2019-09

ANALYSIS OF A POTENTIAL LTE DENIAL-OF-SERVICE TIMING VULNERABILITY

Long, James G.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ANALYSIS OF A POTENTIAL LTE DENIAL-OF-SERVICE TIMING VULNERABILITY

by

James G. Long

September 2019

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	3. REPORT TYPE AND DATES COVERED
	September 2019	Master's thesis

4. TITLE AND SUBTITLE ANALYSIS OF A POTENTIAL LTE DENIAL-OF-SERVICE TIMING VULNERABILITY	5. FUNDING NUMBERS
6. AUTHOR(S) James G. Long	
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	12b. DISTRIBUTION CODE
Approved for public release. Distribution is unlimited.	A

13. ABSTRACT (maximum 200 words)

There are 3.7 billion long-term evolution (LTE) subscribers worldwide, according to the *Ericsson Mobility Report* for the first quarter of 2019. To the average user, the exchange of this cellular traffic may seem secure; however, there exists at least one vulnerability: the unencrypted timing advance (TA). The TA is responsible for maintaining time synchronization between the evolved NodeB (eNB) and the user equipment (UE). Without it, the eNB-UE communication link fails, resulting in degraded cell service. By issuing faux TAs, an attacker disrupts the eNB-UE timing synchronization and denies service to the UEs. This thesis investigates specific effects such an attack has on targeted and time-adjacent users' subframe bit-error rate (BER). Moreover, we show the disruption of a single user's communications while leaving other users' communications untouched. Through simulation, we show that delaying a target transmission is less desirable to the attacker since the eNB has delay-correcting capabilities. Additionally, by advancing a target transmission using one TA, we achieve, on average, 50% subframe BERs. Lastly, we demonstrate that the attacker has flexibility in issuing the TAs without interfering with time-adjacent users. Specifically, the attacker can issue roughly 48 TAs before incurring a non-zero BER on time adjacent users. With this functionality, combined with an unsecure timing mechanism, an attacker has the capability of denying service to a targeted individual.

14. SUBJECT TERMS	15. NUMBER OF PAGES
denial of service, dos, long-term evolution, cellular, timing advance, time division multiple access, single carrier frequency division multiple access, physical uplink shared channel, demodulation reference symbol	71
	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.

ANALYSIS OF A POTENTIAL LTE DENIAL-OF-SERVICE TIMING VULNERABILITY

James G. Long
Lieutenant, United States Navy
BS, Towson University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2019

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

There are 3.7 billion long-term evolution (LTE) subscribers worldwide, according to the *Ericsson Mobility Report* for the first quarter of 2019. To the average user, the exchange of this cellular traffic may seem secure; however, there exists at least one vulnerability: the unencrypted timing advance (TA). The TA is responsible for maintaining time synchronization between the evolved NodeB (eNB) and the user equipment (UE). Without it, the eNB-UE communication link fails, resulting in degraded cell service. By issuing faux TAs, an attacker disrupts the eNB-UE timing synchronization and denies service to the UEs. This thesis investigates specific effects such an attack has on targeted and time-adjacent users' subframe bit-error rate (BER). Moreover, we show the disruption of a single user's communications while leaving other users' communications untouched. Through simulation, we show that delaying a target transmission is less desirable to the attacker since the eNB has delay-correcting capabilities. Additionally, by advancing a target transmission using one TA, we achieve, on average, 50% subframe BERs. Lastly, we demonstrate that the attacker has flexibility in issuing the TAs without interfering with time-adjacent users. Specifically, the attacker can issue roughly 48 TAs before incurring a non-zero BER on time adjacent users. With this functionality, combined with an unsecure timing mechanism, an attacker has the capability of denying service to a targeted individual.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

3GPP 3^{rd} Generation Partnership Project

5G 5^{th} Generation

AWGN additive white Gaussian noise

BER bit error rate

CAZAC constant-amplitude, zero-autocorrelation

CC component carriers

CP cyclic prefix

CRC cyclic redundancy check

C-RNTI cell radio network temporary identifier

dB decibels

DL downlink

DoS denial of service

DRS demodulation reference symbol

eNB eNodeB

E-UTRA evolved universal terrestrial radio access

FDD frequency division duplexing

FFT fast Fourier transform

FRC fixed reference channel

IP internet protocol

ISI	inter-symbol interference
LTE	Long Term Evolution
MAC	medium access control
MATLAB	Matrix Laboratory
MIMO	multiple input multiple output
OFDM	orthogonal frequency division multiplexing
PAPR	peak-to-average-power ratio
PCID	physical cell identity
PRB	physical resource block
PSS	primary synchronization signal
RF	radio frequency
QAM	quadrature amplitude multiplexing
QPSK	quadrature phase shift keying
SC-FDMA	single-carrier frequency division multiple access
SCS	subcarrier spacing
SRS	sounding reference symbol
TA	timing advance
TAG	timing advance group
TDD	time division duplexing
TDMA	time-division multiple access
UE	user equipment
UL	uplink

Acknowledgments

First and foremost, I would like to thank my wife, Jennifer, for her patience and encouragement throughout my studies. When I was stressed, your love and support helped more than you know. I love you forever.

I would like to thank my parents, James and Jeanne Long, for their continued support and for always believing in me. You have made me who I am, and I am forever grateful. I love you both.

I would also like to thank my brother, Michael. Even though you're my younger brother, I look up to you. Your diligence and perseverance motivate me to work as hard as you do.

Finally, I would like to thank my advisor, Dr. John Roth, for his continual guidance and mentorship. Your ability to help focus my attention was instrumental in guiding my efforts. For that, I am most appreciative. It was a pleasure conducting research together. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

1.1 Motivation

In order to keep pace with the global demand for internet protocol (IP) traffic, mobile communications companies are positioning themselves to make their networks evermore accessible to potential subscribers. According to the first quarter, 2019 Ericsson Mobility Report [1], the total number of "Long Term Evolution (LTE) subscriptions increased by 160 million during the quarter to reach a total of 3.7 billion, and 47 percent of all mobile subscriptions are for LTE." Additionally, the report remarks that, on average, there is more than one mobile subscription for every mobile subscriber, suggesting that some owners even have multiple devices. Clearly, we have come to rely on consistent, fast data speeds and reliable network access to accomplish everyday tasks. Our continuous demand for data necessitates that communications networks are dependable; therefore, they must also be secured.

Currently, the mechanism LTE implements to achieve user equipment (UE)-eNodeB (eNB) timing synchronization is unencrypted, nor is any form of authentication required. The eNB is the network access point for LTE devices. The timing mechanism is a medium access control (MAC) control element, which ensures a mobile device's transmissions arrive at the eNB when the eNB expects them to [2]. Additionally, this control element is dynamic and is updated often to support device mobility. Timing synchronization is a key concept in digital communications, and without it, the communication link fails. Therefore, the unsecured timing mechanism presents a possible vulnerability, since a UE may interpret an illegitimate (or rogue) timing synchronization message as an authentic command.

Such an attack would be classified as a denial of service (DoS) in that by executing the attack, the device would be *denied* access to the network. It is not hard to imagine the effects such an attack would have on an individual, or possibly, groups of individuals. Additionally, as 5^{th} Generation (5G) technologies are beginning to come on-line, the reliance

we have on our devices is ever-greater. We submit that this security vulnerability is one that ought to be examined to determine the efficacy such an attack would have on mobile users' devices.

1.2 Objective

This thesis assumes that a malicious actor is somehow able to manufacture and transmit a faulty timing command to a unique user's LTE device. Additionally, we assume the user's handset recognizes the false command as an authentic command from its parent eNB and either advances or delays its radio transmissions accordingly. At this point, we now have two primary objectives that we wish to fulfill. The first is to ascertain how the target user's bit error rate (BER) is affected if such an attack were to occur. The second objective is to determine the effects on the users that are time-adjacent to the targeted user's radio frequency (RF) transmissions. Lastly, we explore the possible existence of a middle ground where the targeted user is affected, but the time-adjacent users are unaffected. In doing so, we attempt to determine whether such an attack is surgical enough to affect a single user without creating collateral damage for the time-adjacent users.

1.3 Chapter Outline

From this point, we discuss salient technical aspects of LTE and the author's previous research in Chapter 2. Then, in Chapter 3, we present the simulation's design, our model environment, the metrics of effectiveness, and the attack framework. Next, the experimental results are discussed and analyzed in Chapter 4. Finally, Chapter 5 provides conclusions and offers recommendations for future work in this research area.

CHAPTER 2:
Background

This chapter educates the reader on the knowledge required to understand this thesis. Included in this chapter are a brief review of the prior research in this field, salient technical aspects of LTE, and a summary of the author's previous work.

2.1 Related Work

Exploring and identifying LTE DoS methodologies is nothing new. In essence, the fundamental idea behind a DoS attack is to prevent a user, or users, from utilizing their device as it was designed to be used. According to [3], DoS attacks are defined by two parameters: the amount of malicious traffic load generated and the impact of the attack, also known as the scope of the attack. Here, traffic load can be thought of as the amount of effort required to implement the attack, and scope is defined by the number of affected users. A classic example of a DoS attack is radio jamming. Radio jammers are radio frequency transmitters designed to block, jam, or otherwise interfere with authorized radio communications [4]. In this method of DoS, the transmitted signal is subjected to artificially created noise to disrupt signal integrity, thereby denying the receiver a copy of the transmitted signal and making the received signal useless. The case of classic radio jamming can be qualified as high traffic load and high scope per the model presented by [3]. One notable aspect of radio jamming is that it usually is not used to target individuals. Radio jamming affects all users in a given area (e.g., high scope). Basic electromagnetic theory tells us that the closer a jamming transmitter is to the receiver, the more affected the receiver is by the jammer. However, in general, a malicious actor has less control over who and what they affect by employing a blanket radio jamming DoS attack. Also, a radio jamming attack requires the affected user(s) to be close to the jamming transmitter. As soon as the affected user moves sufficiently far from the jamming transmitter, they are no longer affected by the attack.

Presented in [5] is an overview of the possible jamming vulnerabilities of LTE communications. The authors present three possible methods of jamming specific to LTE: synchronization signal jamming, primary synchronization signal (PSS) jamming, and

physical uplink (UL) control channel jamming. The UL refers to the transmissions from the UE to the eNB. In the first, the attack jams the UE by constantly flooding the frequency spectrum the UE uses to communicate with the eNB. This bars the UE from acquiring information needed to connect to the eNB. In the second, the attacker would again jam the UE, but would do so in a particular manner. Instead of continuously barraging the UE with energy, the jammer targets specific symbols in the downlink (DL) to block the UE from receiving the PSS. Additionally, the jammer creates three false PSSs for the UE to associate with the eNB. However, the authors quickly identify a solution to this DoS scheme. The solution involves the UE creating a list of fake PSSs that the UE learns to ignore. Finally, the third method involves forcing the eNB to assign too many resources to the UE, eventually leading to failed service. In conclusion, the authors offer that each of these attacks are realizable, and that it would be in the public's best interest to mitigate LTE vulnerabilities.

In contrast to the methods presented in [5], this work draws attention to a novel method of DoS in mobility managed networks. Similar to the vulnerabilities presented in [5], we are working from the perspective that there is a possible LTE susceptibility that leverages eNB control signaling–the time alignment mechanism. However, we present a different method that targets another type of control signalling. Normally, that specific control signaling is used to ensure proper time alignment of UE UL transmissions [6]. We work from the point of view that the UL timing command has been falsified in order to intentionally create timing misalignment in UE subframes, and then we analyze the effect on BER. The BER is calculated by comparing the transmitted bits to received bits and computing the proportion of bit mismatches in the transmission. This vulnerability requires low traffic load, just a single packet containing falsified control signaling is needed. The scope of the attack is also localized to the recipient of the falsified control signaling with minimal second-order effects, as we will see. The proposed vulnerability is unique in that the physical signals themselves do not need to be overwhelmed, such as in classical jamming. Rather this attack method takes advantage of how the protocol structure requires devices to synchronize with the eNB.

2.2 LTE Technical Background

In this section, we give a thorough treatment of LTE network architecture, mobility management and physical resources, and the structure and purpose of a timing advance (TA)

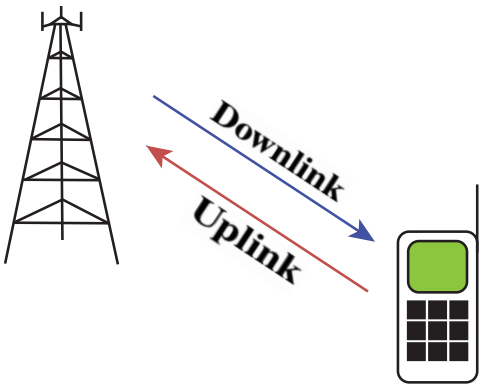

Figure 2.1. LTE air interface.

and the demodulation reference symbol (DRS).

2.2.1 LTE Network Architecture

In LTE, the most familiar device to people is the UE in their pockets. But in order for that device to operate, it needs to connect to a larger network. The channel that a UE and a eNB communicate over is termed the air interface. Among other functions, the eNB is responsible for transmitting the DL signal, and receiving the UL signal from the handset (i.e., UE) [2]. See Figure 2.1.

Also worth mentioning is the duplexing scheme that is used between the eNB and UE to communicate. In LTE, there are three methods of duplexing: half-duplex time division duplexing (TDD), full duplex TDD, and frequency division duplexing (FDD). In this thesis, we pay specific attention to the FDD mode only. However, the TA mechanism also supports the other two duplex modes, and therefore it is not unreasonable to expect that those duplexing schemes would likely experience effects similar to those observed in the FDD scenario, as we will come to see. In FDD, the frequency spectrum is divided into two frequency ranges, one dedicated to the UL and one dedicated to the DL (see Figure 2.2). Typically, there is a band of frequencies between the UL and DL to prevent interference between the communications [7]. FDD supports the ability for the UE and eNB to transmit simultaneously, thereby reducing the amount of standby time where one of the two network components would need to wait for the other to cease transmitting before starting their own transmissions.

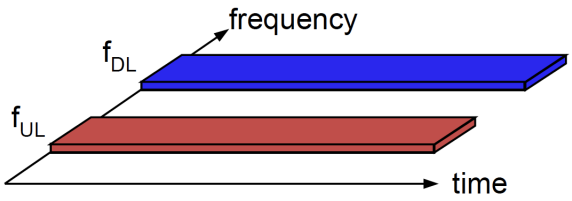

Figure 2.2. FDD in time and frequency. Source: [2].

