This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2017 conference.

Need of Physical Layer Security in LTE: Analysis of Vulnerabilities in LTE Physical Layer

T. Pushpalata[1] and Shashikant Y. Chaudhari[2]
Central Research Laboratory, Bharat Electronics Limited, Bangalore, India
Email: [1]tpushpalata@bel.co.in [2]cshashikantyeshwant@bel.co.in

***Abstract*—In Wireless/mobile communication, the requirement of higher throughput and data rates are increasing day-by-day. For meeting this requirement, Long Term Evolution (LTE) technology has become the prime choice. Communication using wireless technology has vulnerabilities. LTE wireless technology has vulnerabilities associated with the processing technique as well as well-defined positioning of channels and signals of physical layer. This drawback is of concern, as it can completely or partially block the communication, due to intentional jamming or unintentional interference. To understand the jamming vulnerabilities in LTE, it is essential to understand various physical channels, signals, frame structure, decoding protocols and various types of jamming. This paper provides jamming vulnerability analysis of LTE physical layer, physical channels and signals. Practical lab test setup for measuring jamming margins along with the result is provided in this paper. Various mitigation techniques have been provided in this paper to reduce jamming vulnerabilities.**

***Index Terms*—LTE. Physical layer security. Jamming. Jamming Margin. Mitigation techniques**

I. Introduction

3rd Generation Partnership Project (3GPP) has standardized Long Term Evolution (LTE) technology to meet the demand of growing data rates and higher throughput for cellular communication. As compared to the existing cellular technology, LTE provides higher data rate, lower latency, higher spectral efficiency and higher capacity [1]. Hence, LTE has become the prime choice to meet the growing demand of high data traffic. LTE has already been proposed for public safety network and is in investigation for end use in military application fields.

Wireless technologies are vulnerable to radio frequency interference and jamming, due to which the communication link may suffer partial or complete blocking. Unfortunately, wireless communication link undergoes unintentional interference and intentional jamming. Like any wireless technology, LTE is also vulnerable to disruption. Various types of attack possible on LTE are Denial of Service (DoS) and information extraction [2]. Typically, DoS is caused by jamming attacks due to which communication link gets disrupted. DoS at higher layers and attacks for extracting information, falls under cyber attack. In this paper, we have focused to assess the physical layer vulnerabilities and threats which can potentially cause DoS by intentional jamming. The objective of the paper is to provide the insight to the jamming vulnerabilities in LTE physical layer and the techniques to mitigate and withstand jamming.

The paper is organized as follows. Section II provides a brief on LTE physical layer, physical channels, signals and frame structure. Section III provides physical layer decoding protocol for downlink (DL). Sections II and III are essential to understand and assess the jamming vulnerabilities in physical layer. Section IV provides jamming types in multi carrier scenario. Section V provides jamming vulnerability analysis of LTE physical layer and Section VI provides the test setup for measuring jamming margin along with the test results. Section VII provides the possible mitigation techniques to overcome jamming vulnerabilities and concluded in Section VIII.

II. LTE Physical Layer

To completely understand and assess the jamming threats associated with physical layer, we have to understand the functionality of “Physical Channels”, “Physical Signals” and the “Frame Structure”. All the physical channels and signals as per 3GPP standard Release 10 in downlink and uplink (UL) has been listed below along with the frame structure.

A. Downlink Physical Channel

A downlink physical channel corresponds to a set of resource elements carrying information originating from higher layers and acts as the interface between 3GPP standard 36.211 [3] and 36.212 [4]. The following downlink physical channels are defined as per 3GPP standard [3]:

1) Physical Downlink Shared Channel (PDSCH): PDSCH carries data and signaling messages from Downlink Shared Channel (DL-SCH). It also carries paging messages from Paging Channel (PCH).
2) Physical Broadcast Channel (PBCH): PBCH carries the Master Information Block (MIB) from the Broadcast Channel (BCH).
3) Physical Multicast Channel (PMCH): PMCH carries multimedia broadcast/multicast service data of Multicast Channel (MCH).
4) Physical Control Format Indicator Channel (PCFICH): PCFICH carries Control Format Indicator (CFI), which carries organization of data and control information in the downlink.
5) Physical Downlink Control Channel (PDCCH): PDCCH carries Downlink Control Information (DCI), which consists of mainly scheduling commands and scheduling grants.

