considerable work on the problem of designing error detection and correction techniques in conventional binary packet transmission. All error-detection and correction schemes add some redundancy (i.e., some extra data) to a message, which receivers can use to check consistency of the delivered message, and to recover data that has been determined to be corrupted. Error-detection and correction schemes can be either systematic or non-systematic. In a systematic scheme, the transmitter sends the original data, and attaches a fixed number of check bits (parity or CRC data), which are derived from the data bits by some deterministic algorithm. In a system that uses a non-systematic code, the original message is transformed into an encoded message carrying the same information and that has at least as many bits as the original message.

However, such redundancy bits in each packet PDU for error correction reduce the energy-efficiency of sensor network and data information transmission per unit of energy. In PPCP, the

proposed architecture-based error detection for pulse-based transmission has been discussed in Chapter 3, Chapter 4, and Chapter 5. the research on this topic can be further pursued for developing error-correction techniques towards pulse-based PDU transmissions without adding redundant pulses. Since there are limited number of pulses with a fixed width in a PPCP PDU architecture, most of false pulses (due to noise or power fluctuation) can be detected due to its narrow pulse width. Based on the pulse width difference, a pulse width can be carefully chosen for PPCP PDU to further distinguish the real pulse with false pulse. The received PDU corrupted by false pulses can be recovered to avoid the energy consumption of data retransmission.

The following research perspectives should be considered in order to design a reliable PPCP architecture-based error correction mechanism. (1) The positions and formats of false pulses which happen in a PPCP should be analyzed, either in inter-pulse interval or in the middle of data pulses. (2) When a narrow false pulse occurs in a PPCP pulse, a receiver can detect three or four rising or falling edges of pulses in a real pulse duration. Three or four edges can generate less than or equal to 2^4 receiving patterns. A state machine and a transition table should be clearly developed based on the above receiving patterns. (3) A detection window, which allowed the maximum number of edges to be analyzed simultaneously, should be selected for reducing the complexity of multi-state transition, and at the same time, to guarantee the PPCP error correction rate. (4) A strict screening mechanism should be established to eliminate the false pulse and to avoid false positive PPCP decoding.

7.4. Quadrature Amplitude Modulation (QAM) based Pulse Position Coded PDU

PPCP architecture was developed based on the ASK or QMSK modulation, which constrains PPCP into the applications which require a high-rate data flow or a burst of data flow. Quadrature amplitude modulation (QAM) technique is a method of combining two amplitude-

modulated (AM) signals into a single channel, which has been widely used in 4G/LTE and IoT applications to carry higher data rates than ordinary amplitude modulated schemes and phase modulated schemes in digital transmission. A combination of PPCP and M-QAM ($M \geq 2$) can increase the PPCP data transmission rate for supporting a wider range of IoT applications, for example, video data transmission in a WSN.

In order to combine PPCP with multi-order QAM, the following research items should to be considered: (1) Since $\beta + 1$ (β is the base) patterns are used to represent different data symbols during each PPCP PDU transmission. In order to combine with QAM, a constellation diagram, which shows all the possible symbols that can be transmitted by the system as a collection of points, should be specifically designed to fit the PPCP architecture. (2) The base β should be also deduced for the tradeoff between minimizing the energy consumption and supporting the required data transmission rate for a specific IoT application. (3) A flexible modulation architecture should be established for PPCP to support multi-order QAM in variety of channel noise levels. For example, the base β should fit both for low order of QAM in a high SNR channel and for high order of QAM in a low SNR channel. Meanwhile, PPCP architecture should achieve a high utilization efficiency of points for a high data transmission rate in each QAM constellation.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] A. A. Bavarva and P. V. Jani , "Improve the channel performance of Wireless Multimedia Sensor Network using MIMO properties," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2015.

[2] B. Blaszczyszyn and B. Radunovic, "Using Transmit-Only Sensors to Reduce Deployment Cost of Wireless Sensor Networks," in *IEEE 27th Conference on Computer Communications*, 2008.