2.2.2 Mobility Management in LTE

The designation given to the UE-eNB synchronization process is *random access*. During this process, a UE can request to connect to the network at any time, thus the use of the terminology "random" [6]. The necessity for UE to be time-synchronized with an eNB is driven by the mobility of the UE. As the UE changes position, it is handed off from one eNB to another, allowing for uninterrupted service. Due to the movement of the UE, the transmitted subframes take different amounts of time to get from the UE to the servicing eNB. The time it takes for the UL to traverse the distance from the UE to the eNB depends on the relative distance between the two. The farther the UE is from the eNB, the more time it will take for the subframe to arrive at the eNB than it would if the UE were located directly next to the eNB. Due to UE mobility, the distance between the UE and the eNB changes. Thus, the time taken for the UL to reach the eNB also changes.

For example, assume that every UE position change equal to 78.125 meters demands an adjustment to the timing control element. If a user were in a car travelling at 60 miles per hour straight toward the eNB, it would take the car just 2.913 seconds to travel that distance. Therefore, the timing mechanism demands continual updates. If that does not happen, the transmissions from your UE may arrive too early or too late at the eNB resulting in a possible loss of network access due to failed timing synchronization. Clearly, this is an undesirable situation demonstrating the timing management mechanism's necessity to sustain communications between the UE and the eNB as the UE moves about. Otherwise, users would constantly drop cell service.

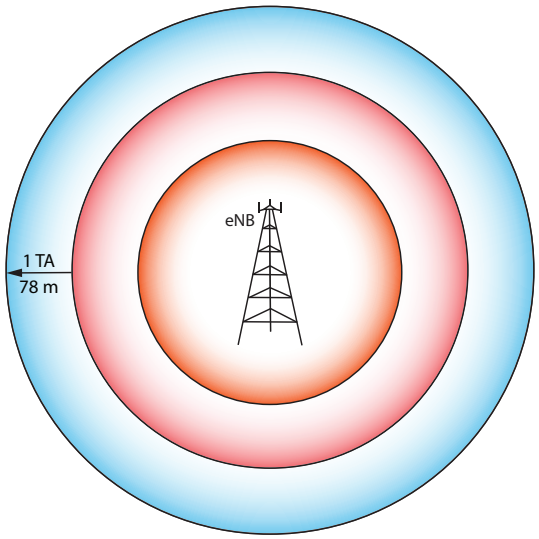

Figure 2.3. LTE timing advance.

2.2.3 The LTE Timing Advance

Time-domain synchronization between the UE and the eNB is managed by a specific MAC control element in the control signaling called the TA. The purpose of the TA is to control advancing or delaying the UL transmission timing to ensure the UL arrives at the eNB when expected [8].

In view of Figure 2.3, we see that the servicing eNB is in the center of concentric rings. Each of those rings can be thought of as having their own, unique TA. Each of the black circles is the border between one TA and the next. They are also where, if the UE were directly located, the UL would arrive at the eNB perfectly time-aligned. However, to be located exactly on one of these lines is unlikely and therefore one TA describes a set of possible locations, extending radially away from the eNB, between one black circle and the next. However, the farther the UE is from its black TA ring, the more delay there will be between the expected and actual UL arrival time at the eNB. Within the rings, the color opacity indicates the amount of delay between the assigned TA and the actual UL arrival time at the eNB. In this way, the eNB has a tiny amount of leeway in getting the TA exactly right. In Section 2.2.5, we will see how the eNB accounts for this delay.

In order for the UE to acquire its initial TA command, it must undergo the random access process as specified in [6] and summarized in [2]. First, the UE transmits a random access preamble that allows the eNB to approximate the UL timing of the UE. Second,

the eNB issues an initial TA to the UE to better adjust the UL timing. The initial value of a TA is an 11-bit number that ranges between 0-1282 [9]. Each value of TA corresponds to $16T_s$ where T_s is the LTE base unit of time and is dependent on the subcarrier spacing (SCS) and the maximum fast Fourier transform (FFT) size, N_{FFT} [10]. The SCS is the distance, in frequency, between one carrier frequency and another. In LTE 4G, the SCS is fixed at 15 kHz (i.e., 15,000 symbols per second). Thus, T_s, as defined in [9], is

$$T_s = \frac{1}{SCS \times N_{FFT}} = \frac{1}{15000 \times 2048} = 32.55 \ \frac{\text{ns}}{\text{sample}}.$$

and represents the shortest sampling time, which occurs when the UE is allocated the most time-frequency resources. Finally, because $T_A = 16T_s$, each incremental change in T_A is equivalent to an advance or delay of

$$T_A = 16T_s = 16 \times 32.55 \ \text{ns} = 0.52 \ \mu\text{s}.$$

This value coincides with our UL sampling period, t_s (i.e., the time difference between one UL waveform sample and the next). In this case, when the fewest time-frequency resources are allocated to the UE, the sampling frequency, f_s, is 1.92 MHz. Thus, $t_s = \frac{1}{f_s} = \frac{1}{1.92 \ \text{MHz}} = 0.52 \ \mu$s. Therefore, the eNB has very fine-tuned control over the timing of UL transmissions.

As we will see in Section 2.2.4, the eNB also allocates time and frequency resources to the UE during the random access procedure. Finally, the UE is granted access to the network after the eNB resolves any contention between multiple UEs trying to access the same time-frequency resource, if necessary. Then, once the UE is connected to the network, it must maintain timing synchronization with the eNB. For now, assume that our UE is assigned a specific time slot, while the other adjacent time slots are assigned to other UEs. Therefore, if UL transmissions are sent at the wrong time, they will arrive misaligned and can interfere with other UL transmissions occupying time-adjacent frequency resources. To rectify this issue, the eNB continuously adjusts the TA of the UE. The updated TA commands are based on the previous TA values. This method of TA adjustment greatly reduces the number of bits needed to describe the TA. After the initial 11-bit TA, the new TA commands are 6-bit numbers, assuming values between 0 and 63. The new TA updates

using the following formula

$$N_{T_A,new} = N_{T_A,old} + 16 \times (T_A - 31) \tag{2.1}$$

where $N_{T_A,new}$ is the updated TA and $N_{T_A,old}$ is the previous TA. This is significant because the TA commands essentially accumulate on top of of another. This can significantly impact the UL timing if the values are inaccurate, or are issued too frequently or infrequently.

Lastly, there are two additional bits in the TA called the timing advance group (TAG). The TAG is implemented to manage the UE TA when the UE supports multiple component carriers (CC), possibly from multiple eNBs. In other words, the UE is transmitting and/or receiving using multiple carrier frequencies simultaneously. In this case, the TA associated with each CC may need to be different depending on, for example, how many unique servicing cells there are. Thus, the TAG delineates which TA is associated with each CC. In the case of the same servicing cell, there is one TAG associated with multiple CC. The legacy TA (used in LTE releases 8 and 9) does not make use of the first two bits. However, in releases 10 through 14, which are synonymous with LTE-Advanced (LTE-A), the subject bits are implemented. As customer resource demand continues to rise and 5G technologies such as heterogeneous networks start to phase into society, the TAG is becoming a more important factor in the overall TA [11]. However, for the purposes of this thesis, we are only interested in the effects on a single CC associated with just one eNB.

2.2.4 Physical Time and Frequency Resources

LTE utilizes time-division multiple access (TDMA), a scheme designed to share and distribute scarce physical resources between users. As in all multiple access techniques, there is a common, finite resource that multiple users are trying to gain access to. Here, that resource is the collection of frequencies allocated to the LTE spectrum. In a TDMA scheme, the multiple users are assigned segments of time in which they are granted access to the common resource. Time is segmented into frames which is then subdivided and subsequently allocated to users [12]. In LTE, the multiple users are individual handsets and the smallest assignable time segment is called a subframe.

For further subdivisions, Figure 2.4 depicts the LTE time-domain structure. Here, we can see that one frame is 10 ms in length, which is then divided in 10 subframes, each

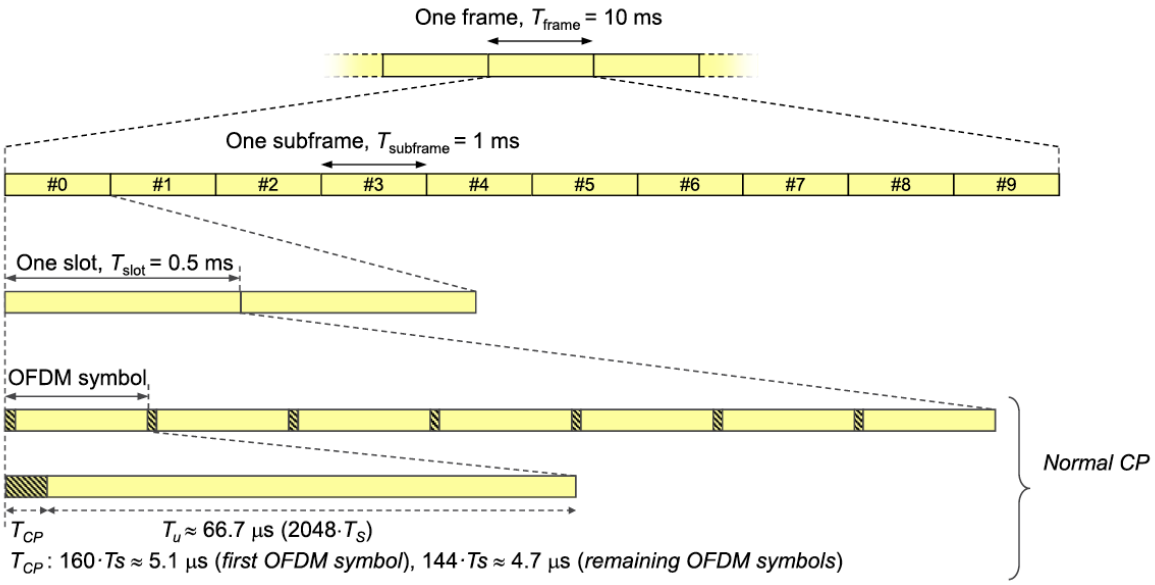

Figure 2.4. LTE time-domain structure. Source: [2].

1-ms in time duration. Furthermore, one subframe is comprised of two slots, each of which are 0.5 ms. Lastly, in the case of the normal cyclic prefix (CP), each slot contains seven orthogonal frequency division multiplexing (OFDM) (or single-carrier frequency division multiple access (SC-FDMA)) symbols. These symbols contain the data bits and special channel estimation symbols that the UE transmits to the eNB.

Modern LTE architecture attempts to optimize resource efficiency by servicing as many customers as possible. LTE devices are each assigned specific time and frequency resources to use for communicating with the eNB. Setting the frequency component aside, the time-width of the smallest scheduled resource, a subframe, is one millisecond [13]. Therefore, the computers that keep the network running are required to work with extremely small units of time. Thus, they must also maintain high levels of timing accuracy in order to function properly. Because UL signals propagate at the speed of light, changes in relative distance from one position to another can have significant impacts on the UE-eNB timing synchronization.

Now that we have seen how things are structured in the time domain, we need to discuss the frequency domain as well. Referring to Figure 2.5, we observe the frequency dimension with respect to the physical resource block (PRB). One PRB is comprised of

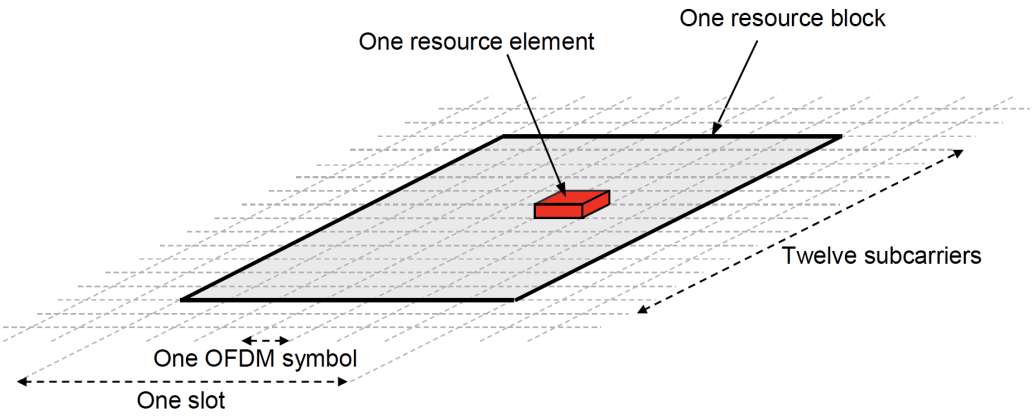

Figure 2.5. Physical time-frequency resource block. Source: [2].

multiple resource elements. Specifically, one PRB is seven OFDM (or SC-FDMA) symbols by 12 subcarriers and thus one PRB is comprised of 84 resource elements. The smallest scheduled resource in LTE is the resource block pair [14], which is two time-adjacent PRBs that occupy 12 subcarriers over a 1 ms duration (i.e., one subframe). The number of subcarriers that a UE transmits on is dictated by the number of PRBs that are assigned to the UE by the eNB.

Recall that multiplexing allows for multiple data streams to be combined into one communications channel and transmitted at the same time. In LTE, multiple orthogonal subcarriers transmit concurrently to increase the data rate. The DL implements an OFDM scheme, whereas the UL implements SC-FDMA. SC-FDMA is similar to OFDM, except there is an extra FFT operation [10] used to distribute symbol power evenly. The extra FFT operation reduces power fluctuations in the UL thereby reducing the UL overall peak-to-average-power ratio (PAPR) [15]. This means the transmitted waveforms are less taxing on the UE transmitter and thus consume less power. In contrast, the eNB is usually connected to the power grid and therefore can forego any considerations necessary to optimize battery life.