978-1-5090-4442-9/17/$31.00 ©2017 IEEE

6) Physical Hybrid ARQ Indicator Channel (PHICH): PHICH carries hybrid ARQ indicators (HIs). HI is evolved Node-Bs (eNodeBs) acknowledgment of User Equipments (UEs) uplink transmission.

B. Downlink Physical Signal

A downlink physical signal is used by the physical layer but does not carry information originating from higher layers. The following uplink physical signals are defined as per 3GPP standard [3]:

1) Primary Synchronization Signal (PSS): PSS carries information of physical layer identity and is used by User Equipment (UE) for cell acquisition.
2) Secondary Synchronization Signal (SSS): SSS carries information of physical-layer cell-identity group and is used by UE for cell acquisition.
3) Cell-specific Reference Signal (C-RS): C-RS is sent by evolved Node-B (eNodeB) to support channel estimation at UE.
4) MBSFN Reference Signal (MBSFN-RS): MBSFN-RS is reference signal for Multimedia Broadcast Multicast Service (MBMS) and is used for channel estimation.
5) UE-Specific Reference Signal (UE-RS): UE-RS is sent for channel estimation to the UEs using beamforming.
6) Positioning Reference Signal (P-RS): P-RS is sent by eNodeB to support location based services.

C. Uplink Physical Channel

An uplink physical channel corresponds to a set of resource elements carrying information originating from higher layers and acts as the interface between 3GPP standard 36.211 [3] and 36.212 [4]. The following uplink physical channels are defined as per 3GPP standard [3]:

1) Physical Uplink Shared Channel (PUSCH): PUSCH carries data and signalling messages from the Uplink Shared Channel (UL-SCH). PUSCH also carries the Uplink Control Information (UCI), if UE is transmitting data at the same time.
2) Physical Uplink Control Channel (PUCCH): PUCCH carries UCI, in-case UE has to transmit only control information.
3) Physical Random Access Channel (PRACH): PRACH carries random access transmissions from Random Access Channel (RACH).

D. Uplink Physical Signal

An uplink physical signal is used by the physical layer but does not carry information originating from higher layers. The following uplink physical signals are defined as per 3GPP standard [3]:

1) Demodulation Reference Signal (D-RS): D-RS is transmitted by UE in uplink along with PUSCH and PUCCH. D-RS is used by eNodeB for channel estimation.
2) Sounding Reference Signal (S-RS): S-RS is transmitted in uplink, but configured by eNodeB for power reference to support frequency dependent scheduling at eNodeB.

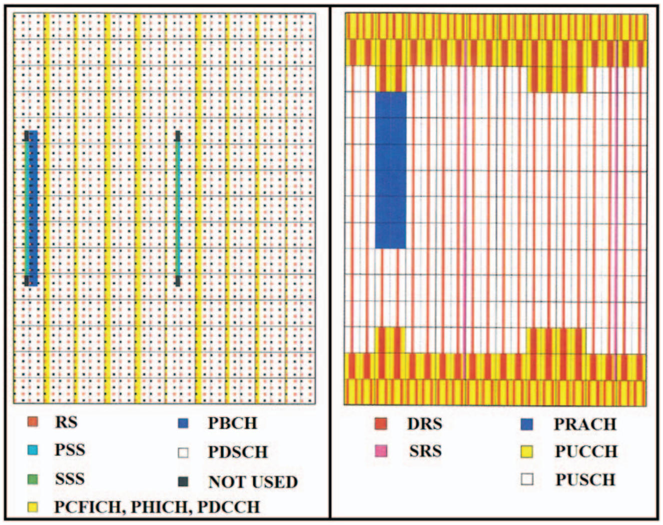

Fig. 1. Downlink and uplink frame structure.

E. Frame Structure

Downlink and uplink frame structure of LTE for 10 ms (x-axis) and 3 MHz bandwidth (y- axis) is shown in Fig. 1. For simplicity, frame structure type 1 of 3GPP standard applicable to FDD duplexing mode has been considered [3]. From the figure it is very much clear that all the physical channels and signals mentioned in the previous sub-section has well defined position in the frame structure. Fig. 1 is provided for a frame length of 10 ms, consisting of 10 subframes. Each subframe is of 1 ms and consists of 2 slots, each of 0.5 ms.

Fig. 1 clearly depicts in DL, PSS and SSS are transmitted twice in a frame situated at center 62 subcarriers and PBCH is transmitted ones in frame at center 72 subcarriers. The Reference Signal (RS) is distributed throughout the frame enabling channel estimation in both time and frequency domain. The control channels (PDCCH, PCFICH and PHICH) are transmitted at the start of every subframe. The width of control channel allocation varies from 1 to 4 OFDM symbols depending on the channel bandwidth and control information for the subframe. The remaining DL lattice is filled with PDSCH.