[3] D. Feng, Y. Shi, S. Das and S. Biswas, "Chaotic Pulse Position Coded PDUs for Secure and Energy-Efficient Data Networking," in *IEEE Globe Communications Conference (GLOBECOM)*, 2018.

[4] S. Biswas, D. Feng, F. Hajiaghajani and S. Das, "Method for Transmitting Data using Inter-Pulse Interval Modulation Technique". United States Patent 10051663, 2018.

[5] O. Mokrenko, "Energy management of a Wireless Sensor Network at application level," Automatic.Universite Toulouse III Paul Sabatier, 2015.

[6] R. C. O'Reilly and Y. Munakata, Computational explorations in cognitive neuroscience: Understanding the mind by simulating the brain, London, England: The MIT Press, 2000.

[7] Charles Stangor, Beginning Psychology, vol. 298, N.p., n.p, 2012, pp. 556-562.

[8] F. Rieke, D. Warland, R. R. Steveninck and W. Bialek, Spikes: Exploring the Neural Code, MIT Press, 2014.

[9] I. Nemenman, G. D. Lewen, W. Bialek, and R. R. Steveninck, "Neural Coding of Natural Stimuli: Information at Sub-Millisecond Resolution," *PLoS Computational Biology,* vol. 4, no. 3, 2008.

[10] W. B. Levy and R. A. Baxter, "Energy efficient neural codes," *Neural Computation,* vol. 8, no. 3, 1996.

[11] L. Grobe, A. Paraskevopoulos, J. Hilt, etc, "High-speed visible light communication systems," *Communications Magazine, IEEE,* vol. 51, no. 12, pp. 60-66, 2013.

[12] IEEE P802.15 working group for Wireless Personal Area Networks (WPANs) DS-UWB physical layer submission to 802.15 task group 3a, 2005.

[13] K. Kil, B. Song, S. Jung and D. Park, "New preamble design for reduced-complexity timing acquisition in UWB systems," in *Proceedings of Vehicular Technology Conference (VTC)*, 2006.

[14] R. Gupta, K. Sultania, P. Singh and A. Gupta, "Security for wireless sensor networks in military operations," in *Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* , 2013.

[15] J. Grover, S. Sharma and M. Sharma, "Optimized GAF in Wireless Sensor Network," in *IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)*, 2014.

[16] S.V. Annlin Jeba, B. Paramasivan and D. Usha, "Security Threats and its Countermeasures in Wireless Sensor Networks: An Overview," *International Journal of Computer Applications,* vol. 26, no. 9, pp. 15-22, 2011.

[17] S. Zhu, S. Setia and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN),* vol. 2, no. 6, pp. 500-528, 2006.

[18] H. Modares, R. Salleh and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," in *2011 Third International Conference on Computational Intelligence, Modelling & Simulation*, 2011.

[19] C. Karlof, N. Sastry and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *SenSys '04 Proceedings of the 2nd international conference on Embedded networked sensor systems*, 2004.

[20] P. Stavroulakis, Chaos Applications in Telecommunications, New York, NY, USA: CRC Press, 2005.

[21] K. Fallahi, R. Raoufi and H. Khoshbin, "An application of Chen system for secure chaotic communication based on extended Kalman filter and multi-shift cipher algorithm," *Communications in Nonlinear Science and Numerical Simulation,* vol. 13, no. 4, 2008.

[22] J.M.V. Grzybowski, M. Rafikov and J.M.Balthazar, "Synchronization of the unified chaotic system and application in secure communication," *Communications in Nonlinear Science and Numerical Simulation,* vol. 14, no. 6, 2009.

[23] O. Gonzales, G. Han, J. Gyvez, and E. Sanchez-Sinencio, "Lorenz-based chaotic cryptosystem: a monolithic implementation," *EEE Trans Circuits Syst. I,* vol. 47, p. 1243–1247, 2000.

