March 2019

Methods and Algorithms to Enhance the Security, Increase the Throughput, and Decrease the Synchronization Delay in 5G Networks

Asim Mazin
University of South Florida, asimmazin@gmail.com

Methods and Algorithms to Enhance the Security, Increase the Throughput, and Decrease the Synchronization Delay in 5G Networks

by

Asim Mazin

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Richard D. Gitlin, Sc.D.
Nasir Ghani, Ph.D.
Ismail Uysal, Ph.D.
Srinivas Katkoori, Ph.D.
Gabriel Arrobo, Ph.D.

Date of Approval:
February 21, 2019

Keywords: Physical Layer Security, MAC, NOMA, Recurrent Neural Network, mmWave

DEDICATION

To my parents, Mohamed and Hurra whose love and guidance are with me in whatever I pursue; my beloved wife Salma for her sacrifices; my sons, Mohamed and Ayyub, who are the source of strength and unending inspiration; my siblings, Ghada, Abduallah, Hamza, Amer and Al-zubayr for their support.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor Dr. Richard D. Gitlin, for his invaluable guidance, support, patience, encouragement, and life teachings. Besides my advisor, I would like to thank Dr. Nasir Ghani, Dr. Ismail Uysal , Dr. Srinivas Katkoori and Dr. Gabriel Arrobo for serving in my doctoral committee.

Finally, I am grateful to colleagues at the *i*nnovations in Wireless Information Networking Laboratory (*i*WINLAB) and my family for their encouragement during my time as a Ph.D. student at the University of South Florida.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

This dissertation presents several novel approaches to enhance security, and increase the throughput, and decrease the delay synchronization in 5G networks.

First, a new physical layer paradigm was proposed for secure key exchange between the legitimate communication parties in the presence of a passive eavesdropper was presented. The proposed method ensures secrecy via pre-equalization and guarantees reliable communications using Low Density Parity Check (LDPC) codes. One of the main findings of this research is to demonstrate through simulations that the diversity order of the eavesdropper will be zero unless the main and eavesdropping channels are almost correlated, while the probability of key mismatch between the legitimate transmitter and receiver will be low. Simulation results demonstrate that the proposed approach achieves very low secret key mismatch between the legitimate users, while ensuring very high error probability at the eavesdropper.

Next, a novel medium access control (MAC) protocol Slotted Aloha-NOMA (SAN), directed to Machine to Machine (M2M) communication applications in the 5G Internet of Things (IoT) networks was proposed. SAN is matched to the low-complexity implementation and sporadic traffic requirements of M2M applications. Substantial throughput gains are achieved by enhancing Slotted Aloha with non-orthogonal multiple access (NOMA) and a Successive Interference Cancellation (SIC) receiver that can simultaneously detect multiple transmitted signals using power domain multiplexing. The gateway SAN receiver adaptively learns the number of active devices using a form of multi-hypothesis testing and a novel procedure enables the transmitters to

independently select distinct power levels. Simulation results show that the throughput of SAN exceeds that of conventional Slotted Aloha by 80% and that of CSMA/CA by 20% with a probability of transmission of 0.03, with a slightly increased average delay owing to the novel power level selection mechanism.

Finally, beam sweeping pattern prediction, based on the dynamic distribution of user traffic, using a form of recurrent neural networks (RNNs) called Gated Recurrent Unit (GRU) is proposed. The spatial distribution of users is inferred from data in call detail records (CDRs) of the cellular network. Results show that the users spatial distribution and their approximate location (direction) can be accurately predicted based on CDRs data using GRU, which is then used to calculate the sweeping pattern in the angular domain during cell search. Furthermore, the data-driven proposed beam sweeping pattern prediction was compared to random starting point sweeping (RSP) to measure the synchronization delay distribution. Results demonstrate the data-drive beam sweeping pattern prediction enable the UE to initially assess the gNB in approximately 0.41 of a complete scanning cycle that is required by the RSP scheme with probability 0.9 in a sparsely distributed UE scenario.

CHAPTER 1: INTRODUCTION

The Fifth Generation (5G) mobile network is envisioned to support a wide range of use cases, that fall under three main categories: enhanced mobile broadband (eMBB), massive Machine-type communication (mMTC), and ultra-reliable and low-latency communication (URLLC). It worth noting that these usage scenarios may not necessarily fit all use cases, however, they identify the capabilities needed for the 5G new radio (NR) interface. The high data rates and capacity requirements of eMBB make frequency bands above 24 GHz a key enabler for 5G networks. These bands are called the mmWave band since the wavelength is in the millimeter range, which introduces new technical challenges due to the propagation characteristics of the frequencies at that band [1]. One of the main challenges in mMTC, where a substantial number of connected devices with sporadic traffic is the design of the medium access control (MAC) protocol that is scalable, cost-effective, energy efficient and has low delay access (latency) [2]. The URLLC use cases are envisioned to have extremely low latency (1 ms) and high reliability. The 5G networks will support a wide range of data that needs to be protected against unauthorized access. Cryptosystems have been used to ensure security; however due to the dynamic and heterogeneous nature of 5G Networks the cryptographic key distribution and management are challenging.

Next, the research areas investigated in this dissertation will now be described in the following sections.

1.1 Secure Key Management in Symmetric Cryptography via Physical Layer Security

The broadcast nature of the wireless medium makes wireless transmissions vulnerable to eavesdropping. To ensure that the information is conveyed securely, cryptographic encryption techniques are often employed in the upper layers of the communication protocol stack. For example, symmetric cryptography methods (e.g., the Advanced Encryption Standard [AES]) use a common private key that is pre-shared between the source and destination, referred to Alice and Bob, will be assumed in this dissertation to encrypt/decrypt data. In contrast to the symmetric cryptography, asymmetric cryptography methods such as Public Key Cryptosystems (PKC) use public and private keys. In today's mobile communication systems, symmetric cryptography has been used due to its low computational cost and fast execution speed compared to PKC. However, if the legitimate parties do not pre-share a common key, then key distribution is recognized as a major problem. Key distribution includes establishing the session key and securely conveyed to both parties (Alice and Bob) through a wireless channel, that is prone to be intercepted by an eavesdropper, referred to as Eve and as illustrated in Figure 1.1. For next generation, wireless networks, such as 5G wireless, the process of key management (key generation and secure key exchange) will become even more critical as the number of nodes increases to a massive scale and nodes become more heterogeneous in their computational capabilities. We envision that physical layer security methods may be used as an additional layer of security to complement traditional cryptographic methods.

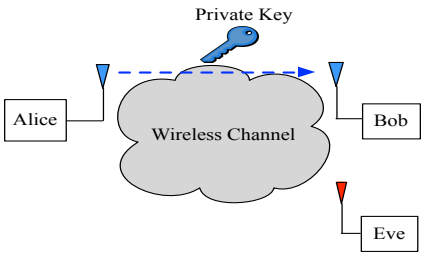


Figure 1.1 Sharing a key in symmetric key cryptography

Our research is directed towards a novel and secure key management technique that passes the locally generated session key through a transmit filter that "inverts" the channel between Alice and Bob [3].

1.2 Medium Access Protocol for M2M in IoT Networks

The rapid growth of both the number of connected devices and the data volume that is expected to be associated with emerging Internet-of-Things (IoT) applications, has increased the popularity of Machine-to-Machine (M2M) type communication within 5G wireless communication systems [4]. The vast number of devices in M2M communications, their diverse service requirements, and the unique traffic characteristics pose a real MAC layer design challenge. For example, in a smart home use case, as depicted in Figure 1.2, the smart devices may randomly and infrequently transmit a small burst of data to the smart home cloud server through an IoT gateway. Uncoordinated random access schemes have attracted lots of attention in the standards of the cellular network as a possible MAC protocol for making a massive number of M2M communication possible with a low signaling overhead [5], [6].

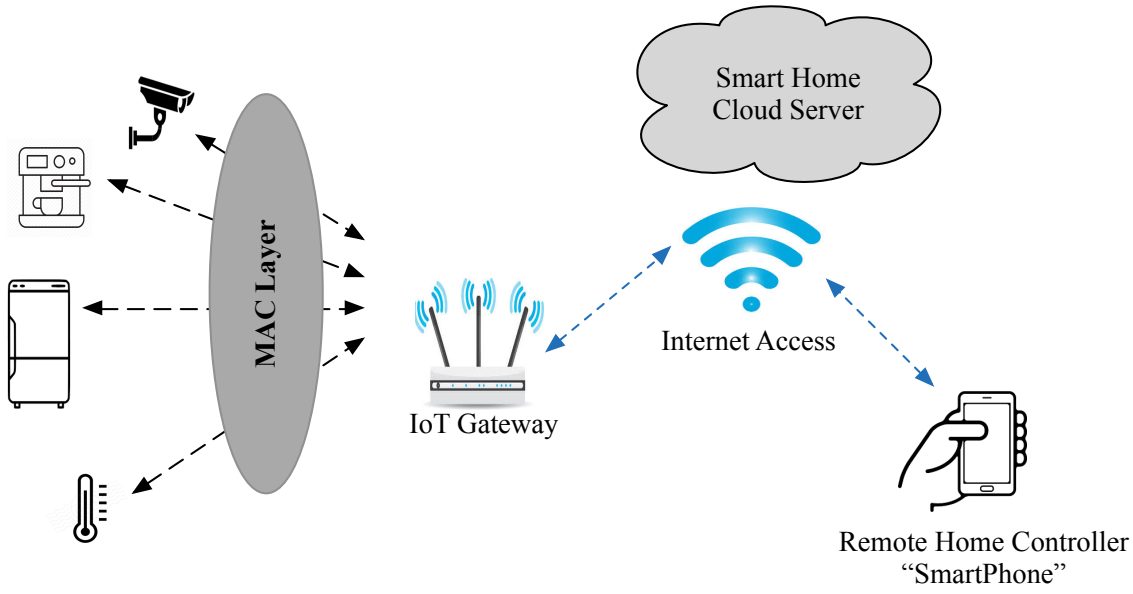


Figure 1.2 Smart home with IoT

Our research is directed towards inventing, analyzing, and implementing an uncoordinated MAC protocol, that guarantees access to the IoT gateway with high throughput, yet is simple to implement. In [7], we present an enhancement to the slotted Aloha-Non-Orthogonal Multiple Access (NOMA) protocol, where the IoT gateway adaptively learns the number of active devices (which is not known *a priori*) using a form of multi-hypothesis testing [8]. Furthermore, we compare the Slotted Aloha-NOMA (SAN) with the state of the art CSMA/CA protocol, which is widely adopted as a MAC protocol by many IoT technologies, in terms of throughput and average delay channel access.

1.3 Deep Learning Based Initial Access in mmWave 5G Cellular Systems

Millimeter wave (mmWave) communications is an enabling technology for the 5G eMBB use cases due to the available bandwidth at these frequencies. However, the initial access in mmWave cellular systems is challenging compared to the current long-term evolution (LTE) system for two reasons. First, due to the high isotropic path-loss, the mmWave communications requires highly directional transmission. But the user equipment (UE) and 5G base station (gNB) do not know in which directions to transmit (receive) during the initial access. Second, since the mmWave link is vulnerable to blockage and beam misalignment, more frequent initial access needs to be performed [9]- [12]. The reliance on directional transmission (beamforming), however, makes the cell discovery (cell search) challenging since both gNB and UE jointly perform a search over angular space to locate potential beams to initiate communication. In the cell discovery phase, sequential beam sweeping is performed through the angular coverage region to transmit synchronization signals as shown in Figure 1.3. The sweeping pattern can either be a linear rotation or a hopping pattern that makes use of additional information.

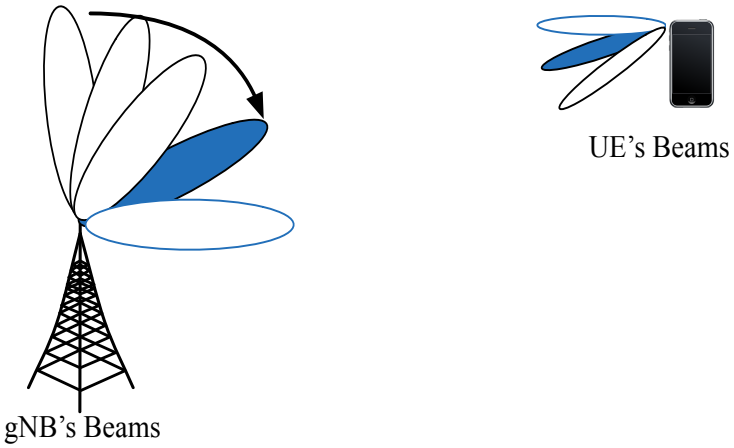


Figure 1.3 Beam sweeping during initial access in mmWave 5G cellular systems

Our research is focused on the time required for initial access in mmWave 5G cellular systems. In [13]-[14] we applied a deep learning Neural Network algorithm to accelerate the synchronization process during the initial access phase by leveraging intelligence from call detail records (CDR) data from Milan to rapidly determine the sweeping direction pattern during the cell discovery phase using Recurrent Neural Networks (RNN) to predict the user spatial distribution from the evolution of the CDR.

1.4 Contributions and Organization of This Dissertation

The contributions presented in this dissertation are directed to exploring and evaluating novel approaches for improving security, throughput, and latency in 5G systems and include the following:

- *Secure key management for 5G:* Propose and evaluate through simulation a novel physical layer security approach for secure key management in symmetric cryptography that is optimized for 5G networks that operate in the mmWave spectrum.
- *Medium Access Control for M2M in IoT Network:* Create a novel MAC layer protocol, SAN, that is a synergistic combination of the low complexity slotted Aloha protocol with

the high throughput feature of NOMA by using the successive interference cancellation (SIC) receiver.

- *Data-Driven Beam Sweeping for 5G mmWave Cellular systems:* Propose a data-driven Machine Learning approach for initial access in the mmWave cellular system to reduce the synchronization delay compared to the random starting point beam sweeping.

This dissertation is organized as follows. Chapter 2 presents a literature review for the different research areas in this dissertation. The physical layer approach for secure key management in symmetric cryptography and the simulation results are given in Chapter 3. A novel medium access protocol for M2M communication SAN is presented and evaluated in Chapter 4. A data-driven beam sweeping approach for initial access in mmWave 5G NR is presented in Chapter 5. Chapter 6 concludes the dissertation and provides future research direction.

CHAPTER 2: LITERATURE REVIEW

This chapter provides a literature review of the prior art in the three main topics of this dissertation. First, different prior art physical layer security techniques are reviewed. Second, prior MAC layer protocols for M2M (Machine-to-Machine) communications are described, with a focus on Carrier-Sense Multiple Access with Collision Avoidance CSMA/CA, due to its widespread use. Next, the prior art in the initial access for 5G mmWave cellular systems will be presented. Finally, a brief review of the use of machine learning in wireless communications is presented.

2.1 Physical Layer Security Overview

Physical layer security has gained much attention lately since, under the right circumstances, the technology is capable of providing wireless networks with basic security requirements such as confidentiality, integrity, and authenticity. The fundamental concept of physical layer security is to exploit the randomness of the wireless channel to enable security.

Physical layer security offers enhanced wireless network security by exploiting wireless channel characteristics to generate a secret key between the communication nodes. Using training sequences (probing signals), both parties can measure the channel parameters such as the received signal strength indicator (RSSI) [15]- [18], the channel state information (CSI) [19]- [20], or the power spectral density (PSD) [21] of the probing signals to agree on a secret key using one or more of these parameters. However, the randomness that can be extracted from the channel through the signal processing techniques proposed in [15]- [21] is limited by the randomness in the channel.

For stationary or low-mobility users, the channel randomness is very low, and the number of uncorrelated bits that can be generated from the channel is very few. Furthermore, the techniques proposed in [15]- [21] are prone to manipulation. An adversary may physically introduce blockage or digitally transmit/not transmit jamming signals to manipulate the distribution of bits. In [22]- [25], precoding matrix indicator (PMI) based key generation methods were proposed, which employ predefined codebooks to generate unique keys for devices with multiple antennas. To increase the key generation rate, a channel independent approach was proposed in [26] for fast secret key extraction. In [26], the receiver with a full-duplex transmission capability jams one of the two copies of the secret key sent by the transmitter. An Artificial Noise Injection (ANI) based physical layer approach was proposed in [27] to secure space-time block codes. ANI symbols are added to the information symbols such that they are aligned at the intended receiver and can be subtracted from the information symbols, while they degrade the unintended receiver performance. However, despite its good performance, this approach requires the legitimate transmitter to know the instantaneous channel of the eavesdropper, which may not be possible in many practical applications. Another drawback of [26]- [27] is that jamming and ANI-based techniques increase the interference in the system and they are not energy efficient.

2.2 MAC Layer for M2M Communications

The MAC protocols for wireless networks have been intensively investigated in the existing literature and can be classified into three main categories as contention-based, contention-free, and hybrid protocols that incorporate the advantages of contention-based and contention-free protocols. Table 2.1 presents several MAC protocols and their associated technology. ZigBee is among those technologies and one of the most commonly used standards in IoT. The MAC protocol in ZigBee is IEEE 802.15.4 and uses CSMA/CA, which is a multiple access mechanism

Table 2.1 Overview of MAC protocols for IoT

	Channel access mechanisms	Technology							
		ZigBee	BLE[1]	RFID[2]	WiFi	LTE-M	NB-IoT	Sigfox	LorRaWAN
Contention-based	Pure Aloha							√	√
	Slotted Aloha			√		√	√		
	Non-slotted CSMA/CA	√			√				
	Slotted CSMA/CA	√							
Scheduled-based	Frequency Division Multiple Access				√	√			
	Time Division Multiple Access		√						
	Code Division Multiple Access								√

used to reduce collisions in wireless networks[3]. Long Term Evolution for Machines (LTE-M) is designed to meet M2M and IoT requirements. It is an LTE radio network protocol to enable simple and low-cost devices. Long battery life is enabled by optimizing the efficiency of the transmission and higher layer protocols. Enhanced coverage is designed to reach deep indoor and rural areas.

[1] Bluetooth Low Energy (BLE) uses a contention-free MAC with low latency.

[2] Radio frequency identification system (RFID)

[3] Carrier-sense multiple access with collision avoidance (CSMA/CA) is a network multiple access method in which carrier sensing is used, where nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle". When they do transmit, nodes transmit their packet data in its entirety. Sensing is particularly important for wireless networks, where the collision detection (CD) of the alternative CSMA/CD, used in wired Ethernet, is unreliable due to the hidden node problem.

The narrowband internet of things (NB-IoT) is a technology based on the LTE that can be deployed in three different modes (1) stand alone and occupying 200 kHz, (2) in-band within the wideband of LTE and occuping only one physical resource block of LTE (180 kHz), and (3) within the guard band of LTE and occuping one physical resource block [28]. Sigfox and LoRaWAN both operate in the unlicenced band. In both technologies, the IoT devices access the base station by sending their packets using pure Aloha, where each active IoT device transmits at a random time in a randomly selected channel [29]. For IoT use cases, including M2M, MAC protocols need to be reconsidered to meet several requirements such as data throughput, scalability, energy efficiency, coexistence, and cost-effectiveness [30].

2.2.1 Contention-Based MAC Protocols

As the name implies, the nodes in the M2M scenario contend to access the shared medium. Although the contention-based MAC protocols match the M2M requirements in terms of satisfying the cost-efficient implementation requirements, they are unsuited to the dense M2M deployment due to frequent collisions, which results in low throughput. Pure-Aloha, Slotted Aloha, and CSMA/CA are examples of such contention-based MAC protocols [31].

This dissertation focusses on improving on the performance of CSMA/CA based protocols such as IEEE 802.11 (WiFi), which are among the most widely deployed MAC protocols that use CSMA/CA. However, as the network size increases in the M2M application, CSMA/CA does not scale accordingly due to the increased probability of collisions. Another shortcoming is the energy wasted by CSMA/CA based protocols due to collisions and idle listening.

