NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PHYSICAL LAYER AUTHENTICATION OF 5G DEVICES IN MOTION USING PLANAR REFLECTORS

by

Ryan P. Breckenridge

June 2021

Thesis Advisor:	John D. Roth
Second Reader:	Murali Tummala

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
PHYSICAL LAYER AUTHENTICATION OF 5G DEVICES IN MOTION USING PLANAR REFLECTORS

5. FUNDING NUMBERS

6. AUTHOR(S) Ryan P. Breckenridge

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Network authentication between users is commonly performed through the process of exchanging cryptographic keys. However, this security practice could leave users vulnerable if an eavesdropper managed to ascertain these private keys and the manner that they are exchanged. As a result, alternative security methods can add new factors to uniquely authenticate trusted users and improve network security. Through signal multipath, previous research analyzed the time delay measurement between a channel tap's indirect path from a physical reflector and that same channel tap's direct, line-of-sight path to uniquely establish a stationary user's identity to their physical position. Because these channel taps are dependent on the location of network users, an eavesdropper faces a difficult challenge to precisely imitate the same tap delay to gain unauthorized access. This thesis explores how tap delay measurements incrementally change as an authenticated user moves within a space. Through statistical analysis, our research aims to determine an acceptable tap delay interval that network users can use to track and maintain authentication for various speeds through a coverage area.

14. SUBJECT TERMS 5G, physical layer, authentication	**15. NUMBER OF PAGES** 55
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

PHYSICAL LAYER AUTHENTICATION OF 5G DEVICES IN MOTION USING PLANAR REFLECTORS

Ryan P. Breckenridge
Lieutenant Commander, United States Navy
BS, U.S. Naval Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: John D. Roth
Advisor

Murali Tummala
Second Reader

Douglas J. Fouts
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Network authentication between users is commonly performed through the process of exchanging cryptographic keys. However, this security practice could leave users vulnerable if an eavesdropper managed to ascertain these private keys and the manner that they are exchanged. As a result, alternative security methods can add new factors to uniquely authenticate trusted users and improve network security. Through signal multipath, previous research analyzed the time delay measurement between a channel tap's indirect path from a physical reflector and that same channel tap's direct, line-of-sight path to uniquely establish a stationary user's identity to their physical position. Because these channel taps are dependent on the location of network users, an eavesdropper faces a difficult challenge to precisely imitate the same tap delay to gain unauthorized access. This thesis explores how tap delay measurements incrementally change as an authenticated user moves within a space. Through statistical analysis, our research aims to determine an acceptable tap delay interval that network users can use to track and maintain authentication for various speeds through a coverage area.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. MOTIVATION....1
B. THESIS OBJECTIVE....2
C. CHAPTER OVERVIEW....2
D. CONTRIBUTIONS....3

II. BACKGROUND....5
A. PHYSICAL LAYER AUTHENTICATION....5
B. LITERATURE REVIEW....8
C. CHANNEL TAP DELAY FOR PHYSICAL LAYER AUTHENTICATION....10
D. TAP-DELAY INTERVAL TO AUTHENTICATE A MOVING USER....14
E. SUMMARY....15

III. SIMULATION....17
A. TAP-DELAY MEASUREMENTS OF A USER IN MOTION....17
B. TAP-DELAY DIFFERENTIAL MEASUREMENTS....18
C. TAP-DELAY DIFFERENTIAL PROBABILITY DISTRIBUTION FUNCTION FOR DIFFERENT SPEEDS....19
D. PROBABILITY OF DETECTION VERSUS FALSE ALARM....19
E. SUMMARY....21

IV. RESULTS AND ANALYSIS....23
A. TAP-DELAY MEASUREMENTS OF A PEDESTRIAN MOVING AT DIFFERENT SPEEDS....23
B. TAP-DELAY DIFFERENTIAL MEASUREMENTS OF A PEDESTRIAN MOVING AT DIFFERENT SPEEDS....26
C. PDF CURVES TO CHARACTERIZE TAP-DELAY DIFFERENTIALS....28
D. ROC CURVES: PROBABILITY OF DETECTION VERSUS FALSE ALARM....30
E. SUMMARY....32

V. CONCLUSION....33
A. SIGNIFICANT CONTRIBUTIONS....33
B. FUTURE WORK....33
1. Reflector Dimensions....33

2. Reflector Material 34
3. Other Reflectors 34

LIST OF REFERENCES 35

INITIAL DISTRIBUTION LIST 37

LIST OF FIGURES

Figure 1. OSI Model....5

Figure 2. SDN-enabled secure-context-information transfer between 5G UE, APs, and AM in SDN controller. Source: [10]. 6

Figure 3. User-SCI-based authentication handover. Source: [11]....7

Figure 4. Wireless MOTS targeting RF fingerprint authentication. Source: [15]. 9

Figure 5. Eve imitates Bob's signaling to a vulnerable Alice. Source: [17]. 10

Figure 6. Power-delay-line profile of a 28 GHz signal caused by reflectors. Source: [18]....11

Figure 7. Simpler example of a power-delay-line profile 12

Figure 8. Illustration of specular reflector geometry. Source: [20]. 14

Figure 9. Example of a tap delay calculated outside of tap-delay interval 15

Figure 10. Tap-delay measurements for Alice moving at 1 m/s 24

Figure 11. Tap-delay measurements for Alice moving at 5 m/s 25

Figure 12. Tap-delay differential measurements for Alice moving at 1 m/s 26

Figure 13. Tap-delay differential measurements for Alice moving at 5 m/s 27

Figure 14. Exponential PDF of tap-delay differentials for various speeds 29

Figure 15. ROC curve: Carol randomly walks around with Alice....31

Figure 16. ROC curve: three other users walking around with Alice 32

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Alice's maximum and minimum tap delays 25

Table 2. Tap-delay differential minimum and maximum for different speeds.....27

Table 3. Parameters for tap-delay differential exponential PDFs.....28

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

5G	fifth generation
AP	access point
AHM	authentication handover module
CPA	closest point of approach
CSI	channel state information
eMBB	enhanced mobile broadband
DOD	department of defense
ERD	energy ratio detector
gNB	gNodeB
IEEE	Institute of Electrical and Electronics Engineers
IoS	internet of skills
IoT	internet of things
LOS	line of sight
m/s	meters per second
MIMO	multiple input multiple output
mMTC	massive machine type communications
mmWave	millimeter wave
MOTS	man-on-the-side
mph	miles per hour
NIST	National Institute of Standards and Technology
NLOS	non-line of sight
NPS	Naval Postgraduate School
OSI	open systems interconnected
P_D	probability of detection
PDF	probability distribution function
P_{FA}	probability of false alarm
RF	radiofrequency
RFID	radiofrequency identification
ROC	receiver operating characteristic
RV	random variable

SBR	single bounce reflection
SDN	software defined network
TOA	time of arrival
UE	user equipment
URLLC	ultra-reliable low latency communications
V2X	vehicle to everything

ACKNOWLEDGMENTS

I would like to acknowledge my advisor, Dr. John Roth, and my wife, Cristina, for sticking with me through this endeavor.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

The next phase in wireless technologies, Fifth Generation (5G), promises to provide even higher data rates and lower latency to a wide variety of affordable and energy efficient devices. Recent projections forecast 3.5 billion users by 2026 as mobile subscribers switch from older generations to 5G [1]. Beyond furnishing telephone and data services to people with its enhanced mobile broadband (eMBB), 5G also promises to make its unique, wireless contributions to other networks, such as Internet of Things (IoT), Internet of Skills (IoS), augmented reality (AR), virtual reality (VR) and vehicle-to-everything (V2X) technologies. Introducing two additional categories of capabilities, 5G plans to extend its services beyond conventional cell phone coverage and into massive machine type communications (mMTC) and ultra-reliability low latency communications (URLLC). Service providers anticipate an additional 5 billion devices dedicated to machine-type communications linked to the 5G network by 2025 [2]. With the potential advancements in industry, transportation, and manufacturing sectors, it is unsurprising that the United States Department of Defense (DOD) is eager to explore new ways to modernize its own defense systems with the release of the "5G Strategy" in 2020 [3]. The DOD has already begun prototyping ground combat training with AR and VR, integrating wireless access to avionics for aircraft maintenance, and installing 5G into smart warehouses for efficient logistic support over the past year [4].

Research into innovative security practices is becoming increasingly important to meet the commercial and government demand for 5G access into their own technologies. As systems become more interconnected, this rapid materialization of simpler endpoint devices presents new challenges to security. To address the protection of data from wireless devices that are too constrained and resource-limited to perform more complex encryption algorithms, the National Institute of Standards and Technology (NIST) has outlined its approved lightweight cryptography standards [5]. However, key-based cryptography, especially when it is adjusted for smaller devices, does not help strengthen the ability for a network to verify the identity of its sensors. Instead of authenticating a device by what it

possesses (like a key) or by what it knows (like an answer to a question), network users can inferentially confirm its devices by measuring the transmitted and received signal characteristics, which are harder for an attacker to imitate and gain unauthorized access.