[24] H. C. Keong, K. M. S. Thotahewa and M. R. Yuce, "Transmit-Only Ultra Wide Band Body Sensors and Collision Analysis," *IEEE SENSORS JOURNAL,* vol. 13, no. 5, 2013.

[25] A. K. Dhulipala, C. Fragouli, and A. Orlitsky, "Silence-based communication," *IEEE Trans. on Information Theory,* pp. 350-366, 2010.

[26] J. Long, M. Dong, K. Ota and A. Liu, "A Green TDMA Scheduling Algorithm for Prolonging Lifetime in Wireless Sensor Networks," *IEEE Systems Journal,* vol. 11, no. 2, pp. 868 - 877, June 2017.

[27] C. Gomez, J. Oller, and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," *Sensors,* vol. 12, no. 9, pp. 11734-11753, 2012.

[28] D. Wang and J. Zhang, "Variable-base tacit communication: a new energy efficient communication scheme for sensor networks," in *Conference on Integrated internet ad hoc and sensor networks*, Nice, France, May 30, 2006.

[29] P. Karn, "MACA-a new channel access method for packet radio," in *ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, 1990.

[30] K. P. Geethapriya, I. Kala and S. Karthik, "A study on data aggregation scheme over wireless sensor network," in *10th International Conference on Intelligent Systems and Control (ISCO)*, 2016.

[31] J.N. Al-Karaki, R. Ul-Mustafa and A.E. Kamal, "Data aggregation in wireless sensor networks - exact and approximate algorithms," in *2004 Workshop on High Performance Switching and Routing*, 2004.

[32] C. Schurgers and M.B. Srivastava, "Energy efficient routing in wireless sensor networks," in *MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force*, 2001.

[33] J.N. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications,* vol. 11, no. 6, pp. 6-28, 2004.

[34] M. Bakshi, B. Jaumard, M. Kaddour, and L. Narayanan, "On TDMA scheduling in wireless sensor networks," in *Electrical and Computer Engineering (CCECE), 2016 IEEE Canadian Conference on*, May 2016.

[35] S. Chen, T. Sun, J. Yuan, X. Geng, C. Li, S. Ullah and M. A. Alnuem, "Performance Analysis of IEEE 802.15.4e Time Slotted Channel Hopping for Low-Rate Wireless Networks," *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS,* vol. 7, no. 1, 2013.

[36] Zigbee Alliance, "ZigBee Document 053474r06, Version 1.0, ZigBee Specification," 2004. [Online].

[37] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," *IEEE/ACM transactions on networking,* vol. 12, no. 3, June 2004.

[38] T. Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *SenSys '03 Proceedings of the 1st international conference on Embedded networked sensor systems* , Los Angeles, California, 2003.

[39] S. Ray, I. Demirkol and W. Heinzelman, "ADV-MAC: Analysis and optimization of energy efficiency through data advertisements for wireless sensor networks," *Ad Hoc Networks,* vol. 9, no. 5, p. 876–892, July 2011.

[40] S. Yessad, F. N. Abdesselam, T. Taleb, and B. Bensaou, "R-MAC: Reservation Medium Access Control Protocol for Wireless Sensor Networks," in *IEEE Conf. on Local Computer Networks*, October 2007.

[41] Y. Zhu and R. Sivakumar, "Challenges: communication through silence in wireless sensor networks," in *Proceedings of the International Conference on Mobile Computing and Networking (MobiCom)*, 2005.

[42] Y. Fujiwara, "Self-synchronizing pulse position modulation with error tolerance," *IEEE Transactions on Information Theory,* vol. 59, p. 5352–5362, 2013.

[43] H. Park and J.R. Barry, "Performance of multiple pulse position modulation on multipath channels," in *IEE Proceedings - Optoelectronics*, Dec. 1996.

[44] D. S. Shiu and J.M. Kahn, "Differential pulse-position modulation for power-efficient optical communication," *IEEE Trans. on Communications,* vol. 47, 1999.