The IEEE 802.15.4 standard specifies the MAC and physical (PHY) layers for low-rate wireless personal area networks (LR-WPANs). The CSMA/CA mechanism is used to reduce collision probability due to simultaneous node transmissions. In the standard, two-channel access

modes are defined — a beacon-enabled, where periodic beacons are used in the personal area network (PAN) for synchronization. In this case, the MAC sublayer employs the slotted version of the CSMA/CA algorithm and exponential backoff for re-transmissions in the contention access period (CAP) of the superframe [32], while in the unslotted version the CSMA/CA algorithm is used in non-beacon-enabled mode.

In the slotted CSMA/CA algorithm of IEEE 802.15.4, each device's MAC sub-layer initiates three variables for each transmission attempt. The number of times (NB) the CSMA-CA algorithm was required to back off while attempting the current transmission, the contention window (CW) length, which defining the number of backoff periods that need to be clear of channel activity before the transmission can start and the bakeoff exponent (BE), which is related to the number of bakeoff periods an IoT device waits before attempting to assess the channel. Figure 2.1 depicts the flowchart of the IEEE 802.15.4 slotted CSMA/CA scheme.

Consider an IoT device trying to transmit a packet. In IEEE 802.15.4 with slotted CSMA/CA, the number of backoffs and the contention window are initialized (NB = 0 and CW = 2). Depending on the value of the Battery Life Extension MAC attribute, the backoff exponent is initialized to BE = 2 or BE = min (2, macMinBE), where macMinBE is a constant defined in the standard [31]. Next, the algorithm starts counting down a random number of backoff periods (BPs) uniformly generated within $[0, 2^{BE}-1]$ at the boundary of a BP. When the timer expires, the algorithm then performs one clear channel assessment (CCA) operation at the BP boundary to assess channel activity. If the channel is busy, CW is reset to 2, NB and BE are incremented, where BE must not exceed aMaxBE (default value equal to 5) [32]. Observe that incrementing BE increases the probability of greater backoff delays. Once the maximum number of backoffs (NB = macMaxCSMABackoffs = 5) is reached, a failure is reported to the higher layer. Otherwise, the

IoT device performs another backoff operation. If the channel is sensed as idle, CW is decremented. The CCA is repeated if CW ≠ 0 to avoid collisions with acknowledgment frames. If the channel is again sensed as idle, the IoT device attempts to transmit, if the remaining BPs in the current CAP is sufficient to transmit the frame and the subsequent acknowledgment. If not, the CCAs and the frame transmission are both postponed to the next superframe.

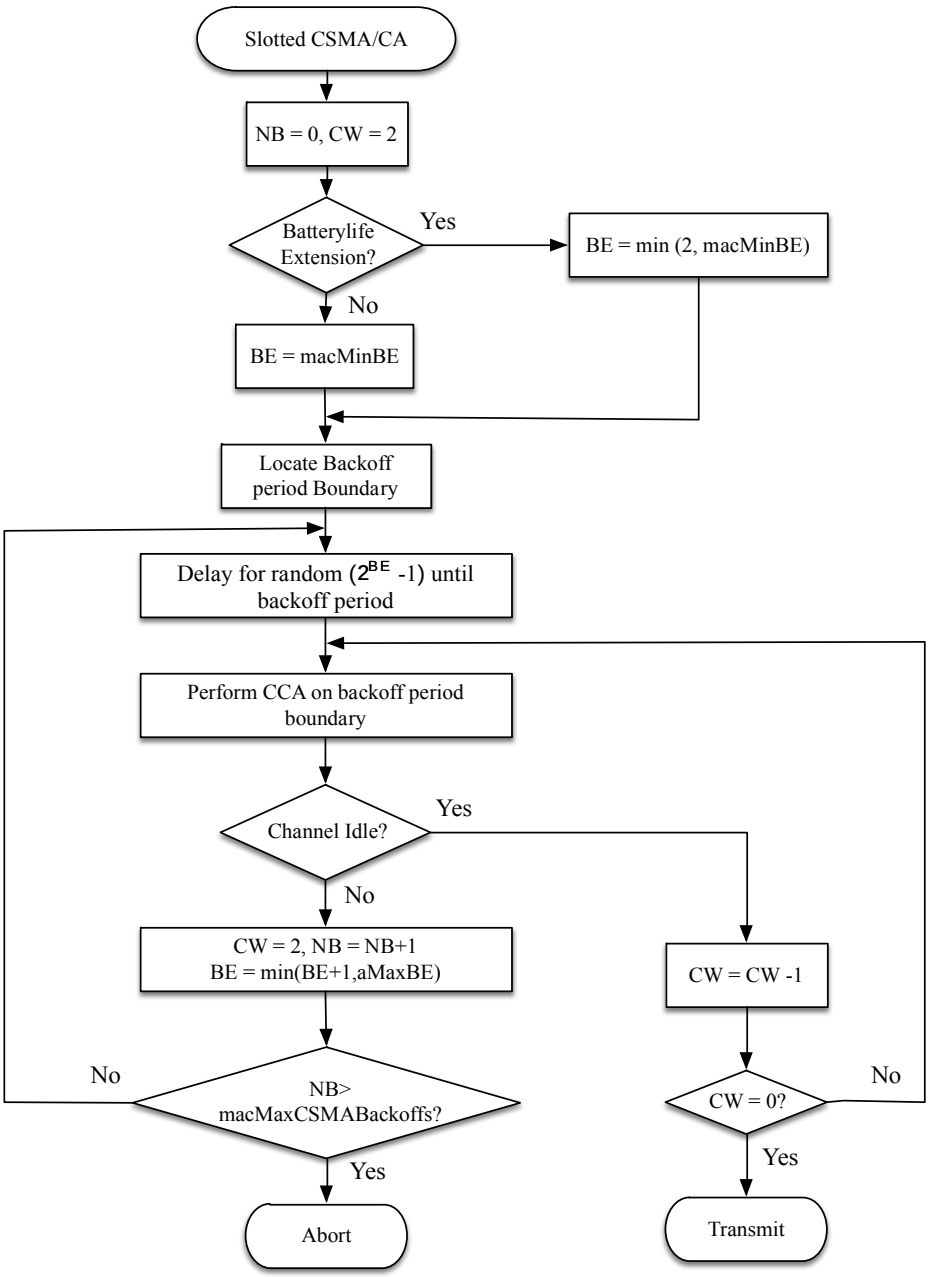


Figure 2.1 IEEE 802.15.4 slotted CSMA/CA protocol flowchart [31].

2.2.2 Contention-Free MAC Protocols

Contention-free protocols (scheduled-based) pre-assign the resources to the devices in the network. Based on the assigned resources, there are three common scheduled based protocols. First, time division multiple access (TDMA), where the bandwidth is a located to the device for a fraction of the time. Second, frequency division multiple access (FDMA), where the devices are assigned a portion of the spectrum all the time. Third, code division multiple access (CDMA), where orthogonal codes are assigned to the devices in the network. In the context of M2M communications, the static channel allocation results in poor utilization at low loads (where the number of active devices is small) [31]. Dynamic contention-free protocols that assign the resources adaptively based on the active devices in the network are better suited for M2M in terms of resource utilization; however, the dynamic allocation of the resources demands extra overhead.

2.2.3 Hybrid MAC Protocols

Hybrid MAC protocols are designed to combine the advantages of the contention-free and the scheduled-based MAC protocols. In [33] CSMA is used during the contention period (CP) and TDMA during the transmission period (TP). The successful devices during the contention period are guaranteed time slots during the transmission period. In [34] the performance of framed hybrid MAC protocol was formulated as an optimization problem to determine the trade-off between CP and TP lengths that increase the total system throughput in M2M. The high rate of collisions during the reservation stage is the bottleneck that prevents hybrid protocols from achieving high utilization in dense M2M networks. The slotted Aloha-NOMA protocol [7] exploits the simplicity of slotted Aloha (used during the CP) and the superior throughput of non-orthogonal multiple access (NOMA) (used during TP) [35] and its unique ability to resolve collisions via the use of a successive interference cancellation (SIC) receiver [36], [37]. The recently introduced Aloha-

NOMA protocol [38] and subsequent enhancements [39] are a promising candidate MAC protocol that can be utilized for low complexity IoT devices. In [39] NOMA is applied to multichannel slotted Aloha to enhance the throughput with respect to conventional multichannel slotted Aloha [40] without the need for any bandwidth expansion [39]. The slotted Aloha-NOMA protocol is a promising method for not requiring any scheduling, apart from frame synchronization, in which all IoT devices transmit to the gateway at the same time on the same frequency band. In Chapter 4, we present an enhancement to the slotted Aloha-NOMA protocol where the receiver adaptively learns the number of active devices (which is not known *a priori*) using a form of multi-hypothesis testing and comparison of Slotted Aloha-NOMA with CSMA/CA in terms of throughput and average delay [7].

2.3 Initial Access in mmWave 5G Cellular Systems

The initial access procedure in 5G mmWave network has been investigated by the IEEE and 3GPP standards groups and the IEEE 802.11ad standard adopted two levels of initial beamforming training for 60 GHz operation, where a coarser sector sweep phase is followed by an optional beam refinement phase [41]. The sector sweep phase consists of four components: the initiator (the station (STA) that initiates the beam training) sector sweep, the receive sector sweep (the recipient STA), feedback and acknowledgment [42]. The beam adaptation is illustrated in Figure 2.2 and can be summarized as having the following phases: (1) The initiator transmits training signals on all sectors sequentially, while the responder is receiving the training signal using a quasi-omni radiation pattern, (2) the same procedure is done during the receive sector sweep and (3) both the initiator and the receiver inform each other of the best sector they have heard during the training by exchangings feedback messages. Next, the beams from the sector level training may be further refined in the beamforming refinement phase. The IEEE 802.11ad standard

supports beam tracking by sending the measurement results of the acquired beams in the subsequent packets [43]-[44]. In [45] a technical specification for mmWave cellular systems is introduced, where the gNB employs beam sweeping during the cell search, and the beam reference signal (BRS) is transmitted to facilitate the UE to determine the gNB beamforming directions. The standardization of initial access in mmWave cellular is still in the early stages, however, several research efforts have been directed toward this problem [46]- [50]. An exhaustive approach to sequentially searching all transmit-receive beam pairs has been introduced in [46]. The hierarchical search, which is used in IEEE 802.11ad is introduced in [47], where gNB first applies exhaustive search over wide beams, then in a second phase refines the search to narrow beams. A comparative analysis between brute force search and hierarchal schemes is presented in [48], which concludes that the hierarchal approach has smaller initial delay access compared to the exhaustive search, but the exhaustive search provides better coverage to cell-edge users. It is reported in [49] that the initial access delay can be reduced by transmitting the synchronization signals omni-directionally. The initial access efficiency is enhanced by leveraging synchronization from a macro base station eNB (operating at sub 6 GHz), followed by a sequential spatial search from the mmWave gNB[50]-[51]. In [52] the authors consider the availability of context information (CI) (the location information of the mmWave gNB) at the UE, so that the UE, rather than searching the whole angular space, will form its combining beam only in the direction provided by the CI. Recently context information (e.g., vehicle's position) and past beam measurements stored in a database (maintained in the roadside unit in vehicular communications) has been used as a hint to determine potential beam pairs. The idea of the proposed approach is to learn a scoring function that can be used to predict the scores of beam pairs and provide a means to rank them [53]. Generally speaking, the initial access procedure can be improved by using "richer" information, e.g., terminal

positions, channel gain predictions, user spatial distribution, antenna configurations successfully used in previous accesses, and so on.

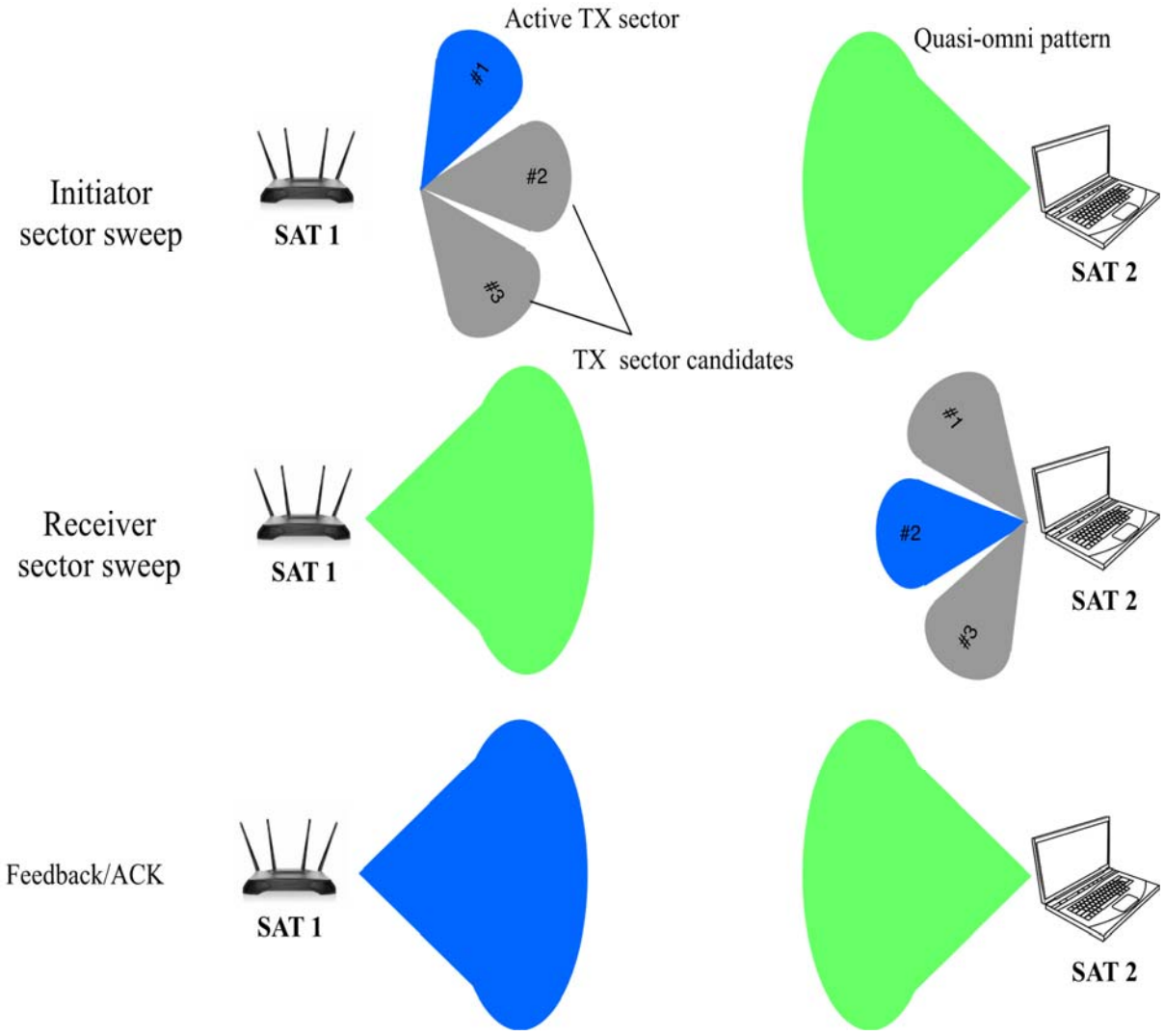


Figure 2.2 IEEE 802.11ad beam training protocol

2.4 Machine Learning in Wireless Communications

Machine learning (ML) has grown rapidly due to several reasons including tremendous improvements in ML algorithms and computational power, as well as access to a large amount of data. Researchers in many disciplines such as computer vision, voice recognition, natural language processing, medical imagery, and finance have contributed to many of the state-of-the-art ML

algorithms. Building upon the success of ML in the previous areas, the data analytic approach started to gain momentum in different research areas in wireless communications. Since many problems in wireless communications can be converted to clustering, classification, or regression problems, ML algorithms can be trained to solve them. Deep Learning is a sub-division of ML, which learns from raw data through multiple layers of nonlinear units, to realize a Deep Neural Network that can predict or act based on the target objective.

Deep Learning has been broadly investigated in the mobile network context. In [54] Deep Learning is used to estimate user's Quality of Experience (QoE) in a cellular network with high accuracy. A Multilayer Perceptron (MLP) neural network applied to estimate the QoE based on key performance indicators (KPI), such as the average user throughput, the number of active users in the cell, and the channel quality indicators (CQI). Deep reinforcement learning has also been applied to cloud radio access networks (C-RANs) to determine the on/off modes of remote radio heads given, the current mode and user demand for power-efficient resources allocation [55]. Deep Learning is leveraged as a tool for mobility analysis due to its ability to capture spatial dependencies in sequential data. A trajectory prediction using Deep Learning is studied in [56]. A proactive resource allocation using a recurrent neural network (RNN) was proposed in [57] to predict the next base station from the received signal strength (RSS) values, which provide higher channel capacities for multiple users and alleviate the problem of frequent handovers for high mobility users. In [58] a convolutional neural network (CNN) was used as a modulation classifier.

2.5 Concluding Remarks

In this chapter, an overview of selected physical layer security techniques was presented. Then potential MAC protocols for M2M application and design challenges were presented. Next, the initial access issues in 5G mmWave a different wireless technology than heretofore used, was

described. Finally, an overview of applying ML across diverse wireless communications applications was presented.

CHAPTER 3: SECURE KEY MANAGEMENT IN SYMMETRIC CRYPTOGRAPHY

3.1 Introduction

In this chapter[4], we present a new physical layer paradigm for secure key exchange in symmetric cryptography between the legitimate communication parties in the presence of a passive eavesdropper. The proposed method ensures secrecy via pre-equalization and guarantees reliable communications by the use of Low-Density Parity-Check (LDPC) codes. LDPC codes are class of linear block codes that were first introduced by Gallager in his doctoral dissertation in 1963[59]. LDPC codes were chosen for the proposed scheme due to its powerful capability of correcting errors. In addition to its high coding gain, the LDPC codes are computationally more efficient than other popular Turbo codes because they require fewer operations to achieve the same target block error rate [60]. The latest release (Release 15) of the 3rd Generation Partnership Project (3GPP) has adopted LDPC for data channels (user plane) and Polar code for the control channels (control plane) due to its better performance at a moderate payload, typical of control information [61].

3.2 System Model and Proposed Method

Consider a generic wireless network system model as depicted in Figure 3.1, where Alice and Bob are the legitimate communication nodes and Eve is the passive eavesdropper. Alice wants to share a secret sequence (private key) with Bob in the presence of Eve by pre-filtering the secret sequence using a filter that inverts the main channel, i.e., the channel between Alice and Bob h_{AB}. The received signals at Bob and Eve can be respectively expressed

[4] The content of this chapter has been published in [3] and it is included in this dissertation with permission from the IEEE. Permission is included in Appendix A.

$$y_B(k) = \sum_m h_{AB}(m)s(k-m) + n_B(k) \tag{3.3}$$

$$y_E(k) = \sum_m h_{AE}(m)s(k-m) + n_E(k)\,, \tag{3.4}$$

where $m = 0, 1, \cdots$ and k is the discrete time index and h_{AB}, h_{AE} are the main and the wiretap channels as depicted in Figure 3.1. It is assumed that channels remain fixed during the transmission of a few symbols but may randomly change over time, the symbol s is the coded secret sequence (private key), and $n_B(k)$, $n_E(k)$ represent the i.i.d. additive Gaussian noise at Bob and Eve, respectively. The objective is to securely share a private key between Alice and Bob. Before the transmission, a secret key $\boldsymbol{x}$ with a length of N bits is generated by the transmitter (Alice) to ensure a low probability of interception at Eve. The proposed signaling procedure is shown in Figure 3.2 and the steps are as follows:

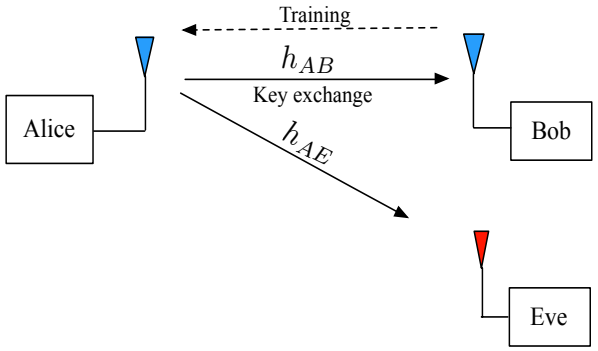


Figure 3.1 System model

1. Bob transmits a training sequence to Alice (and known to Alice) for channel estimation.
2. Alice estimates the channel and determines the transmit filter that inverts the channel. Using this filter, there is now a "perfect" (distortionless) channel between Alice and Bob (of course there is still background noise in the channel)..
3. Alice sends the secret key to Bob after passing it through a LDPC encoder with a rate $r = 1/2$ and a transmitter filter.