Unlike previous cellular technology, the communication link between 5G user equipment (UE) and service towers, called gNodeB (gNB), employs beamforming and multiple input multiple output (MIMO) technologies for the uplink and downlink channels [6]. Since these channels must be constantly monitored and physically adjusted to provide service for a moving UE, the network can use these channel characteristics to confirm the identity of a device by its physical position to receive cell service. Previous research in physical layer authentication has demonstrated that measuring the difference in time of arrival (TOA) between the reflected channel path and the line of sight (LOS) channel path of a signal in a multipath environment can act as a technique to verify the identity of network user [7]. Because the relative position of a transmitting device between a receiver and reflector causes this difference in TOA measurements, their location is the authenticating factor that establishes authorized access to network services. For an eavesdropper to gain unauthorized access to this physical channel between a gNB and UE, they would have to be physically standing in the same environment as their victim.

B. THESIS OBJECTIVE

For a UE that is moving in relation to a stationary reflector and a receiving gNB, the authentication measurement changes as the reflected and LOS distances of a signal vary based on position. To maintain track of the UE, the gNB can establish an interval around the most recent measurement based on what location the network anticipates the next delay measurement to occur. This thesis analyzes statistical data from multiple simulation runs to determine an appropriate interval size for a network to maintain authentication of a UE based on its speed and among other things, like competing UE devices also transmitting in the environment.

C. CHAPTER OVERVIEW

We provide the background information and context from other research that established our assumptions and methods in Chapter II. We discuss our procedures to setup

and run simulations in Chapter III and analyze their results in Chapter IV. We conclude and summarize our research results and provide recommendations for future work in Chapter V.

D. CONTRIBUTIONS

Our research recommends networks use a tap-delay interval as a physical-layer authentication method to predict the next, expected tap-delay measurement to maintain authenticated status of its users. We statistically analyze the viability of this method as it relates to a transmitter physically moving at various ambulatory speeds through a multipath environment as well as with other signal transmissions producing their own channel taps that may interfere with this authentication practice.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter provides the necessary context as it relates to other research sources on the topic of 5G and physical-layer authentication, and it establishes our assumptions and initial setup for our simulations.

A. PHYSICAL LAYER AUTHENTICATION

Using the Open Systems Interconnected (OSI) Model, we can categorize the accessibility, security, or vulnerability of information as data moves within and between each of the seven layers as shown in Figure 1 based on [8]. The application layer is the highest, and its protocols are user-defined. The physical layer is the lowest, and its information flows functionally (mechanically or electrically). For 5G networks, one of the physical layers is the radiofrequency (RF) communication link between a UE and gNB. This is the physical layer that we focused on in our authentication simulations.

OSI Model Layers	
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Figure 1. OSI Model

5G, like other networks, includes common information security services, such as data confidentiality, key management, availability, privacy, and authentication. Of these services, our research concentrated on authentication, which is defined as the verification of identity to allow authorized network access. To demonstrate an example of a 5G network physical layer authentication, [9] illustrates the 5G core as a software defined network (SDN) that uses weighed secure-context-information (SCI) transfers to perform

authenticated hand-offs of a user between gNB. SCI is a non-cryptographic authentication method that efficiently supports frequent handovers between different cells. Rather than have network entities spend time using key-based authentication and potentially delaying service as a user moves between cells, SCI keeps authentication without entities needing to compute complex algorithms. The SDN watches and anticipates the user physical location to the next applicable gNB base stations are ready to receive the user through full authentication on larger gNB or via fast authentication on smaller access points (AP), as shown in Figure 2.

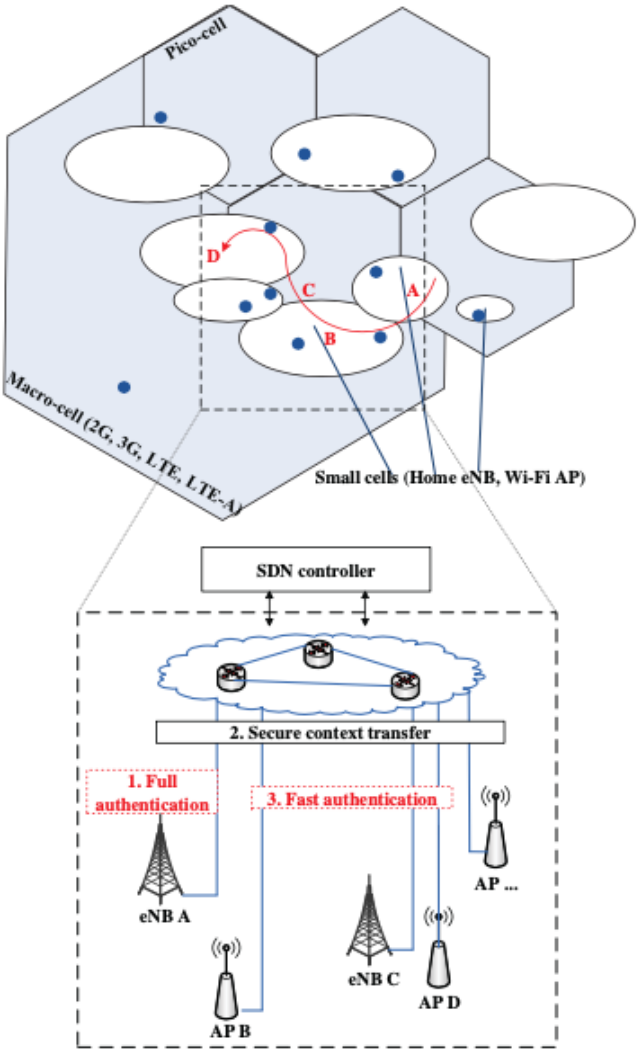

Figure 2. SDN-enabled secure-context-information transfer between 5G UE, APs, and AM in SDN controller. Source: [10].

The information about a user contained in SCI can be any information that is unique to the UE that the 5G network is providing service to, such as any physical-layer measurements, its location, its speed, or its direction. The authors in [11] proposed a user-SCI-based authentication handover algorithm, where the 5G SDN controller implements an authentication handover module (AHM) that predicts user movement and prepares cells in advance to provide seamless service while maintaining authenticated status of that user to the network. An example of a user-SCI-based authentication algorithm is provided in Figure 3, where cell *A* has authenticated user *U*, which is traveling towards coverage areas of cells *B* and *C*. The SDN controller employs the AHM to inform cells *B* and *C* of the identity and SCI of user *U* prior to its arrival to their service areas. Cells *A* and *B* perform a handoff with user *U*, and then cell *B* authenticates user *U* with the SCI received from the SDN via the AHM. *B* confirms *U* with its SCI from *A*, and then *B* updates the SDN controller with the new *U* SCI via the AHM with current locational, speed, or direction information. Cell *C* continues to monitor *U* as it stays in the service area of *B*.

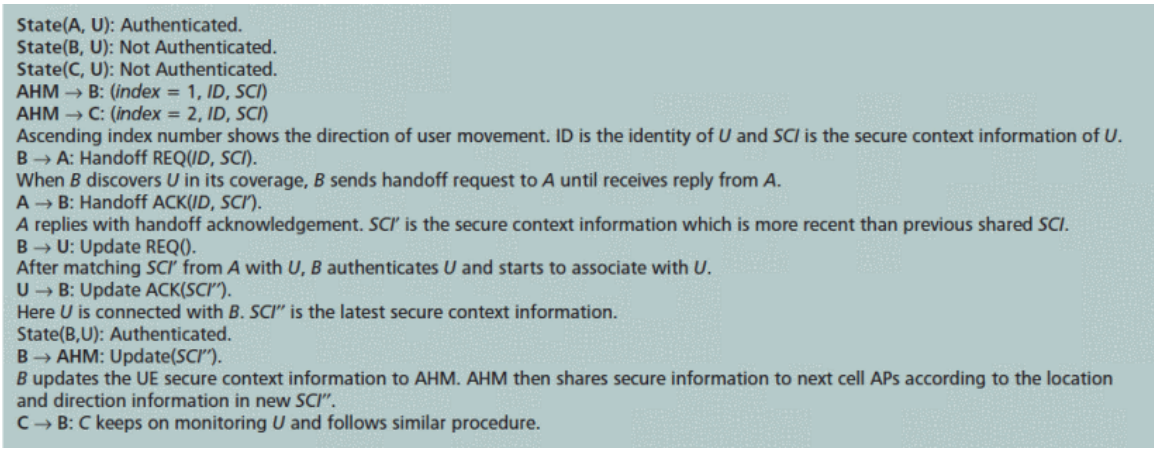

Figure 3. User-SCI-based authentication handover. Source: [11].

This user-SCI-based authentication handover method illustrates one way that a 5G network can establish and maintain physical layer authentication without having to use key-based cryptography. The network monitors measurements and data that are only unique to its users, which makes imitation of these metrics impossible for an eavesdropper or attacker.

