LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation

Marc Lichtman[1], Roger Piqueras Jover[2], Mina Labib[1],
Raghunandan Rao[1], Vuk Marojevic[1], Jeffrey H. Reed[1]
[1]Virginia Tech, Blacksburg, VA, USA
[2]Bloomberg LP, New York, NY, USA

Abstract

LTE is currently being proposed for use in a nationwide wireless broadband public safety network in the US as well as for other critical applications, where reliable communication is essential for safety. Unfortunately, like any wireless technology, disruption of these networks is possible through radio jamming. This article investigates the extent to which LTE is vulnerable to RF jamming, spoofing, and sniffing and assesses different physical layer threats that could affect next-generation critical communication networks. In addition, we examine how sniffing the LTE broadcast messages can aid an adversary in an attack. The *weakest links* of LTE are identified and used to establish an overall threat assessment. Lastly, we provide a survey of LTE jamming and spoofing mitigation techniques that have been proposed in open literature.

Index Terms

Long-Term Evolution (LTE), LTE-Advanced, LTE security, jamming, spoofing

I. Introduction

The Long Term Evolution (LTE) has been standardized by the 3rd Generation Partnership Project (3GPP) to meet the growing demand in cellular data traffic. LTE offers better coverage, enhanced system capacity, higher spectral efficiency, lower latency, and higher data rates than its predecessors in a cost effective manner. True to its namesake, LTE has been be able to keep pace with the rapid evolution of technology by introducing LTE-Advanced (LTE-A) for even higher data rates and capacity, more reliable coverage, and higher spectral efficiency. At the time of writing, there are 422 commercially launched LTE networks in 147 countries, out of which 95 operators have commercially launched LTE-A carrier aggregation systems. LTE/LTE-A is unarguably the primary standard for 4G cellular technology and is

well on its way to becoming the primary global cellular standard. In addition to providing commercial communications services, cellular networks are used to broadcast emergency information, announcing natural disasters and other crises. Over the next decade we will likely become further dependent on commercial cellular networks based on LTE, which is why we must ensure it is secure and available when and where it's needed. Unfortunately, like any wireless technology, disruption through deliberate radio frequency (RF) interference, or jamming, is possible.

In the U.S., LTE is being used as a framework for the nationwide public safety network known as FirstNet. The objective of FirstNet is to provide a nationwide wireless broadband interoperable public safety network that provides reliable communications among first responders. Of greatest concern are emergencies caused by an adversary, such as a terrorist organization, whose attack may involve radio jamming against cellular networks (including FirstNet) to ensure disarray and cause further panic. As such, anti-jamming countermeasures need to be considered.

The U.S. military has considered using ad-hoc LTE-based networks to keep soldiers on the battlefield connected, as well as for shipborne communication with naval aircraft. Unlike military standards, cellular standards are publicly available, meaning that adversaries may leverage this knowledge and target weak points in the protocol to enhance the efficacy of their attacks. Radio jamming attacks are a serious threat to any military or battlefield communications link and must be accounted for.

Attacks on LTE can be grouped into two broad categories: Denial of Service (DoS) and information extraction. Jamming attacks are typically used to cause service disruption or DoS; attacks that extract information or cause DoS by targeting the higher layers fall under the category of cyber-attacks. Radio jamming is broadly defined as an attack in which a jammer transmits energy to disrupt reliable data communication. Jamming is performed through a RF attack vector, while cyber-attacks use network attack vectors. In this article we are only concerned with jamming. An important property of jamming is that it always targets the receiver (as opposed to the transmitter), regardless of how close the jammer is to the transmitting node. Thus, jamming the LTE downlink, the signal transmitted by a base station and received by mobile devices, targets the mobile devices, whereas jamming the uplink targets the base station. RF spoofing refers to transmitting a fake signal meant to masquerade as an actual signal [1].

Protocol-aware jamming attacks against LTE networks are primarily enabled by the openness of the protocol. Moreover, the broadcast messages transmitted by LTE base stations do not use any means of encryption. As a result, all sorts of essential network configuration details can be easily eavesdropped with low-cost software radios, a process we refer to as sniffing. This information can aid attackers in optimizing and crafting attacks against LTE-based networks.