[45] D. Feng, F. Hajiaghajani, S. Das, and S. Biswas, "Pulse Position Coded PDUs: A New Approach to Networking Energy Economy," in *IEEE Consumer Communications & Networking Conference*, Las Vegas, Jan 2017.

[46] J. Grover and S. Sharma , "Security issues in Wireless Sensor Network — A review," in *5th International Conference on Reliability, Infocom Technologies and Optimization*, 2016.

[47] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *International Journal of Bifurcation and Chaos,* vol. 03, no. 06, 1993.

[48] G. Kolumban, G. Kis, Z. Jákó and M. P. Kennedy, "FM-DCSK: A robust modulation scheme for chaotic communications," *IEICE Trans. Fund.,* Vols. E81-A, no. 9, 1998.

[49] N. F. Rulkov and L. S. Tsimring, "Synchronization methods for communication with chaos over band-limited channels," *Int. J. Circuit Theory Appl. ,* vol. 27, no. 6, pp. 555-567, 1999.

[50] M. Hasler, "Synchronization of Chaotic Systems and Transmission of Information," *Int. J. Bifurcation Chaos,* vol. 08, no. 04, 1998.

[51] W. M. Tam, F. C. M. Lau, and C. K. Tse, Digital Communication with Chaos Multiple Access Techniques, Amsterdam, The Netherlands: Elsevier Science, 2006.

[52] C. C. Chen and K. Yao, "Numerical Evaluation of Error Probabilities of Self-Synchronizing Chaotic Communications," *IEEE COMMUNICATIONS LETTERS,* vol. 4, no. 2, 2000.

[53] M. M. Sushchik, N. Rulkov, L. Larson et al., "Chaotic pulse position modulation: a robust method of communicating with chaos," *IEEE Communication Letters,* vol. 4, no. 4, p. 128–130, 2000.

[54] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Digital communication using chaotic-pulse-position modulation," *IEEE Trans. on Circuits and Systems,* vol. 48, no. 12, 2001.

[55] N. X. Quyen, V. V. Yem, and T. M. Hoang, "A Chaotic Pulse-Time Modulation Method for Digital Communication," *Abstract and Applied Analysis,* 2012.

[56] V. P. Vijayan and E. Gopinathan , "Improving Network Coverage and Life-Time in a Cooperative Wireless Mobile Sensor Network," in *International Conference on Advances in Computing and Communications*, 2014.

[57] P. R. Dike, V, M. Rohakle, T. S. Vishwanath and N. N. Pachpor , "Wireless sensor network multirate signal processing for channel capacity and delay improvement," in *International Conference on Inventive Computation Technologies (ICICT)*, 2016.

[58] I. Rhee, A. Warrier, M. Aia, J. Min and M. L. Sichitiu, "Z-MAC: a hybrid MAC for wireless sensor networks," *IEEE/ACM Transactions on Networking (TON),* vol. 16, no. 3, 2008.

[59] N. Abramson, "The ALOHA System - Another Alternative for Computer Communications," in *Fall Joint Computer Conference*, 1970.

[60] C. Pham, "Investigating and experimenting CSMA channel access mechanisms for LoRa IoT networks," in *IEEE Wireless Communications and Networking Conference*, 2018.

[61] A. F. Molisch et al., "IEEE 802.15.4a Channel Model-Final Report," Tech. Rep., Document IEEE 802.1504-0062-02-004a, 2005.

[62] V. Stangaciu, M. V. Micea, V. I. Cretu and V. Groza, "General slot stealing TDMA scheme to improve the low channel utilization factor," in *International Symposium on Intelligent Signal Processing (WISP)* , 2015.

[63] R. Zhang, X. Cheng, X. Cheng and L. Yang , "Interference-Free Graph Based TDMA Protocol for Underwater Acoustic Sensor Networks," *IEEE Transactions on Vehicular Technology,* vol. 67, no. 5, 2018.

[64] S. Zhuo, Y. Q. Song, Z. Wang and Z. Wang, "Queue-MAC: A queue-length aware hybrid CSMA/TDMA MAC protocol for providing dynamic adaptation to traffic and duty-cycle variation in wireless sensor networks," *IEEE International Workshop on Factory Communication Systems,* 2012.