B. LITERATURE REVIEW

The user-SCI-based authentication method and algorithm covered in the earlier section is only an example of physical layer security in a 5G network. There is a multitude of published research about physical layer security in a 5G network as it applies to authentication, confidentiality, and data integrity. The authors in [12]–[14] perform their own in-depth surveys of papers on the subject and reveal the constraints of implementing physical-security methods in wireless networks.

Most of the constraints on physical layer security impact how a 5G network can guarantee its information is kept confidential. Multiple-antenna technology for MIMO and the multiple channels that are induced from a multipath environment make digital network coding a dynamic process. This inconsistent variability in the physical layer presents a challenge to employ key-based cryptography and provide confidentiality, when a key is designed to encrypt or decipher a set size of information between a transmitter and receiver. These confidentiality challenges to physical-layer security do not play as much of a role in authentication, unless a network relies on keys being securely exchanged to confirm identity.

In terms of physical-layer authentication, the literature is concerned about security vulnerabilities that can allow an attacker to impersonate or imitate credentials that are not their own. For instance, a network receiver can develop its own library of RF fingerprints associated to devices that wirelessly access its service [15]. RF fingerprints are not deliberately designed into devices like RF identification (RFID) that we commonly experience with hotel keys or security badges that we use to unlock a door without a physical key. Instead, RF fingerprints seem to be more authentic and less imitable than RFID because the identifier is based on manufacturing or design imperfections unintentionally unique to the way a device transmits information. However, [16] demonstrates how an attacker can record and reuse RF fingerprints from other devices to steal their credentials with a man-on-the-side (MOTS) attack as illustrated in Figure 4.

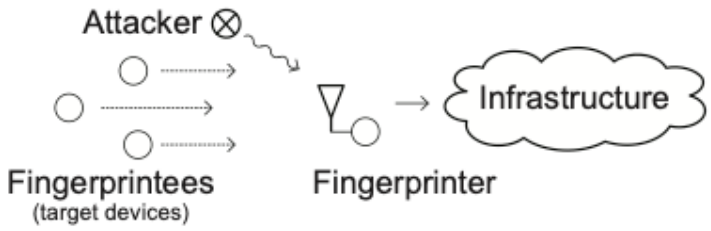

Figure 4. Wireless MOTS targeting RF fingerprint authentication. Source: [15].

Instead of RF fingerprinting, a network could use channel state information (CSI) instead as an authentication method. CSI is the shared information to assist both UE and gNB in making energy efficient decisions in uplink and downlink channel selection. Since this information is unique between a UE and a gNB, then reasonably CSI could be a physical-layer authentication method. However, [17] demonstrates a pilot-spoof attack that interferes with a device performing channel estimation. Since the pilot signals are repeatedly broadcast and are known to the public, an eavesdropper can act like a local gNB and broadcast the same pilot signal to a victim UE and interfere with their ability to perform channel estimation. This shows a vulnerability when a UE authenticates the identity of a servicing gNB based on CSI when an attacker can imitate the same pilot signal as seen in Figure 5, where Eve, who is a single-antenna attacker, is imitating Bob, who is the real single-antenna network provider. Meanwhile, Alice is equipped with multiple antennas and is trying to authenticate, who the real network provider is between Bob and Eve. This scenario illustrates how an attacker can imitate the CSI in the pilot signal without another mechanism to authenticate an attacker from the actual network. This thesis does recommend a solution to this vulnerability, where Alice employs an energy ratio detector (ERD), which indicates higher than normal energy level for a pilot signal when Eve is transmitting with Bob.

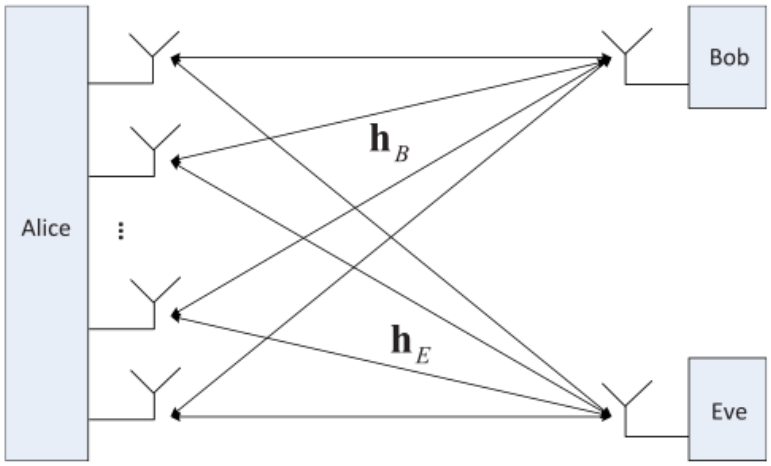

Figure 5. Eve imitates Bob's signaling to a vulnerable Alice. Source: [17].

In summary, this section showed how physical-layer security is a diverse subject for technical research and presents vulnerabilities and recommendations on how a wireless 5G network can improve its security practices. Of the security functions in the physical layer, our review shows that there is more information addressing confidentiality than authentication methods. We explored some examples on how a network can use pre-existing information that is normally shared as a means of authentication, such as RF fingerprinting the transmission from a device or using the parameters contained in CSI, to uniquely associate one entity from another. This review of the technical literature establishes what methods have already been explored on the subject of physical-layer security and substantiates the originality of our proposed authentication method discussed in the upcoming sections.

C. CHANNEL TAP DELAY FOR PHYSICAL LAYER AUTHENTICATION

In a multipath environment, a single, transmitted signal can be received multiple times at varying power levels based off the multiple paths this signal takes, as demonstrated in [18]. The power of these received taps can be plotted over time as a power-delay-line profile. An example of what this profile looks like is shown in Figure 6, where the paths for all the single-bounce reflections (SBR) caused by physical reflectors arrive at a receiver with varying power levels at varying times.

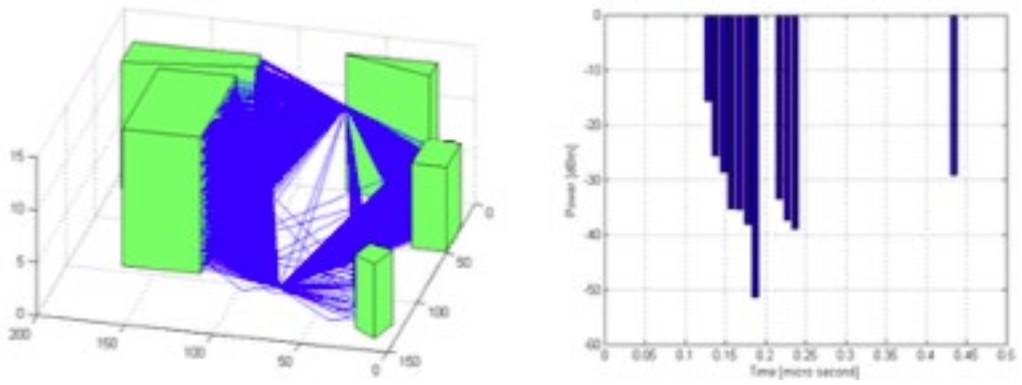

Figure 6. Power-delay-line profile of a 28 GHz signal caused by reflectors. Source: [18].

By using a power-delay-line profile, we can calculate the channel-tap delay, which is the amount of time that a reflected signal reaches a receiver subtracted by the same signal LOS path to the same receiver. Figure 7 is a simpler example of power-delay-line profile to illustrate some information that we can derive from this type of plot. The peak amplitude occurs with the first and earliest signal tap (τ_1). Because this signal takes a direct path, it does not experience as much path loss as the next, detected tap (τ_2) of the same signal that travels its longer, reflected path [19]. The tap delay ($\Delta\tau$) is the time between the earliest signal and the next detectable tap from the same signal.