The objectives of this article are to outline and motivate the need for high availability LTE networks, provide insight into physical layer vulnerabilities of LTE, and survey mitigation techniques that can harden the physical layer of next generation LTE and LTE-A deployments. The remainder of this article is organized as follows. Section II provides a brief background on the physical layer of LTE. In Section III we investigate the individual channels and signals of LTE and analyze their vulnerabilities to jamming and spoofing. Section IV offers a comparison of attacks in terms of efficiency and complexity, Section V surveys mitigation techniques found in literature, and Section VI concludes.

II. Background of LTE

Orthogonal frequency-division multiple access (OFDMA) is the channel access scheme used in the LTE downlink. OFDMA uses orthogonal frequency division multiplexing (OFDM) as the underlying modulation scheme and transmits a large number of parallel subcarriers with different blocks designated to different users. For example, when LTE is configured for a 10 MHz bandwidth (the most common configuration in the U.S.), there are 600 subcarriers in the downlink signal. Within one symbol, each subcarrier carries separate bits of information, resulting in information being mapped in both the time and frequency domains. This leads to the OFDM time-frequency lattice, which is a two-dimensional grid used to represent how information is mapped to physical resources. In LTE, one subcarrier over one OFDM symbol interval is called a resource element, as shown in Figure 1. The entire frame is 10 milliseconds long, and frames repeat continuously.

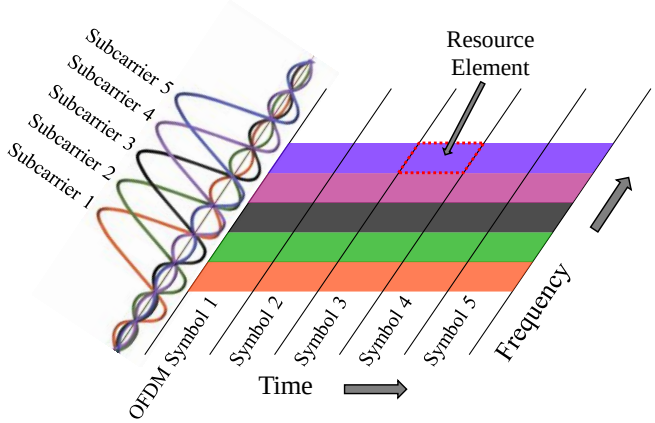

Fig. 1. Depiction of the OFDM time-frequency lattice

Single carrier-frequency division multiple access (SC-FDMA) is the multiple-access scheme used for the LTE uplink. Uplink and downlink transmission happen either in different bands (frequency-division

duplex mode) or in the same band (time-division duplex mode). However, unlike in OFDMA, information is spread across several subcarriers.

LTE user devices–cellphones, tablets, and dongles, among others–are known as User Equipment (UE). The UE accesses the LTE network by connecting to an LTE base station, called an evolved NodeB or eNodeB. A UE typically attaches to only one eNodeB at a time, but constantly monitors the surrounding cells for the purpose of assisting the network in the handover process. In addition, UEs can sometimes roam (depending on the network's policy) in other 4G, 3G, or 2G networks when their home LTE network is unavailable.

The LTE downlink and uplink signals are made up of "physical channels" and "physical signals". These physical channels and signals are multiplexed together in time and frequency, and mapped onto the time-frequency frame lattice. The mapping of physical channels within the LTE frame is defined in the broadcast messages sent by each base station. This method of information mapping allows a jammer to selectively jam information contained in specific Resource Elements (RE) or interfere with specific physical downlink channels or signals. Figures 2 and 3 show the mapping of downlink and uplink LTE frames respectively, when using frequency division duplex mode. Each color represents a different physical control channel or signal, whereas the white spaces represent data.

LTE-A networks are an evolution of LTE. They use the same resource structure as LTE (shown in Figures 2 and 3) and add additional signalling and resources to support carrier aggregation, coordinated multi-point (CoMP) transmission and reception, and other LTE-Advanced features that are beyond the scope of this paper.