The UL frame structure is also shown in Fig. 1. D-RS for PUSCH and PUCCH is distributed throughout the frame, enabling channel estimation for PUSCH and PUCCH at eNodeB. SRS help eNodeB to measure the received signal power across a wide transmission bandwidth, hence transmitted in one OFDM symbol. PUCCH is transmitted symmetrically at both the edges of the bandwidth. The PRACH is transmitted over a bandwidth of six resource blocks and duration from one to three subframes, while its position in the resource grid is configured by eNodeB. The remaining UL lattice is filled with PUSCH.

The openness of the frame structure and decoding protocol makes LTE physical layer prone to jamming and eavesdropping [5]. The decoding protocol for downlink has been discussed in the next section.

III. Downlink Physical Layer Decoding Protocol

In order to attach with any base station, the UE has to synchronize with the base station with a procedure called cell acquisition. In the course of synchronization, UE has to search and decode PSS and SSS for obtaining the Cell-ID of the strongest base station. The UE first searches for the PSS in the whole frame. After PSS detection, UE gets the information of Physical Layer Identity ($N_{ID}^{(2)}$) and symbol timing.

After achieving symbol timing, UE searches for SSS, to detect the Physical-layer cell-identity group ($N_{ID}^{(1)}$) and subframe number. As, UE now has the information of both $N_{ID}^{(1)}$ and $N_{ID}^{(2)}$, can derive the Cell-ID of the base station with which it is attached. Indirectly, in the course of decoding SSS, UE gets the information of the duplex mode, cyclic prefix type and frame timing. The information derived in this process is very vital to UE, as without this information, further decoding is not possible.

Once Cell-ID is known to UE, it can decode the PBCH for getting the Master Information Block (MIB). But before decoding PBCH, UE has to perform channel estimation and equalization for receiving the MIB content properly. Hence, UE has to look for the pilot symbols i.e. Cell-specific Reference Signal (C-RS) in the frame. C-RS is a 31-bit Gold sequence, initiated by Cell-ID as a seed value. While decoding C-RS, UE gets channel estimation matrix and the number of antennas base station is using for transmission.

With the help of channel estimation and equalization, UE is now able to remove the impairments from PBCH and decode the content of MIB. The MIB carries the information of operating bandwidth, frame number and PHICH configuration i.e. PHICH duration and PHICH resources. By this procedure, UE has the broadcast message available for further decoding. After receiving broadcast message, UE decodes PCFICH for getting the Control Format Indicator (CFI) value. CFI carries the number of symbols allocated for control channel. Hence, UE has the information of the lattice in the frame, where it has to search for PHICH and PDCCH.

PHICH carries ACK/NACK information of uplink which enables UE to make decision, whether to transmit a new data or retransmit the previous data. For getting the information of scheduled data in the subframe, schedule grant for the new data in uplink and Downlink Control Information (DCI), UE has to decode PDCCH. After this only UE will have the information of resources allocated in PDSCH and hence, will be able to decode the data.

It is clear that in downlink, if UE has to get the information of resource allocation in PDSCH or the information of uplink grant, UE has to decode a chain of physical signals and channels. If any of the physical signal or channel is compromised, then it could lead to disruption of communication link. Hence, it becomes very necessary to analyze the possible threats and the weakest link to harden the physical layer.

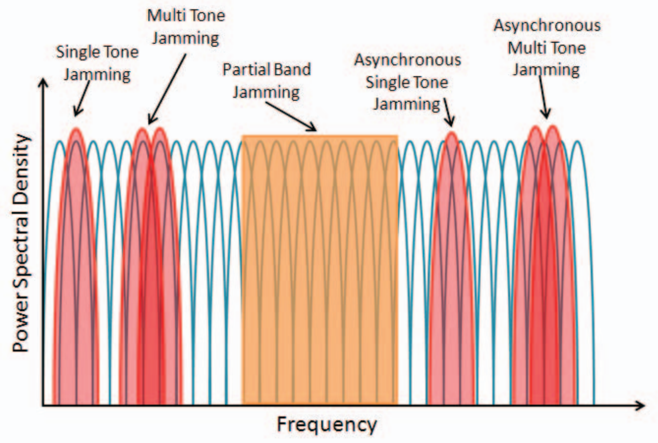

Fig. 2. Jamming types in a multi-carrier scenario.