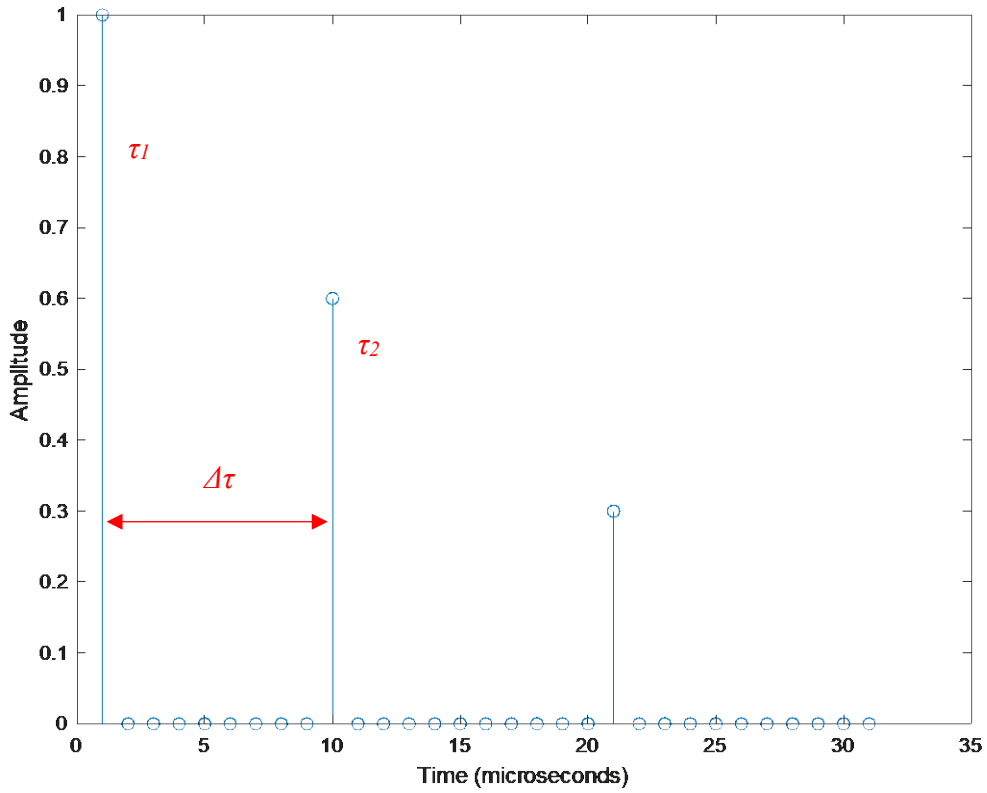

Figure 7. Simpler example of a power-delay-line profile

Let us assume that we surveyed our physical environment and found a large object with material that can reliably reflect a signal tap from a transmitter to the receiver for a wide range of locations in our environment. Let us also assume that for every tap from this large reflector, the receiver can also reliably detect the LOS path of the tap directly from the transmitter in this environment. If we can identify and filter out any other non-line-of-sight (NLOS) signal paths caused by other reflectors within our environment, then we can calculate tap delay without having to use a power-delay-line profile. We can measure the LOS distance (d_{LOS}) using Pythagorean theorem and the NLOS distance (d_{NLOS}) from the reflector using both Pythagorean theorem and Snell's law, where the incident angle on a reflector will equal the reflected angle. By taking the difference of these two distances and dividing it by the signal propagation speed represented by the speed of light (c), we can calculate tap delay from a known reflector with the following equation:

$$\Delta\tau = \frac{d_{NLOS} - d_{LOS}}{c}. \tag{2.1}$$

Since the NLOS and LOS distances are dependent on the location of the transmitter relative to both the location and orientation of the large reflector and the location of the receiver, this tap-delay measurement can act as a measure of authentication. Because it is associated to the transmitter position in the environment, this measurement is difficult to imitate by an eavesdropper without physically being co-located with the transmitter. Previous research in [20] demonstrates that this is an effective authentication method that easily distinguishes an actual entity from an imitator in the same, physical environment.

The author of [20] also provides another equation to calculate the tap delay using scalar values in a Cartesian grid. In this equation, the line-of-sight distance between transmitter and receiver is d_{LOS}. The receiver and the transmitter both have their own closest point of approach (CPA) distances to the large reflecting plane. Both of these CPA distances are indicated as h_{Rx} and h_{Tx}. We can then calculate the difference of these CPA distances with $\Delta h = h_{Tx} - h_{Rx}$. We can divide all of the distance computations by the speed of light (c) as seen here

$$\Delta\tau = \frac{\sqrt{d_{LOS}^2 + 4h_{Rx}\Delta h + 4h_{Rx}^2} - d_{LOS}}{c}. \tag{2.2}$$

This tap-delay equation is used for our simulations, setup in Chapter III, where the positions of our transmitter ($\boldsymbol{p_{Tx}}$) and receiver ($\boldsymbol{p_{Rx}}$) with the position ($\boldsymbol{p_r}$) and orientation ($\boldsymbol{n}$) of the reflector are given in Cartesian-vector format. Figure 8 shows how these locational values are physically arranged to calculate the tap delay, where h_{Tx} and h_{Rx} are the CPA distances between $\boldsymbol{p_{Tx}}$ and $\boldsymbol{p_{Rx}}$ and the reflector, respectively.

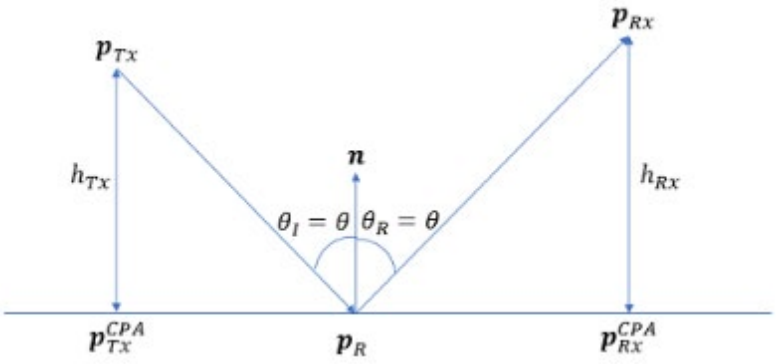

Figure 8. Illustration of specular reflector geometry. Source: [20].

D. TAP-DELAY INTERVAL TO AUTHENTICATE A MOVING USER

Bearing some similarities with [9]–[11], we propose a method to continue to use tap-delay measurements as a means of physical layer authentication for a user moving at pedestrian speeds. A network can theoretically maintain authenticated track of a moving transmitter by setting up a tap-delay interval ($\pm\delta\Delta\tau$) around its most recent, authenticated tap-delay measurement ($\Delta\tau_n$) of a transmitter. If the next tap-delay measurement ($\Delta\tau_{n+1}$) is inside this tap-delay interval, then the transmitter maintains its authenticated status on the network. However, if the next tap-delay measurement ($\Delta\tau_{n+1}$) is outside the tap-delay interval ($\pm\delta\Delta\tau$), as shown in Figure 9, then the transmitter loses its authenticated status and must re-authenticate to the network.

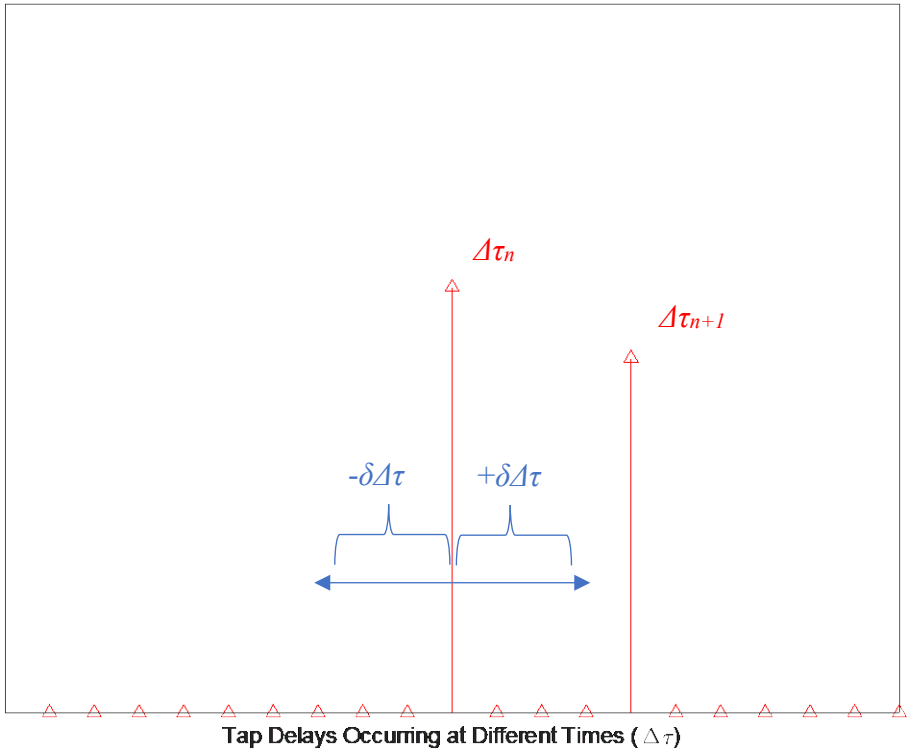

Figure 9. Example of a tap delay calculated outside of tap-delay interval

E. SUMMARY

This chapter provided the requisite background and context to our research and proposed physical-layer authentication method for a moving user. At a high level, we classified the term "physical-layer authentication." We performed a literature review on physical-layer security as it relates to wireless 5G networks to see what research has already revealed in vulnerabilities and recommended security precautions. Based on our review, we investigated a new method that relates tap-delay calculations to authenticate entities based on their physical position. This tap-delay calculation will be used as we evaluate a way to maintain authentication of a transmitting device that is moving in a simulated environment in Chapter III.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SIMULATION

To understand how a network can maintain authentication of a moving user in a space with a planar reflector that enables multipath measurements, the proceeding simulations are designed to answer the following questions:

1. What is the expected range of values for channel-tap delays ($\Delta\tau$) for a pedestrian walking through our simulated environment at different speeds?
2. When we take the difference of one channel-tap delay value from the next ($\delta\Delta\tau$), what is the range of values for $\delta\Delta\tau$ as a transmitter moves through the environment, and how much does it change based on a pedestrian's speed?
3. What is the probability that a network can maintain authentication of a pedestrian based on its tap-delay interval size?
4. If a network pre-selects a threshold value for its tap-delay interval to maintain authentication of a pedestrian, what is the probability that a network can maintain track of its user with other pedestrians transmitting in the same test environment?