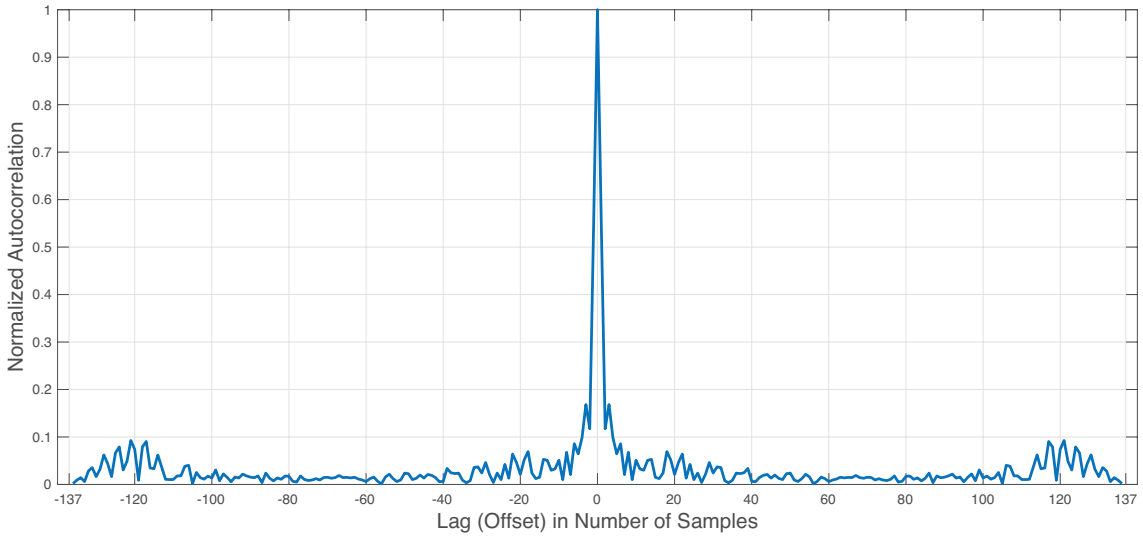

Figure 2.6. Normalized autocorrelation of one DRS

2.2.5 The Uplink Demodulation Reference Symbol and Channel Estimation

There are two types of reference signals used in the UL: the DRS and the sounding reference symbol (SRS). The SRS are used by the eNB for resource scheduling and the DRS are used for channel estimation. Channel estimation is the process of removing possible phase shifts that occur during transmission due to the exact position of the UE [10]. In other words, because the TA assumes discrete values, but the distance of the UE from the eNB is continuous, there is a quantization error that occurs in assigning a TA to the UE. Thus, the need for channel estimation exists.

In this thesis, we will only need to focus on the DRS since we assume that the necessary time-frequency resources have already been scheduled for the UE. That is, the SRS have already executed their role and are of no concern to us. However, the DRS are instrumental in channel estimation. Their role is to detect the beginning of a subframe and help correct for any time delays (i.e., phase shifts) the UL waveform may experience [10], [16].

The DRS are constructed using Zadoff-Chu sequences. Zadoff-Chu sequences are desirable because the peak value of autocorrelation occurs at zero lag and they have near-zero autocorrelation at non-zero lags [17]. This property allows the eNB to accurately determine

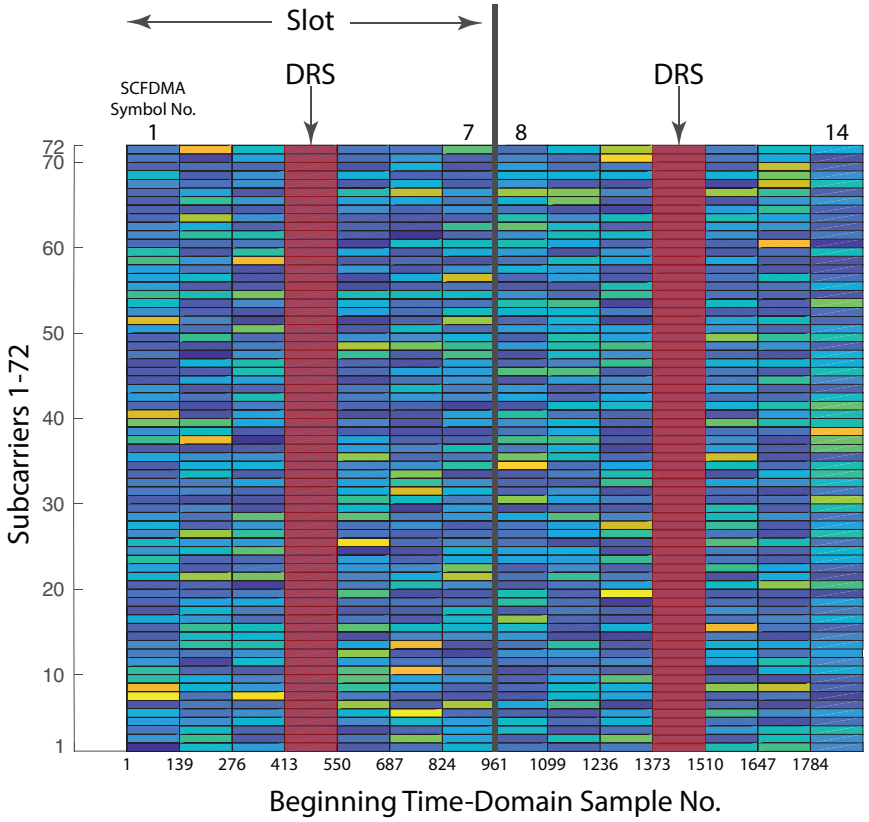

Figure 2.7. DRS within an LTE UL subframe.

the time delay offset, in number of samples, for a UL transmission while minimizing the chances of making a mistake. Thus, when the phase shift is known the eNB can then define the beginning of the subframe. Referring to Figure 2.6, we have the autocorrelation sequence of the actual DRS used in our model. Here, it is easy to see that the sequence peaks at zero lag, indicating the exact location of the DRS within the subframe. To do this, the receiver at the eNB computes the cross-correlation between the expected DRS and the received DRS to estimate the beginning of a subframe. Moreover, the correlation for all non-zero lags (or offsets) quickly diminishes thereby reducing the chances of misidentifying the beginning of the subframe.

The DRS are determined using a sequence group number assigned to each cell by the eNB [10]. According to [9], there are 30 unique sequence groups, each comprised of multiple base sequences of differing lengths. These base sequences are the aforementioned Zadoff-Chu sequences, except in some unlikely circumstances. Which base sequence the

UE uses to generate the corresponding DRS is dependent on the eNB-assigned PRB size, expressed in number of subcarriers. Therefore, the UE ultimately obtains its DRS using its cell sequence group number and the assigned number of subcarriers. Thus, combining the received DRS with the anticipated arrival time of a UE's UL, known by the eNB, allows the eNB to associate each incoming subframe with the transmitting UE.

Of note, the eNB can schedule cyclically shifted versions of the base sequences to individual UEs. However, that function is typically reserved for the possibility of scheduling more than one UE in the same PRB, such as in the case of UL multiple user multiple input multiple output (MIMO) [10]. This thesis assumes the point of view that the eNB scheduled the UEs with the same number of, but different, time-adjacent PRBs. That is, we assume that each UE within a single cell have the same DRS, not cyclically shifted DRS.

With respect to Figure 2.7, there are two DRS per subframe, or one DRS per slot, and they are orthogonal to one another. We believe this orthogonality prevents the receiver from unintentionally misidentifying the beginning of a subframe using the wrong DRS. We have highlighted the SC-FDMA symbols in the figure that represent the DRS in red. The DRS appear in the middle of each slot, which are SC-FDMA symbols 4 and 11 in each subframe.

Since the eNB is in charge of assigning the dynamic DRS to the UE, it then knows which particular sequence of symbols to expect at the DRS location within the UL. Therefore, in order to estimate the waveform timing offset, the eNB computes the cross-correlation sequence between the known, assigned DRS and the received waveform. We found that the functionality in the Matrix Laboratory (MATLAB) toolbox assumed that the eNB ignores all values corresponding to a negative offset (e.g., a time-advanced UL transmission). Finally, assuming that the eNB truly exhibits this behavior, the eNB estimates the offset by choosing the lag (timing delay in number of samples) corresponding to the greatest cross-correlation value. Using this value of offset, the eNB can adjust for any time delays the UL may have undergone and know exactly where the arriving UL transmission begins and ends.

2.3 Previous Work

Here, we briefly summarize the authors' prior research in this field contained within [18], and is titled *A Novel Denial of Service Vulnerability in Long Term Evolution Cellular Networks*. Initially, we investigated this type of DoS as a proof of concept and therefore we chose to exclude certain LTE features. Not taken under consideration in the paper were various features including the cyclic prefix, OFDM/SC-FDMA, error correction techniques, and channel estimation. In addition to simulating timing advances and delays, we implemented noise using additive white Gaussian noise (AWGN). Our research paper concluded that by interfering with the TA of a UE, an attacker could intentionally create inter-symbol interference (ISI) issues at the eNB between multiple UEs leading to bit errors at the receiver [18].

Our previous results indicated that in the case of a UE subjected to this vulnerability, and for very noisy environments, noise is the dominant factor in BER performance–not the ISI. Specifically, the BER at -5 dB and below clustered around 50% irrespective of magnitude of symbol overlap. In other words, depending on the severity of channel noise, the presented DoS vulnerability may have little impact on BER. However, as the channel noise decreased, the most effective factor that accounted for BER was the amount of SC-FDMA symbol overlap, rather than the level of environmental noise. In general, the BER approached one-quarter of the symbol overlap as a percentage. That is, if out of 2048 quadrature phase shift keying (QPSK) symbols, 64 of them experienced the ISI, then the BER approached 0.78%. Mathematically, that is

$$\frac{1}{4} \times \frac{\text{ISI Symbols}}{\text{Total Symbols}} = \frac{1}{4} \times \frac{64}{2048} = 0.78\%.$$

Similarly, if all 2048 symbols experienced ISI, then the BER was 25%. The vulnerability made the most significant impact in the region where the signal-to-noise ratio is greater than 0 decibels (dB). In this region, the noise by itself is not enough to force unacceptable BERs, but under the influence of the vulnerability the minimum BER was 0.195% which occurred when the 16 of 2048 QPSK symbols experienced ISI.

In conclusion, for unknown channel noise conditions, greater ISI leads to more consistent non-zero BER. This research proposed the possibility of an innovative DoS technique that could affect a single user, with minimal second-order effects. Due to its lack

of security, the TA mechanism makes it possible to create intentional UL signal interference. Additionally, this deficiency could extend beyond LTE to the other technologies that implement unencrypted TDMA controls.

In contrast, all of the aforementioned LTE error management features are included in the research covered by this thesis. The inclusion of which lead us to our present conclusion that the core issue this DoS method creates is a timing misalignment at the receiver, not ISI. Since we did not include those features, the effects of ISI appeared more important in the previous paper than we would come to find out.

2.4 Summary

This thesis investigates the subject vulnerability given the current status of the LTE protocol due to its ubiquitous implementation worldwide. However, we note that the vulnerability is generally applicable to any wireless network that implements TDMA and mobility management.

CHAPTER 3:
Methodology

In this thesis, we model a theoretical attack on a targeted user LTE device, the UE. To do this, we simulated an environment that included multiple UEs and a single eNB for them to communicate with. Below, we compare and contrast how the eNB and the UE operate before and after the DoS attack. The foundation of the attack is that a malicious actor generated a false TA command, transmitted it, and the target UE interpreted it as an authentic TA command. In response, the target UE incorrectly advances or delays its UL signal. To quantify the attack effects, we calculate the BER of each UE on a subframe basis.

3.1 Model Experimental Design Environment

The first step to determining the effects of this false TA command is to initiate the model environment. Using the MATLAB R2018b LTE Toolbox, we created an environment containing three UEs and one eNB. Each of the UEs are contained within the same sector of the eNB and therefore they all have the same physical cell identity (PCID). Of the three UEs, one was designated as the target (UE1) and the other two represented time-adjacent users (UE0 and UE2). The target, UE1, is the handset that receives the theoretical false TA command and incorrectly adjusts its UL timing.

Using the MATLAB LTE toolbox, each UE had one subframe of data randomly generated for use in this experiment. Once the data bits were generated for each UE, we transformed the bitstreams into their equivalent, LTE-compliant, time-domain waveforms. Chronologically, the order in which the subframes are supposed to arrive at the eNB are UE0 (first), UE1 (second), and UE2 (third). See Figure 3.1.

By advancing or delaying a UL transmission, it is possible that the transmission will arrive at the eNB concurrently with another user's UL, thus creating interference between the inbound transmissions and possible synchronization issues. Therefore, in order to model the effects of the false TA command, we slid the UE1 waveform either to the left or the right. Then, we added the two overlapping waveforms together. In doing so, we simulated the effects of an advance or delay in UL timing and the additive effects that

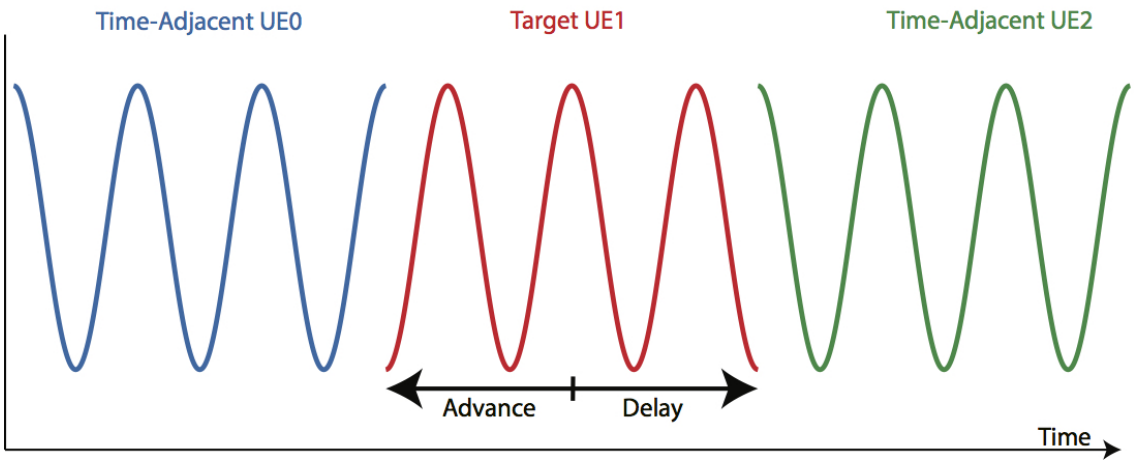

Figure 3.1. Basic structure of UE waveforms in time.

occurs at the receiver due to interfering transmissions.

Because the TA commands are cumulative, the range of possible overlap extends from entire subframe overlap (all samples) to no overlap (zero samples). In addition to studying the effects on the target UE, we also wanted to gain an understanding of the collateral damage that would occur to the adjacent users, UE0 and UE2. Once we simulated the time-advanced and additive effects, we then performed the channel estimation process and the processing necessary to extract the received bits. Finally, we calculated the BER for each UE by comparing the transmitted bits to the received bits relative to each device.