III. Vulnerability of Physical Channels and Signals

The following subsections investigate the various LTE physical channels and signals as well as discuss potential threats that could cause communications denial. All threats analyzed in this paper are fundamental to the protocol and thus apply to LTE and LTE-A networks. Table I highlights the parameters associated with each physical channel and signal and will be referenced throughout the remainder of this article.

A. Synchronization Signals

The Primary Synchronization Signal (PSS) is a downlink synchronization signal, received by the UE in order to find and synchronize to a cell (macro-cell base stations typically have three cells, also known as sectors, each). By detecting the PSS, the UE determines the cell's physical layer identity and acquires

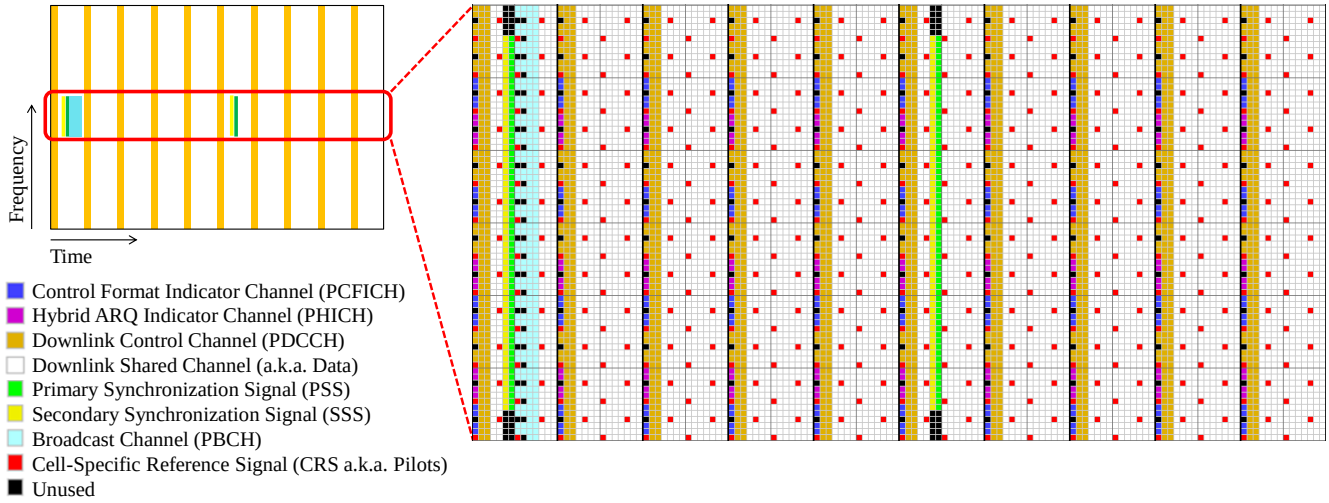

Fig. 2. The LTE Downlink Signal, showing one full 10 millisecond frame (left), and the central 1.4 MHz of the same frame (right)

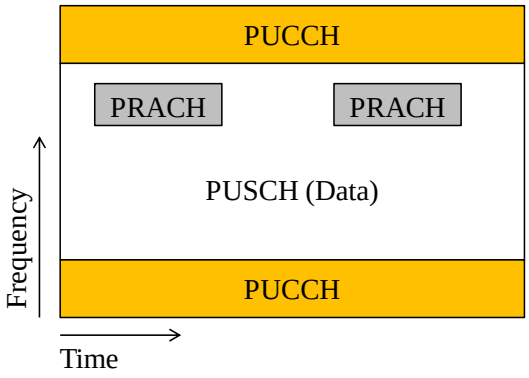

Fig. 3. The LTE Uplink Signal

time and frequency synchronization. The Secondary Synchronization Signal (SSS) provides the UE with the physical cell identity group. The physical cell identity group together with the physical layer identity provides the full Physical Cell Identity (PCI). Through the SSS, the UE also learns about the Cyclic Prefix (CP) type and the duplexing mode used by the cell.