This chapter focuses on the setup for each of these simulations while analysis of the results will be discussed in the proceeding chapter.

A. TAP-DELAY MEASUREMENTS OF A USER IN MOTION

For this portion of the experiment, we set up a virtual test environment with a planar reflector, and two authenticated entities, named Alice and Bob. Alice is using Bob's network and is moving in a specified direction at a constant speed. Bob is stationary and wants to maintain Alice's authenticated status by measuring her position based on the time delay between her channel taps. It is assumed that Bob either knows or can obtain four values to calculate Alice's channel tap delay, which are Alice's position vector ($\boldsymbol{p_A}$), Bob's position vector ($\boldsymbol{p_B}$), the vector location of the planar reflector ($\boldsymbol{p_r}$), and the orientation of the reflector represented by its normal vector ($\boldsymbol{n}$). With this information Bob can calculate

Alice's tap delay for any of her positions in the environment using the tap-delay equation (2.2).

To introduce some realism to our simulations, our virtual environment did not exceed 200 meters to resemble a millimeter-wave (mmWave) 5G cellular coverage area in an urban location. Likewise, we kept Alice's height at 1 meter to represent someone walking with their UE, and Bob's height at 15 meters to resemble gNB. These measurement decisions are based on the research done in New York City discussed in [21]. We took tap-delay measurements for Alice moving at 1 m/s (approximately 2.24 mph), and again for Alice for moving at 5 m/s (approximately 5 mph).

We randomly assigned a Cartesian coordinate position and direction for Alice to start moving at one of these constant speeds. We also randomly assigned a Cartesian coordinate position for Bob to stand and measure Alice's channel tap delays as she moves in relation to him on the same side of a planar reflector. A single trial involves Alice walking a distance in ten seconds. Bob will take a channel tap-delay measurement on Alice's position every second, so that he will have ten tap-delay measurements for Alice's single walk-by trial. We will repeat this trial 100,000 times to survey for all the possible channel tap delays in this environment for both speeds. Performing this many simulations will reveal the maximum and minimum channel tap delays Alice can have in this environment, and the data can also be statistically analyzed to see how frequently Alice's channel tap delay lands on certain values over others.

B. TAP-DELAY DIFFERENTIAL MEASUREMENTS

The term, tap-delay differential, is the difference between a current channel tap-delay measurement taken at some time, *n*, compared to the previous channel tap-delay measurement for the same user from *n*-1, which is represented by

$$\delta\Delta\tau = \Delta\tau_n - \Delta\tau_{n-1}. \tag{3.1}$$

Since a channel-tap delay is related to user location, the difference from one sequential measurement to the next can act as a scalar indicator of distance and direction for a moving user, based on their speed and how frequently a network calculates channel-

tap delays. The tap-delay differential can help establish the tap-delay interval around the most recent tap-delay measurement, where the network would expect the next tap delay from their moving user to maintain their authentication.

In this set of simulations, we incrementally increased Alice's speed by 1 m/s at a time from 1 to 5 m/s to see how much the range of tap-delay differential values change for each of her speeds. Like the tap-delay measurements in the previous simulation, we ran 100,000 trials for each of Alice's speed increments. The deliverables for this set of simulations are histograms for her slowest and fastest speeds as well as a table of results reporting the approximate range of maximum and minimum values of the tap-delay differentials for each of her five speeds.

C. TAP-DELAY DIFFERENTIAL PROBABILITY DISTRIBUTION FUNCTION FOR DIFFERENT SPEEDS

Based on the tap-delay differential results from the previous simulation, Bob has a range of tap-delay differential values to inform his tap-delay interval to keep a moving Alice authenticated to his network. To determine the probability of positively detecting Alice's next tap-delay position based on Bob's selection of a tap-delay differential threshold, we characterized the tap-delay differential results with a probability distribution function (PDF). For these simulations, we varied Alice's speed from 1 to 5 m/s incrementing by 1 m/s for each simulation. We then fit a PDF curve based on the tap-delay differential results for each of these simulations. This information answers the third question posed at the beginning of this chapter.

D. PROBABILITY OF DETECTION VERSUS FALSE ALARM

This final set of simulations presented other channel tap delays that occur coincidentally with Alice's tap delays but are not Alice. At any point in time, Bob has two tap delays to consider; one is Alice, and the other is not Alice. For simplicity, we considered these other tap delays belonging to a benign actor named, Carol. She is considered benign because she is not deliberately trying to interfere with Bob's ability to accurately authenticate Alice. Rather, Carol only exists in the same coverage area as Alice, and Bob can confuse Carol's tap delays from Alice's.

After the first set of simulations earlier in this chapter, we have an idea of what the maximum tap delay is for our coverage area. From this, we can randomize Carol's tap delay to be any value between the tap-delay maximum and zero. Bob must calculate two, unknown tap-delay differentials ($\delta\Delta\tau_1$ and $\delta\Delta\tau_2$) without knowing which of the measured tap delays belongs to Alice ($\Delta\tau_{n,Alice}$) or Carol ($\Delta\tau_{n,Carol}$). Bob only remembers Alice's last measured tap delay ($\Delta\tau_{n-1,Alice}$). The first unknown tap delay differential is

$$\delta\Delta\tau_1 = \Delta\tau_{n,Alice} - \Delta\tau_{n-1,Alice} \tag{3.2}$$

and the second unknown tap delay differential is

$$\delta\Delta\tau_2 = \Delta\tau_{n,Carol} - \Delta\tau_{n-1,Alice} \tag{3.3}$$

If Alice's tap delay falls within his established tap-delay interval for her, then Bob calls a positive detection for Alice. There is a chance that Carol's tap delay can cause her to fall inside Alice's tap-delay interval, and Bob will confuse Carol for Alice.

Alice randomly walks in different directions with Bob measuring her tap delay, like we have done in the previous simulations, and Bob calculates Carol's tap-delay measurements as she walks around the same environment. We kept a normalized tally of every time Bob correctly detected Alice based on the difference between her current and previous positions, and we kept a normalized tally of every time Bob incorrectly detected Carol for Alice. We incrementally swept Bob's tap-delay interval size for Alice from zero to the maximum tap-delay differential.

We plotted receiver operating characteristic (ROC) curves to display the relationship between the probability of positive detection (P_d) versus the probability of false alarm (P_{FA}) as we incrementally increase the width of the tap-delay interval. We overlaid ROC curves for each speed of Alice from 1 to 5 m/s to see how her speed impacts the relationship between probability of detection and false alarm. This illustrates the balance Bob must strike, when selecting a tap-delay interval width. While he may opt to select the maximum possible threshold to guarantee tracking Alice's tap delay every time, a large interval also means that he is more likely to confuse Carol for Alice. Instead, Bob

must select an interval size that is wide enough to have a high probability of detection for Alice's tap delay but is narrow enough to avoid false alarms for Carol.

E. SUMMARY

In this chapter we identified four questions to consider, when a network wants to maintain authentication of a user moving in their coverage area using multipath channel tap delays caused by a physical reflector in the area. Then we designed simulations to obtain results to help us address these questions in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS AND ANALYSIS

Now that we have setup our simulation environment to answer the questions posed in Chapter III, the results of these simulations help us better understand how to track a network user with their channel tap delay to maintain their network authentication within a small service coverage area. The Monte Carlo simulations used no less than 100,000 trials to generate the plots below.

A. TAP-DELAY MEASUREMENTS OF A PEDESTRIAN MOVING AT DIFFERENT SPEEDS

To determine expected range of tap-delay values for our simulated environment, Figure 10 is a histogram plot of Bob's tap-delay measurements of Alice, when she moved through our simulated environment at 1 m/s. Bob measured Alice's tap delay ten times for each walk-by trial. Since we performed 100,000 trials, we have a total of 1,000,000 tap-delay measurements. By selecting a uniform, 5-nanosecond bin size, we can incrementally tally of all 1,000,000 tap-delay measurements into each of these bins from zero to the maximum tap-delay value. This helps us visualize how frequently some values occurred compared to others. Most of Alice's tap-delay measurements occur near zero, and the number of occurrences for each bin of values declines as the tap-delay value increases.