4. Bob receives the pre-equalized signal (containing the session key). The signal is then passed through an LDPC decoder.
5. Thus, the secure key sequence is conveyed from Alice to Bob with high reliability due to the powerful error correcting capability of LDPC codes.
6. Bob sends an ACK/NACK to Alice based on the error detection capability of the LDPC code . If the detected errors cannot be corrected, a NACK is sent to Alice and Steps 1-5 are repeated. Otherwise, an ACK signal is sent indicating that the session key was successfully received and the key exchange procedure is complete.
7. Key exchange for secure transmission has now been established between Alice and Bob. To convey the data in a secure way, the generated secret key is input to a random number generator (RNG) as a seed by Alice and Bob. The data bit sequence is XORed with the outputs of the RNGs to confuse Eve further, even if she perfectly estimates the received signal.

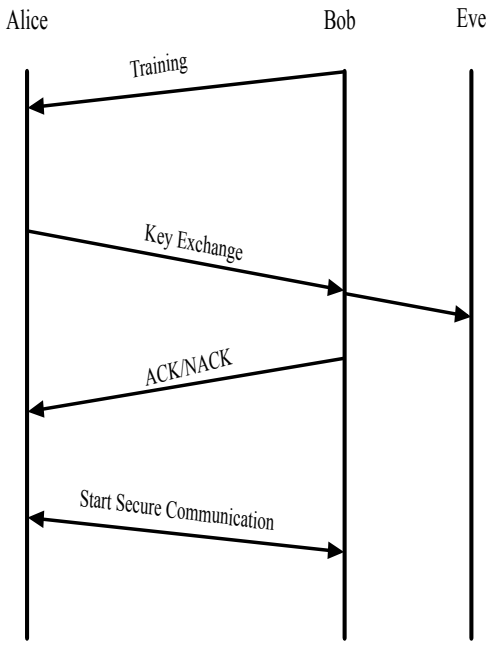


Figure 3.2 Signaling procedure

The proposed transmitter and receiver structures for key exchange are depicted in Figure 3.3. The encoded secret key bits $\boldsymbol{u}$ (LDPC encoder output) are mapped to b QPSK symbols. Next, the modulated symbols b are passed through the transmit filter w to form

$$s(k) = \sum_m w(k-m)b(m), \tag{3.5}$$

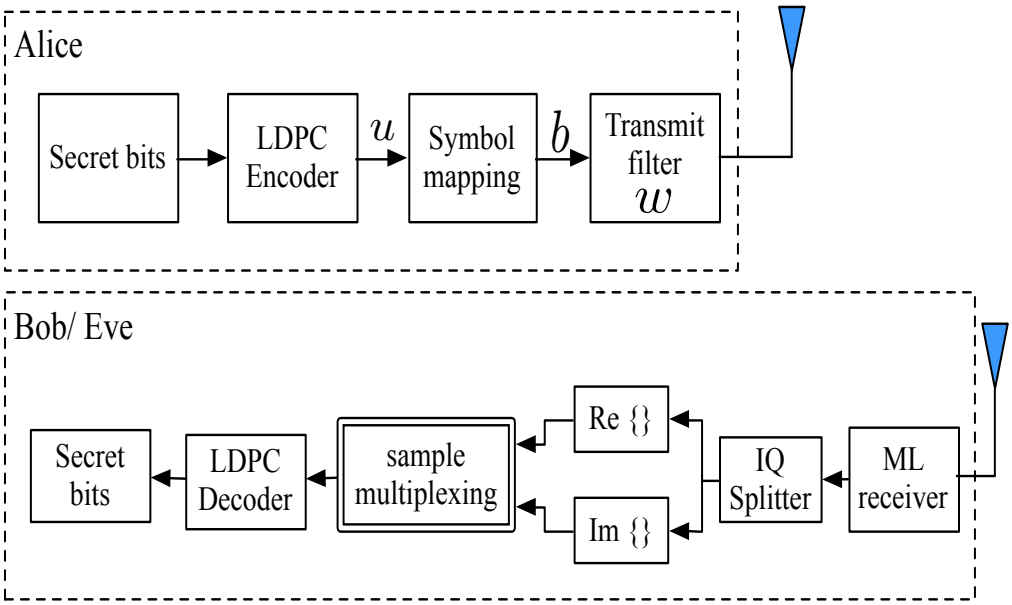


Figure 3.3 Proposed key management exchange

where $s(k)$ is the transmitted signal in (3.1) and (3.2). The transmit filter w that inverts the main channel is designed to achieve high secrecy even if Eve knows her channel h_{AE} and even if the wiretap channel is less noisy than the main channel, i.e., Eve has a high signal-to-noise ratio (SNR) compared to Bob. Since Alice estimates the main channel h_{AB} using the training sequence sent by Bob, through a reciprocal main channel where $h_{AB} = h_{BA}$, the transmit filter w can be determined as

$$h_{BA}w = \|h_{BA}\|. \tag{3.6}$$

The normalized coefficients of the transmit filter w are determined by inverting h_{BA} in (3.4) directly, or by using Moore-Penrose Pseudoinverse [62] if the channel h_{BA} contains nulls. Therefore, the received signal at Bob can be rewritten as

$$y_B(k) = \|h_{BA}\| b(k) + n_B(k) \tag{3.7}$$

Bob can detect $\hat{b}$ by estimating the received signal power

$$\|h_{BA}\|^2 = \sum_{i=1}^{j} |y_B(k)|^2. \tag{3.8}$$

The security of the proposed scheme lies in the fact that Eve is unable to correctly decode the pre-filtered secret key in (3.3) due to the uncorrelated main and wiretap channels as we will discuss in next section.

3.3 Correlation Model

3.3.1 Phenomenological Model

The transmit filter w depends on the main channel which is expected to be uncorrelated with the eavesdropping channel for link distances larger than a half wavelength due to the spatial property of wireless transmission. However, in practice, there exists some correlation between the two channels as reported in [63]. To capture the correlation effects, without loss of generality, we consider the following correlation model [64]

$$h_{AE} = \rho h_{AB} + \sqrt{1-\rho^2} h_{iid}, \tag{3.9}$$

where ρ is the correlation coefficient and $0 \leq \rho < 1$ is the correlation coefficient between the normalized channel impulse responses h_{AE} and h_{AB}. The term h_{iid} represents an i.i.d. Rayleigh fading channel that, ideally, has a zero correlation with h_{AB}. If $\rho = 0$, the main and wiretap channels are uncorrelated, whereas non-zero values of ρ indicate a higher correlation which increases the probability of successful eavesdropping. When Eve is located very close to Bob (within a few wavelengths), a higher correlation between the main and wiretap channels may occur, which would help Eve detect the transmitted symbols by using processing similar to Bob using (3.5) and (3.6). This would result in a higher probability of key intercept by Eve, which will be presented in terms of frame error probability in the results section. The previous correlation

model is a phenomenological correlation model and does not capture either the effect of spatial parameters or the operating frequency of the system.

3.3.2 Spatial Correlation

To illustrate the spatial correlation between the Rayleigh fading channel impulse response realizations at Bob and Eve we used the deterministic channel model for spatially correlated Rayleigh fading [65], the channel responses are given by

$$h_{AB} = \frac{1}{\sqrt{L}}\sum_{k=1}^{L}\cos\left(2\pi f_k t + \psi^{(I)}{}_k\right) + j\cos(2\pi f_k t + \psi^{(Q)}{}_k), \tag{3.10}$$

$$h_{AE} = \frac{1}{\sqrt{L}}\sum_{k=1}^{L}\cos\left(2\pi f_k t + \phi^{(I)}{}_k\right) + j\cos(2\pi f_k t + \phi^{(Q)}{}_k), \tag{3.11}$$

where $\psi^{(I)}{}_k - \phi^{(Q)}{}_k = \pi/2$ to suppress the cross correlation between in-phase (I) and Quadratic (Q) components of the channel realizations and $f_k = f_d \sin(k\pi/2L)$ models the temporal correlation (f_d is Doppler shift). The cross-correlation between the channel realizations (fading waveforms) is given by

$$\rho = E\{h_{AB}h_{AE}{}^{*}\} = \frac{1}{L}\sum_{k=1}^{L}\exp(-j\Delta\varphi_k), \tag{3.12}$$

where $\Delta\varphi_k = \psi^{(I)}{}_k - \phi^{(I)}{}_k$. The spatial correlation is given by

$$R(d/\lambda) = \int_{-\pi}^{\pi} exp(-j2\pi d\sin\theta/\lambda)\, f_\theta(\theta)\, d\theta, \tag{3.13}$$

where d is the separation distance between Bob and Eve, λ is the wavelength of the operating frequency and $f_\theta(\theta)$ is the function of the incident angle, $\theta \in (-\pi, \pi)$ is normalized $\int_{-\pi}^{\pi} f_\theta(\theta)d\theta = 1$. The integral in (3.13) can be approximated as

$$R(d/\lambda) \cong \frac{1}{L}\sum_{k=1}^{L} exp(-j2\pi d\sin\theta_k/\lambda), \tag{3.14}$$

by assuming equality between the (3.10) and (3.12), we have

$$2\pi d\sin\theta_k/\lambda = \Delta\varphi_k, \tag{3.15}$$

and from (3.15) $\Delta\varphi_k$ is calculated using the incident angle θ_k that is determined from the Gaussian

or Laplacian distribution of $f_\theta(\theta)$. Once $\Delta\varphi_k$ is obtained, it is used to find ${\psi^{(I)}}_k$ and ${\phi^{(I)}}_k$ under the condition that was previously defined ${\psi^{(I)}}_k - {\phi^{(Q)}}_k = \pi/2$. Using the previous information, L spatially correlated channel realizations can be generated using (3.10) and (3.11), which are used to evaluate the performance of the proposed scheme for secure key management.

3.4 Simulation Results

In this section, we present the simulation results of the proposed method. We have simulated the secure key management algorithm in MATLAB and obtained the performance results in terms of Frame Error Probability (FEP) of the decoded signals (when the secret key is transmitted) to Bob and also received by Eve during the secure key exchange phase. In the simulations, we used a 512-bit key length and assumed Rayleigh block fading channels at the main and wiretap channels using the correlation model in (3.7). All nodes are equipped with one antenna.

To simulate the main and wiretap channels using the deterministic models in (3.8) and (3.9), the distribution of the incident angle $f_\theta(\theta)$ is a Gaussian with mean $\mu = 10\pi/180^o$ and standard deviation $\sigma = 3\pi/180^o$. The σ is used as the measure of the incident angle spread. The number of sinusoids is L = 32 to generate channel responses at two different locations (Eve and Bob locations) separated by distance d for three different frequencies 2.14 GHz (LTE Band 1 Downlink central frequency), 28 GHz and 60 GHz. The correlation coefficient $\rho \approx 0.99$ when d = 0.01 m in the LTE band case, $\rho \approx 0.99$ when d = 0.001 m when 28 GHz used as a carrier frequency and, $\rho \approx 0.99$ when d < 0.001 m in case of 60 GHz as shown in Figure 3.4. Observe that at higher frequency the proposed scheme provides secure key exchange between Alice and Bob because the main and wiretap channels are almost correlated when the separation distance between Bob and Eve is very small, which shrinks the radius (R) of the vulnerable (insecure) zone (i.e. the area where Eve has low FEP) as illustrated in Figure 3.5 and summarized in Table 3.1.

Table 3.1 The radius of the insecure zone for different frequencies.

Frequency	**Radius (m)**
2.14 GHz	0.01 m
28 GHz	0.001 m
60 GHz	< 0.001 m

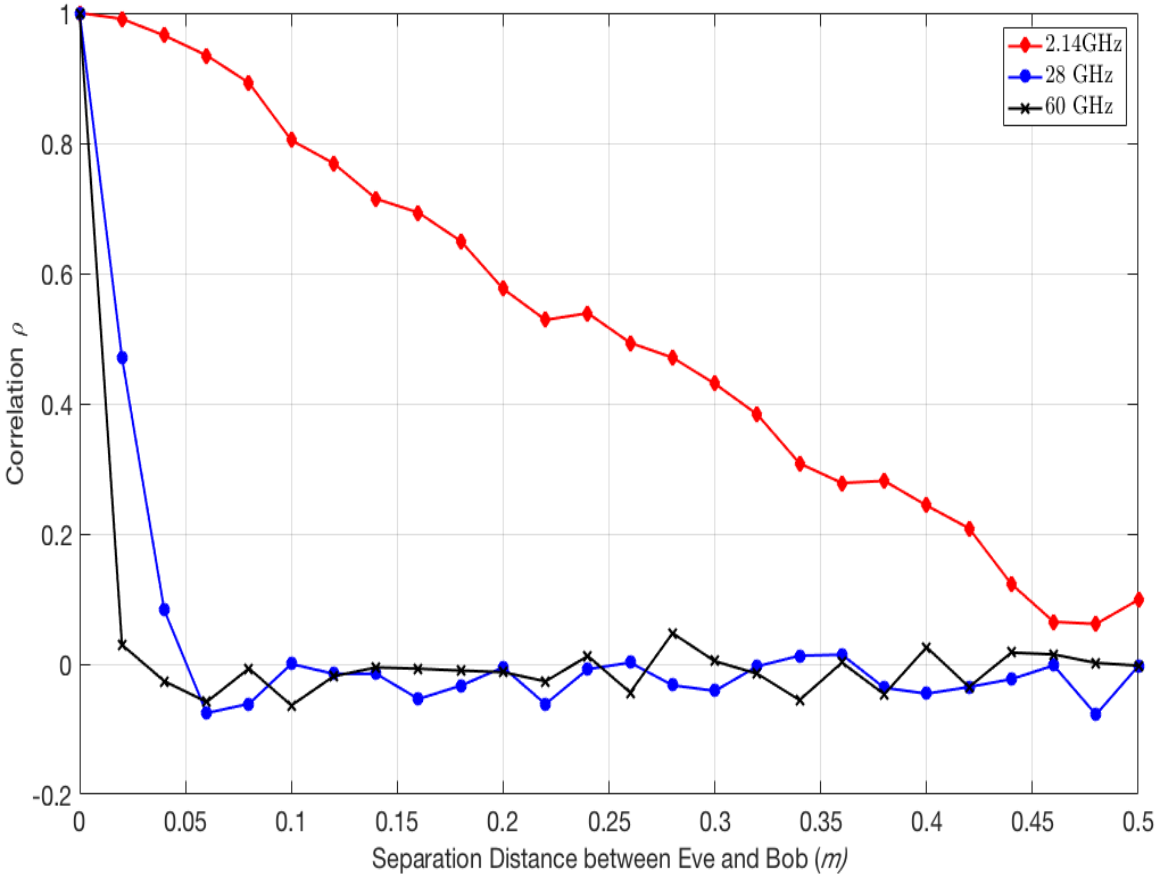


Figure 3.4 The correlation of the generated Rayleigh fading channels responses as a function of the separation distance between Eve and Bob at different frequencies.

Figure 3.6 illustrates the FEP for Bob and Eve for different channel correlations. The SNR of Bob and Eve are assumed to be the same and varied between 0 dB and 5 dB in 0.5 dB increments. We observe that due to the channel capacity achieving LDPC code, the probability of a key

mismatch between Alice and Bob essentially goes to zero when the SNR > 2.5 dB, whereas the FEP at Eve is very high for all SNR values for $\rho < 0.9$. This demonstrates that the proposed algorithm achieves a diversity order of zero for Eve when $\rho < 0.9$. In other words, the number of independent fading links between Alice and Eve is zero. When $\rho < 0.9$ the FEP of Eve is unity, and the diversity order, which is defined as $\lim_{SNR \to \infty} \frac{\log(\text{FEP(SNR)})}{\log SNR}$ [66], is zero. The diversity order, which can be interpreted as the number of independent communication links between Alice and Eve, is zero. However, when the main and eavesdropping channels are almost correlated, i.e., $\rho = 0.99$, then the probability of key intercept increases at Eve and the system security decreases. In fact, this is not a surprising result since the present physical layer security method relies on the uniqueness between the main and wiretap channels, which can be observed from Eve's FEP for different correlation values in Figure 3.7. As the difference between the two channels disappears, so does the security. Note that for $\rho = 0.99$, the channels are not essentially the same and it is for this reason, there exists a slight difference in the FEP curves of Bob and Eve in Figure 3.6.

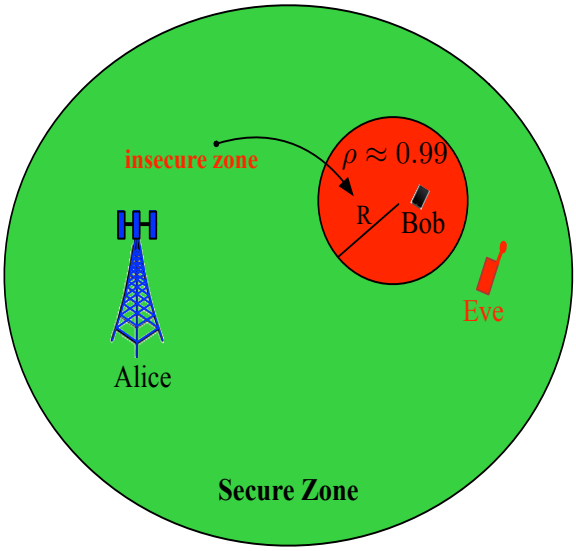


Figure 3.5 The insecure zone radius.

Next, we fix the SNR of the wiretap channel at 10 dB and vary the SNR of Bob from 0 dB to 5 dB. This simulation scenario considers the case where Eve is closer to Alice than Bob. Even though the previous scenario cannot physically exist when the channels are almost correlated, yet it is an interesting point to simulate. The key-mismatch FEP results for Bob and Eve are shown in Figure 3.8 for different correlation coefficients ρ between the wiretap channel and the main channel. Although Eve has a better SNR than Bob, her FEP remains high for all $\rho < 0.9$ values. For clarity in Figures 3.6 and 3.7, we have only presented results for a correlation of $\rho = 0.9$, but the results are true for all $\rho < 0.9$. Note that when the channels are almost correlated, with $\rho = 0.99$, Bob makes errors until the SNR exceeds 2.5 dB, whereas Eve does not make an error since her SNR is fixed at 10 dB. This is again due to the same reason as above where the security that can be achieved with physical layer methods degrades as the main and wiretap channels become highly correlated.