Jamming the PSS or SSS requires fairly high power, because they are designed to be detectable at a low signal-to-noise ratio (SNR). It has been shown that a more effective method for attacking the PSS is to use RF spoofing, to prevent the UE from detecting the real PSS of a given cell [2]. PSS spoofing essentially means that the attacker transmits a fake PSS, asynchronous to the LTE frame (i.e.,

not overlapping in time with the real PSS) and at higher power.

In order to understand the effect of PSS spoofing, we point out that the 3GPP LTE specification states that "the UE needs to search only for the strongest cell" at any given frequency [3]. The LTE specifications do not specify the behavior of the UE when it detects a valid PSS with no associated SSS. Hence, this will be implementation-specific. However, if the PSS and SSS are both spoofed, the 3GPP specification for the Radio Resource Control (RRC) layer [4] states that if the UE is in the idle mode and does not receive the Master Information Block (MIB) message after receiving the PSS and SSS, the UE shall treat this cell as "barred" and is allowed to select the second strongest cell within the same frequency. Since the 3GPP specifications do not allow the UE to select the second strongest cell in most cases, as mentioned before, UE baseband chips may overlook the importance of choosing the second strongest cell in this particular case for the sake of simplifying the interface between the physical layer (PHY) and the RRC layer.

B. Downlink Reference Signal

An OFDM receiver needs to estimate the channel and perform equalization prior to decoding information. In OFDM systems, pilots or reference symbols are therefore transmitted on specific subcarriers in parallel with the data. These reference symbols are generated at the PHY layer and collectively called the Cell-Specific Reference Signal (CRS) in the LTE downlink (see Figure 2). The CRS occupies roughly 14% of the resource elements in a frame. The symbols are modulated with Quadrature Phase Shift Keying (QPSK) and are generated from a length-31 Gold sequence, which is initialized with a value based on the cell ID. The cell ID also determines the location of the CRS in LTE resource lattice.

It has been shown that jamming a subcarrier that carries pilots leads to a higher error rate than jamming one that contains only data [5], [6]. This is so because the adjacent subcarriers are also affected, due to the nature of channel estimation. For a jammer to surgically transmit noise on top of the CRS, it must detect the target eNodeB's PSS and SSS first to retrieve the cell ID. The jammer must also synchronize its transmissions with the target cell, using the PSS and SSS. However, it does not need to be perfectly synchronized, due to LTE's long symbol duration of 66.7 microseconds. Even if the difference in the signal path lengths to the UE were 5 miles, the propagation delay difference would only be 27 microseconds, which could easily be compensated for, if needed, by the jammer transmitting a fraction of a symbol longer each time. This applies to all synchronous jamming attacks discussed in this article.

Asynchronous multi-tone jamming of CRS is also possible for a jammer with a low-complexity transceiver, where there is no need for synchronization of the jammer with the eNodeB. This strategy

involves transmitting noise on all CRS subcarriers (one third of all subcarriers) at a 100% duty-cycle. However, this would come at the cost of about seven times more power than the synchronous case and would lead to a threat that is only slightly more effective than jamming the entire downlink frame.

C. Downlink Broadcast Channel

After synchronizing with the cell and with the help of the CRS, the UE receives more information about the cell by decoding the Master Information Block (MIB), which is transmitted over the Physical Broadcast Channel (PBCH). The MIB contains information essential for initial access to a cell. It consists of 14 bits that contain the downlink system bandwidth, information allowing frame synchronization, and other control information [7]. It is mapped to the center 72 subcarriers, on the first 1 millisecond subframe of every frame. The PBCH is transmitted using QPSK, and uses a 16-bit cyclic redundancy check (CRC) as a form of error detection. Against a 10 MHz signal, PBCH jamming only requires jamming about 10% of the downlink subcarriers with a 3% duty-cycle, making it a very efficient synchronous jamming attack.

While jamming the PBCH is of concern, simply sniffing it may give the adversary information useful to more efficient attacks. Information carried over the PBCH allows the UE to determine the location of the System Information Block (SIB) messages, which are carried over the Physical Downlink Control Channel (PDCCH). These messages indicate the complete configuration of the cell and other critical information of the mobile network, including the eNodeB's idle timer [4], the configuration of the Physical Random Access Channel (PRACH), and the configuration of the Paging Channel (PCH).