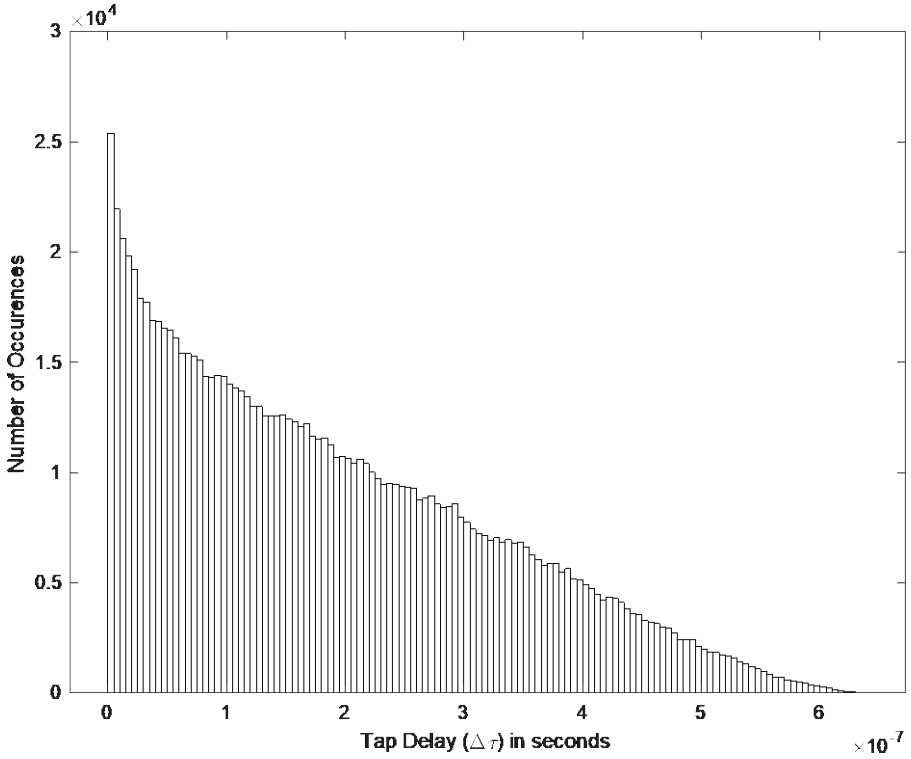

Figure 10. Tap-delay measurements for Alice moving at 1 m/s

Figure 11 is a histogram plot of Bob's tap-delay measurements for Alice moving through our simulated environment at 5 m/s, which looks like Figure 10. Most of Alice's tap-delay measurements occur near zero, and there are fewer occurrences each, five-nanosecond bin of tap-delay values as it increases from zero to the maximum recorded tap-delay value for Alice.

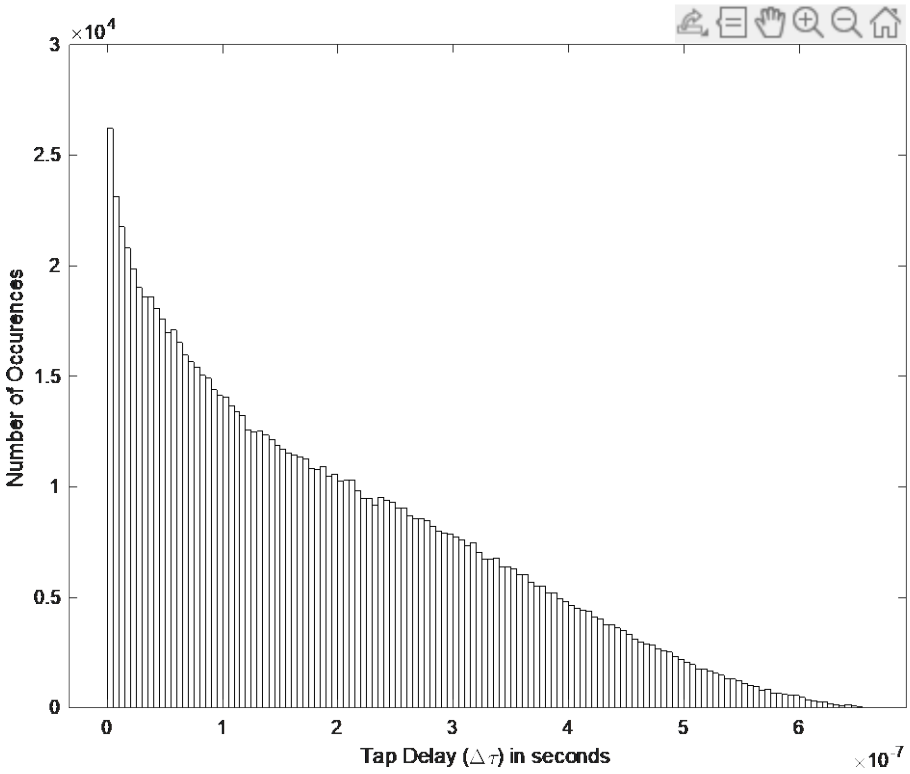

Figure 11. Tap-delay measurements for Alice moving at 5 m/s

Table 1 reports the minimum and maximum tap-delay values for Alice moving at her different speeds.

Table 1. Alice's maximum and minimum tap delays

Alice's Speed (m/s)	**Minimum $\Delta\tau$ (nanoseconds)**	**Maximum $\Delta\tau$ (nanoseconds)**
1	0	639
5	0	660

For both of Alice's speeds, the tap-delay measurement is never negative. This makes sense because we are subtracting the distance of the NLOS path from the distance of the LOS path and then dividing that distance by the speed of light to calculate channel's tap. A negative tap delay value is not possible, because the reflected path will always be

longer than the LOS path. The lowest possible tap delay is zero, and that would occur only when Alice presses her UE against the reflector to get an equal NLOS path and LOS path.

Alice's maximum tap delay for her speed at 5 m/s is about 21 nanoseconds greater than when she moves at 1 m/s. Although this difference in maximum values appears small, Alice will travel 40 more meters in ten seconds at her top speed than she would at 1 m/s.

B. TAP-DELAY DIFFERENTIAL MEASUREMENTS OF A PEDESTRIAN MOVING AT DIFFERENT SPEEDS

Figure 12 is a histogram of Alice's tap-delay differential values for her slowest speed of 1 m/s. The range of values is symmetrically balanced over the y-axis with the extrema being ± 6.6 nanoseconds.

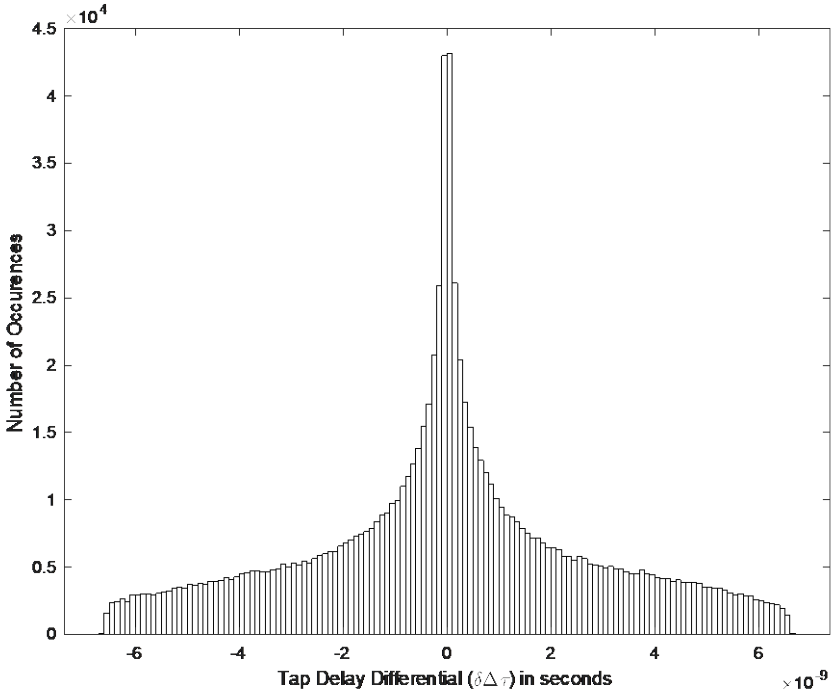

Figure 12. Tap-delay differential measurements for Alice moving at 1 m/s

Figure 13 is a histogram of Alice's tap-delay differential values. The range of values is also symmetric over the y-axis with the extrema being ±33.2 nanoseconds.