IV. Types of Jamming

Before analyzing the threats to physical layer, it is essential to know the types of jamming. This section describes different types of narrowband jamming for multi-carrier scenario.

Conventionally, jamming the entire band of the transmitter with band limited noise is inefficient way of jamming. Some of the effective way of jamming are partial band jamming, single tone jamming, multi tone jamming, asynchronous single tone jamming and asynchronous multi tone jamming as shown in Fig. 2.

A. Partial Band Jamming

Partial Band Jamming (PBJ) uses transmission of Additive White Gaussian Noise (AWGN) over specific band. The effectiveness of this type of jamming is directly proportional to the ratio of jamming bandwidth to signal bandwidth, when the jamming power is kept constant [6], [7]. From Fig. 2, it is clear that a portion of continuous subcarrier can be jammed using this method.

B. Single Tone Jamming

Single Tone Jamming (STJ) uses a very high power single impulse of AWGN noise to jam a single subcarrier. This type of jamming requires the knowledge of exact frequency of the subcarrier as shown in Fig. 2. Single tone jamming can also be used to jam the cell specific reference signal to reduce the overall system capacity, but the jammer has to perfectly synchronize itself with the network.

C. Multi Tone Jamming

Multi tone jamming (MTJ) is useful to jam multiple subcarriers. Unlike single tone jamming, it has to generate multiple impulses of AWGN noise [8]. Like single tone jamming, MTJ also requires the knowledge of exact frequency of the subcarrier as shown in Fig. 2.

D. Asynchronous Jamming

Asynchronous type of jamming can be classified into two types Asynchronous Single Tone Jamming (ASTJ) and Asynchronous Multi Tone Jamming (AMTJ) as shown in Fig. 2. The concept of asynchronous jamming is to jam the target signal with a frequency offset to the subcarrier, due to which the jamming signal can interfere with adjacent subcarriers. This type of jamming does not directly jam the signal; instead it creates a scenario of Inter Carrier Interference (ICI) at the receiver [7]. Asynchronous jamming has superior performance as compared to the other jamming types mentioned above.

V. Jamming Vulnerability Analysis of LTE Physical Layer

In this paper the vulnerability assessment in downlink is carried out for synchronization signal, reference signal, broadcast channel, control channel and data channel.

A. Synchronization Signal

As per 3GPP standard, there are two types of synchronization signals in downlink namely PSS and SSS. PSS is generated using Zadoff-Chu (ZC) sequence and SSS is generated using m-sequence [3]. PSS and SSS are located at center 62 subcarriers. As the positions of these signals are fixed in the frame structure, these signals can be jammed using partial band jamming. Unfortunately, if any one of these signals is compromised, further decoding is not possible.

B. Reference Signal

3GPP standard has defined four reference signals in the downlink, out of which C-RS is very important because it is used mandatorily for doing channel estimation to remove the impairments at the receiver by doing channel equalization. The C-RS is distributed throughout the frame, both in frequency and time domain, allowing channel estimation for broadcast channel, control and data channel. If C-RS is jammed, the bit error rate of the complete network would increase tremendously [9], [10]. Resource elements allocated for C-RS in SISO mode are approximately 5% of the complete frame (20 MHz bandwidth) and about 15% in 4×4 MIMO modes [14], [15]. Hence jamming C-RS using MTJ is more effective as compared to complete bandwidth jamming. Jamming C-RS requires the jammer to synchronize with the base station and knowledge of PSS and SSS.

C. Broadcast Channel

Broadcast channel carries MIB information, which is required by any UE to get initial access to the cell. Like PSS and SSS, PBCH is also located at center 72 subcarriers which can be jammed using PBJ [13]. Without PBCH, UE cannot decode PHICH, which carries ACK/NACK information for the uplink. Jamming PBCH does not require the jammer to synchronize with the cell, if the jammer is continuously transmitting at center 72 subcarriers. Anyhow, if jammer wants to jam PBCH in efficient manner by transmitting only at first subframe, then it requires the jammer to get synchronized with the cell. Hence jamming PBCH is more effective as compared to reference signal jamming.