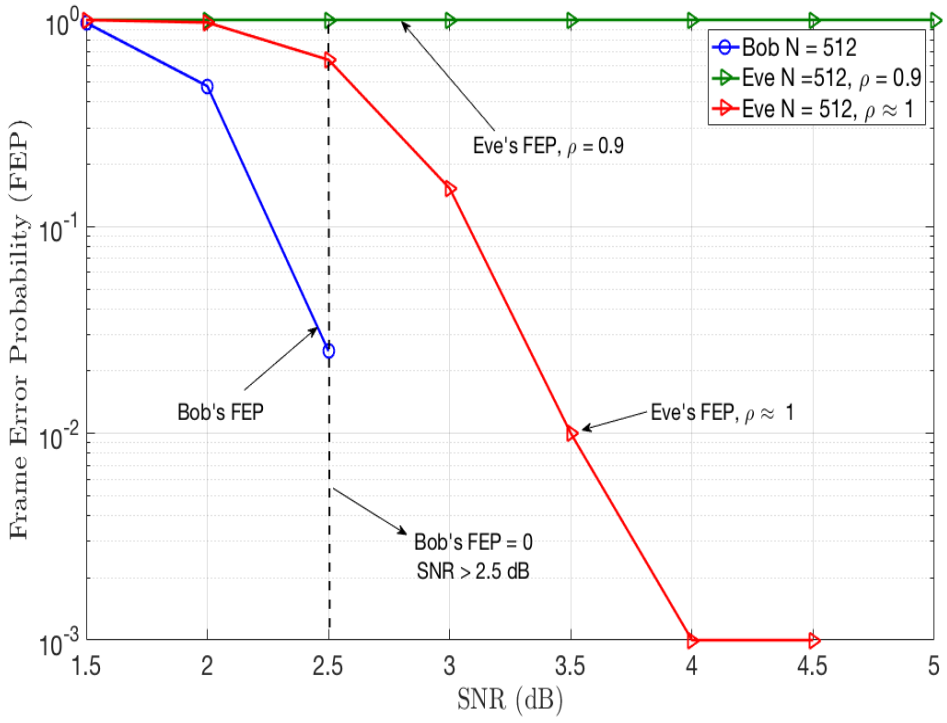


Figure 3.6 Bob FEP results and Eve 's FEP results for key exchange mismatch for different correlation values ρ between the main and wiretap channel.

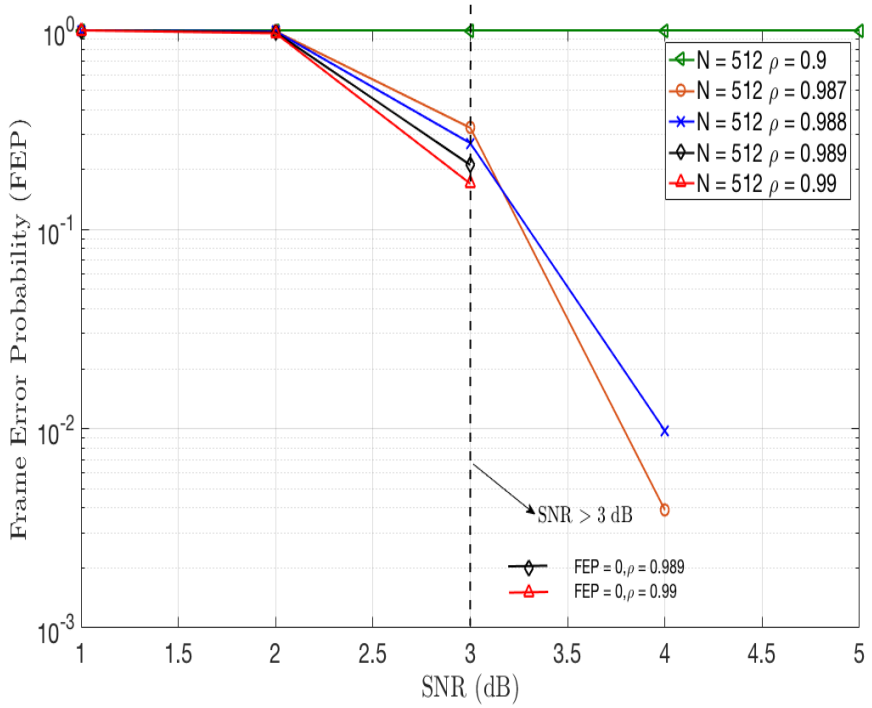


Figure 3.7 Eve FEP results for different correlation values.

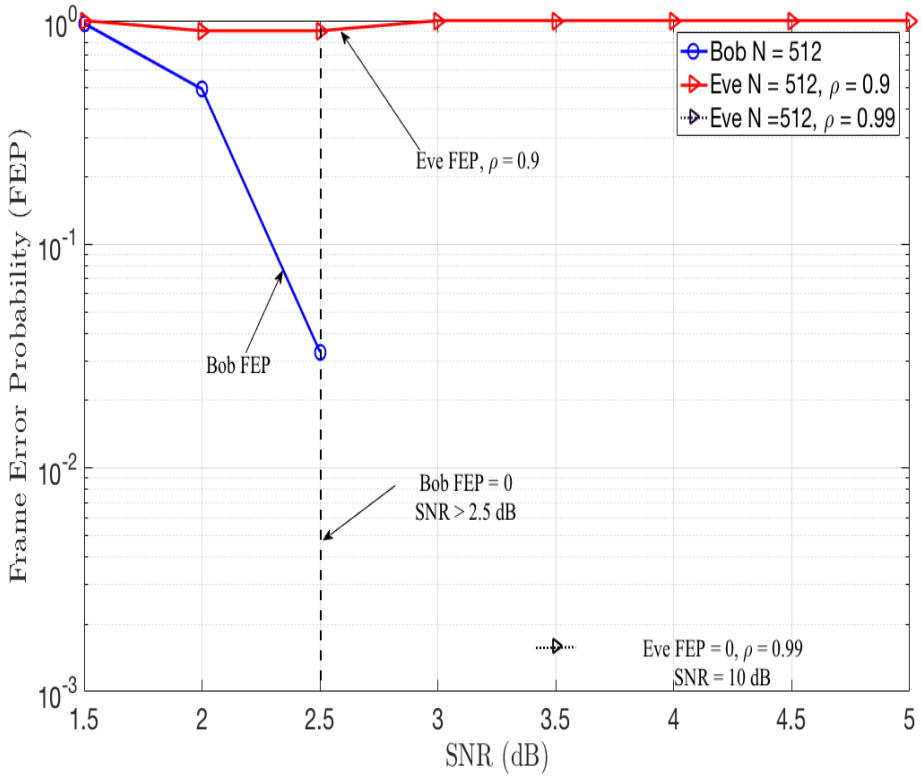


Figure 3.8 Key exchange mismatch FEP at Bob and Eve for different ρ between the main and the wiretap channel and the SNR of Eve is fixed to 10 dB.

3.5 Concluding Remarks

In this chapter, a novel method is proposed to exchange a secret key between two legitimate users using a novel physical layer security method. The uniqueness of the wireless channel between the legitimate users and an eavesdropper is exploited to create a low probability of interception and magnify the FEP at the unintended receiver (the eavesdropper), while the intended receiver successfully receives the transmitted signal with a very low FEP. The proposed method utilizes a pre-equalization filter and LDPC encoding at the transmitter. The simulation results demonstrate that secure communication can be established unless the main and eavesdropping channels are almost correlated. Furthermore, the proposed technique becomes more attractive at mmWave frequencies because the correlation between the main channel and the wiretap channel is small, which implies a low probability of key interception by Eve.

CHAPTER 4: MEDIUM ACCESS CONTROL FOR M2M COMMUNICATIONS IN IoT NETWORKS

4.1 Introduction

The Internet of Things (IoT), which is the network of physical devices embedded with sensors, actuators, and connectivity, is being accelerated into the mainstream by the emergence of 5G wireless networking that will support of Machine-to-Machine (M2M) communications. Due to the simplicity of IoT devices and their generally sporadic traffic in such application, a simple medium access control (MAC) protocol is needed to connect M2M devices to the Internet through a hub (IoT gateway).

In this chapter[5], the novel Slotted Aloha-non-Orthogonal Multiple Access (SAN) protocol for M2M communications is presented and compared with the well-known Slotted Aloha and carrier sensing multiple access with collision avoidance (CSMA/CA) protocol. The comparison is based on two metrics, the throughput and the average delay. Simulation results show that the throughput of SAN is higher than CSMA/CA at low probability of transmission at the cost of increased average delay caused by a novel power level selection mechanism.

4.2 Non-Orthogonal Multiple Access (NOMA)

NOMA has emerged as a promising technology in 5G networks for many applications [67]. The concept of NOMA relies on the ability of the receiver to separate the non-orthogonal signals.

[5] The content of this chapter has been published in [7] and it is included in this dissertation with permission from the IEEE. Permission is included in Appendix A

In contrast to orthogonal multiple access schemes relying on time, frequency, code or their combination, in power domain NOMA multiple devices share the same time-frequency and their signals can be separated at the receiver in the power domain. In the SAN protocol, power domain NOMA is used to allow multiple devices in the uplink to access the Internet through the IoT gateway. The received signal at IoT gateway in Figure 4.1, where $K = 2$, is given by

$$y = \sum_{i=1}^{K} h_i \sqrt{P_i}\, s_i + n, \tag{4.1}$$

where h_i, P_i, s_i and n are respectively the channel gain between the i^{th} device and the IoT gateway, the power scaling coefficient, transmitted signal of the i^{th} device and the additive Gaussian noise. Successive interference cancellation (SIC) is used at the receiver (IoT gateway), where the strongest signal (e.g., Device 1 s_1) is decoded first and the other signal (Device 2 s_2) is considered as a noise. Then, the detected signal (Device 1 s_1) is subtracted from the from the superimposed signal to detect s_2[68].

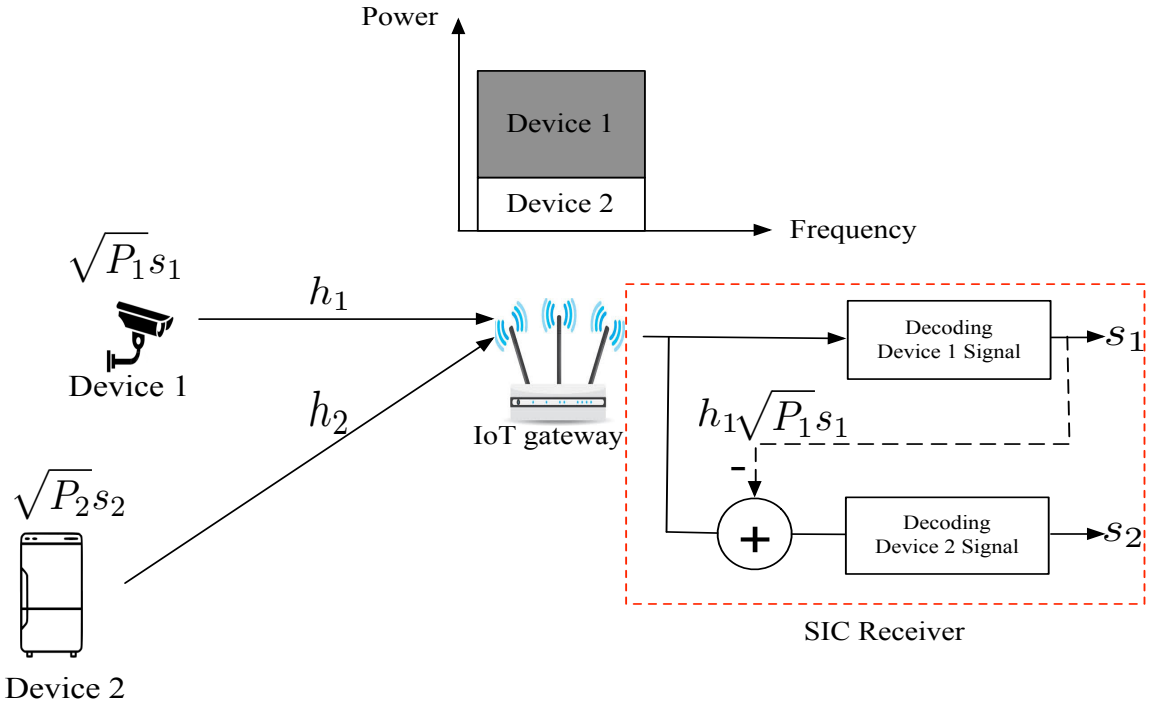


Figure 4.1 Power domain NOMA with two devices and with a SIC receiver.

4.3 SAN Protocol

4.3.1 Overview

The SAN protocol is a synergistic combination of the low complexity Slotted Aloha protocol with the high throughput feature of NOMA. In the SAN protocol, both the power and time slots form multiple sub-channels as shown in Figure 4.2. During time slot 1, three devices transmit with each device using distinct power levels, so there is no collision since the SIC receiver can separate the signals in power domain. However, during time slot 3 the SIC receiver failed to separate the signals (collision) from three devices because two devices transmitted at the same power level. The main bottleneck of Slotted Aloha systems is the low throughput caused by the high number of collisions, which can be addressed by NOMA. In SAN the signaling overhead is reduced in the detection phase of the proposed protocol where the number of active IoT devices are detected by the gateway using a form of multiple hypotheses testing, which is further explained below. SAN is also an energy efficient protocol due to the fact that under most circumstances a SIC receiver can resolve collisions, and thus minimize retransmissions. The SAN protocol can be suitable for various scenarios where many IoT devices are transmitting simultaneously on the same frequency with different power levels to an IoT gateway and the received signals can be separated via the use of a SIC receiver. A sample illustration of this scenario is depicted in Figure 4.3 as a smart home with an IoT network. Here, IoT devices send their data to the IoT gateway at the beginning of the slot using the SAN protocol and if the received power levels have been properly chosen, then the IoT gateway distinguishes the signals with a SIC receiver. The SAN scheme increases the throughput significantly beyond that of conventional Slotted Aloha due to the use of multiple power levels, which are additional channels in the power domain.

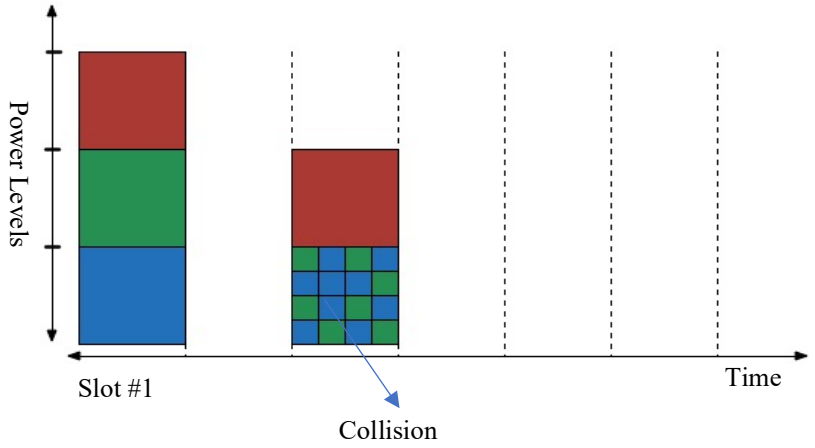


Figure 4.2 The synergic combination of Slotted Aloha and NOMA in SAN protocol. The figure shows optimum performance in slot #1 (the devices choose distinct power levels and hence no collision) and a collision in slot #3 where 2 device have chosen the same power level.

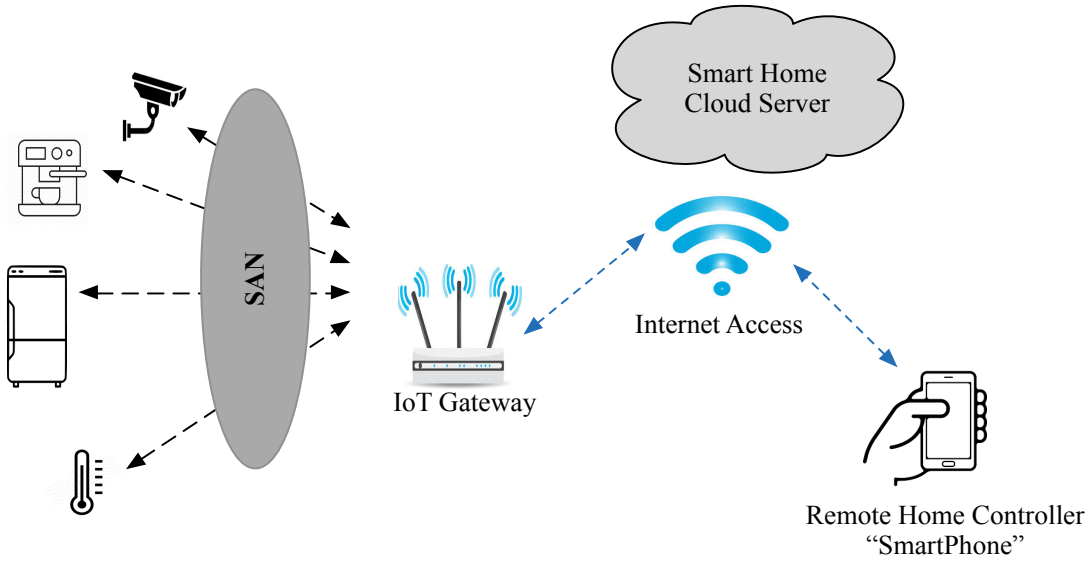


Figure 4.3 A use case of SAN in the smart home with IoT.

The SAN protocol flowchart is depicted in Figure 4.4. First, the IoT gateway transmits a beacon signal to announce its readiness to receive packets. Next, the IoT devices with packets ready to transmit send a training sequence to aid the gateway in detecting the number of active IoT devices in the medium. The IoT gateway detects the number of devices requesting transmission via a form

of multiple hypotheses testing, as further explained next, and adjusts the degree[6] of the SIC receiver for the optimum power levels. In practice, the SIC receiver has a fixed range of optimum power levels (e.g., $m = 2, 3$) corresponding to the number of devices that have been detected that wish to transmit. If the IoT devices are registered with the gateway instead of using multi-hypothesis testing, implementation would be more straightforward; however, this will significantly increase the length of the control phase and thus decrease the payload or throughput considering the potentially large number of IoT devices. Third, if the detected number of active IoT devices is not in the range of the SIC capability (that is, the number of devices wanting to transmit exceeds the SIC degree), the IoT gateway aborts the transmission and starts the frame again by sending a new beacon signal and the active transmitters use a random backoff. If the detected number of devices is within the SIC degree, the IoT gateway broadcast the SIC degree to the transmitters and then each active IoT device randomly picks one of the optimum power levels. If the choices of power levels are distinct, the SIC receiver can decode the self-identifying signals (device ID + payload) and then the gateway sends an ACK. However, if the active IoT devices did not select distinct power levels, the reselection process is repeated and after a few attempts, say k, if there is no successful transmission, the users receive a NACK and enter a random back-off mode. This will improve fairness among the users and will allow for the possibility of fewer active users in the next session (which will improve the probability of successful transmission). It should be clear, that the proposed protocol will be most efficient when there are a small number of active devices, so that the probability of "randomly" choosing distinct optimum power levels, after one or two random tries, is high.

[6] We denote a SIC receiver that can process m signals as SIC(m) and we refer to m as the SIC degree.

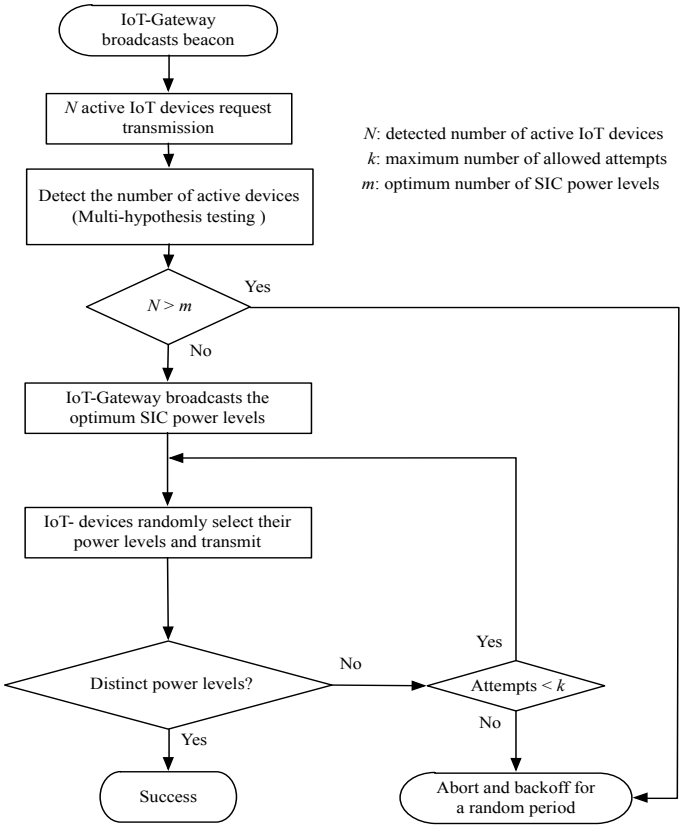


Figure 4.4 SAN protocol.