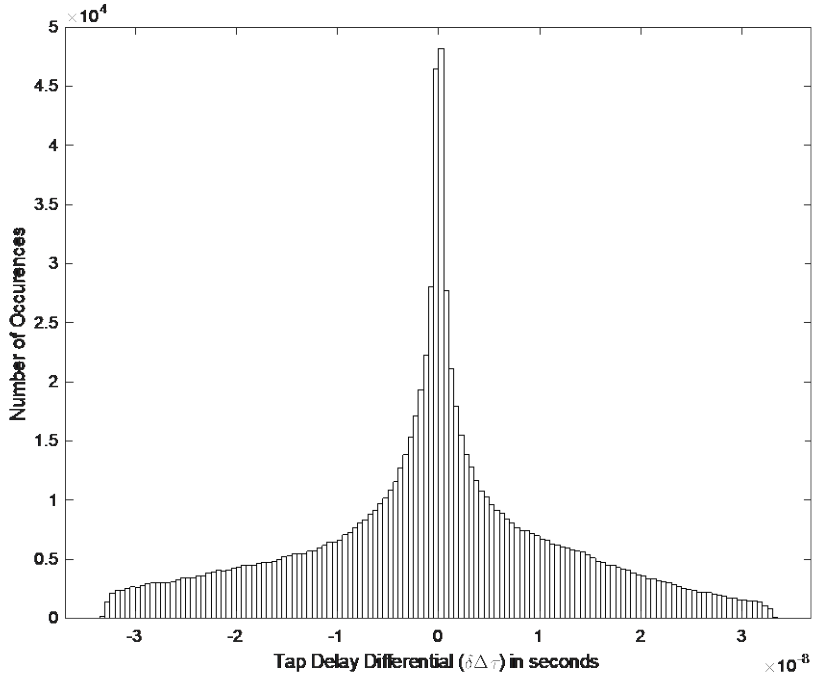

Figure 13. Tap-delay differential measurements for Alice moving at 5 m/s

Table 2. Tap-delay differential minimum and maximum for different speeds

Alice's Speed (m/s)	**Minimum $\delta\Delta\tau$ (nanoseconds)**	**Maximum $\delta\Delta\tau$ (nanoseconds)**
1	-6.62	6.63
2	-13.2	13.3
3	-19.9	19.9
4	-26.5	26.5
5	-33.2	33.1

Figures 12 and 13 have similar shapes, but Alice's increased speed has broadened the tap-delay differential range from ± 6.63 nanoseconds to ±33.2 nanoseconds. these simulations were incrementally re-run varying Alice's speed from 1 to 5 m/s, to calculate the maximum tap-delay differentials in Table 2. Characterizing the extrema for Alice's various speeds is important for later simulations when Bob has to select a tap-delay differential threshold in order to positively detect Alice from one tap delay to the next.

The information from the simulations in this part of Chapter IV answers the first two questions presented in Chapter III. We determined the expected range of values for channel tap delays ($\Delta\tau$) for a pedestrian walking through our simulated environment to range from 0 to 660 nanoseconds. We also learned that these tap delay values are dependent on Alice's position in the simulated environment, and that her slowest and fastest speeds had little impact on the maximum tap delays. This section also revealed the range of values for channel tap-delay differentials ($\delta\Delta\tau$) and how much they change based on Alice's speed.

C. PDF CURVES TO CHARACTERIZE TAP-DELAY DIFFERENTIALS

Based on the shape of the histograms for Alice's channel tap-delay differentials values, we chose to use an exponential PDF to characterize the data. Even though an exponential PDF is not a perfect representation of our data, which has a clear stopping point at approximately 33 nanoseconds, this PDF fit is simple to calculate and for a network to implement, when creating a tap-delay interval. We took the absolute value of all the tap-delay differential values from the previous simulation, so that they are all positive and we fit an exponential PDF over that data using the following equation

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases} . \tag{4.1}$$

We calculated the mean (μ) of the absolute value of the tap-delay differential measurements for each of Alice's speeds to obtain rate parameter (λ), which is the inverse of the mean (μ) as seen in Table 3.

Table 3. Parameters for tap-delay differential exponential PDFs

Speed (m/s)	**Mean $\delta\Delta\tau$ (nanoseconds)**	**Rate Parameter (λ) (s^{-1})**
1	2.02	4.94×10^8
2	3.02	3.31×10^8
3	3.99	2.51×10^8
4	4.91	2.04×10^8
5	5.80	1.724×10^8

The exponential PDFs for Alice's various speeds, shown in Figure 14, provide insight to answering the third question posed in Chapter III. To maintain authentication of a pedestrian, Bob can create a tap-delay interval size and compare it to the PDF plot or take the integral from zero to his selected interval maximum value of the exponential PDF equation corresponding to Alice's speed. From this, he can determine the probability of maintaining authenticated track of Alice from one second to the next. For instance, if Bob selected a tap-delay interval that is ± 5 nanoseconds-wide for Alice moving at 1 m/s, Figure 14 reveals a lot of area under the exponential curve from zero to 5 nanoseconds. Taking the integral of the exponential PDF equation for Alice moving at 1 m/s, more precisely reveals that Bob has a 91.5% chance of maintaining authentication of Alice. Going deeper, if Alice decides to start running and Bob keeps his 5-nanosecond threshold, the integral of the 4 m/s exponential PDF indicates that Bob now has a 58.5% chance of maintaining Alice's authentication. Therefore, Bob is needs to increase his tap-delay interval width to raise his chances of keeping Alice authenticated based on her position.

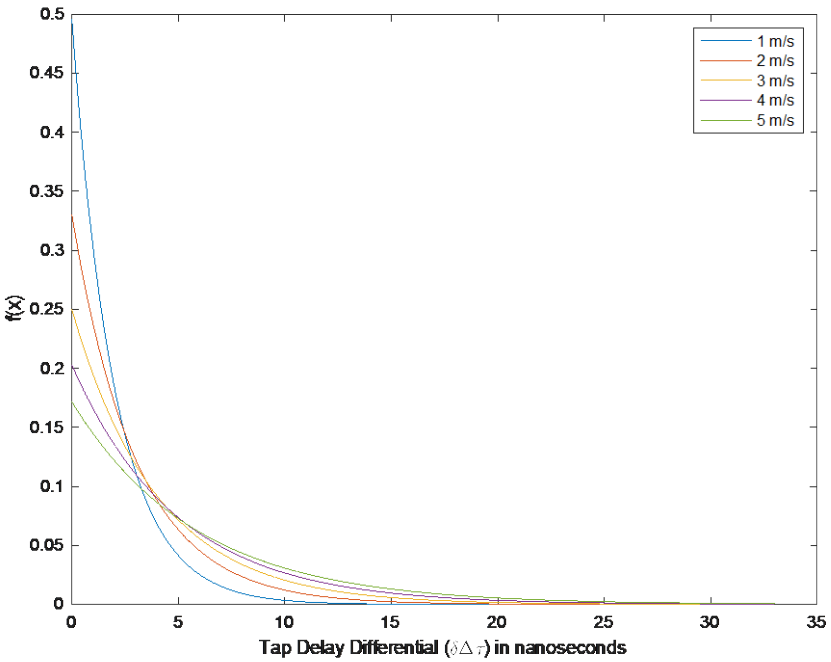

Figure 14. Exponential PDF of tap-delay differentials for various speeds

D. ROC CURVES: PROBABILITY OF DETECTION VERSUS FALSE ALARM

Referring to Figures 10 and 11 of Alice's tap-delay measurements in our first simulation, it is realistic to model Carol as another transmitter with a random start point and direction (like Alice). This causes Bob to have to measure Carol's tap delays and compare them to Alice's tap-delay interval.

For our first simulation, Carol walks around our virtual environment like Alice does, and Bob must measure and compare both of their tap-delay measurements to keep Alice authenticated. We increased the tap-delay interval width for Alice in 100-picosecond increments from 0 to 33 nanoseconds, which is the maximum tap-delay differential that we saw when Alice moves at 5 m/s in the results of the earlier simulations. We measured the positive detections of Alice versus false alarms caused by Carol's tap-delay measurements landing in Alice's tap-delay interval for each increment and the different speeds for Alice to produce the ROC curves in Figures 15. Based on the ROC Curve, Alice's 100% authentication occurs with a minimum probability of false alarm ranging from 11% to 32% depending on Alice's speed.

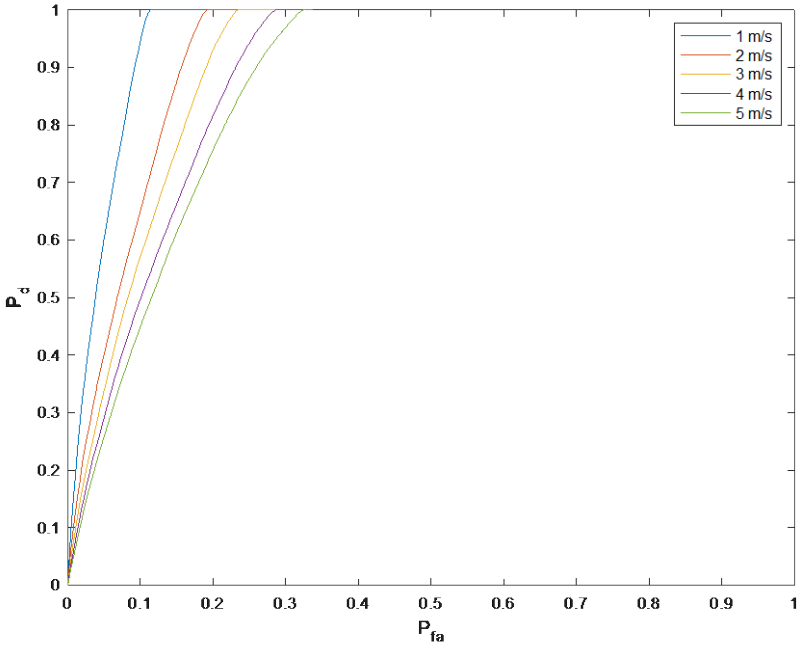

Figure 15. ROC curve: Carol randomly walks around with Alice

To add more realism to our simulations, there could be more people walking in vicinity of Alice than just Carol. In this final simulation, we modeled two more moving transmitters, Dennis and Frank, and then plotted a ROC curve based on three transmitters. To maintain Alice's authenticated status as she moves around the environment, Bob is going to have to compare the tap-delay measurements of Alice, Carol, Dennis, and Frank to Alice's tap-delay interval. Because there are more people in this environment, the ROC curve in Figure 16 shows more degradation between the probability of detection and false alarm. For Alice to maintain her authenticated status based on her tap-delay measurement 100% of the time, the network will have to accept a probability of false alarm ranging from 34% to 98% based on Alice's speed as shown in Figure 19.