[65] C. Huebner, R. C. Oliver, S. Hanelt, T. Wagenknecht and A. Monsalve, "Long-range wireless sensor networks with transmit-only nodes and software-defined receivers," *WIRELESS COMMUNICATIONS AND MOBILE COMPUTING,* vol. 13, no. 17, 2013.

[66] P. Bahl, R. Chandra and J. Dunagan, "SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks," in *International conference on Mobile computing and networking*, 2004.

[67] B. Radunovic, H. L. Truong and M. Weisenhorn, "Receiver architectures for UWB-based transmit-only sensor networks," in *ICUWB*, 2005.

[68] L. Zhong, J. Rabaey and A. Wolisz, "Does proper coding make single hop wireless sensor networks reality: the power consumption perspective," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, 2005 .

[69] D. chmidt, M. Berning and N. Wehn, "Error correction in single-hop wireless sensor networks—a case study," in *Design, Automation and Test in Europe Conference and Exhibition*, 2009.

[70] A. El-Hoiydi and J. Decotignie, "Low power downlink MAC protocols for infrastructure wireless sensor networks," *ACM Mobile Networks and Applications,* vol. 10, no. 5, pp. 675-690, 2005.

[71] "https://www.sparkfun.com/products/10534 and /products /10532," [Online].

[72] "http://www.airspayce.com/mikem/arduino/VirtualWire/," [Online].

[73] M. Siekkinen, M. Hiienkari, J. K. Nurminen and J. Niemi, "How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4," in *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Paris, April 2012.

[74] "Transceiver (SparkFun)," Ref. No.: WRL-10534 and WRL-10532, [Online]. Available: https://www.sparkfun.com/products/10534, https://www.sparkfun.com/products//products/10532.

[75] "Arduino Pro Mini (SparkFun)," Ref. No.: DEV-11114 RoHS, [Online]. Available: https://learn.sparkfun.com/tutorials/using-the-arduino-pro-mini-33v/all.pdf.

[76] "Bluetooth v4.0 (Laird)," Ref. No.: BL600-SA, [Online]. Available: assets.lairdtech.com/home/brandworld/files/Datasheet%20-%20BL600.pdf.

[77] "Energy Harvester (Linear Technologies)," Ref. No.: BOB-09946, [Online]. Available: https://cdn.sparkfun.com/datasheets/BreakoutBoards/35881fc.pdf.

[78] "Supercapacitor (SparkFun)," Ref. No.: COM-00746, [Online]. Available: https://www.sparkfun.com/datasheets/Components/TS12S-R.pdf.

[79] J. G. Proakis, Digital Communications, Singapore: McGraw Hill, 1995.

[80] G. Kennedy and B. Davis, Electronic Communication Systems (4th edition), McGraw-Hill International, 1992.

[81] M. C. Gleichert, A. Hsu and Y. C. Wang, "Method and apparatus for transmitting and receiving both 8B/10B code and 10B/12B code in a switchable 8B/10B transmitter and receiver". US Grant Patent US5387911A, 1992.

[82] V. Bharghavan, A. Demers, S. Shenker and S. Shenker, "MACAW: a media access protocol for wireless LAN's," in *In the Proc. ACM SIGCOMM Conference (SIGCOMM '94)*, 1994.

[83] L. E. Larson, J. M. Liu, and L. Tsimring, Digital Communications Using Chaos and Nonlinear Dynamics, Heidelberg: Germany: Springer-Verlag.

[84] D. Feng, Y. Shi, S. D. S. Biswas, "Energy-Efficient and Secure Data Networking Using Chaotic Pulse Position Coded PDUs," *IEEE Transactions on Green Communications and Networking,* 2019.

[85] S. Haykin and M. Moher, Modern wireless communications, 2004.