4.3.2 Multiple Hypothesis Testing

The detection of active devices starts after the IoT devices send their transmission request to the IoT gateway as illustrated in Figure 4.3. After receiving the beacon, all the IoT devices send at the same power level (with the same modulation level) a training sequence of length L using the Slotted Aloha protocol. The superimposed received signal at the IoT gateway from N active transmitting IoT devices is given by

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{s} + \boldsymbol{w}, \tag{4.2}$$

where $\boldsymbol{H} = [h_1, h_2, \dots, h_N] \in \mathbb{R}^{\mathbf{1}\times\mathbf{N}}$ and h_n is the channel gain between the nth IoT device and the IoT gateway. $\boldsymbol{s} \in \mathbb{R}^{N\times L}$ is the transmit sequence (e.g., BPSK) from N IoT active devices and $\boldsymbol{w} \in \mathbb{R}^{1\times L}$ is the additive white Gaussian noise with zero mean and variance σ^2. The multiple hypothesis test is used to detect the number of N active IoT devices from the total M IoT devices.

The following hypotheses testing procedure is used to sequentially detect the number of active devices:

$\mathcal{H}_0$: Received signal contains only noise

$$\boldsymbol{y} = \boldsymbol{w} \tag{4.3}$$

$\mathcal{H}_1$: Received signal contains data from at least one IoT device

$$\boldsymbol{y} = h_1\boldsymbol{s}_1 + \boldsymbol{w}, \tag{4.4}$$

$\mathcal{H}_N$: Received signal contains data from at most N IoT devices

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{s} + \boldsymbol{w}. \tag{4.5}$$

We assume $h_n = 1, \forall\, n \in \{1, 2, \dots, N\}$. Using the Neyman-Pearson (NP) test [69], we can write the Likelihood Ratio (LR) testing $\mathcal{H}_N$ vs. $\mathcal{H}_{N-1}$ as

$$\frac{p(\boldsymbol{y};\sum_{n=1}^{N}\boldsymbol{s}_n,\mathcal{H}_N)}{p(\boldsymbol{y};\sum_{n=1}^{N-1}\boldsymbol{s}_n;\mathcal{H}_{N-1})} = \frac{exp\left[-\frac{1}{2\sigma^2}(\boldsymbol{y}-\sum_{n=1}^{N}h_n\boldsymbol{s}_n)^T(\boldsymbol{y}-\sum_{n=1}^{N}h_n\boldsymbol{s}_n)\right]}{exp\left[-\frac{1}{2\sigma^2}(\boldsymbol{y}-\sum_{n=1}^{N-1}h_n\boldsymbol{s}_n)^T(\boldsymbol{y}-\sum_{n=1}^{N-1}h_n\boldsymbol{s}_n)\right]} \gtrless_{\mathcal{H}_{N-1}}^{\mathcal{H}_N} \gamma, \quad N = 1, \dots . M, \tag{4.6}$$

where $\boldsymbol{s}_n \in \mathbb{R}^{1\times L}$ is the transmitted sequence from the n^{th} IoT device. By taking the logarithm, (4.6) is simplified to

$$T(y) = \frac{1}{L}\sum_{l=0}^{L-1}\boldsymbol{y} \gtrless_{\mathcal{H}_N}^{\mathcal{H}_{N-1}} \frac{2\sigma^2\ln\gamma - ((\sum_{n=1}^{N-1}h_n\boldsymbol{s}_n)(\sum_{n=1}^{N-1}h_n\boldsymbol{s}_n)^T + (\sum_{n=1}^{N}h_n\boldsymbol{s}_n)(\sum_{n=1}^{N}h_n\boldsymbol{s}_n)^T)}{-2(\sum_{n=1}^{N-1}h_n\boldsymbol{s}_n + \sum_{n=1}^{N}h_n\boldsymbol{s}_n)} = \gamma' \tag{4.7}$$

The NP detector, or the test statistic, in (4.7) compares the sample mean of the received signal to the threshold γ' to decide on a hypothesis $\mathcal{H}_N$ or $\mathcal{H}_{N-1}$. The NP test terminates if the number of detected devices exceeds the SIC degree (the number of receiver optimum power levels, which is taken as 3 levels in this section). To compute the threshold γ' in (4.7) for a desired probability of false alarm P_{FA}, which occurs when deciding $\mathcal{H}_N$ if the test in (4.7) is greater than the threshold γ', so that P_{FA} can be written as

$$P_{FA} = P(T(\boldsymbol{y}) > \gamma';\, \mathcal{H}_N). \tag{4.8}$$

Since the test in (4.7) under both hypotheses is a Gaussian distribution, that $T(\boldsymbol{y}) \sim \mathcal{N}(\sum_{l=0}^{L-1}\sum_{n=1}^{N-1}\boldsymbol{s}_n, \frac{\sigma^2}{L})$ under $\mathcal{H}_{N-1}$ and $T(\boldsymbol{y}) \sim \mathcal{N}(\sum_{l=0}^{L-1}\sum_{n=1}^{N}\boldsymbol{s}_n, \frac{\sigma^2}{L})$ under $\mathcal{H}_N$ we rewrite (4.8) as

$$P_{FA} = Q\left(\frac{\gamma' - \sum_{l=0}^{L-1}\sum_{n=1}^{N} s_n}{\sqrt{\sigma^2/L}}\right) \tag{4.9}$$

Thus, the threshold γ' is given by

$$\gamma' = Q^{-1}(P_{FA})\sqrt{\sigma^2/L} + \sum_{l=0}^{L-1}\sum_{n=1}^{N}\boldsymbol{s}_n. \tag{4.10}$$

Following the same steps, the probability of detecting the number of active devices is

$$P_D = Q\left(\frac{\gamma' - \sum_{l=0}^{L-1}\sum_{n=1}^{N-1} s_n}{\sqrt{\sigma^2/L}}\right). \tag{4.11}$$

From (4.8), (4.9) we can write the P_D as a function of energy to noise ratio as

$$P_D = Q\left(Q^{-1}(P_{FA}) + \frac{\sum_{l=0}^{L-1}\sum_{n=1}^{N}\boldsymbol{s}_n - \sum_{l=0}^{L-1}\sum_{n=1}^{N-1}\boldsymbol{s}_n}{\sqrt{\sigma^2/L}}\right). \tag{4.12}$$

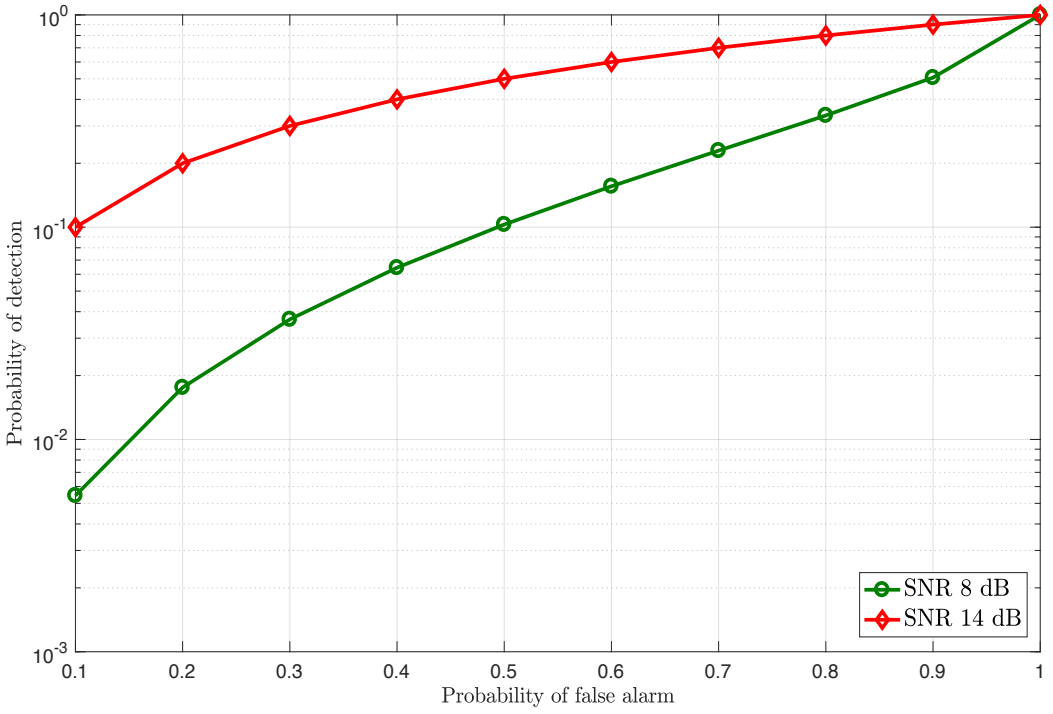


Figure 4.5 The Receiver Operating Characteristic (ROC) of the energy detector.

Figure 4.5 illustrates the receiver operating characteristic (ROC) curve of the energy detector. Observe that the detection performance increases monotonically and smoothly with increasing SNR.

4.4 Simulation Results

In this section, the simulation results are presented to evaluate the performance of the SAN and CSMA/CA protocols based on throughput and average delay. Throughout the simulation, we assume there is one IoT gateway and a total of *M* IoT devices. A binomial distribution is considered to model the random number of active IoT devices N, each with a probability of transmission p_T.

$$P_r(N;\ p_T, M) = \binom{M}{N}\ {p_T}^N\ (1 -\ p_T)^{M-N}\ . \tag{4.13}$$

Figure 4.6 shows the throughput of SAN for different values of p_T, and $k = 3$ maximum attempts for the random selection of distinct optimum power levels (so, the probability of success should be 0.4 within 3 attemps). The throughput is the average number of successful transmissions for each probability of transmission over time. As expected, we observe that the throughput decreases with increasing probability of transmission in both protocols. More importantly, we can see that the throughput of the SAN protocol is weighted by the average payload of successful transmissions and always higher than that of the Slotted Aloha protocol. When the probability of transmission is 0.03, the throughput of SAN with 3 power levels performs better than the CSMA/CA and has 5 times higher throughput than that of (conventional) Slotted Aloha. This demonstrates that NOMA with a SIC receiver can significantly improve the throughput of Slotted Aloha. However, the throughput of SAN becomes lower than CSMA/CA for a probability of transmission greater than 0.06 (i.e., increase of offered load from the IoT devices), which is not surprising since for *M* = 50 the average number of active devices exceeds the number of acceptable power levels (SIC capability). The improved performance of CSMA/CA in a higher probability of transmission regime is due to the collision avoidance mechanism. It can be noted from Figure 4.7

that adding more power levels (6 power levels) to SAN increase the throughput at the expense of the average delay, which is discussed next.

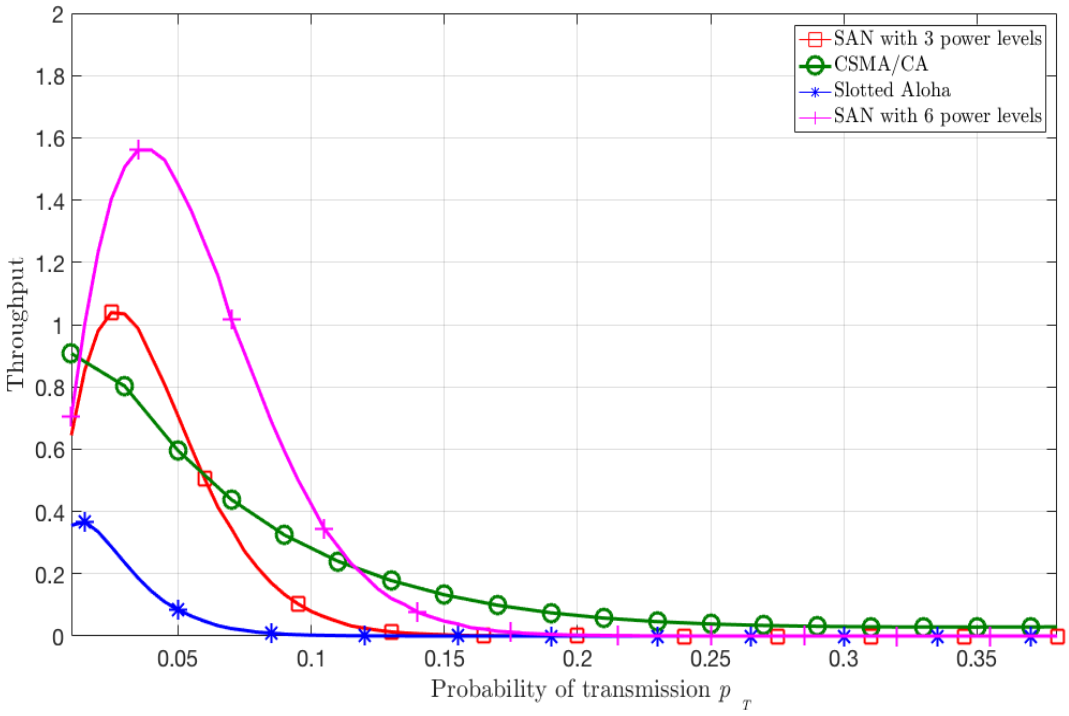


Figure 4.6 The throughput of SAN $k = 3$ vs. Slotted Aloha and CSMA/CA for different values of probability of transmission M=50.

The second performance metric is the average delay as shown in Figure 4.5. In the simulation, the average delay is composed of propagation delay, data processing delay, random backoff delay, sensing delay (in CSMA/CA) and selecting distinct power levels attempts (in SAN). Observe that the average delay of SAN exceeds that of CSMA/CA in the low probability of transmission case due to the unique power level selection process, which enables the higher throughput as mentioned above. The more attempts allowed for picking the optimum power levels, the higher the throughput that can be achieved at the cost of increased delay. Since the backlogged IoT devices (i.e., those that failed to transmit in the previous try) have not been considered as

rejoining the transmission queue[7], the average delay reported at a higher probability of transmission is the propagation delay and the random backoff delay.

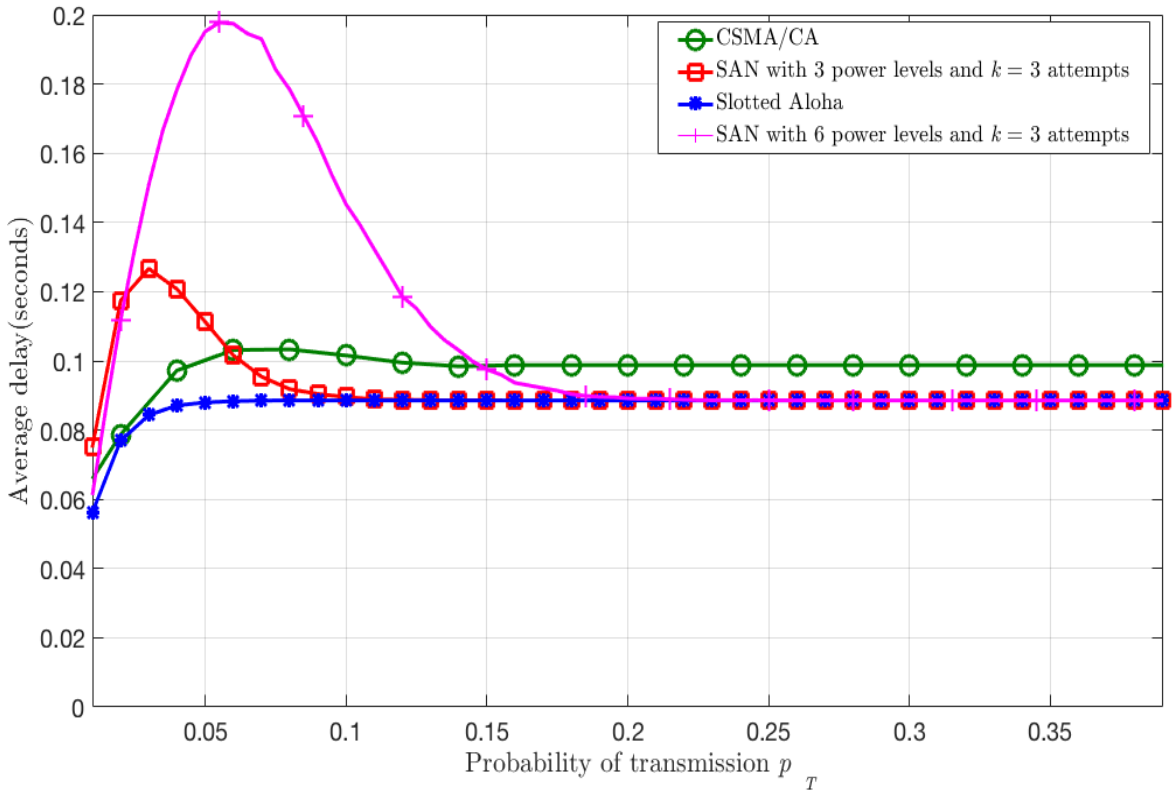


Figure 4.7 The average delay of SAN and CSMA/CA.

4.5 Concluding Remarks

A novel protocol (SAN) for M2M communications in IoT networks was presented and compared to CSMA/CA protocol in terms of throughput and delay access. The synergistic combination in SAN of Slotted Aloha, NOMA, and SIC reception was demonstrated to significantly improve the throughput performance with respect to the CSMA/CA and Aloha protocols at a low probability of transmission. Simulation results show that the SAN protocol can outperform CSMA/CA at a higher probability of transmission by increasing the number of received signals (that is, the power levels) at the cost of average delay.

[7] The same assumption is made in Abramson's original Aloha analyis [70].

CHAPTER 5: DATA DRIVEN BEAM SWEEPING FOR 5G mmWAVE CELLULAR SYSTEMS

5.1 Introduction

The vast available spectrum at mmWave frequencies between 24 GHz to 100 GHz offers orders of magnitude greater bandwidths for cellular communication. However, the propagation environment at the mmWave bands are poor (high pathloss and blocking) compared to the frequency bands used by previous cellular system generations. To cope with the harsh propagation conditions, the user equipment (UE) and gNB[8] must establish a highly directional transmission link using beamforming. However, the directional transmission links required fine beam alignment between the transmitter and receiver. It is worth mentioning that significant Non- line-of-sight (NLOS) street-level coverage is possible up to approximately 200 m from a base station based on the measurements in New York City at 28 and 73 GHz [71].

In this chapter[9], beam sweeping pattern prediction to determine the beam hopping sequence during cell search that is based on the dynamic distribution of user traffic is investigated. This is done by using a form of recurrent neural networks (RNNs) called a Gated Recurrent Unit (GRU).

5.2 Beam Sweeping in mmWave Cellular Systems

The standalone 5G mmWave system is subject to significant coverage issues if beam sweeping (directional transmission) is not applied during cell search. In the current 4G LTE

[8] gNB is the 5G New Radio term for a base station.

[9] The content of this chapter has been published in [13]- [14] and it is included in this dissertation with permission from the IEEE. Permission is included in Appendix A.

system, the initial access is performed on omnidirectional channels, whereas the beamforming transmission is performed after establishing the physical link [69]. On another hand, to cope with the converge issue resulting from the increased isotropic path loss in mmWave frequencies, in 5G standalone mmWave cellular systems, the initial access must be performed on directional-limited channels [72].