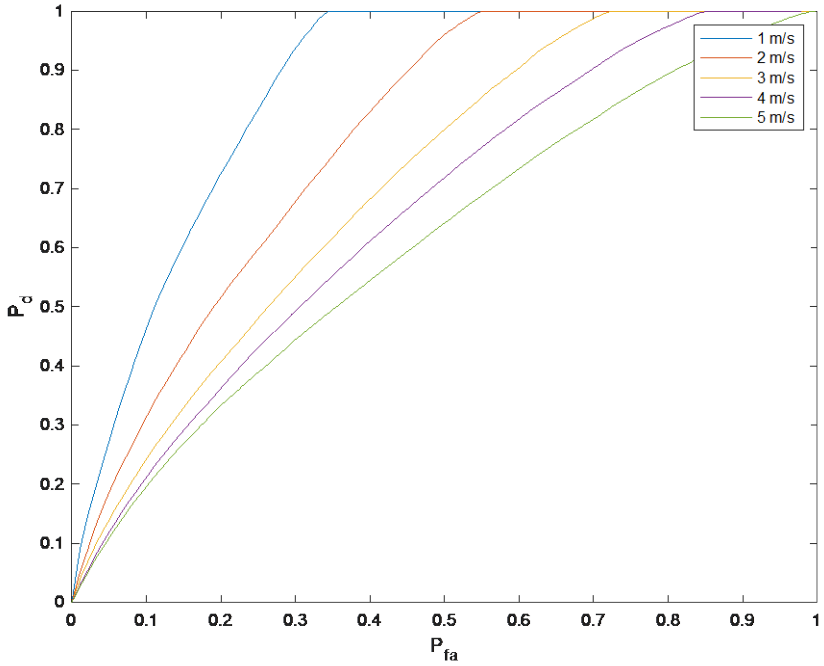

Figure 16. ROC curve: three other users walking around with Alice

E. SUMMARY

This chapter produced plots and metrics based on the simulation methodology set out in Chapter III. With the information that we gathered from these simulations; we were able to answer the questions that we posed to evaluate how well Bob can maintain authentication of Alice as she moves in an environment with a reflector.

V. CONCLUSION

A. SIGNIFICANT CONTRIBUTIONS

This thesis built from previous research that demonstrated that a network could improve its authentication mechanisms beyond common cryptologic practices by linking a network user identity to their physical location based on a tap-delay measurement in a multipath environment. However, when an authenticated user begins to move in this environment with a reflector, the network would have to reauthenticate and calculate their new channel tap delay when they eventually stop moving. As discussed in Chapter II, authentication processes can be cumbersome depending on the physical-layer-security practices of the network.

We proposed a way that a network can maintain authentication of its moving users by establishing a tap-delay interval around the most recent measurement of a moving target. By correctly anticipating when the next tap delay will occur, a network will not have to reauthenticate its users in motion as often. We analyzed how a pedestrian's speed from a slow walk to a sprint can impact the size of this tap-delay interval, which demands that the network must dynamically tailor its interval size to ensure successful tracking of their authenticated user, while also preventing false alarm detection from other users' tap-delay measurements. We showed through ROC curve analysis that other users randomly moving within an environment can cause their tap-delay measurements to interfere with a network maintaining authenticated status of its users.

B. FUTURE WORK

To improve and validify this physical-layer authentication method, we recommend further tests in an environment with a live 5G network to address some of our assumptions, specifically presuppositions that we made with our reflector.

1. Reflector Dimensions

For our simulations, we assumed a reflector with infinite dimensions. This guaranteed that every transmitted signal had a NLOS path to the receiver from the reflector.

Realistically, a reflector with limited dimensions can impact the ability to measure the delay between channel taps when a transmitter is at a location, where the reflector cannot produce a NLOS signal path back to the authenticating receiver. Also, our research does not explore how edge diffraction can cause signals to propagate back to a receiver to calculate their channel tap delay.

2. Reflector Material

Our research also assumes that the material of the simulated reflector perfectly reflects energy from the transmitter to the receiver. We do not take into consideration what materials a real reflector must have to reliably reflect channel taps back without absorption. Additional research into materials that reliably reflect 5G energy can help improve this authentication method.

3. Other Reflectors

Finally, our simulation assumed that there was only one reflector in our test environment. An environment with many reflectors can interfere with the ability to calculate the delay between channel taps. Other reflectors may obstruct and shadow signal propagation to the reflector.

LIST OF REFERENCES

[1] "Mobile Subscriptions Outlook." Ericsson. https://www.ericsson.com/en/mobility-report/dataforecasts/mobile-subscriptions-outlook (accessed May 15, 2021).

[2] "5G Wireless Access: An Overview," White Paper, Ericsson, April 2020.

[3] Secretary of Defense, "Department of Defense 5G Strategy," 2020. Available: https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf (accessed May 20, 2021).

[4] Secretary of Defense, "Department of Defense 5G Strategy Implementation Plan," 2020. Available: https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf (accessed May 20, 2021).

[5] K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, "Report on Lightweight Cryptography," National Institute of Standards and Technology, Gaithersburg, MD, USA, Internal Report 8114, March 2017.

[6] Ali, E., Ismail, M., Nordin, R. et al. "Beamforming techniques for massive MIMO systems in 5G: overview, classification, and trends for future research." *Frontiers Inf Technol Electronic Eng* 18, 753–772 (2017). https://doi.org/10.1631/FITEE.1601817

[7] S. Lord, J. Roth, J. McEachen, and M. Tummala, "A novel method for physical-layer authentication via channel state information," in *2018 12th International Conference on Signal Processing and Communication Systems* (ICSPCS), Dec 2018, pp. 1–9.

[8] J. D. Day and H. Zimmermann, "The OSI reference model," in *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1334-1340, Dec. 1983, doi: 10.1109/PROC.1983.12775.

[9] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[10] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," 2016 *IEEE International Conference on Communications (ICC),* 2016, pp. 1-6, doi: 10.1109/ICC.2016.7510994.

[11] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," in *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28-35, April 2015, doi: 10.1109/MCOM.2015.7081072.

[12] Y. Liu, H. Chen and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347-376, Firstquarter 2017, doi: 10.1109/COMST.2016.2598968.

[13] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014, doi: 10.1109/SURV.2014.012314.00178.

[14] X. Wang, P. Hao and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," in *IEEE Communications Magazine*, vol. 54, no. 6, pp. 152-158, June 2016, doi: 10.1109/MCOM.2016.7498103.

[15] X. Guo, Z. Zhang and J. Chang, "Survey of Mobile Device Authentication Methods Based on RF Fingerprint," IEEE INFOCOM 2019 - *IEEE Conference on Comput. Communications Workshops* (INFOCOM WKSHPS), 2019, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS47286.2019.9093755.

[16] B. Danev, H. Luecken, S. Capkun, and K. E. Defrawy, "Attacks on physical-layer identification," in *Proc. ACM Conf. Inf. Wireless Netw. Security*, Hoboken, NJ, USA, 2010, pp. 89–98.

[17] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[18] M. U. Sheikh and J. Lempiäinen, "Analysis of multipath propagation for 5G system at higher frequencies in microcellular environment," *13th Intl. Wireless Commun. and Mobile Comput. Conf. (IWCMC),* 2017, pp. 1660-1664, doi: 10.1109/IWCMC.2017.7986533.

[19] F. Capar and F. Jondral, "A Rayleigh fading channel model for multicarrier systems: a tapped delay line model," *IEEE 59th Vehicular Tech. Conf. VTC* 2004-Spring (IEEE Cat. No.04CH37514), 2004, pp. 181-185 Vol.1, doi: 10.1109/VETECS.2004.1387938.

[20] S. Lord, LCDR, "5G millimeter-wave physical-layer authentication with planar reflectors," Ph.D. dissertation, Dept. of Elect. and Comput. Eng, Naval Postgraduate School, Monterey, CA, USA, 2019.

[21] 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.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California