[86] M. Hayashi, "Second-Order Asymptotics in Fixed-Length Source Coding and Intrinsic Randomness," *IEEE TRANS. ON INFORMATION THEORY,* vol. 54, no. 10, Oct. 2008.

[87] L. O. Martin, P. P. Sanchez, P. P. Lopez and J. Tapiador, "Heartbeats Do Not Make Good Pseudo-Random Number Generators: An Analysis of the Randomness of Inter-Pulse Intervals," *Entropy,* vol. 20, no. 2, 2018.

[88] D. Sen and S. K. Pal, "Generalized Rough Sets, Entropy, and Image Ambiguity Measures," *IEEE TRANS. ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS,,* vol. 39, no. 1, 2009.

[89] V. Paunic, L. Gragert, A. Madbouly, J. Freeman and M. Maiers, "Measuring Ambiguity in HLA Typing Methods," *PloS one,* 2012.

[90] S. K. Pal and S. Kundu, "Granular Social Network: Model and Applications," in *Handbook of Big Data Technologies*, Springer, 2017, pp. 617-651.

[91] Z. Lin and P. Wei, "Pulse Position Modulation Time Hopping Ultra Wideband Sharing Signal for Radar and Communication System," in *International Conference on Radar, CIE '06.*, 2006.

[92] J.A.N. da Silva and M.L.R. de Campos, "Performance comparison of binary and quaternary UWB modulation schemes," in *GLOBECOM '03. IEEE*, Dec. 2003.

[93] N. Tahir, N. M. Saad, B. B. Samir, V. K. Jain and S. A. Aljunid, "Binary Pulse Position Modulation Simulation System in Free Space Optical Communication Systems," in *International Conference on Intelligent and Advanced Systems (ICIAS)*, 2011.

[94] F. R. Mireles, "Performance of ultrawideband SSMA using time hopping and M-ary PPM," *IEEE Journal on Selected Areas in Communications,* vol. 19, no. 6, 2001.

[95] A. Fort; J. Ryckaert; C. Desset; P. De Doncker; P. Wambacq; L. Van Biesen, "Ultra-Wideband Channel Model for Communication Around the Human Body," *IEEE Journal on Selected Areas in Communications,* vol. 24, no. 4, pp. 927 - 933, 2006.

[96] Q. Wang, T. Tayamachi, I. Kimura and J. Wang, "An On-Body Channel Model for UWB Body Area Communications for Various Postures," *IEEE Transactions on Antennas and Propagation,* vol. 57, no. 4, pp. 991-998, 2009.

[97] J. R. Foerster, M. Pendergrass and A. F. Molisch, "A Channel Model for Ultrawideband Indoor Communication," 2003. [Online]. Available: http://www.merl.com/reports/docs/TR2003-73.pdf.

[98] P. J. Vial, B. Wysocki and T. Wysocki, "An Ultra Wide Band Simulator Using MATLAB/Simulink," in *18-21st Dec. DSPCS05' & WITSP'05*, Noosa Heads, Queensland, 2005.

[99] S. Guo, L. He, Y. Gu, B. Jiang and T. He, "Opportunistic Flooding in Low-Duty-Cycle Wireless Sensor Networks with Unreliable Links," *IEEE Transactions on Computers,* vol. 63, no. 11, 2014.

[100] D. Feng, S. Das, F. Hajiaghajani, Y. Shi and S. Biswas, "Pulse Position Coded Medium Access in energy-starved networks," *Computer Communications,* vol. 148, 2019.

[101] G. Miao, J. Zander, K. W. Sung and B. Slimane, Fundamentals of Mobile Data Networks, Cambridge University Press, 2016.

[102] S. Sudevalayam and P. Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications," *IEEE Communications Surveys & Tutorials,* vol. 13, no. 3, 2011.

[103] D. Feng, S. Das, and S. Biswas, "Packet Position Modulation: A Technique for Enhancing Information Transfer Capacity in Ultra-low Duty Cycle Networks," in *Proceedings of the 21st International Conference on Distributed Computing and Networking*, 2020.