3.2 Model Metrics and Parameters

Here, we used BER per subframe as the metric to measure attack effectiveness. According to [10] and [19], the *timeAlignmentTimer* is responsible for dictating to the UE how long the UL is considered to be time-aligned. The range of values the *timeAlignment-Timer* assumes is between 500 and 10,240 subframes, or 0.5 to 10.24 seconds. If a TA command is not updated or reissued by the time the *timeAlignmentTimer* expires, then the UE considers the time synchronization with the eNB lost. Thus, a single TA command is guaranteed to be valid for the duration of one subframe, thereby allowing us to compare the BER on a subframe basis for incremental changes in TA. Finally, after the attack was simulated and once we demodulated and decoded the waveform, the BER was computed by comparing the received bits to the transmitted bits. Here, the BER is a function of timing

advance (or delay) due to false TA commands.

For this research, we consulted [20] to determine specific parameters on how we configured our UEs. The term "fixed reference channel (FRC)" is somewhat of a misnomer because it does not describe anything about the actual channel. Rather, an FRC is a standard set of parameters describing a signal, and they dictate the UE configuration. FRCs are used in conformance testing to ensure that the network is running as intended before it is employed in the field. In order to isolate the DoS attack, the actual channel we used was noiseless, allowing us to highlight the attack's effects.

As this is a proof of concept, QPSK was chosen as the preferred modulation method because it is more resilient than both 16-quadrature amplitude multiplexing (QAM) and 64-QAM. The idea being that if we could force bit errors in the QPSK case, then we would more than likely also be able to force bit errors in the the higher order modulation schemes as well. By deciding to use QPSK as the modulation scheme, we narrowed down the list of possible FRCs to implement. Eventually, we implemented FRC A1-1. Of note, A1-1 yields the same waveform as A3-2, and A8-2. The only difference between the collection of A1, A3, and A8 FRCs is that each sub-reference channel (e.g., A1-1, A3-2, etc.) changes the number of allocated PRBs. The eNB-assigned quantity of PRBs eventually leads to changes in the number of frequencies the UE is given and thus, the number of transmitted data bits per subframe. The allocation of more resource blocks leads to higher data bits per subframe, and vice versa. Table 3.1 below consolidates the parameters used to generate individual subframes conforming to FRC A1-1 and their corresponding waveforms.

The allocated resource blocks are the time-frequency resources assigned to a specific UE. With respect to Figures 2.4 and 2.5, we can see that the number of SC-FDMA symbols matches the value in Table 3.1, not including the DRS symbols. The number of SC-FDMA symbols per subframe can change depending of the length of the CP. The code rate, R, is the rate at which the data bits are Turbo-coded, after cyclic redundancy check attachment. The Turbo-code is an error correction code implemented to reduce the number of bit errors at the receiver [21]. After the data bits have their cyclic redundancy check bits appended, and are Turbo-coded at $R = \frac{1}{3}$, then 12 trellis bits are appended to yield a coded block size equal to 1884 bits. Subsequently, this code block is rate-matched to produce total of 1728 bits per subframe. Finally, those 1728 bits are QPSK modulated to provide

864 symbols for transmission. For an overview of this process, please refer to Figure A-1 contained in Annex A of [20].

Table 3.1. Consolidated simulation parameters.

Parameter	Value
Allocated Physical Resource Blocks	6
SC-FDMA Symbols per Subframe	12
Modulation	QPSK
Code Rate (R)	1/3
Payload Size (bits)	600
Coded Block Size (bits)	1884
Total bits per Subframe	1728
Total Symbols per Subframe	864
Cyclic Prefix Length	Normal
Total Length of Waveform (Samples)	1920

3.3 Attack Framework

Here, we present the proposed attack in contrast to the eNB-UE normal mode of communication.

3.3.1 Operation under Normal Conditions

Referring to Figure 3.2, we will demonstrate the use of the TA to account for propagation delay (i.e., the time it takes to traverse the UE-eNB distance). In this figure, there are three separate UEs and one eNB operating under normal conditions. Here, we see that time and frequency are on the horizontal and vertical axes, respectively. Thus, all of the UL transmissions are arriving at the same time, but on different frequencies. Also, the length of the arrow extending from each UE toward the eNB is indicative of the distance from the handset to the cell tower. Thus, in order for the signals to all arrive at the same time, they each need their own unique TA. In addition, the farther away the handset is from the eNB, then the earlier the UL needs to be transmitted, and vice versa.

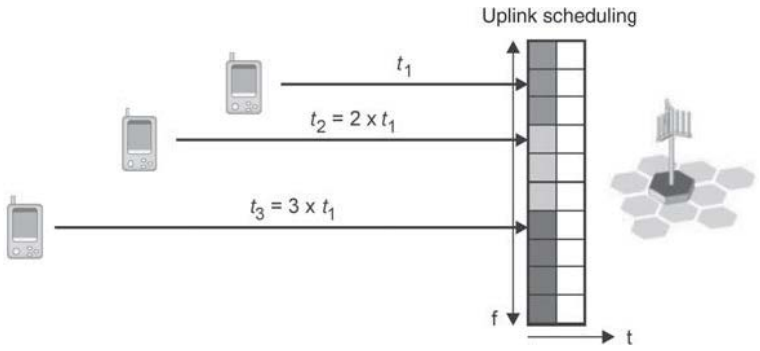

Figure 3.2. Various uplinks arriving simultaneously to account for propagation delay. Source: [7].

In Figure 3.3, we have a similar structure to Figure 3.2. However, this figure holds frequency constant across all devices, and thus their respective transmissions must arrive at different times so as to not interfere with one another. Because the signals arrive sequentially, they ought not to experience any interference with the time-adjacent users. From the perspective of UE1, its time-adjacent users are UE0 and UE2. This is actually

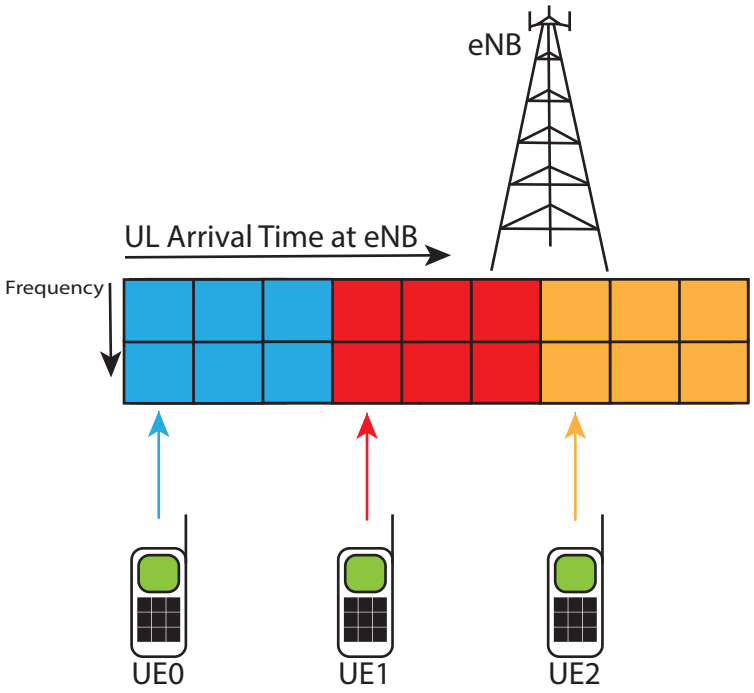

Figure 3.3. Various uplinks arriving sequentially to maintain time alignment and prevent interference.

how the eNB manages the incoming transmissions in order to keep everything orderly. Not demonstrated here is how the TA affects the scenario. In essence, it is a combination of the two figures such that the UEs are at different distance, but their ULs must arrive consecutively. Therefore, the eNB alters each of their TAs individually in order to achieve the scenario presented in Figure 3.3.

3.3.2 Proposed Attack

In this thesis, we work from the perspective that a falsified TA has been generated, transmitted, and interpreted by the UE as a valid control command. In this sense, these false TA commands inhibit the UE-eNB time synchronization, causing the UL signals to arrive either too early, or too late. With respect to Figure 3.4, this is akin to the red subframes mixing with either the blue or yellow subframes, respectively. On the left side of the figure, we show the target UE forced to transmit its UL too early, causing it to arrive in the time slot allocated to UE0. On the other hand, the right side of the figure depicts the scenario when the UE is told to transmit later than necessary, causing the UL to arrive at the same time as the UE2 UL. The disruptive command causes the UE to shift when it transmits its UL

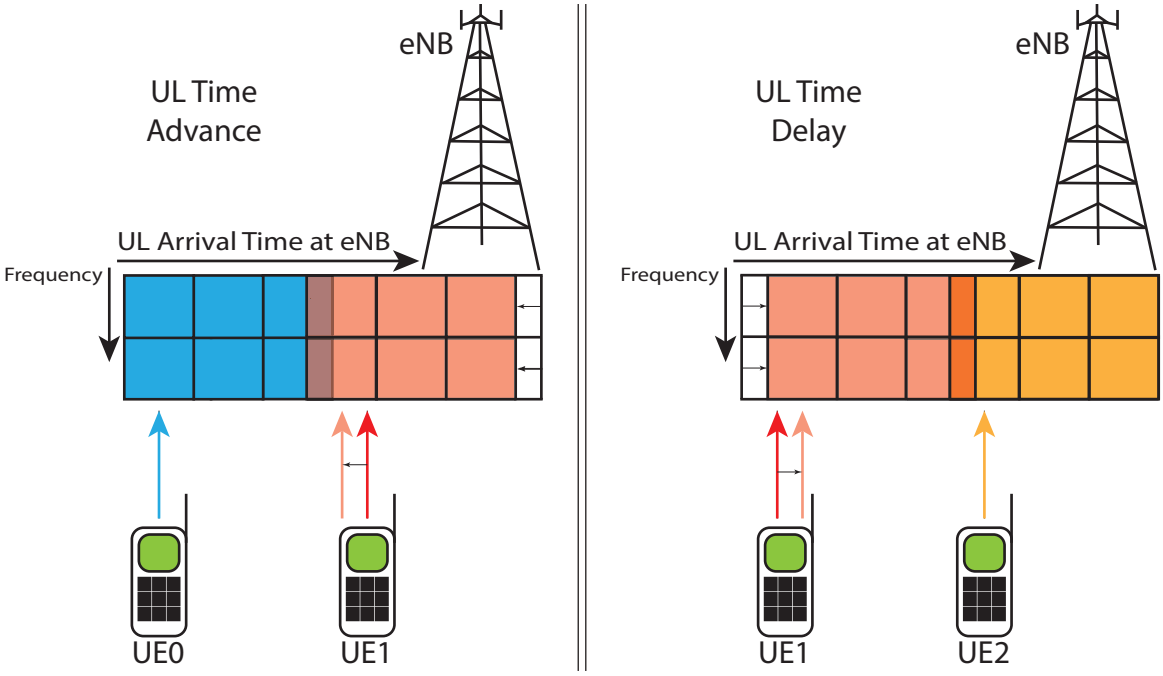

Figure 3.4. Uplinks arriving time advanced and time delayed.

frame resulting in misaligned subframes arriving at the eNB. Such an attack would disrupt and degrade the ability of the UE to interface with the larger network, thereby rendering the user unable to communicate.

As we already know, a TA can take on values between 0 and 63; therefore, the false TA can either advance or delay a UE's UL transmission. In this research, we inspect both cases, as well as measure the effects such an attack would have on time-adjacent users. Additionally, we take this one step farther to determine what the effects would be if the TA commands accumulated enough in order to overlap an entire subframe of the adjacent users.

3.4 Summary

In this section, we have explained the design of our simulation environment to include the theoretical framework of how our proposed attack would be implemented. To assist in the explanation we discussed how the eNB and the UE normally operate and how we expect them to operate after the proposed timing attack. Finally, we proposed the use of the BER on a subframe basis to quantify the efficacy of such an attack.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Results and Analysis

The numerical results show that if an attacker were able to execute an attack by creating false TAs, the victim would be subject to significant bit errors. A UE is particularly susceptible in the case where an attacker forces an intentional *advance* in UL timing rather than a delay. This is due mostly because of the channel estimation process that the receiver implements leveraging the DRS. We also show the effects such an attack would have on unintended, time-adjacent users. Most interestingly, the collateral damage is not very significant, thus allowing for the possibility of an attack on just a single user.

4.1 Effects on Target User Equipment BER Due to a Single TA Command

In the beginning, we wanted to determine the effects on the target user BER as a function of a single false TA that was interpreted as an authentic command from the eNB. Below, in Figure 4.1, we depict the BER as a function of a single TA command. The figure shows how the target UE BER is affected from just a single TA command which ranges from 0 to 63. The x-axis has been reversed to aid the reader in associating timing advances and delays with their respective TA values. By setting $N_{T_A,old}$ to zero in (2.1), the TA values less than 31 (in blue) are delays in time, whereas TA values greater than 31 (in orange) represent advances in time. Thus, a TA value equal to 31, denoted by the black asterisk in the figure, corresponds to "no change." The vertical axes is the BER and represents the percentage of total bits received in error.

Referring to Figure 4.1, we can see that for a TA command equal to 31, the BER is zero. That is because the attacker did not update the TA, which is akin to the attack not occurring. This is a useful command from the eNB for when the mobile is stationary. Recall that the TA commands are cumulative and dependent on the previous TA value. Therefore, a TA command corresponding to 31, is essentially the command to *continue what you are currently doing*.