D. Control Channel

According to 3GPP standard, LTE has three control channels in downlink, namely PDCCH, PCFICH and PHICH. For decoding DCI from PDCCH, UE has to decode the CFI value from PCFICH. PCFICH gives the information of the frame structure carrying PDCCH. Hence, PCFICH is the key to decode the control information and becomes highly vulnerable. PCFICH jamming requires the jammer to synchronize with the cell. If PCFICH is jammed, the jammer need not jam PDCCH. Even, if jammer wants to jam PDCCH, it requires the jammer to get synchronized with the cell.

If PHICH is jammed, the downlink communication will not suffer. Anyhow, PHICH jamming has an adversary on uplink, as PHICH information is vital for uplink communication. PHICH jamming also requires the jammer to synchronize with the cell.

E. Data Channel

Jamming PDSCH in the downlink has least threat, as this requires the jammer to decode the protocol till PDCCH. The eavesdropper/sniffer can take the advantage to get the complete system information. PDSCH carries System Information Block (SIB) messages, which are not encrypted. SIB1 message carries vital information like PLMN identity [11], [12], [16], which can be used by attacker for higher layer attacks. SIB2 message carries radio resource configuration [1], one of those configuration is PRACH configuration, which can be used by the attacker to create a scenario where UE has to compromise with PRACH procedure in uplink.

VI. Test Setup for Jamming Margin Measurement

From above section it is clear that PSS, SSS, PBCH and PCFICH are highly vulnerable to RF jamming in DL. PSS, SSS and PBCH can be jammed without the requirement of synchronization. For jamming PBCH in efficient way, it requires the jammer to synchronize with the cell. Even for PCFICH jamming, it requires the jammer to synchronize with the cell and the jammer has to be protocol aware.

This paper provides the lab test setup for measuring the jamming margin of synchronization signal and broadcast channel without getting synchronized with the cell is shown in Fig. 3. The setup consists of transmitter, receiver and a jammer.

The transmitter and receiver shown in Fig. 3 are implemented using PC interfaced with USRP via Ethernet cable. LTE physical layer for both DL and UL is implemented in Matlab using LTE System Toolbox. The physical layer code for both transmitter and receiver is running in individual PC. The Matlab code is interfaced with USRP using Communications System Toolbox Support Package for USRP Radio. The transmitter and receiver are configured to transmit and receive PSS, SSS and PBCH under cell search procedure.

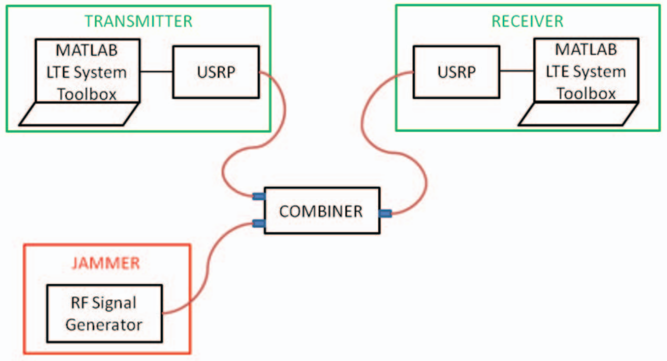

Fig. 3. Test setup for measuring jamming margin.

TABLE I
MEASURED JAMMING MARGIN.

Sl.No.	Signal/Channel	Jamming Margin (J/S)
1.	PSS	3 dB
2.	SSS	10 dB
3.	PBCH	0 dB

The jammer to the setup is introduced using RF signal generator. Jamming signal is generated for center 72 subcarriers and is pushed through RF signal generator. The jamming signal is combined with transmitter signal and fed to the receiver. The gain of the jamming signal is increased in a step of 1 dB to determine the jamming margin of synchronization signal and broadcast channel. The transmitter power is kept constant while conducting the measurement.

The setup was able to handle jamming to signal ratio as shown in Table I. The Jamming margin provided for PSS is against spoofing.

VII. Mitigation Techniques

LTE downlink physical layer has been analyzed for jamming. Based on the previous sections described in this paper, it is clear that, to mitigate jamming, customization at physical layer has to be carried out. Highly vulnerable downlink physical channels/signals to jamming in descending order can be listed as PSS, SSS, PBCH, PCFICH and C-RS.

As PSS and SSS are located at center 62 subcarriers i.e. 0.93 MHz, it is vulnerable to PBJ. One of the possible customization to mitigate this threat would be employing spread spectrum technique to the synchronization signal. The cost paid for this type of customization would be reduction in throughput as compared to the conventional way of transmitting synchronization signal. Other possible customization would be changing the position of PSS and SSS in time domain. By implementing this customization, the jammer will not have frame timing and duplex mode information. This type of customization will prohibit the jammer to attack the physical channels/signals which require synchronization. Lastly, PSS and SSS can use customized way of generating sequence. This type of customization will prohibit eavesdropping.