In the ongoing 5G NR standalone mmWave standards meetings, the so-called synchronization signal block (SSB) was introduced, which comprises a primary synchronization signal (PSS), a secondary synchronization signal (SSS), and a physical broadcast channel (PBCH)[72]. The synchronization signal burst was allocated 250 microseconds, which was further divided into 14 SSB as illustrated in Figure 5.1. The gNB may sweep 14 different directions (per antenna port) for the sync transmission. The exact choice of the sweeping pattern can be left to the cells; this pattern should occur periodically and the maximum periodicity must be known by the UE [73].

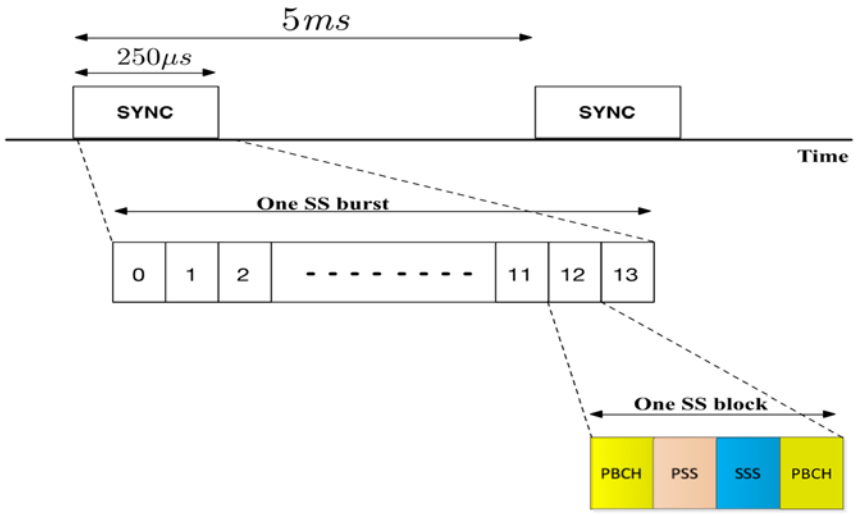


Figure 5.1 Resources allocated to sync transmission in 5G NR.

The initial access in 5G New Radio (NR) standalone millimeter-wave systems is a time-consuming search to determine suitable directions of transmission and reception. The overall

procedures of cell acquisition in standalone mmWave systems is composed of four operations under the term beam management as depicted in Figure 5.2 [74].

- *Beam sweeping*. Transmitting the synchronization signals to cover a spatial area using a set of predetermined directions (beamforming vector) and time interval.
- *Beam measurement*. Evaluating the quality of the received at the gNB or at UE.
- *Beam determination*. The UE selects the beam (optimal directional communication link) that provides the maximum SNR and above a predefine threshold according to the beam measurement.
- *Beam reporting*. After beam determination, the UE wait for the gNB to schedule directional (Random Access Channel) RACH resource to send its RACH preamble.

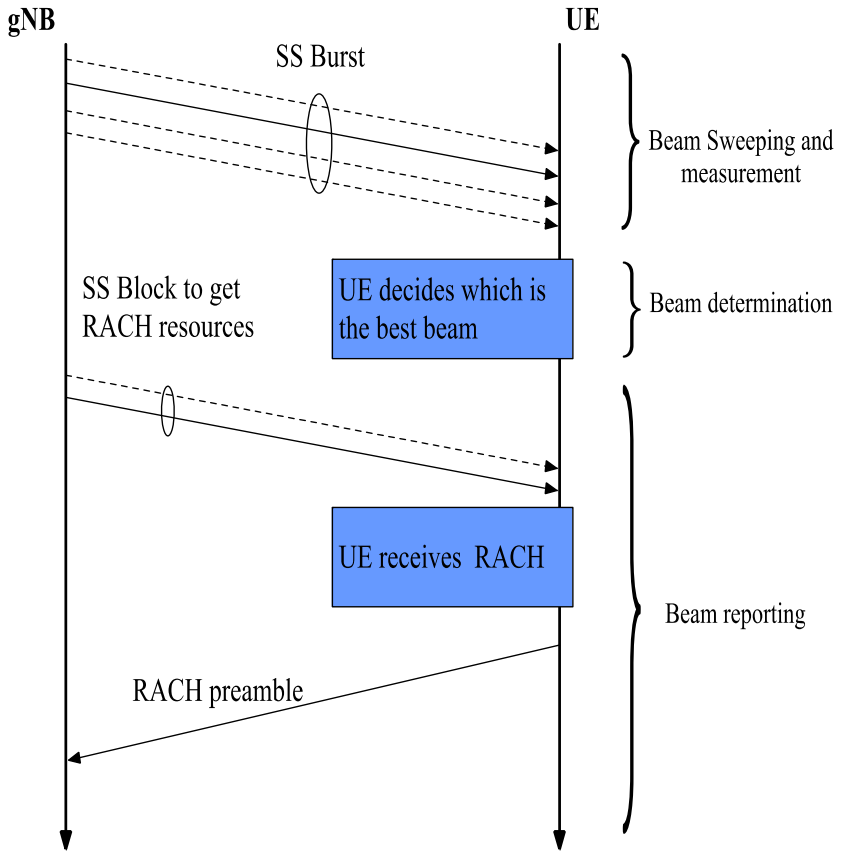


Figure 5.2 Beam management procedures in standalone mmWave cellular system.

The problem of interest in this research is the cell discovery. In the cell discovery phase, one approach is sequential beam sweeping by the base station that requires a brute force search through many beam-pair combinations between the UE and the gNB to find the optimum beam-pair (i.e. the one with the highest RSRP[10]-level) as shown in Figure 5.3. The sequential search may result in a large access delay and low initial access efficiency. It is worth mentioning that a UE does not only need to carry out cell search at power-up, but to support mobility. It also needs to continuously search for and synchronize to neighboring cells and estimate their reception quality. The reception quality of the neighboring cells, in relation to the reception quality of the current cell, is then evaluated to determine if a handover (for devices in RRC CONNECTED) or cell reselection (for devices in RRC IDLE) should be carried out [75].

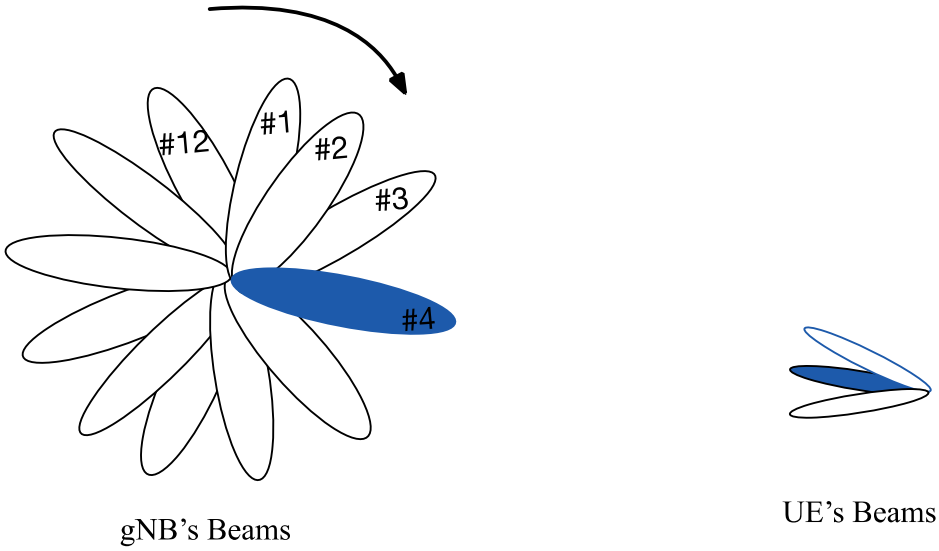


Figure 5.3 Beam sweeping during initial access.

5.3 Recurrent Neural Network Beam Sweeping

To ensure that users can be quickly accessed, a form of machine learning can be used to optimize the sweeping pattern of the gNB, including beam direction and sweeping pattern

[10] RSRP: Reference signal received power

according to the predicted user's spatial distribution from users' historical data (e.g. delay access, access success rate and beam direction etc.). The focus of this research is the sweeping pattern (hopping) in the cell discovery phase. The proposed approach leverages intelligence from the call detail record CDR data collected from the Milan City network, provided by Telcom Italia as part of their Big Data challenge [76].

5.3.1 Dataset

The data used in this dissertation is in form of CDRs of Internet activity, calling and text messages as given in Table 5.1. The dataset measures the level of interaction of the users and the cellular network by temporally aggregating CDRs in timeslots of 10 minutes. The datasets provide spatial information about each CDR by using the Milano Grid [77] CDR data, which contains numbered squares (square ID) that are overlaid over Milan city as shown in Figure 5.4.

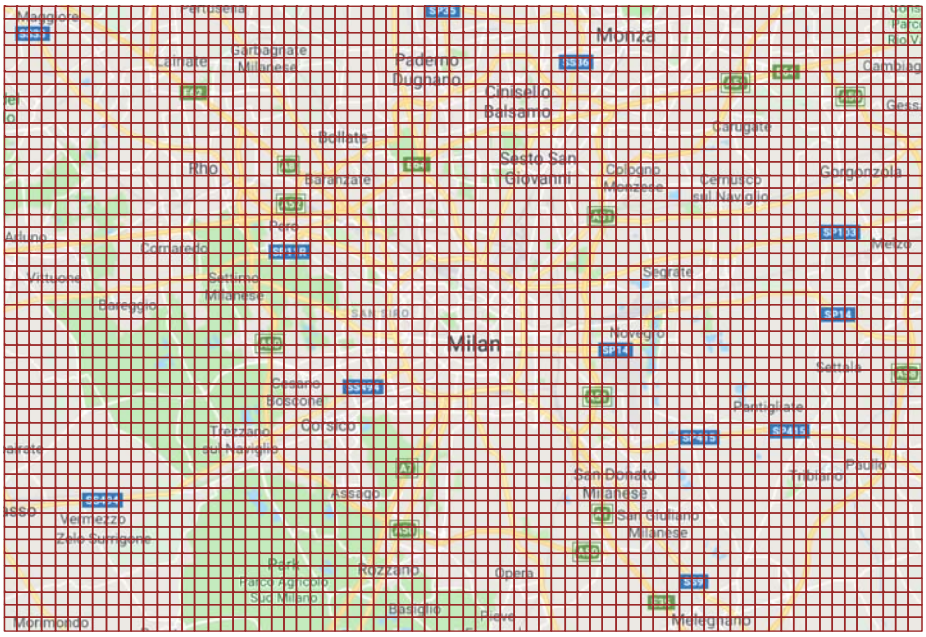


Figure 5.4 Milano Grid

The data takes the coordinates of each CDR and only provides the square ID. Therefore, to achieve the objective of the proposed data-driven sweeping pattern, we assume that a cell is made

of four squares in the Milano grid and each square represents a sector (direction). In order to determine the users' activity in each sector, the raw data in Table 5.1 is preprocessed by counting the number of CDRs (non-zero activity in Table 5.1 in each square ID) that was recorded in the same timestamp in a given sector. The resulting sample data points are presented in in Table 5.2, which show the number of CDRs on "2013-11- 03" at five timestamps in four sectors denoted by A, B, C and D (Square ID 1,2,101,102 in Table 5.1). In this research the pseudo-omni beam (i.e., widest beam width) transmission is adapted (i.e., the gNB transmits the synchronization signal for a longer duration with a pseudo-omni beams). The order of the beam sweeping is determined based on time series prediction using a Neural Network as discussed later.

Table 5.1 Samples from Milan dataset

Square ID	Time	SMS-in-activity	SMS-out-activity	Call-in-activity	Call-out-activity	Internet-traffic
1	2013-11-03 23:00:00	0.108039	0	0	0	0
1	2013-11-03 23:00:00	0.109257	0	0	0	0
1	2013-11-03 23:00:00	0.027356	0.029144	0.027356	0.055578	9.282384
2	2013-11-03 23:00:00	0.088022	0	0	0	0
101	2013-11-03 23:00:00	0.042141	0.55355	0.026832	0.052954	8.114206
101	2013-11-03 23:00:00	0.027706	0.027244	0.027706	0.055225	9.246850
102	2013-11-03 23:00:00	0.109438	0	0	0	0
102	2013-11-03 23:00:00	0.026137	0.030875	0.026137	0.055225	9.260190
102	2013-11-03 23:00:00	0.19	0.109900	0.027244	0	9.228577
1	2013-11-03 23:10:00	0	0	0.028502	0.05789	8.235573
1	2013-11-03 23:10:00	0.042141	0	0	0.055233	8.134563

Table 5.2 Number of CDRs per sector after preprocessing

Time	A	B	C	D
2013-11-03 23:00:00	7	1	10	10
2013-11-03 23:10:00	6	4	7	9
2013-11-03 23:20:00	8	2	9	6
2013-11-03 23:30:00	11	5	12	11
2013-11-03 23:40:00	5	7	8	13

5.3.2 Recurrent Neural Networks

The number of CDRs in each sector in Table 5.2 is a time series. To determine the sweeping pattern, a recurrent neural network (RNN) is used to predict the number of CDRs in all sectors, which is used to prioritize the sweeping hopping pattern. The RNN architecture can capture dependencies at different time scales. This is achieved by passing some information from the previous time step to contribute to the output at the present time step, that addition of memory allows the time dependencies in the data to affect the prediction. Figure 5.5 illustrates a "rolled" and "unrolled" RNN diagrams in time with a layer of neurons *A*. Observe that the output at time h_t, depends on the current input X_t and the previous state (t-1) of layer *A* as shown in the unrolled version of the RNN in Figure 5.5.

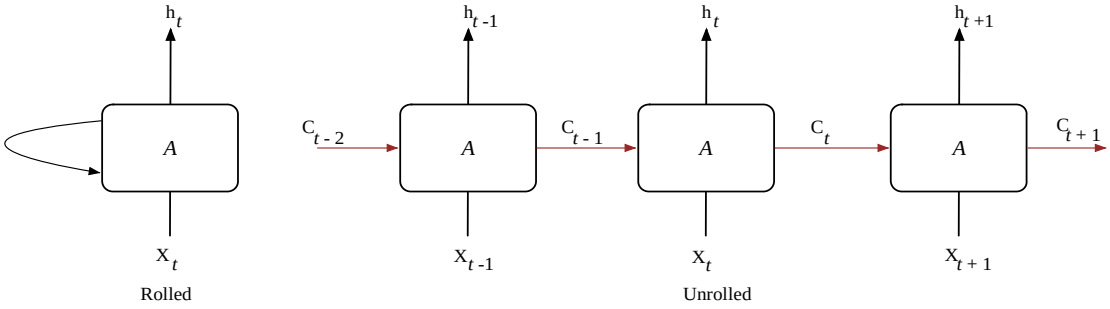


Figure 5.5 Rolled RNN (left) and its unrolled version (right)

The traditional RNNs are very hard to train using backpropagation because of the gradient vanishing, i.e. the derivatives of the activation functions used in the neural network approach zero quickly, which means the typical RNN can only capture a short temporal pattern in the data sequence. Spatial gates were introduced to solve the gradient vanishing problem such as Gated Recurrent Unit (GRU)[78].

5.3.3 Gated Recurrent Unit Architecture

The GRU neural net was first introduced by Cho et al. [78] for a statistical machine translation task. Figure 5.6 illustrates the architecture of a GRU cell. A GRU made of two gates. The first is the update gate, which controls how much of the current cell content should be updated with the new candidate state. The second is the reset gate, which resets the memory of the cell if it is closed i.e. the unit acts as if the next processed input was the first in the sequence. The following steps explained the operations of the state equations of the GRU [79].

- First, the *updated gate* $\mathbf{u}[t]$ is calculated using

$$\mathbf{u}[t] = \sigma(\mathbf{W}_u\mathbf{h}[t-1] + \boldsymbol{R}_u\mathbf{x}[t] + \boldsymbol{b}_u), \tag{5.1}$$

  where $\mathbf{x}[t]$ is the input data sequence (number of CDRs in all sectors), $\mathbf{h}[t-1]$ is the state from the previous time step, $\boldsymbol{R}_u$ is the weight matrix for the input at the update gate, $\mathbf{W}_u$ is the weight matrix for the previous state and $\boldsymbol{b}_u$ is the bias vector. A sigmoid activation function σ is applied to scale the results between 0 and 1.

- The *reset gate* is used to decide how much of the past information in the previous states to forget and can be obtain by

$$\mathbf{r}[t] = \sigma(\mathbf{W}_r\mathbf{h}[t-1] + \boldsymbol{R}_r\mathbf{x}[t] + \boldsymbol{b}_r), \tag{5.2}$$

  Note that the *rest gate* is similar to the *update gate* with a difference in the weight matrices, the bias plus the functionality of the gate, which is given by

$$\mathbf{h}'[t] = \mathbf{h}[t-1] \odot \mathbf{r}[t], \tag{5.3}$$

where the element-wise product $\odot$ (Hadamard product) between $\mathbf{h}[t-1]$ and $\mathbf{r}[t]$ determines what to remove from the previous time steps.

- Next, the candidate state is calculated by

$$\mathbf{z}[t] = tanh(\mathbf{W}_z\mathbf{h}'[t-1] + \boldsymbol{R}_z\mathbf{x}[t] + \boldsymbol{b}_z), \tag{5.4}$$

where $\mathbf{h}'[t-1]$ the information from the previous state after applying the *rest gate* in (5.3).

- Finally, the information for the current state is calculated by

$$\mathbf{h}[t] = (1 - \mathbf{u}[t]) \odot \mathbf{h}[t-1] + \mathbf{u}[t] \odot \mathbf{z}[t], \tag{5.5}$$

In this chapter, a Gated Recurrent Unit (GRU) Neural Network with 512 units is used to predict the number of CDRs in all sectors.

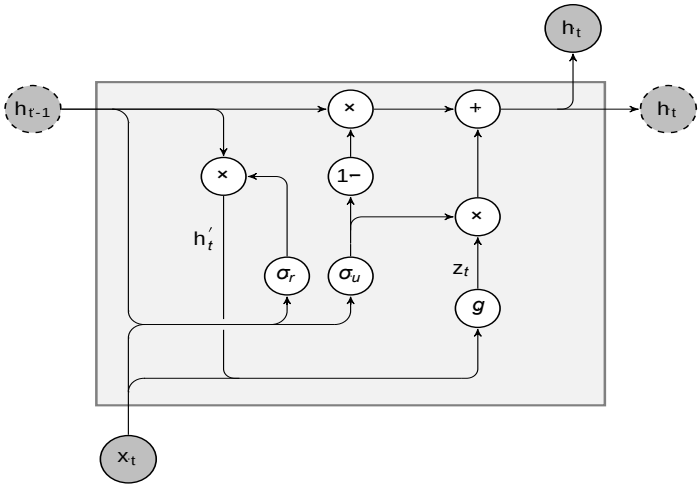


Figure 5.6 A recurrent unit in the GRU architecture. Dark gray circles with a solid line are the variables whose content is exchanged with the input and output of the network. Dark gray circles with a dashed line represent the internal state variables, whose content is exchanged within the cells of the hidden layer. White circles with +, 1 and × represent linear operations.

5.4 Comparing the RNN Beam Sweeping with Random Starting Point Beam Sweeping

In this section, the delay analysis of two approaches is compared to quantify how much faster the data-driven approach is than the random starting point scheme. In both schemes, we

assume that the gNB sweeps through L possible directions. We will call each such cycle of L transmissions a "scanning cycle." Since the transmission period is T seconds, each scan cycle will take LT seconds as depicted in Figure 5.7.

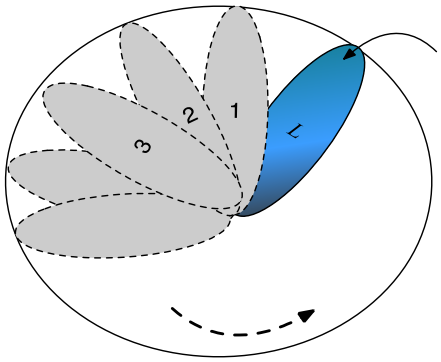


Figure 5.7 The scanning cycle in the initial access.