Regarding a TA command less than 31, which represents a timing delay, the BER

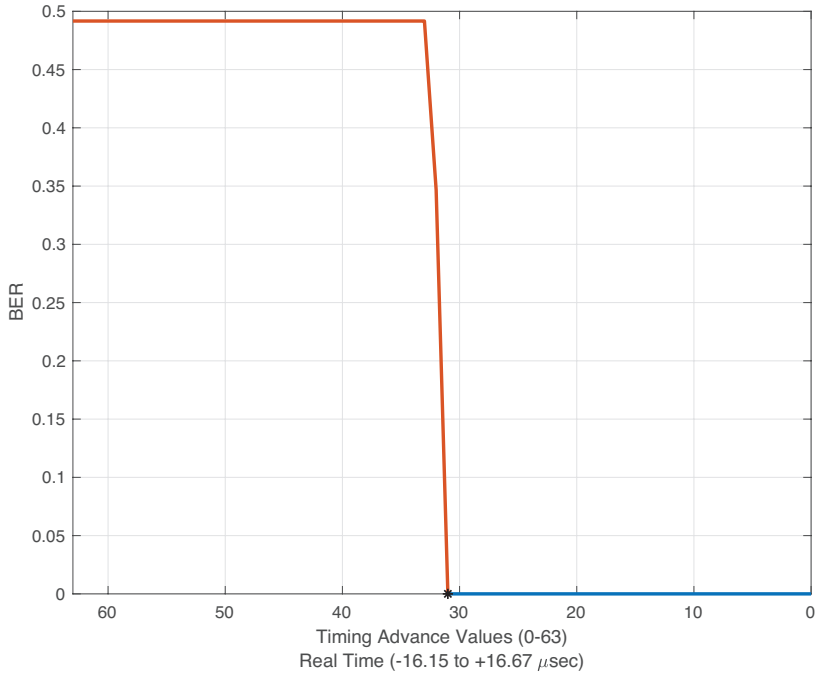

Figure 4.1. Target UE BER as a function of a single TA command.

is still zero. In this instance, the eNB is capable of rectifying incorrect timing delay commands using the DRS and the channel estimation process. Additionally, the would -be effects of the interference between the target UE and the UE2 waveforms is mitigated by the CP and Turbo coding mechanisms, allowing for perfect reception of the information bits. Channel estimation is demonstrated using Figure 4.2. In this figure, we arbitrarily selected two TAs of values 21 and 6. Then, by (2.1), those two values correspond to delays of 10 and 25 samples, respectively. Figure 4.2 depicts the cross-correlation sequence the eNB computes and shows how the eNB can identify the correct timing offset (i.e., delay). Then, the eNB uses this offset value and corrects for the UL timing misalignment. This feature was likely implemented so that the eNB did not have to get the TA value exactly right for each transmission. Also, *crucially*, the channel estimation process can account for any unpredictable errors in timing *delay*, but not advance. To verify this, we dissected the *lteULFrameOffset.m* function. To ensure our findings were accurate, we contacted MathWorks to confirm that the *lteULFrameOffset.m* command mimics real-world behavior. MathWorks assured us that the functions they release undergo rigorous tests to ensure their validity before employing them in their toolboxes. Therefore, the outputs of

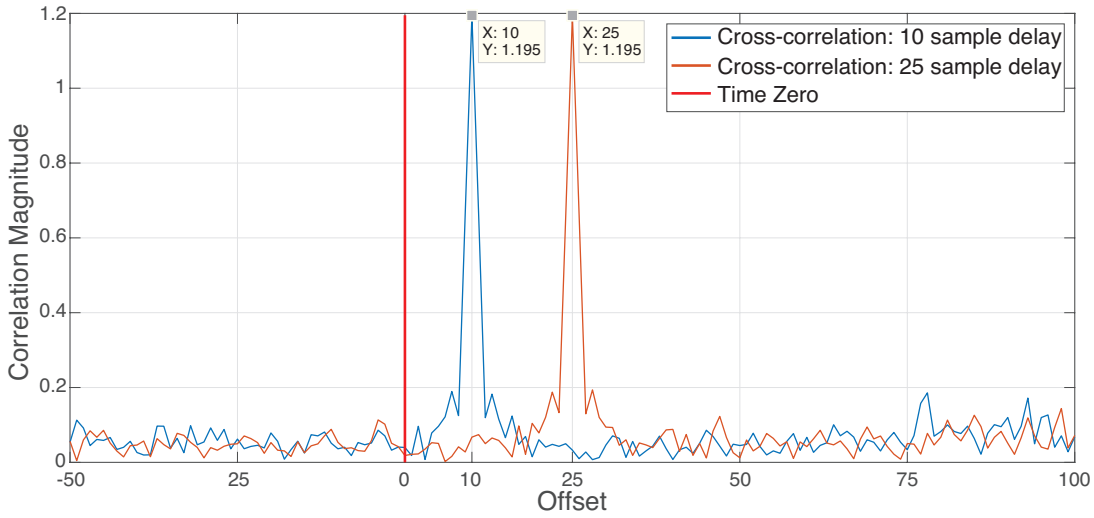

Figure 4.2. DRS cross-correlation sequences indicating UL delays.

lteULFrameOffset.m and our other results that rely on that function are reliable and to be trusted.

Finally, we arrive at the region where the TA is greater than 31 in Figure 4.1. Here we observe the BER quickly approach 50%. To reiterate, the eNB is unable to correct for unforeseen UL timing *advances*. In this situation, the BER jumps to the worst possible case because the eNB-UE communication link loses time alignment (i.e., synchronization). Here, because of the inability to correct for UL advances, the arriving UL appears as a random bitstream to the receiver. Thus, the received transmission is unintelligible to the eNB. The best the eNB can do is guess at the timing offset value–which is inevitably incorrect since the channel estimation function instantly ignores all negative values of timing offset. The possibility that a signal could have been accidentally (or intentionally) advanced in time is not even a consideration to the eNB.

To illustrate this point, the scenario is best-viewed in regard to Figure 4.3. Here, the blue curve represents all of the cross-correlation values, which are dependent on the time-difference (i.e., lag) between the received DRS and the eNB reference DRS. The vertical axis represents the non-normalized magnitude of correlation. In the example illustrated by this figure, the false TA injected has a value of 50. By (2.1), this TA value is representative of an advance of 19 samples in the time domain. This is demonstrated by the peak of the curve at an offset value corresponding to -19. However, the issue arises

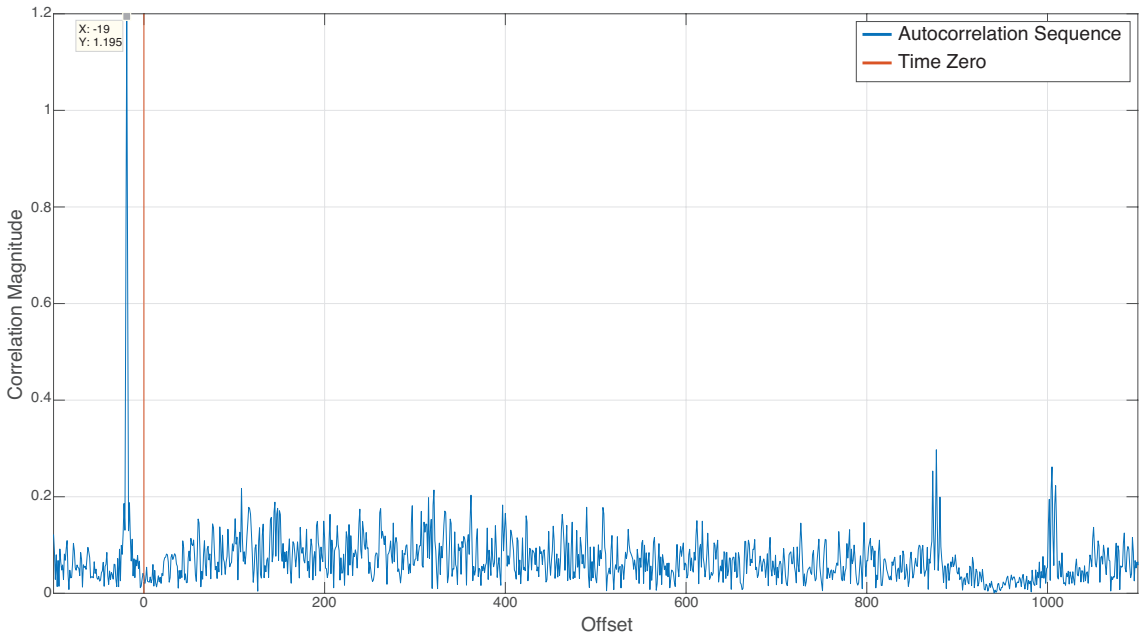

Figure 4.3. DRS cross-correlation sequence indicating an UL advance.

because the eNB *only* considers values of timing offset at zero, the red line, and greater (e.g., timing delays). Thus, the eNB ignores negative timing offset values, and then chooses the offset corresponding to the maximum correlation that is right of the red line. Then, the eNB estimates when it thinks the subframe arrived using the incorrect offset value thereby ruining any chances of correct channel estimation and, subsequently, signal recovery.

Linking Figures 4.1 and 4.3 reveals a relationship between estimated timing offset and the BER. The BER is constant for TA commands greater than 31 because the estimated offset tracks the TA value exactly, as shown in Figure 4.2. That is, as the TA changes, so too does the estimated timing offset. With respect to Figure 4.3, the eNB will estimate the offset using the highest peak to the right of the red line. In this example, that peak is located at offset value of 877 samples. The eNB interprets this as the UL arriving 877 samples later than expected. From here, the eNB uses this value to determine what it thinks is the beginning of the UL. At this point, the eNB estimates that the waveform arrived beginning at sample 896 of 1920 rather than at sample 1. The length of the waveform for one subframe in the time-domain is 1920 samples which is determined by the sampling period, $t_s \approx 0.52$ μsec, and the length of one subframe, (i.e., 1 millisecond). We determined sample 896 using the fact that the UL actually arrived 19 samples early plus the estimated

delay of 877 samples. Furthermore, if the scenario used a TA of 51 instead of 50, then everything in the figure would shift left by 1. The peak to the left of the red line would appear at -20 (not -19) and the new estimated offset would be 876 vice 877. Because the UL arrived one sample earlier than in the case of a TA value of 50, then it also shifted the estimated offset by one sample too. However, in both cases, eNB determine the beginning of the UL as the same, incorrect waveform sample. Following the same process as above, the aceNB again estimates that the waveform arrived at sample 896 of 1920 because the UL arrived 20 samples early plus the estimated delay of 876 samples. Therefore, the eNB estimates the same sample number as the beginning of the UL regardless of the value of TA as long as the TA is greater than 31. During this process of incorrect channel estimation, it is the lost synchronization between the UE and eNB, not ISI, that results in unacceptable BERs and a loss of communications.

4.2 Effects on Time-Adjacent User Equipment BER Due to a Single TA Command

Naturally, the next step is to analyze the collateral effects such an attack would have on the target time-adjacent users (i.e., UE0 and UE2). Recall that the targeted user experiences a synchronization issue whereas time-adjacent user ULs are arriving time aligned. Again, we operate under the same assumption as before: the attack is limited to only one false TA command. That is, the greatest effect on the target would be to delay or advance their UL signal by 31 or 32 samples, respectively. For this range of falsified timing offset, the effect on the time-adjacent users is zero. In other words, an attacker could cause the target handset to transmit early and create a non-zero BER for the target communications while also leaving time-adjacent user communications completely unaffected.

The reasons for this can be attributed to ISI mitigation and error correction techniques that LTE implements. First, the goal of error correction techniques is to ensure that the transmitted message bits are recovered and decoded at the receiver without any errors. In short, the UE transmits roughly 2.8 times more bits than actual message bits. These transmissions are called codewords. Thus, what is actually obtained at the receiver are corrupted codewords. However, using the soft-decision decoding process outlined in [22], the decoder can leverage the extra bits. This enables the receiver to rectify any codeword errors and extract the useful message bits.

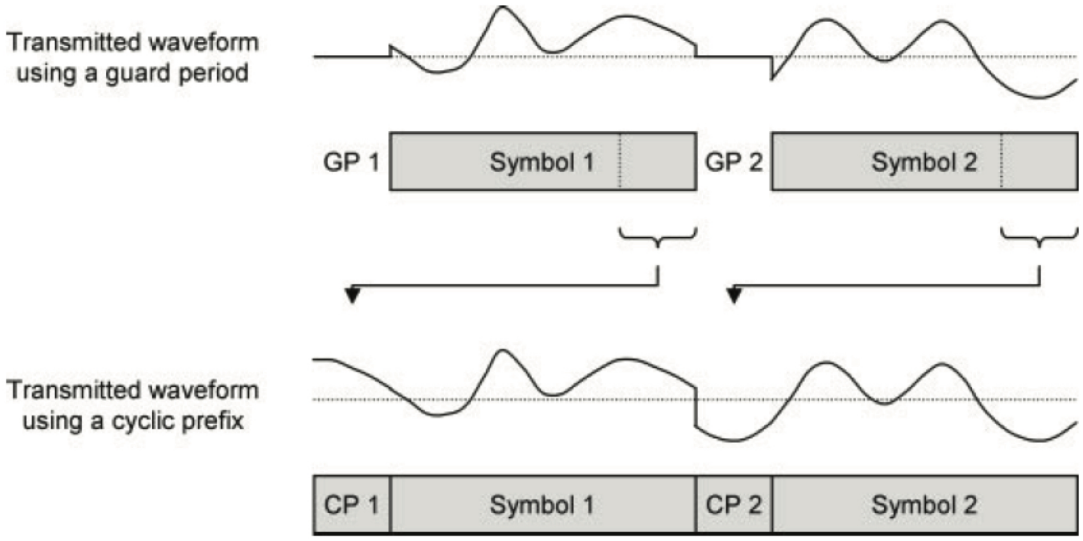

Figure 4.4. Depiction of the cyclic prefix in LTE. Source: [10].

Additionally, another desirable feature of SC-FDMA is that instead of using one carrier frequency per UL, the eNB assigns multiple *sub-carrier* frequencies for each UL. In LTE, each UE is allocated 12 sub-carriers per each assigned PRB. Thus, each UL is distributed across 72 sub-carriers, spaced 15 kHz apart, because each UE is assigned 6 PRBs in this experiment. Therefore, the data rate on each sub-carrier is just a fraction of what it would be using a single carrier frequency. An effect of SC-FDMA is an increased pulse width in time since we reduce the frequency bandwidth. Therefore, by holding the time overlap constant, then the ratio of affected time-domain pulse to the unaffected portion of the pulse is reduced. Thus, the employment of SC-FDMA reduces the ISI between user transmissions, and therefore the BER at the receiver [10].