Like synchronization signals, PBCH is also located at center 72 subcarriers i.e. 1.08 MHz, hence it is also vulnerable to PBJ. The customization discussed for synchronization signal can also be extended to broadcast channel. Securing PBCH against sniffing may require the alteration of position of 21 bits in the frame format of MIB. By employing customization to synchronization signal and broadcast channel, probability of jamming PCFICH and C-RS decreases.

Customizing frame structure could play a vital role to reduce the jamming attacks discussed in this paper. Resource mapping is done at physical layer for all the channels and signals transmitted over the air. Hence, changing the frame format will merely have any implication on higher layers. Instead of all these customization, threat of Barrage Jamming (BJ) still persists. The only key to overcome BJ would be frequency hopping and spread spectrum communication.

VIII. Conclusion

Jamming vulnerability for downlink physical layer of LTE against jamming has been analyzed. It is found that PSS, SSS and PBCH are highly vulnerable to RF jamming, so appropriate mitigation technique has to be applied as discussed in the previous section. For jamming PCFICH, jammer has to get synchronized with the cell. C-RS jamming is a costly affair for jammer, but once jammed can increase the BER of the system tremendously. Jamming of physical channels and signals which requires the jammer to get synchronized with the cell are less vulnerable, because it would lead the jammer to have a decoding protocol. The jammers with decoding protocol are active jammers which are costly, as well as power consumption is high. PDSCH and PDCCH are least vulnerable in terms of RF Jamming. Eavesdropping PDSCH is a threat, as it carries SIB1 and SIB2. PDSCH system information should be encrypted because this information is vital and may lead to higher layer attack.

References

[1] Christopher Cox, *An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications*. John Wiley & Sons Ltd., 2012.

[2] Murat Ogul and Selcuk Baktr, "Practical attacks on mobile cellular networks and possible countermeasures," *Future Internet*, 2013, vo. 5, 474–489; www.mdpi.com/journal/futureinternet.

[3] 3GPP TS 36.211: Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation.

[4] 3GPP TS 36.212: Evolved Universal Terrestrial Radio Access (E-UTRA); Multiplexing and channel coding.

[5] Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, and Jeffrey H. Reed, A Communications Jamming Taxonomy.

[6] J. Luo, J. Andrian, and C. Zhou, "Bit error rate analysis of jamming for OFDM systems," in *Wireless Telecommunications Symposium*, 2007. WTS 2007, pp. 1–8, Apr. 2007.

[7] Chowdhury Shariar, Shabnam Sodagari, Robert McGwier, and T. Charles Clancy, Performance Impact of Asynchronous Off-tone Jamming Attacks against OFDM.

[8] S. Chao, W. Ping, and S. Guozhong, "Performance of OFDM in the presence of multitone jamming," in *Robotics and Applications (ISRA), 2012 IEEE Symposium on*, pp. 118–121, June 2012.

[9] C. S. Patel, G. L. Stuber, and T. G. Pratt, "Analysis of OFDM/MC-CDMA under channel estimation and jamming," in *IEEE Wireless Communications and Networking Conference*, vol. 2, 2004, pp. 954–958.

[10] T. Clancy, “Efficient OFDM denial: Pilot jamming and pilot nulling,” in *Communications (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1–5.

[11] 3GPP TS 36.300: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2.

[12] M. Labib, V. Marojevic, and J. Reed, “Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing,” in *IEEE Conference on Standards for Communications and Networking Proces. (CSCN)*, Oct. 2015, pp. 160–165.

[13] R. P. Jover, J. Lackey, and A. Raghavan, “Enhancing the security of LTE networks against jamming attacks,” *EURASIP J. on Inform. Security*, 2014.

[14] M. Lichtman, J. Reed, T. Clancy, and M. Norton, “Vulnerability of LTE to hostile interference,” in *IEEE Global Conference on Signal and Inform. Proces. (GlobalSIP)*, Dec. 2013, pp. 285–288.

[15] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed, LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation.

[16] Mina Labib, Vuk Marojevic, Jeffrey H. Reed, and Amir I. Zaghloul, “How to Enhance the Immunity of LTE Systems against RF Spoofing,” in *International Conference on Computing, Networking and Communications (ICNC 2016)*, Feb. 2016.