The synchronization delay is the time it takes the UE to detect the presence of the synchronization signal in the initial access phase. Assuming the ideal case where UE can reliably detect and decode the synchronization signal in the first scanning cycle, the synchronization delay of the data-driven approach and the random starting point scheme is compared in two different scenarios: (1) UEs are uniformly distributed over the angular space (transmission directions) as illustrated in Figure 5.8 (a) and (2) UE are sparsely distributed over the angular space (transmission directions) as illustrated in Figure 5.8 (b)

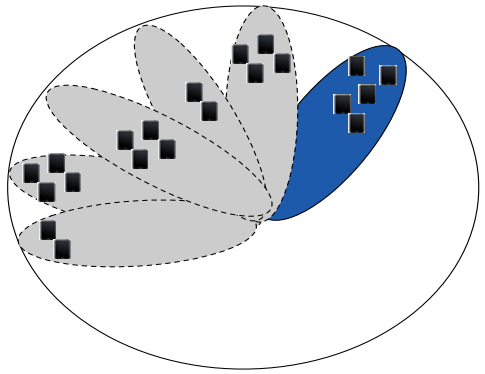
5.4.1 Uniformly Distributed UE

In this case, the UE are distributed over the transmission directions uniformly, i.e. there are UE in all sectors as in Figure 5.8 (a). Intuitively, both schemes have similar synchronization delays in terms of accessed UE per scanning cycle as will be demonstrated next.

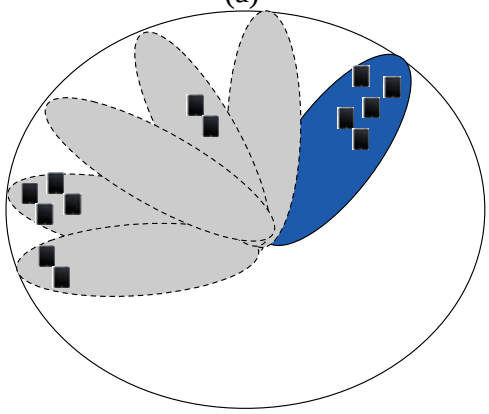
5.4.2 Sparsely Distributed UE

In this scenario, the data-driven approach using a RNN outperforms the random starting point scheme in terms of the number of accessed UE per scanning cycle during the initial access phase. This can be demonstrated by the following scenario:

suppose that there are eight sectors (transmission directions) with 16 UE distributed as shown in Figure 5.9 and analog beamforming is used to scan the angular space during the initial access phase. In the random starting point, the gNB starts the sweeping by randomly picking one direction out of eight possible directions. Then, it could either continue with the remaining directions using the sequential sweeping clockwise/anti-clockwise from the randomly selected starting points or pick randomly from the remaining directions until all directions are swept. Note that, in the random starting point scheme the gNB must scan all the directions i.e. complete one scanning cycle to access all 16 UE. On the other hand, in the initial access using a RNN the gNB need only scan the populated directions relaying on the accurate prediction from the RNN. Thus, the initial access based on the RNN may access 16 UE in a fraction of the scanning cycle (in Figure 5.9 16 a UE can initially access the gNB in half a scanning cycle).



(a)



(b)

Figure 5.8 (a) UE are uniformly distributed over the transmission directions. (b) UE have a sparse distribution over the transmission directions.

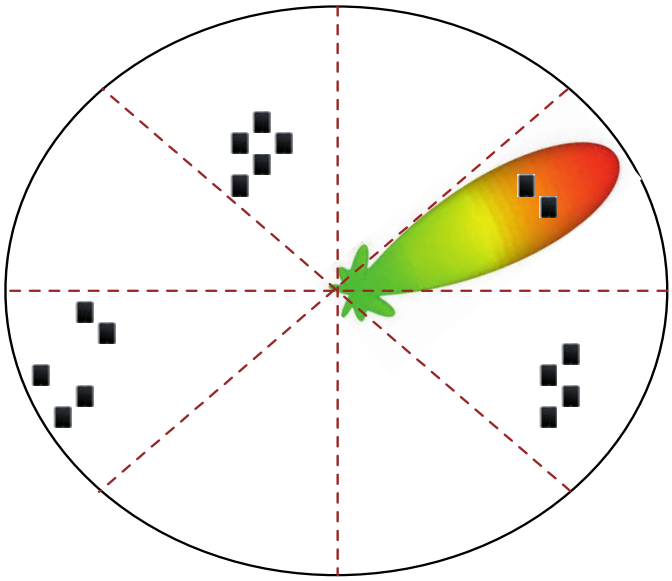
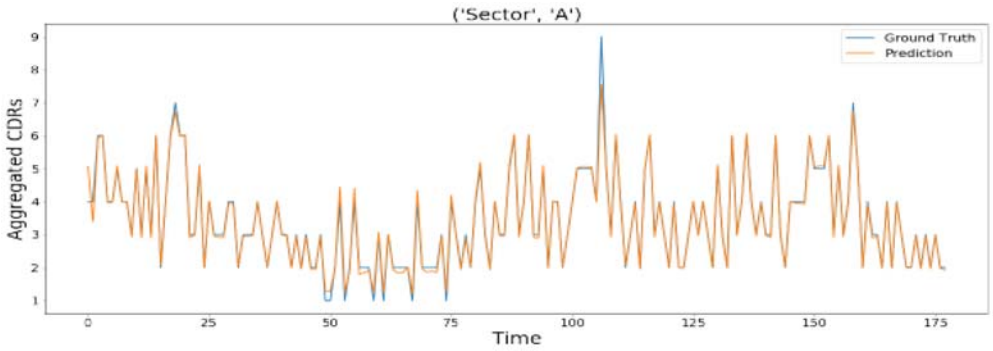


Figure 5.9 The UE are sparsely distributed over eight transmission directions.

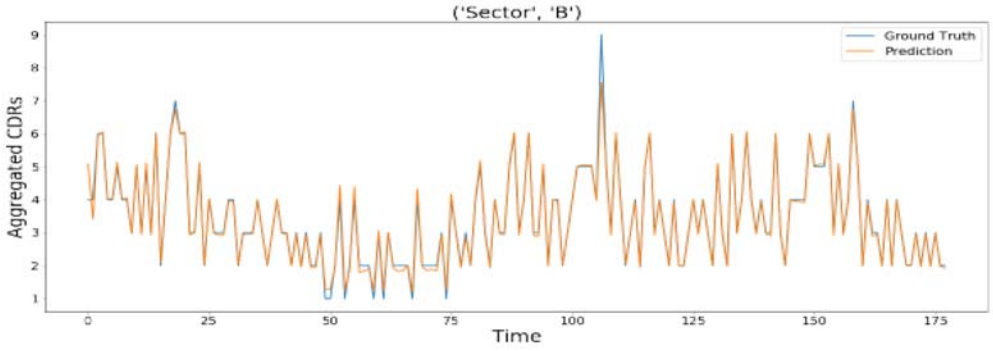
5.5 Simulation Results

In our study, two weeks of Milan CDR data (Nov 04, 2013 to Nov 17, 2013) were used to predict the user distribution in four sectors between the instants when the CDRs are measured. A total of 1684 sequences was used to train the GRU model and 188 to test it. The model was trained with 20 epochs, each with 50 steps. The model takes 28min 55s to train with the above-mentioned epochs and needs to be re-trained offline once every several days. Figure 5.10 depicts the prediction performance of the GRU model on the tested sequences, which is the aggregated CDR per direction as a function of time (every 10 minutes). It can be seen that the prediction is very close to the ground truth[11] most of the time. Based on the prediction the pseudo-omni beam can be directed toward the sector with a maximum number of CDRs. In the case that the number of CDRs are equal, the gNB chooses the sweeping order randomly. The GRU is optimized by minimizing the Mean Square Error (MSE) as a cost function. Figure 5.11 depicts the gradual decrease of the cost function with the epoch number, which results in the rapid learning rate of the model.

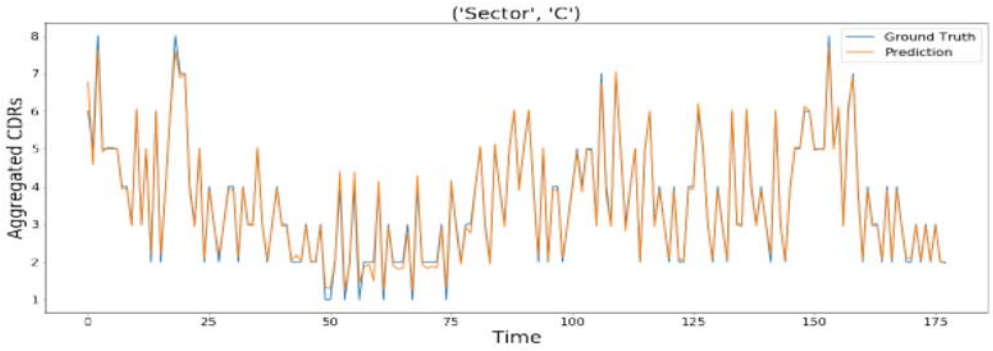
[11] In machine learning, the term "ground truth" refers to the accuracy of the training set's classification for supervised learning techniques.



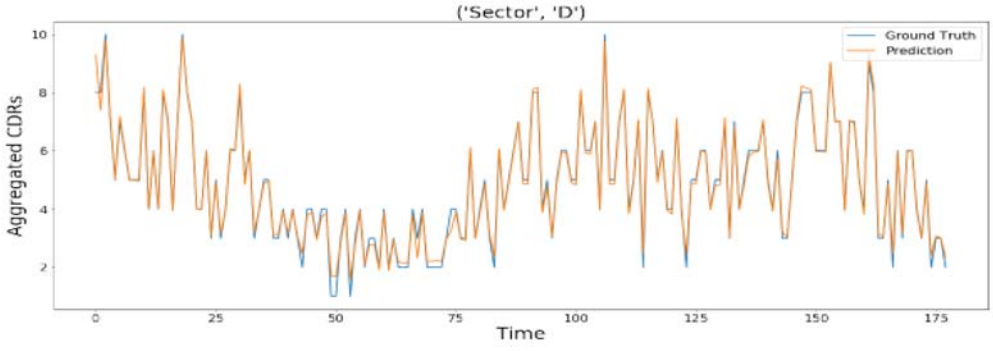
(a)



(b)



(c)



(d)

Figure 5.10 CDRs prediction and ground truth (the actual distribution) for four sectors (a) sector A, (b) sector B, (c) sector C and (d) sector D.

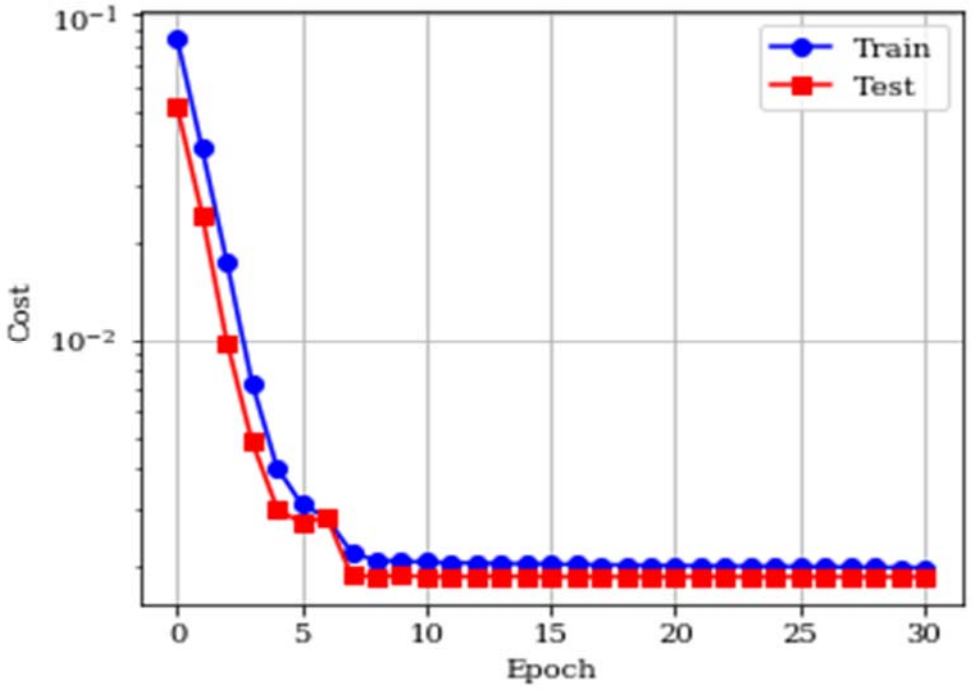


Figure 5.11 Convergence of GRU training model calculated based on MSE cost function

The performance of RNN beam sweeping and random starting point in different UE distribution is illustrated in Figure 5.12. Note that both schemes require one scanning cycle in the uniformly distributed UE scenario, however, the RNN beam sweeping outperforms the random starting point scheme in the sparsely distributed UE as it requires approximately 0.2 scanning cycle on average. Figure 5.13. shows the cumulative distribution function of the scanning cycle when the RNN beam sweeping is applied on eight sectors (transmission directions). The UE distribution over the angular space is derived from the call details record (CDR) of Milan City [2]. Note that the UE can initially assess the gNB in approximately 0.41 of a complete scanning cycle with probability 0.9. As mentioned in section 5.4.1, the random starting point beam sweeping covers the angular space by performing a complete scanning cycle. Thus, the RNN beam sweeping scheme converge faster than the random starting point approach.

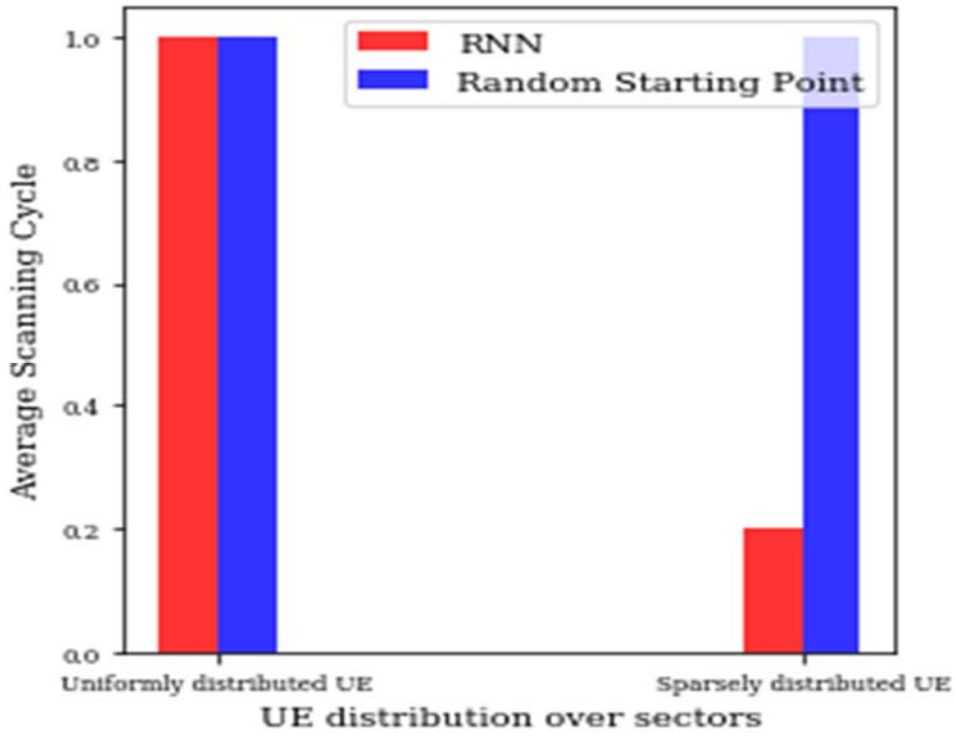


Figure 5.12 Average scanning cycle in different UE distribution.

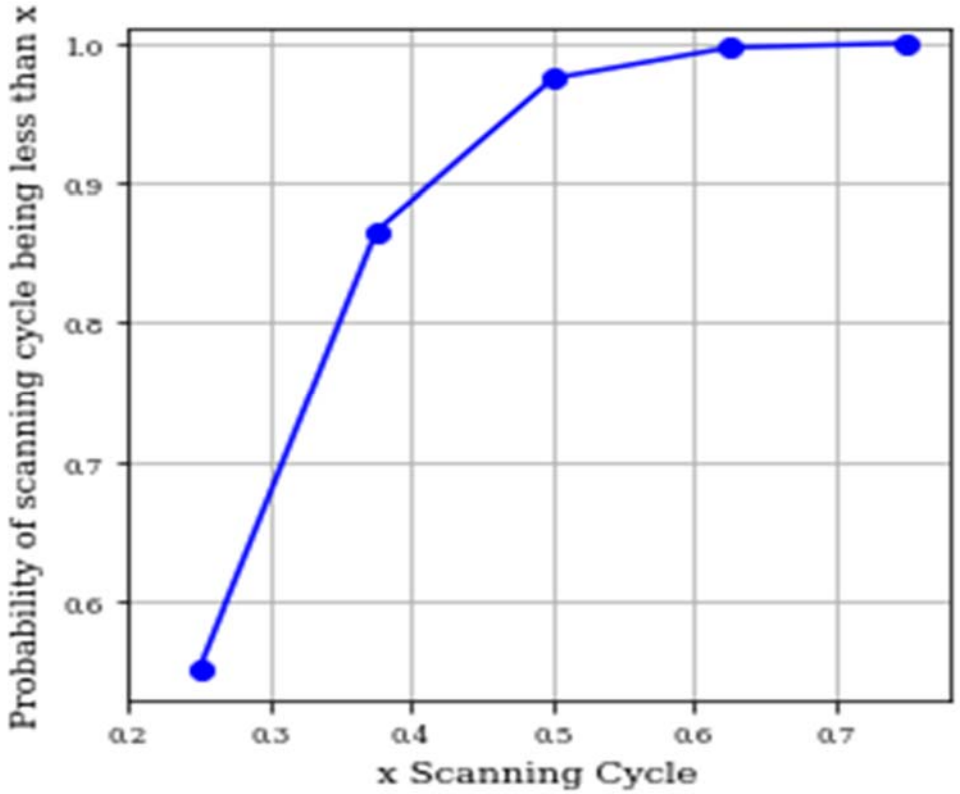


Figure 5.13 The CDF of the scanning cycle of RNN based beam sweeping.

5.6 Concluding Remarks

Data-driven beam sweeping (hopping) patterns have been introduced in this chapter for 5G mmWave cellular system initial access. It is shown that as GRU neural network can predict the CDRs with high accuracy, which is then used to adjust the sweeping pattern in the angular domain. Although, the pseudo-omni approach was considered due to the lack of exact user location in the gNB coverage, sweeping with a narrow beam can be done if the data reveals more information about the locations. The data-driven beam sweeping was demonstrated to significantly reduce the scanning cycle during the initial access with respect to a random starting point in a sparsely distributed UE scenario.

CHAPTER 6: CONCLUSION AND FUTURE DIRECTIONS

6.1 Main Contributions and Conclusions

This dissertation is directed toward investigating, evaluating, and enhancing security, throughput, and latency in a variety of 5G infrastructure networks.

In Chapter 3, a novel physical layer secure key management for symmetric cryptography was presented. The unique wireless channel characteristic between the legitimate users and an eavesdropper is exploited to create a low probability of interception and a large frame error probability (FEP) at the unintended receiver, while the intended receiver successfully receives the transmitted signal with a very low FEP. This technique becomes more attractive at mmWave frequencies because the correlation between the main channel and the wiretap channel is dramatically reduced, which implies a low probability of key interception by the eavesdropper.