Third, in reference to Figure 4.4, LTE implements a guard period in the form of a cyclic prefix. Each SC-FDMA symbol has a CP, and the length of the CP is designated as either *normal* or *extended*. The length of the CP is decided at the eNB and is determined using channel and environmental information. Here, we used the normal CP in all examples. In either case, the CP accounts for a only small fraction of each SC-FDMA symbol. As the name states, the CP is cyclic in that it functions by copying the last samples of an SC-FDMA symbol and appending them to the beginning of the associated SC-FDMA symbol [23]. The purpose of the CP is to further reduce the effects of ISI. Once the receiver processes

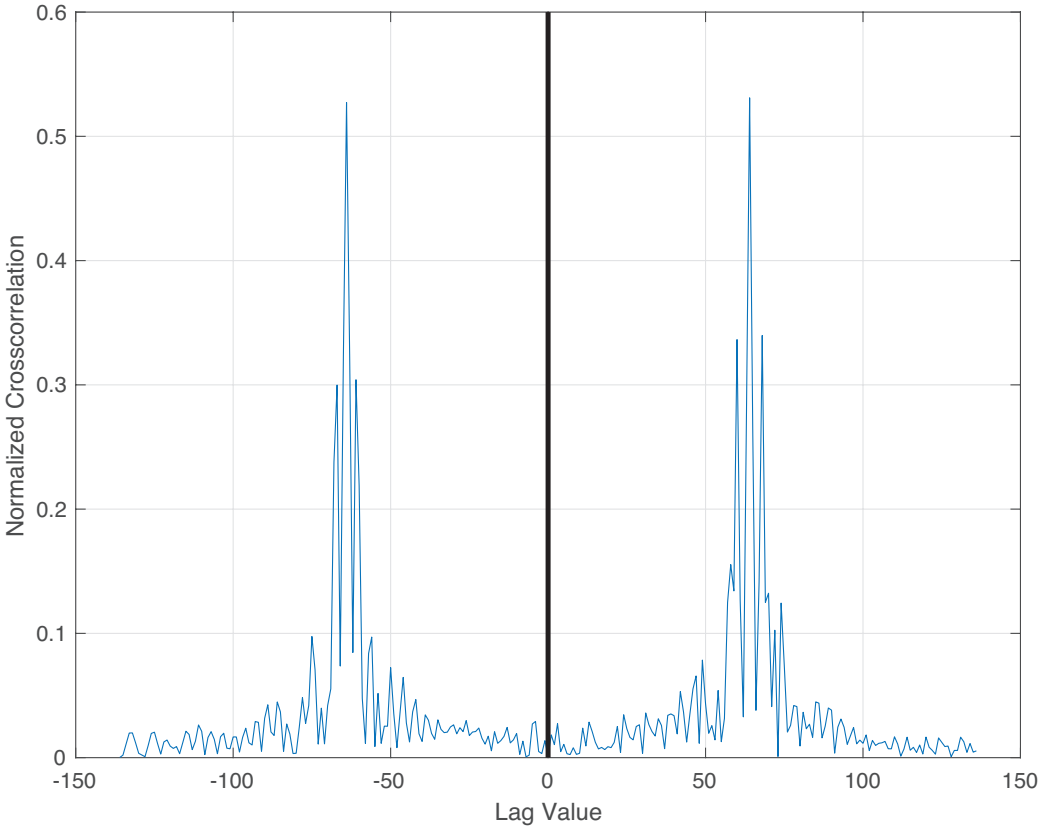

Figure 4.5. DRS cross-correlation.

the waveform, it then throws away the CP portion of each symbol. Ideally, any portion of the symbol that experienced ISI is contained within the CP and thrown away too.

Given these techniques, it is understandable as to why the time-adjacent users were unaffected by the single TA attack executed on the target UE. However, it is unlikely that this is the case for all values of TA. Otherwise, the TA would have no purpose. Therefore, we need to explore the effects on time-adjacent users due to cumulative TA attacks.

4.3 Cumulative TA Command Effects on Time-Adjacent User Equipment

Before exploring the effects on time-adjacent users after the target UE heeds multiple, cumulative TA commands, we need to gain a better understanding of the DRS and the eNB interpretation of what it is receiving. As previously stated, the two DRS

contained within one subframe are orthogonal to one another. However, at non-zero lags, the cross-correlation between the two DRS displays some significant sidelobe behavior as depicted in Figure 4.5.

Figure 4.5 depicts the cross-correlation sequence between two UL DRS within one subframe. In this instance, we have not altered the time-domain waveform in any way, and there is no noise to be taken into account. We have done this to highlight the relationship between the two DRS. What we see here is more-or-less a symmetrical graph. In truth, it is one of these two sidelobes that the receiver chooses to estimate the UL offset. Not coincidentally, if you revisit Figure 4.3 you can see very clearly the two sidelobes on the right-hand side of the figure roughly between offsets 875 and 1,000. In the case of Figure 4.3, the peaks of the sidelobes are asymmetric, and therefore the eNB estimates the channel offset using the highest peak of the two sidelobes. The height of the sidelobe is dependent on the position in the UL waveforms. These waveforms add together at different places depending on the value of the cumulative TA. Thus, their addition can have either constructive or destructive effects on one another. Furthermore, this causes the eNB to randomly choose which sidelobe is used to estimate the timing offset. The reason the choice is random is because the cross-correlation sequence is dependent on the superposition between the two UEs time domain signals. This, combined with the receiver disregarding the negative offsets, is what leads to the incorrect target UE offset calculation, and ultimately a loss of target communications.

Finally, now that we have examined the relationship between the two DRS and how the eNB estimates the offset, our next step was to determine just how much cumulative TA is needed to negatively impact other user BERs. This line of inquiry yielded a limit to the number of cumulative TAs needed before creating issues for time-adjacent users. Thus, in order for an attacker to mitigate their chances of creating collateral damage, they must be aware of how much they are affecting the target signal timing.

Figure 4.6 shows one instance of the time-adjacent user BER as a function of cumulative TA. UE0 (blue) is the time-adjacent user whose subframes arrive at the eNB before the UL of the target UE, and UE2 (orange) is the time-adjacent user whose subframes arrive at the eNB after the target UE UL. The extreme left and right on the horizontal axis represents one full subframe overlap. On the left, we have the BER of the time-adjacent user

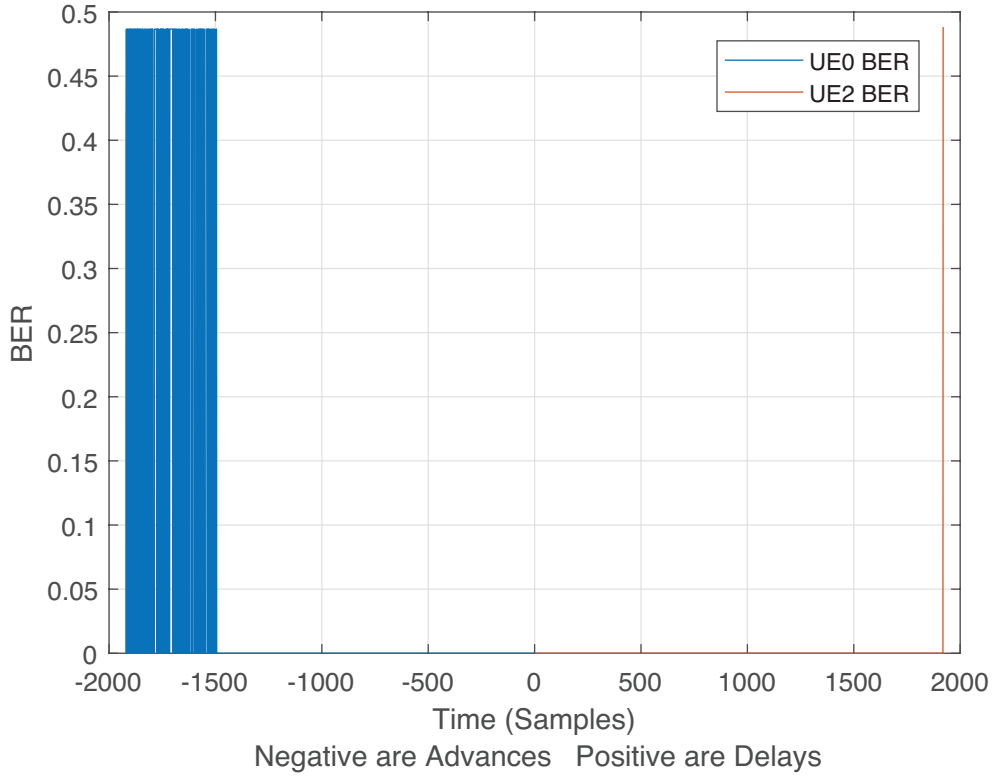

Figure 4.6. Single trial BER as a function of estimated timing offset.

whose UL arrives before the target UL. On the right, we show the BER of the time-adjacent user whose UL arrives after the target UL. The left half of the graph represents a timing *advance* from no advance at time zero to full subframe overlap on the left. Here, the the target UE was forced to transmit too early whereas the right half of the graph depicts timing *delays* from no delay at time zero to full subframe overlap on the right. In this case, the target UE was forced to transmit later than the eNB expected.

However, one instance does not fully characterize the expected behavior of the attack. Therefore, in Figure 4.7, we have performed 10,000 trials of the same process in Figure 4.6 and averaged the results across each value of cumulative TA ranging from -1920 to +1920.

To examine the trends in the data, we will utilize Figure 4.7. First, we examine the effects on UE0 on the left hand side of the figure. Here, we see that the BER is no longer

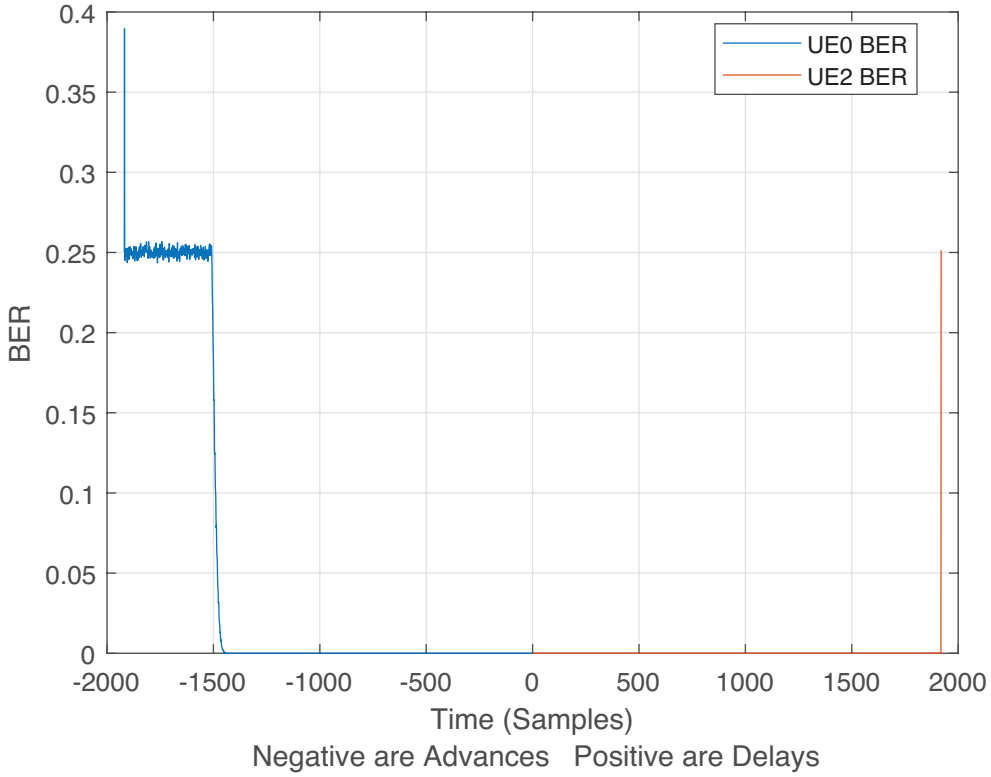

Figure 4.7. Average BER as a function of estimated timing offset. (n = 10,000)

zero once the cumulative TA has advanced the signal by at least 1437 samples (i.e., samples corresponding to -1920 to -1437). In the region between 0 and -1436 offset, the eNB is able to correct for the interference experienced by UE0. This is because in this region of cumulative TA, the target DRS is not interfering with the channel estimation process the eNB is performing on the UE0 UL. Therefore, the eNB can accurately determine when the time-adjacent user, UE0, subframe arrived. On the other hand, in the region on the left of -1436 samples, both of the target UE DRS have interfered with the UE0 waveform.

The presence of both the target UE DRSs effects the ability of the receiver to estimate where the UE0 subframe actually begins. Therefore, when the eNB attempts to estimate the UE0 channel offset, it sometimes associates the target UE DRS as the time-adjacent user, UE0, DRS. Thus, the eNB applies this incorrectly determined offset to UE0, thereby wrongly associating the target UE UL as the UE0 UL.

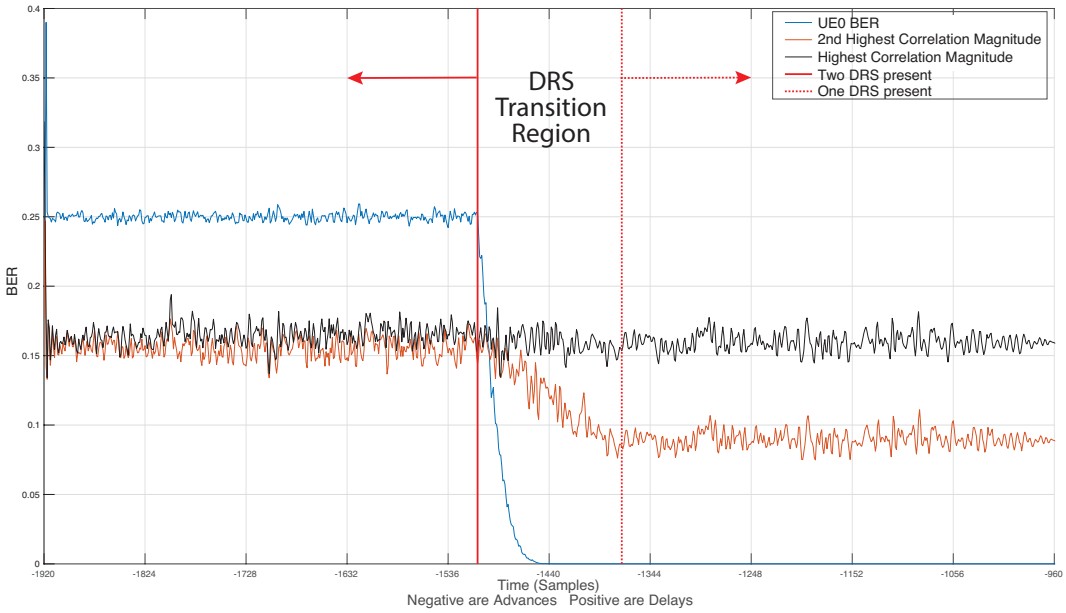

Figure 4.8. The relationship between UE1 BER and the target UE DRS.

To gain a better understanding of what is occurring here, refer to Figure 4.8. In this figure, we have kept the blue line that represents the UE0 BER. In addition, we have zoomed-in to the relevant portion of the graph. The black and orange lines represent the largest and second-largest correlation values, which are used by the eNB to determine the UE0 offset. In the region to the left of the solid red line, both DRS from the target UE are interfering with the UE0 waveform. Also in this region, we see that the orange and black lines are very close to one another. This is the key as to why UE0 experiences disruptions. Every black-orange pair of points for each TA is associated with either UE0 or the target UE, but the eNB cannot distinguish between them. Therefore, because the eNB only uses the largest correlation value, it sometimes chooses the offset corresponding to the target UE and it sometimes chooses the correct offset associated with UE0.

Furthermore, the region between the solid and dashed red lines is the region where one of the target UE DRS is in transition between interfering with and not interfering with the UE0 waveform. As the number of samples the UL has been advanced decays (i.e., moving left to right) the less-and-less the UE0 BER is affected as demonstrated by the downward trajectory of the blue line in this region. Additionally, there is a noticeable separation that begins between the black and orange lines. This separation is indicative of

the fact that the eNB is better able to discern the offset value associated with UE0 and ignore the effects of the time-advanced target UL. At approximately -1440 samples, the eNB no longer confuses the correlation values, allowing the eNB to communicate effectively with the non-targeted, time-adjacent UE0.

Of note, there is anomalous behavior corresponding to a cumulative TA of -1918 samples. Here, the average BER is 39% whereas as the approximate BER for all other TAs between -1920 and -1437 samples is approximately 25%. The reason for this peak is again due to the interaction between the overlapping DRSs. This specific instance is where one DRS is shifted by two samples and then added to itself. Here, the autocorrelation between this new sequence and the reference DRS peaks at an offset indicating a delay of one sample, not zero. In other words, at this specific instance, and only at this instance, the eNB tends to decide on the incorrect offset value more often than the correct value. In contrast, at all other delays in the interval between -1920 and -1437 samples, the eNB is equally likely to choose either the correct or the incorrect offset. Ultimately, the result is insignificant since we know a non-zero BER is incurred long before reaching a cumulative TA corresponding to -1918 samples.

Next, we analyze the right half of the graph associated with timing delays and the UE2 BER. In this instance, the BER is reliably zero up until the target UE is delayed by a full subframe, 1920 samples. At this point, the graph matches the behavior on the far left-hand side, where the time-adjacent user has an average BER of approximately 25%. The reason for the zero BER until the UL of the target UE fully coincides with the UE2 subframe is again because of how the eNB carries out the channel estimation process. As the target UE DRS begin to spill over into the UE2 UL transmission, the cross-correlation sequence at the eNB does not detect two sets of DRS. As before, the eNB discards all cross-correlation values indicating a negative offset. In other words, the presence of the target UE DRS in the UE2 waveform would be construed as the UE2 UL being time-advanced *if* the eNB considered negative offsets. Therefore, the eNB correctly identifies the beginning of the UE2 subframe in every case where the target UE UL is delayed, enabling communications between UE2 and the eNB.

Lastly, the edge cases where the target UE's UL has been advanced or delayed an entire subframe share similar BERs. In this case, the eNB undoubtedly chooses to correct

offset for both UE0 and UE2. This occurs because the DRS have essentially been magnified, leaving no chance for the eNB to choose the incorrect offset. Therefore, we estimate that it is at this point where the interference between the two signals becomes too great for the error mitigation techniques to overcome. However, more research would need to be conducted to verify this claim.

4.4 Summary

Here, we have demonstrated our numerical results of the effects on BER due to a single TA command and cumulative commands. Additionally, we have conveyed the effects from the perspective of both the target UE, and the time-adjacent UEs. Moreover, we analyzed these results and provided the reader with explanations for our outcomes. Finally, we concluded that the most effective implementation of this attack would be to advance the UL of the target UE transmission. An unanticipated advance of the UL (by the eNB) causes the greatest effect to the target while also mitigating collateral damage to the time-adjacent users.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 5:
Conclusion and Future Work

This research is a continuation of previous work conducted by the authors. We have presented results supporting the conclusion that there exists a legitimate LTE vulnerability, which is a product of its unsecured TA mechanism.

5.1 Conclusion

Previously, we concluded that the reason this vulnerability inflicts communication failures was due to ISI between multiple users' UL. However, upon completion of this research, we would re-classify the cause of damage as an attack on the eNB-UE time synchronization. This DoS attack inhibits the ability of the eNB to determine where to look in the time-frequency space for the targeted user's UL. Such an attack renders the target UE-eNB communication link useless. Specifically, time-advancing the target UE UL transmission (i.e., commanding the UE to transmit early) quickly sends its BER to 50% while leaving the time-adjacent user unaffected. It is not until the target UE UL is cumulatively advanced by approximately 1440 samples that UE0 is also effected by the attack. At this point, the UE0 BER steadily increases. Once the target UE UL is cumulatively advanced by 1508 samples, then the expected UE0 BER is 25%. On the other hand, the time delayed time-adjacent user, UE2, does not incur a non-zero BER until the target UE UL fully overlaps the UE2 UL subframe. Similarly, the target UE is unaffected by false timing delays because the eNB corrects for signal delays.

By leveraging the unprotected TA command, and taking advantage of how the eNB estimates a UE transmission, we can definitively say that an attack of this type can put LTE user communications at risk. Moreover, if someone wanted to subject just a single user to an attack, they could do so by slightly advancing (sending early) that user's UL. This method of attack inflicts the maximum effect while also reducing the risk of inflicting unintended damage to the time-adjacent users.

Furthermore, this sort of attack is not limited in scope to LTE. Any TDMA-based services implementing unprotected timing mechanisms are likely candidates for attacks of

this sort. Lastly, as 5G begins to come online, we can only foresee a future where security and protection become more significant.

Moreover, the next generation of wireless communications technology, 5G, plans to continue utilizing the TA. We have found no reference or publication indicating that TA security is being addressed in the design of 5G technologies. Therefore, we can reasonably assume that this security vulnerability will persist even as communications technology advances into the future.

5.2 Future Work

Presented here are three potential follow-on projects. First, improvements can be made to more accurately model real-world scenarios. Implementing features such as noise, channel fading and spatial multiplexing may better characterize attack effects. Additionally, more research into the edge-cases may prove beneficial. For example, an explanation and verification of the cause of the non-zero BER when there is full subframe overlap between the target UE and the time-adjacent UEs may be beneficial. Specifically, understanding the exact cause of the BER may help to better tailor an attack so as to minimize unintended consequences. Not insignificantly, this research may lead to proposing more effective security measures leading to greater communications security.

Next, one could investigate the marginal effects of different error correction techniques. To reduce bit errors, LTE implements various tools including the cyclic prefix, OFDM/SC-FDMA, error correction techniques, and channel estimation. A more in-depth investigation on the marginal benefits each has may lead to more effective attacks and/or signal security.

5.2.1 Proof of Concept

Lastly, a substantial research opportunity would be if someone were to develop a proof of concept and execute an attack of this sort. This entails programming a transceiver that can communicate with LTE handsets and issuing commands to those handsets. However, at least one significant hurdle to accomplishing this is how to address a user's handset.