In Chapter 4, a novel Hybrid MAC protocol (SAN) for M2M communications in IoT networks was presented. The SAN is easy to implement, compatible with low power/complexity of IoT devices and significantly improves the throughput compared to Slotted Aloha and CSMA/CA in a sporadic traffic pattern where IoT devices have a low probability of transmission. The superior throughput of the SAN protocol is a result of using NOMA with a SIC receiver and a novel random modulation algorithm that enables the IoT devices to select distinct power levels during the transmission period of the SAN protocol.

In Chapter 5, RNN neural net based beam sweeping for 5G mmWave cellular systems was proposed. The Call Detail Records (CDRs) of Milan city were leveraged to accelerate the initial acquisition procedure in mmWave 5G new radio by using machine learning (ML) to prioritize the

beam sweeping pattern during the initial access. The ML data-driven based beam sweeping outperforms the random starting point beam sweeping in terms of the required scanning cycle to send the synchronization signals in sparsely distributed UE scenario.

6.2 Future Directions

This section presents some promising directions for future work related to the contributions in this dissertation.

- Implementing the proposed secure key management via physical layer security processing in a real experimental testbed using a Software Defined Radio (SDR) platforms such as the Ettus Research Universal Software Radio Peripheral (USRP). This would demonstrate corroborating results on the correlation between the main and wiretap channels for different spatial and temporal scenarios and verify the theoretical and simulation results presented in Chapter 3. Furthermore, extensions of the proposed algorithm to multiple legitimate users and multiple eavesdroppers are of interest especially at mmWave frequencies where a massive number of antennas at the base station can serve multiple legitimate users leveraging the spatial correlation.
- Extending the evaluating the throughput of the SAN protocol using an imperfect SIC receiver is an interesting research direction. Similarly investigating the fairness of SAN protocols and the effect on performance of the backlogged IoT devices that rejoin the transmission queue. Moreover, extend the multiple hypothesis testing procedure for the Rayleigh channel to investigate the further extension of the use cases of the SAN protocol beyond the Smart Home use case.
- Extending and quantifying the access delay of the data-driven sweeping order using a GRU neural net and a comparison with a random starting point sweeping for the detection of the

synchronization signals using different mmWave channel models is an important research topic. As is, evaluating RNN based beam sweeping when narrow beams are used to transmit the synchronization signals.

REFERENCES

[1] E. Dahlman, S. Parkvall, and J. Skld, “Chapter 1 - what is 5G?” in 5G NR: the Next Generation Wireless Access Technology, E. Dahlman, S. Parkvall, and J. Skld, Eds. Academic Press, 2018, pp. 1 – 6. [Online]. Available: http://www.sciencedirect.com/science/article

[2] A. Rajandekar and B. Sikdar, "A Survey of MAC Layer Issues and Protocols for Machine-to-Machine Communications," in IEEE Internet of Things Journal, vol. 2, no. 2, pp. 175-186, April 2015.

[3] A. Mazin, K. Davaslioglu and R. D. Gitlin, "Secure key management for 5G physical layer security," 2017 IEEE 18th Wireless and Microwave Technology Conference (WAMICON), Cocoa Beach, FL, 2017, pp. 1-5.

[4] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, “Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions,” IEEE Communications Magazine, vol. 52, no. 5, pp. 86–92, May 2014.

[5] 3GPP, “Study on RAN improvements for machine-type communications,” TS 37.868 V11.0, October 2011.

[6] 3GPP, “Evolved universal terrestrial radio access (E-UTRA); medium access control (MAC) protocol specification,” TS 36.321 V13.2.0, October 2016.

[7] A. Mazin, M. Elkourdi and R. D. Gitlin, "Comparison of Slotted Aloha-NOMA and CSMA/CA for M2M Communications in IoT Networks," IEEE 88th Vehicular Technology Conference (VTC2018-Fall), Chicago, IL, USA, August 27-30, 2018.

[8] S. M. Kay, Fundamentals of Statistical Signal Processing: Practical Algorithm Development. Prentice Hall, 2013.

[9] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, “What Will 5G Be?” IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065–1082, June 2014.

[10] Z. Pi and F. Khan, “An introduction to millimeter-wave mobile broadband systems,” IEEE Communications Magazine, vol. 49, no. 6, pp. 101–107, June 2011.

[11] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, “Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!” IEEE Access, vol. 1, pp. 335–349, 2013.

[12] A. Ghosh, T. A. Thomas, M. C. Cudak, R. Ratasuk, P. Moorut, F. W. Vook, T. S. Rappaport, G. R. MacCartney, S. Sun, and S. Nie, “Millimeter-Wave Enhanced Local Area Systems: A High-Data-Rate Approach for Future Wireless Networks,” IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1152–1163, 2014.

[13] A. Mazin, M. Elkourdi and R. D. Gitlin, "Accelerating Beam Sweeping in mmWave Standalone 5G New Radios using Recurrent Neural Networks," IEEE 88th Vehicular Technology Conference (VTC2018-Fall), Chicago, IL, USA, August 27-30, 2018.

[14] Asim Mazin, Mohamed Elkourdi and R. D. Gitlin, "Comparative Performance Analysis of Beam Sweeping Using a Deep Neural Net and Random Starting Point in mmWave 5G New Radio," 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) 2018, New York City, NY, USA,November 8-9, 2018.

[15] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio- telepathy: Extracting a secret key from an unauthenticated wireless channel,” in Proc. of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom ’08). New York, NY, USA, September 2008, pp. 128–139.

[16] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N.B. Mandayam, “Information-theoretically secret key generation for fading wireless channels,” IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 240–254, June 2010.

[17] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, “Exploiting multiple- antenna diversity for shared secret key generation in wireless networks,” in Proc. IEEE INFOCOM, San Diego, CA, USA March 2010, pp. 1–9.

[18] M. Wilhelm, I. Martinovic, and J. B. Schmitt, “Secure key generation in sensor networks based on frequency-selective channels,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 1779–1790, September 2013.

[19] Y. Liu, S. C. Draper, and A. M. Sayeed, “Exploiting channel diversity in secret key generation from multipath fading randomness,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 5, pp. 1484–1497, July 2012.

[20] H. Liu, Y. Wang, J. Yang, and Y. Chen, “Fast and practical secret key extraction by exploiting channel response,” in Proc. of the 32nd IEEE International Conference on Computer Communications (INFOCOM), Turin, Italy, April 2013, pp. 3048–3056.

[21] Y. Qiao, K. Srinivasan, and A. Arora, “Shape matters, not the size: A new approach to extract secrets from channel,” in Proc. of the 1st ACM Workshop on Hot Topics in Wireless (HotWireless’14). New York, NY, USA, September 2014, pp. 37–42.

[22] C.Y. Wu, P.C. Lan, P.C. Yeh, C.H. Lee, and C.M. Cheng, “Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices,” IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 1687–1700, September 2013.

[23] H. Taha and E. Alsusa, “Physical layer secret key exchange using phase randomization in MIMO-OFDM,” in Proc. IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA December 2015, pp. 1–6.

[24] H. Taha and E. Alsusa, “A MIMO precoding based physical layer security technique for key exchange encryption,” in Proc. IEEE Vehicular Technology Conference (VTC Spring), Glasgow, Scotland, May 2015, pp. 1–5.

[25] H. Taha and E. Alsusa, “Secret key exchange under physical layer security using MIMO private random precoding in FDD systems,” in Proc. IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[26] S. Gollakota and D. Katabi, “Physical layer wireless security made fast and channel independent,” in Proc. 30th IEEE Conf. Comput. Commun., (INFOCOM 2011), Shanghai, China, April 2011, pp. 1125–1133.

[27] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, “Secure space-time block coding via artificial noise alignment,” in Proc. Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, November 2011, pp. 651–655.

[28] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert and J. P. Koskinen, ”Overview of narrowband IoT in LTE Rel-13,” 2016 IEEE Conference on Standards for Communications and Networking (CSCN), Berlin, 2016, pp. 1-7.

[29] B. Reynders, W. Meert, and S. Pollin. “Range and coexistence analysis of long range unlicensed commu- nication”. In: 2016 23rd International Conference on Telecommunications (ICT). 2016, pp. 1–6.

[30] A. Rajandekar and B. Sikdar, "A Survey of MAC Layer Issues and Protocols for Machine-to-Machine Communications," in IEEE Internet of Things Journal, vol. 2, no. 2, pp. 175-186, April 2015.

[31] Dharama .P Agrawal and Qing-An Zeng, Introduction to Wireless and Mobile Systems, Boston, MA, USA:Cengage Learning.

[32] IEEE 802.15.4, Standard for Low-Rate Wireless Networks, 2015.

[33] Y. Liu, Chau Yuen, Jiming Chen and Xianghui Cao, "A scalable Hybrid MAC protocol for massive M2M networks," 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, 2013, pp. 250-255.

[34] W. Saad, S. A. El-Feshawy, M. Shokair and M. I. Dessouky, "Optimised approach based on hybrid MAC protocol for M2M networks," in IET Networks, vol. 7, no. 6, pp. 393-397, 11 2018.

[35] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in Proc. IEEE Veh. Technol. Conf. (VTC Spring), pp. 1–5, Jun. 2013.

[36] X. Wang and H. V. Poor, "Iterative (Turbo) soft interference cancellation and decoding for coded CDMA," IEEE Transactions on Communications, vol. 46, no. 7, pp. 1046–1061, July 1999.

[37] F. Al Rabee, K. Davaslioglu, and R. D. Gitlin, "The optimum received power level of uplink non-orthogonal multiple access (NOMA) signals," IEEE Wireless and Microwave Technology Conference (WAMICON), 2017 Cocoa Beach, Fl, USA, pp. 1-4, April 2017.

[38] E. Balevi, F.T. A. Rabee, , and R. D. Gitlin, "ALOHA-NOMA for Massive Machine-to-Machine IoT Communication, " 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-5.

[39] J. Choi, "NOMA-based random access with multichannel Aloha," IEEE Journal on Selected Areas in Communications, vol. 35, no. 12, pp. 2736–2743, Dec 2017.

[40] D. Shen and V. O. K. Li, "Performance analysis for a stabilized multi-channel slotted ALOHA algorithm," in Proc. IEEE PIMRC, vol. 1, pp. 249–253 Vol.1, Sept 2003.

[41] T. Nitsche, C. Cordeiro, A. B. Flores, E. W. Knightly, E. Perahia, and J. C. Widmer, "Ieee 802.11ad: directional 60 GHz communication for multi-gigabit-per-second Wi-Fi [invited paper]," IEEE Communications Magazine, vol. 52, no. 12, pp. 132–141, December 2014.

[42] K. Hosoya, N. Prasad, K. Ramachandran, N. Orihashi, S. Kishi- moto, S. Rangarajan, and K. Maruhashi. Multiple sector ID capture (MIDC): A novel beamforming technique for 60-GHz band multi-Gbps WLAN/PAN systems. IEEE Transactions on Antennas and Propagation, 63(1):81–96, January 2015.

[43] T. S. Rappaport, R. W. Heath, R. C. Daniels, J. N. Murdock, Millimeter Wave Wireless Communications, Englewood Cliffs, NJ, USA:Prentice-Hall, 2014.

[44] V. Va, T. Shimizu, G. Bansal, R. W. Heath, Millimeter Wave Vehicular Communications: A Survey, Hanover, MA, USA:NOW Publisher, 2016.

[45] Verizon 5G Radio Access (V5G RA); Physical Layer Procedures, document TS V5G.213, Jun. 2016.

[46] C. Jeong, J. Park, and H. Yu, "Random access in millimeter-wave beamforming cellular networks: Issues and approaches," IEEE Commun. Mag., vol. 53, no. 1, pp. 180–185, Jan. 2015.

[47] V. Desai, L. Krzymien, P. Sartori, W. Xiao, A. Soong, and A. Alkhateeb, "Initial beamforming for mmWave communications," in Proc. 48th Asilomar Conf. Signals, Syst. Comput., Nov. 2014, pp. 1926–1930.

[48] M. Giordani, M. Mezzavilla, C. N. Barati, S. Rangan, and M. Zorzi, "Comparative analysis of initial access techniques in 5G mmWave cellular networks," in Proc. Annu. Conf. Inf. Sci. Syst., Mar. 2016, pp. 268–273.

[49] V. Raghavan, J. Cezanne, S. Subramanian, A. Sampath, and O. Koymen, "Beamforming tradeoffs for initial UE discovery in millimeter-wave MIMO systems," IEEE J. Sel. Topics Signal Process., vol. 10, no. 3, pp. 543–559, Apr. 2016.

[50] C. N. Barati et al., "Initial access in millimeter wave cellular systems," IEEE Trans. Wireless Commun., vol. 15, no. 12, pp. 7926–7940, Dec. 2016.

[51] H. Shokri-Ghadikolaei, C. Fischione, G. Fodor, P. Popovski, and M. Zorzi, "Millimeter-wave cellular networks: A MAC layer perspective," IEEE Trans. Commun., vol. 63, no. 10, pp. 3437–3458, Oct. 2015.

[52] W. B. Abbas and M. Zorzi, "Context information based initial cell search for millimeter wave 5G cellular networks," in Proc. EuCNC, June 2016, pp. 111–116.

[53] V.Va,T.Shimizu, G.Bansal,and R.W.Heath,"Position-aided millimeter wave V2I beam alignment: A learning-to-rank approach," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Oct 2017, pp. 1–5.

[54] Laura Pierucci and Davide Micheli. A neural network for quality of experience estimation in mobile communications. IEEE MultiMedia, 23(4):42–49, 2016.

[55] Zhiyuan Xu, Yanzhi Wang, Jian Tang, Jing Wang, and Mustafa Cenk Gursoy. A deep reinforcement learning based framework for power- efficient resource allocation in cloud RANs. In 2017 IEEE International Conference on Communications (ICC), pages 1–6.

[56] Cheng Yang, Maosong Sun, Wayne Xin Zhao, Zhiyuan Liu, and Edward Y Chang. A neural network approach to jointly modeling social networks and mobile trajectories. ACM Transactions on Information Systems (TOIS), 35(4):36, 2017.

[57] D. S. Wickramasuriya, C. A. Perumalla, K. Davaslioglu, and R. D. Gitlin, "Base Station Prediction and Proactive Mobility Management in Virtual Cells using Recurrent Neural Networks," IEEE 18th Wireless and Microwave Technology Conference (WAMICON), April 2017.

[58] Timothy O´Shea and Jakob Hoydis. An introduction to deep learning for the physical layer. IEEE Transactions on Cognitive Communications and Networking, 3(4):563–575, 2017.

[59] R. Gallager, Low-Density Parity-Check Codes, thesis, MIT Press, 1963.

[60] T. Richardson and S. Kudekar, "Design of Low-Density Parity Check Codes for 5G New Radio," in IEEE Communications Magazine, vol. 56, no. 3, pp. 28-34, March 2018.

[61] D. Hui, S. Sandberg, Y. Blankenship, M. Andersson and L. Grosjean, "Channel Coding in 5G New Radio: A Tutorial Overview and Performance Comparison with 4G LTE," in IEEE Vehicular Technology Magazine, vol. 13, no. 4, pp. 60-69, Dec. 2018.

[62] G. Strang, Introduction to Linear Algebra. Wellesley, MA: Wellesley-Cambridge Press, 2003.

[63] H. Taha and E. Alsusa, “Physical layer secret key exchange using phase randomization in MIMO-OFDM,” in Proc. IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, December 2015, pp. 1–6.

[64] M. Edman, A. Kiayias, and B. Yener, “On passive inference attacks against physical-layer key extraction?” in Proc. Fourth European Workshop on System Security (EUROSEC ’11), Salzburg, Austria, April 2011, pp. 1–6.

[65] Jin-Kyu Han, Jong-Gwan Yook and Han-Kyu Park, "A deterministic channel simulation model for spatially correlated Rayleigh fading," in IEEE Communications Letters, vol. 6, no. 2, pp. 58-60, Feb. 2002.

[66] Lizhong Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," in IEEE Transactions on Information Theory, vol. 49, no. 5, pp. 1073-1096, May 2003.

[67] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in Proc. IEEE Veh. Technol. Conf. (VTC Spring), pp. 1–5, Jun. 2013.

[68] A. Benjebbour et al., "Concept and practical considerations of non- orthogonal multiple access (NOMA) for future radio access," in Proc. IEEE Intell. Signal Process. Commun. Syst. (IEEE ISPACS), Naha, Japan, Nov. 2013, pp. 770–774.

[69] S. M. Kay, Fundamentals of Statistical Signal Processing: Practical Algorithm Development. Prentice Hall, 2013.

[70] N. Abramson, "THE ALOHA SYSTEM: Another alternative for computer communications", Proc. Fall AFIPS Comput. Conf., pp. 281-285, Nov. 1970.

[71] S. Rangan, T. S. Rappaport and E. Erkip, "Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges," in Proceedings of the IEEE, vol. 102, no. 3, pp. 366-385, March 2014.

[72] 3GPP, "Study on elevation beamforming / full-dimension (FD) multiple input multiple output (MIMO) for LTE (Release 13)," TR 36.897, June 2015.

[73] 3GPP, "Multi-beam sync design Qualcomm Inc," R1 1612024, August 2016.

[74] M. Giordani, M. Polese, A. Roy, D. Castor, M. Zorzi, "A tutorial on beam management for 3GPP NR at mmWave frequencies", 2018, [online] Available: https://arxiv.org/abs/1804.01908.

[75] E. Dahlman, S. Parkvall, and J. Skld, 4G, LTE-Advanced Pro and The Road to 5G: Third Edition, 07 2016.

[76] T. Italia, "Telecommunications - SMS, Call, Internet - mi," 2015. [Online]. Available: https://doi.org/10.7910/DVN/EGZHFV.

[77] T. Italia, "Milano grid," 2015. [Online]. Available at https://doi.org/10.7910/DVN/QJWLFU.

[78] K. Cho, J. Chung, C. Gulcehre, and Y. Bengio, "Empirical evaluation of gated recurrent neural networks on sequence modeling," 2014. [Online]. Available: https://arxiv.org/pdf/1412.3555.

[79] F. M. Bianchi, E. Maiorino, M. C. Kampffmeyer, A. Rizzi, and R. Jenssen, "An overview and comparative analysis of recurrent neural networks for short term load forecasting," 2017. [Online]. Available: https://arxiv.org/pdf/1705.

APPENDIX A: COPYRIGHT PERMISSIONS

The permission below is for the use of the material in Chapter 3.

Title: Secure key management for 5G physical layer security
Conference Proceedings: 2017 IEEE 18th Wireless and Microwave Technology Conference (WAMICON)
Author: Asim Mazin
Publisher: IEEE
Date: April 2017

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

The permission below is for the use of the material in Chapter 4.

The permissions below are for the use of the material in Chapter 5.

Title: Accelerating Beam Sweeping in mmWave Standalone 5G New Radios using Recurrent Neural Networks

Conference Proceedings: 2018 IEEE 88th Vehicular Technology Conference

Author: Asim Mazin

Publisher: IEEE

Date: August 2018

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Title: Comparative Performance Analysis of Beam Sweeping Using a Deep Neural Net and Random Starting Point in mmWave 5G New Radio

Conference Proceedings: 2018 IEEE 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference

Author: Asim Mazin

Publisher: IEEE

Date: November 2018

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

ABOUT THE AUTHOR

Asim Mazin received the B.S. degree in Electronics and Telecommunications engineering in 2007 from the College of Industrial Technology Misurata, Libya and an M.S. degree in Electrical and Computer Engineering with a concentration in wireless communications from Southern Illinois University in 2013. His Master's thesis was Peak-to-Average Power Reduction (PAPR) in OFDM using Particle Swarm Optimization (PSO) technique. Currently, he is pursuing his Ph.D. degree in Electrical Engineering under the supervision of Prof. Richard Gitlin at the University of South Florida with the Innovations in Wireless Information Networking Laboratory (iWINLAB), and his research interests include Physical Layer Security, multiple access in massive M2M IoT networks, applying machine learning in 5G Wireless Networks.