APPENDIX: Model Code

A.1 Main.m

```
1
2  %LT James Long
3  %Dr. John Roth
4  %% Thesis
5
6  clear; clc; close all; %tabula rasa
7
8  %% Create LTE compatible UL signal.
9  % Uplink reference measurement channel (RMC/FRC) configuration
10 % Output is a structure containing the configuration parameters required
11 % to generate a given reference channel waveform
12 RMC = "A1-1";
13 frc=lteRMCUL(RMC);
14 %Generate just one subframe (and not the default 10).
15 frc.TotSubframes=1;
16 %% Randomly generate UE1/2 payload (PUSCH data) to transmit and process
17 UE0txdata=randi([0 1], frc.PUSCH.TrBlkSizes(1)*frc.TotSubframes, 1);
18 UE1txdataSF0=randi([0 1], frc.PUSCH.TrBlkSizes(1)*frc.TotSubframes, 1);
19 UE1txdataSF1=randi([0 1], frc.PUSCH.TrBlkSizes(1)*frc.TotSubframes, 1);
20 UE2txdata=randi([0 1], frc.PUSCH.TrBlkSizes(1)*frc.TotSubframes, 1);
21
22 %acquire the PUSCH indicies for 'A1-1'
23 PUSCHind = ltePUSCHIndices(frc,frc.PUSCH);
24
25 %% generate waveforms
26 [UE0txWaveform,grid0,rmccfgout0] = lteRMCULTool(frc, UE0txdata);
27 [UE1txWaveformSF0,grid1SF0,rmccfgout1SF0] = lteRMCULTool(frc, UE1txdataSF0);
28 [UE1txWaveformSF1,grid1SF1,rmccfgout1SF1] = lteRMCULTool(frc, UE1txdataSF1);
29 [UE2txWaveform,grid2,rmccfgout2] = lteRMCULTool(frc, UE2txdata);
30
31 figure (1)
32 xcorr(UE0txWaveform(412:412+136),UE0txWaveform(.5*1920+412:.5*1920+412+136),'coeff')
33 x=-136:136;
34 plot(x,abs(ans))
35 grid on
36 hold on
37 ylabel('Normalized Crosscorrelation')
38 xlabel('Lag Value')
39 title('Crosscorrelation between the 2 DRS in one Subframe')
40 plot([0 0],[0 .6],'k','LineWidth',2.3)
41
42 %% allocate memory and start with orignal waveform for each iteration
43 % each column is a different iteration
```

```
zerofront=complex(zeros(31,64));
zeroend=complex(zeros(32,64));
manipWAVE0=repmat(UE0txWaveform,[1,64]);
manipWAVE1=repmat(UE1txWaveformSF0,[1,64]);
manipWAVE2=repmat(UE2txWaveform,[1,64]);

% append complex zeros on either side of the waveform s.t. all we need
% to do is slide through each column to see what is rxd at the rxr
% depending on the TA
manipWAVE11=[zerofront; manipWAVE1];

rxWAVE0=manipWAVE0;
rxWAVE1=zeros(1920,64);
rxWAVE2=manipWAVE2;

% %preallocate memory and estb some things as cell arrays
UE0RxGrid=cell(1,64);    %each element is a resource grid
UE0rxCw=cell(1,64);      %each element is a series of 1728 bits
UE0symbols=cell(1,64);   %each element is a series of 864 soft bits
UE0trblkout=cell(1,64);  %each element is a series of 600 decoded bits
UE0blkcrc=cell(1,64);    %each element is a scalar indicating success of decoding
numerr0=zeros(1,64);     %each element is a scalar indicating number of bit errors
BER0=zeros(1,64);        %each element is a scalar indicating BER

%preallocate memory and estb some things as cell arrays
UE1RxGrid=cell(1,64);    %each element is a resource grid
UE1rxCw=cell(1,64);      %each element is a series of 1728 bits
UE1symbols=cell(1,64);   %each element is a series of 864 soft bits
UE1trblkout=cell(1,64);  %each element is a series of 600 decoded bits
UE1blkcrc=cell(1,64);    %each element is a scalar indicating success of decoding
numerr1=zeros(1,64);     %each element is a scalar indicating number of bit errors
BER1=zeros(1,64);        %each element is a scalar indicating BER

% %preallocate memory and estb some things as cell arrays
UE2RxGrid=cell(1,64);    %each element is a resource grid
UE2rxCw=cell(1,64);      %each element is a series of 1728 bits
UE2symbols=cell(1,64);   %each element is a series of 864 soft bits
UE2trblkout=cell(1,64);  %each element is a series of 600 decoded bits
UE2blkcrc=cell(1,64);    %each element is a scalar indicating success of decoding
numerr2=zeros(1,64);     %each element is a scalar indicating number of bit errors
BER2=zeros(1,64);        %each element is a scalar indicating BER


for TA=0:63
    if TA<32
    %cannot have non-postive integers as indices
    rxWAVE1(:,TA+1)=manipWAVE11(TA+1:TA+1920,TA+1);
    [offset(TA+1),corr{TA+1}] = lteULFrameOffset(frc,frc.PUSCH,rxWAVE1(:,TA+1));
    CORRECTwave{TA+1}=[rxWAVE1(1+offset(TA+1):end,TA+1); manipWAVE11(end-offset(TA+1)+1:
        end,TA+1)];
```

```
93      UE1RxGrid{TA+1} = lteSCFDMADemodulate(frc,CORRECTwave{TA+1});
94      [UE1rxCw{TA+1},UE1symbols{TA+1}] = ltePUSCHDecode(frc,frc.PUSCH,UE1RxGrid{TA+1}(
            PUSCHind));
95      [UE1trblkout{TA+1},UE1blkcrc{TA+1},~] = lteULSCHDecode(frc,frc.PUSCH,frc.PUSCH.
            TrBlkSizes(1),UE1rxCw{TA+1},[]);
96      end
97
98      if TA>31
99      % incoming back-to-back subframes due to advancement of signal
100     rxWAVE1(:,TA+1)=[UE1txWaveformSF0(TA-30:end); UE1txWaveformSF1(1:TA-31)];
101     % estimate the offset based on the incoming waveform
102     [offset(TA+1),corr{TA+1}] = lteULFrameOffset(frc,frc.PUSCH,rxWAVE1(:,TA+1));
103     %based off of what the rxr believes the delay to be, create the
104     %associated waveform
105     CORRECTwave{TA+1}=[UE1txWaveformSF0(TA-30+offset(TA+1):end); UE1txWaveformSF1(1:TA-31+
            offset(TA+1))];
106     % continue the demodulation process
107     UE1RxGrid{TA+1} = lteSCFDMADemodulate(frc,CORRECTwave{TA+1});
108     [UE1rxCw{TA+1},UE1symbols{TA+1}] = ltePUSCHDecode(frc,frc.PUSCH,UE1RxGrid{TA+1}(
            PUSCHind));
109     [UE1trblkout{TA+1},UE1blkcrc{TA+1},~] = lteULSCHDecode(frc,frc.PUSCH,frc.PUSCH.
            TrBlkSizes(1),UE1rxCw{TA+1},[]);
110     end
111
112     % calculate BER for each iteration
113     [numerr1(TA+1),BER1(TA+1)]=biterr(UE1txdataSF0, UE1trblkout{TA+1});
114
115     if TA<31 %% delay loop: UE1's symbols affect UE2
116       rxWAVE2(1:31-TA,TA+1)=manipWAVE2(1:31-TA,TA+1)+manipWAVE1(end-(30-TA):end,TA+1);
117     end
118
119     if TA>31 %%advance loop: UE1's symbols affect UE0
120       rxWAVE0(end-(TA-32):end,TA+1)=manipWAVE0(end-(TA-32):end,TA+1)+manipWAVE1(1:TA-31,TA
              +1);
121
122     end
123
124     %proceed with the rx series of systems to get data back
125     UE0RxGrid{TA+1} = lteSCFDMADemodulate(frc,rxWAVE0(:,TA+1));
126     [UE0rxCw{TA+1},UE0symbols{TA+1}] = ltePUSCHDecode(frc,frc.PUSCH,UE0RxGrid{TA+1}(
            PUSCHind));
127     [UE0trblkout{TA+1},UE0blkcrc{TA+1},~] = lteULSCHDecode(frc,frc.PUSCH,frc.PUSCH.
            TrBlkSizes(1),UE0rxCw{TA+1},[]);
128
129     % calculate BER for each iteration
130     [numerr0(TA+1),BER0(TA+1)]=biterr(UE0txdata, UE0trblkout{TA+1});
131
132     % proceed with the rx series of systems to get data back
133     UE2RxGrid{TA+1} = lteSCFDMADemodulate(frc,rxWAVE2(:,TA+1));
```

```
134         [UE2rxCw{TA+1},UE2symbols{TA+1}] = ltePUSCHDecode(frc,frc.PUSCH,UE2RxGrid{TA+1}(
                PUSCHind));
135         [UE2trblkout{TA+1},UE2blkcrc{TA+1},~] = lteULSCHDecode(frc,frc.PUSCH,frc.PUSCH.
                TrBlkSizes(1),UE2rxCw{TA+1},[]);
136
137        % calculate BER for each iteration
138         [numerr2(TA+1),BER2(TA+1)]=biterr(UE2txdata, UE2trblkout{TA+1});
139
140     end
141
142     % Generate Plots
143     TA=0:63;
144     figure (2)
145     plot(TA(1:32),BER1(1:32),'LineWidth',2)
146     grid on
147     hold on
148     plot(TA(32:end),BER1(32:end),'LineWidth',2)
149     plot(31,BER1(32),'k*')
150     % plot(TA, repmat(mean([BER1(1:31) BER1(33:end)]),1,length(TA)),'k','LineWidth',2)
151     ax=gca;
152     ax.XDir='reverse';
153     xlabel({'Timing Advance Values (0-63)','Real Time (-16.15 to +16.67 \musec)'});
154     ylabel('BER');
155     % legend('Delay','Advance','Neither A or D','Location','Best')
156     xlim([0 63]);
157     % title('BER as a function of TA values 0-63');
158
159     figure (3)
160     plot(TA,BER0,'LineWidth',2)
161     grid on
162     hold on
163     xlabel({'Timing Advance Values (0-63)','Real Time (-16.15 to +16.67 \musec)'});
164     ylabel('BER');
165     xlim([0 63]);
166     title('BER as a function of TA values 0-63');
167
168     figure (4)
169     plot(TA,BER2,'LineWidth',2)
170     grid on
171     hold on
172     xlabel({'Timing Advance Values (0-63)','Real Time (-16.15 to +16.67 \musec)'});
173     ylabel('BER');
174     xlim([0 63]);
175     title('BER as a function of TA values 0-63');
176
177     overlap=-1920:1:1920;
178     overUE0wave=repmat(UE0txWaveform,[1,1921]);
179     overUE2wave=repmat(UE2txWaveform,[1,1920]);
180
181     for k=1:length(overlap)
```

```
182     if k<1922
183     %the case for an advance of 1920 samples to 1.
184     overUE0wave(k:end,k)=UE0txWaveform(k:end)+UE1txWaveformSF0(1:end-k+1);
185     [offset2(k),corr{k}] = lteULFrameOffset(frc,frc.PUSCH,overUE0wave(:,k));
186     if offset2(k)== 0
187         offUE0wave(:,k)=overUE0wave(:,k);
188     else
189         offUE0wave(:,k)=[overUE0wave(1+offset2(k):end,k); UE1txWaveformSF0(end-offset2(k)
                +1:end)];
190     end
191     %proceed with the rx series of systems to get data back
192     overUE0RxGrid{k} = lteSCFDMADemodulate(frc,offUE0wave(:,k));
193     [overUE0rxCw{k},overUE0symbols{k}] = ltePUSCHDecode(frc,frc.PUSCH,overUE0RxGrid{k}(
            PUSCHind));
194     [overUE0trblkout{k},overUE0blkcrc{k},~] = lteULSCHDecode(frc,frc.PUSCH,frc.PUSCH.
            TrBlkSizes(1),overUE0rxCw{k},[]);
195
196     %calculate BER for each iteration
197     [overnumerr0(k),overBER0(k)]=biterr(UE0txdata, overUE0trblkout{k});
198
199     end
200
201     if k>1921
202     %the case for a delay of 1 sample to 1920.
203     overUE2wave(1:k-1921,k-1921)=UE1txWaveformSF0(end-(k-1922):end)+UE2txWaveform(1:k
            -1921);
204     %all offset values are equal to 0. therefore the eNB will NOT try to
205     %compensate for delay in UE transmissions from UE2
206     [offset3(k-1921),corr3{k-1921}] = lteULFrameOffset(frc,frc.PUSCH,overUE2wave(:,k-1921)
            );
207
208     %proceed with the rx series of systems to get data back
209     overUE2RxGrid{k-1921} = lteSCFDMADemodulate(frc,overUE2wave(:,k-1921));
210     [overUE2rxCw{k-1921},overUE2symbols{k-1921}] = ltePUSCHDecode(frc,frc.PUSCH,
            overUE2RxGrid{k-1921}(PUSCHind));
211     [overUE2trblkout{k-1921},overUE2blkcrc{k-1921},~] = lteULSCHDecode(frc,frc.PUSCH,frc.
            PUSCH.TrBlkSizes(1),overUE2rxCw{k-1921},[]);
212
213     %calculate BER for each iteration
214     [overnumerr2(k-1921),overBER2(k-1921)]=biterr(UE2txdata, overUE2trblkout{k-1921});
215     end
216 end
217
218
219 figure (5)
220 plot(overlap(1:1921), overBER0)
221 hold on
222 plot(overlap(1922:end), overBER2);
223 xlabel({'Time (Samples)','Negative are Advances   Postive are Delays'});
224 ylabel('BER');
```

```
225 legend('UE0 BER','UE2 BER','Location','Best')
226 grid on
227 title('BER as a Function of Time-Domain Sample Overlap');
228
229 % The following figure magnifies the amplitude of the DRS 20 times.
230 % Ultimately, insignifcant, but aids the user in identifying the DRS
231 grid0(:,[4 11])= 20*grid0(:,[4 11]);
232 wavey=lteSCFDMAModulate(frc,grid0);
233 figure (6)
234 plot(real(wavey));
235 hold on
236 plot([0 0],[-2.5 2],'r','LineWidth',2);
237 plot([138 138],[-2.5 2],'r','LineWidth',2);
238 plot([1098 1098],[-2.5 2],'k','LineWidth',2);
239 plot([275 275],[-2.5 2],'r','LineWidth',2);
240 plot([412 412],[-2.5 2],'r','LineWidth',2);
241 plot([549 549],[-2.5 2],'r','LineWidth',2);
242 plot([686 686],[-2.5 2],'r','LineWidth',2);
243 plot([823 823],[-2.5 2],'r','LineWidth',2);
244 plot([967 967],[-2.5 2],'k','LineWidth',2);
245 plot([960 960],[-2.5 2],'r','LineWidth',2);
246 plot([1098 1098],[-2.5 2],'k','LineWidth',2);
247 plot([1235 1235],[-2.5 2],'k','LineWidth',2);
248 plot([1372 1372],[-2.5 2],'k','LineWidth',2);
249 plot([1509 1509],[-2.5 2],'k','LineWidth',2);
250 plot([1646 1646],[-2.5 2],'k','LineWidth',2);
251 plot([1783 1783],[-2.5 2],'k','LineWidth',2);
252 plot([1920 1920 ],[-2.5 2],'k','LineWidth',2);
253 xlabel({'Time (Samples)'});
254 ylabel('Amplitude');
255 legend('Waveform','SCFDMA Symbols 1-7','SCFDMA Symbols 8-14','Location','Best')
256 title('Real Portion of Time-Domain Waveform highlighting the DRS');
257
258 %Shows how the eNB tracks the delay of the target UE when looking at UE0's
259 %allocated time window
260 figure (7)
261 plot(offset2)
262 grid on
263 xlabel({'Overlap (Samples)'});
264 ylabel('Offset Measurement');
265 title('UE0 DRS Estimation as a function of Overlap');
266 % xlim([-1920 0]);
267 ylim([0 1920]);
268
269 for i=1:1921
270   B{i} = sort(corr{i},'descend');
271   highest(i)=B{i}(1);
272   nexthighest(i)=B{i}(2);
273 end
274
```

```
%plots the highest and 2nd highest correlation values.
figure (8)
plot(1:1921,highest)
hold on
plot(1:1921,nexthighest)

x=(-1920:1:0);
figure (9)
plot(x,nexthighest)

xlabel('Advances No. Samples)')
ylabel('Correlation Magnitude')
title('Plot of 2nd highest correlation value for a given symbol Overlap');
grid on
hold on
plot([-1508 -1508],[0 2],'r','LineWidth',2);
plot([-1371 -1371],[0 2],'k','LineWidth',2);
plot([-412 -412],[0 2],'g','LineWidth',2);
plot(x,highest)
xlim([-1920 0]);
ticks=linspace(-1920,0,11);
xticks(ticks)
legend('2nd Highest Correlation Magnitudes','1st DRS begins to roll off',...
    '1st DRS fully rolled off','2nd DRS fully rolled off',...
    'Highest Correlation Magnitudes');
```

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] Ericsson mobility report. (2019). Ericsson. [Online]. Available: https://www.ericsson.com/assets/local/mobility-report/documents/2019/ericsson-mobility-report-june-2019.pdf. Accessed Jun. 19, 2019.

[2] E. Dahlman, S. Parkvall, and J. Sköld, *4G: LTE-Advanced Pro and the Road to 5G*, 3rd ed. London, UK: Academic Press, 2016.

[3] R. P. Jover, "Security attacks against the availability of lte mobility networks: Overview and research directions," in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, June 2013, pp. 1–9.

[4] Federal Communications Commission. Enforcement Advisory No. 2012-02 FCC Enforcement Advisory Cell Jammers, GPS Jammers, and Other Jamming Devices Consumer Alert: Using or Importing Jammers is Illegal. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/DA-12-347A1.pdf. Accessed July 22, 2019.

[5] J. Reed. (2012). Comments of Wireless@Virginia Tech in the matter of NTIA development of the nationwide interoperable Public Safety broadband network. Virginia Tech. [Online]. Available: http://www.ntia.doc.gov/files/ntia/vatechresponse.pdf

[6] *3GPP; Technical Specification Group Radio Access Network; evolved universal terrestrial radio access (E-UTRA); MAC protocol specification*, TS 36.321, Release 15, 2018.

[7] R. Kreher and K. Gaenger, *LTE Signaling: Troubleshooting and Performance Measurement*, 2nd ed. West Sussex, UK: John Wiley & Sons, Ltd, 2016.

[8] *3GPP; Technical Specification Group Radio Access Network; E-UTRA; Physical layer procedures*, TS 36.213, Release 15, 2018.

[9] *3GPP; Technical Specification Group Radio Access Network; E-UTRA; Physical channels and modulation*, TS 36.211, Release 15, 2015.

[10] C. Cox, *An Introduction to LTE: LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications*, 2nd ed. West Sussex, UK: John Wiley & Sons, Ltd, 2014.

[11] J. D. Roth, M. Tummala, and J. W. Scrofani, "Cellular synchronization assisted refinement (CeSAR): A method for accurate geolocation in LTE-A networks," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Jan 2016, pp. 5842–5850.

[12] B. Sklar, *Digital communications: fundamentals and applications*. Upper Saddle River, N.J: Prentice-Hall PTR, 2001.

[13] *3GPP; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description*, TS 36.201, Release 15, 2018.

[14] Y. Nam, Y. Akimoto, Y. Kim, M. Lee, K. Bhattad, and A. Ekpenyong, "Evolution of reference signals for LTE-advanced systems," *IEEE Communications Magazine*, vol. 50, no. 2, pp. 132–138, February 2012.

[15] X. Hou, Z. Zhang, and H. Kayama, "DMRS design and channel estimation for LTE-advanced MIMO uplink," in *2009 IEEE 70th Vehicular Technology Conference Fall*, Sep. 2009, pp. 1–5.

[16] MathWorks. lteULFrameOffset: PUSCH DM-RS uplink subframe timing estimate. [Online]. Available: https://www.mathworks.com/help/lte/ref/lteulframeoffset.html. Accessed July 22, 2019.

[17] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *IEEE Transactions on Information Theory*, vol. 18, no. 4, pp. 531–532, July 1972.

[18] J. Long and J. Roth, "Novel denial of service vulnerability in long term evolution cellular networks," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Jan. 2019, pp. 7514–7520.

[19] *3GPP; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification*, TS 36.331, Release 15, 2018.

[20] *3GPP; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception*, TS 36.104, Release 10, 2018.

[21] S. Kreher and D. J. Costello, *Error Control Coding*, 2nd ed. Upper Saddle River, New Jersey: Pearson Education, 2004.

[22] F. Tosato and P. Bisaglia, "Simplified soft-output demapper for binary interleaved cofdm with application to hiperlan/2," in *2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No.02CH37333)*, April 2002, vol. 2, pp. 664–668 vol.2.

[23] H. Nourollahi and S. G. Maghrebi, “Evaluation of cyclic prefix length in ofdm system based for rayleigh fading channels under different modulation schemes,” in *2017 IEEE Symposium on Computers and Communications (ISCC)*, July 2017, pp. 164–169.

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California