As illustrated in Figure 4, which was obtained with the Sanjole LTE sniffing tool, the entirety of the information broadcasted by all eNodeBs in the MIB and SIB messages is sent in the clear. This allows an adversary to sniff this traffic and extract all details about cell and network configurations. For example, sniffing the SIB1 message allows identifying the mobile operator running the eNodeB. In the case of a public safety LTE deployment, a passive sniffer could identify the specific cells that are deployed for critical communications and distinguish them from mobile operator eNodeBs.

Having complete knowledge of the MIB and SIB messages could also be leveraged by an attacker to determine the location of the PRACH in order to efficiently jam it, as discussed in Section III-H. Other types of higher-layer network attacks are enabled as well, such as the control plane "signaling overload" threat [8].

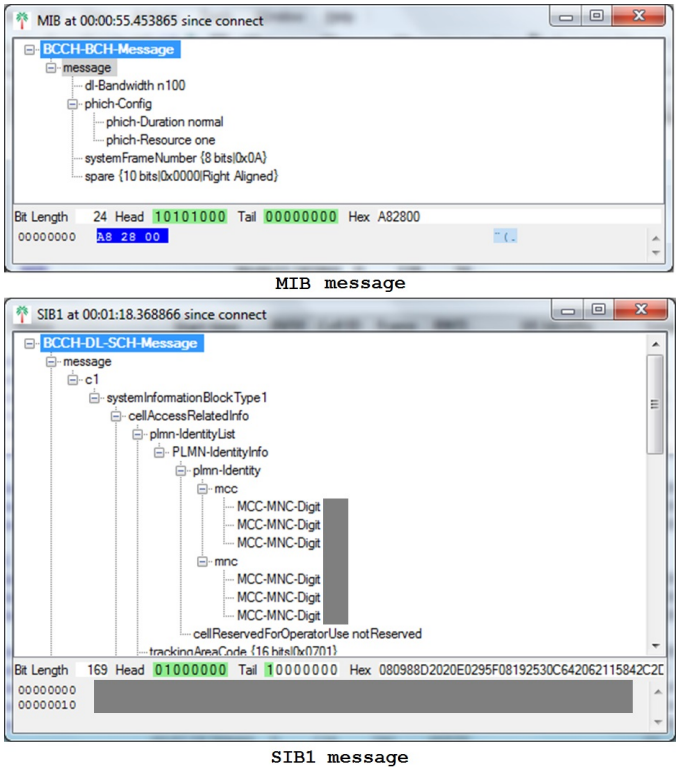

Fig. 4. Real MIB and SIB1 Messages Captured from a Production Network

D. Downlink Control Channels

The Physical Control Format Indicator Channel (PCFICH) is used to send the UE information regarding where the PDCCH is located in the time-frequency lattice. Without successful decoding of this information, the UE will not be able to decode the PDCCH. The PDCCH contains information about the UE uplink and downlink resource allocation, which is vital for receiving LTE service. Although it is possible to jam the PDCCH directly, we will first discuss jamming the PCFICH.

The PCFICH appears only in the first OFDM symbol in each subframe and occupies a total of 16 REs. In other words, it is an extremely sparse channel, making it vulnerable to efficient jamming. Jamming the PCFICH consists of transmitting on top of the 16 REs that carry the PCFICH. The resource elements used for the PCFICH are shown in blue in Figure 2. The resource mapping is not static, but, rather, determined by the eNodeB's PCI [9], which the jammer can acquire through the PSS and SSS. This also limits a PCFICH jamming attack to a single cell, although multiple attacks could be launched by a single jammer.

Jamming the PDCCH also requires synchronization with the cell, but it is much less sparse than the

PCFICH, making it a less effective jamming attack. In addition, since the PDCCH size varies between one and three OFDM symbols, the jammer needs to decode the PCFICH first in order to launch an effective attack with the least amount of power.

E. Hybrid-ARQ Indicator Channel

Positive and negative acknowledgments (ACKs/NACKs) for uplink packets are sent on the downlink channel called the Physical Hybrid-ARQ Indicator Channel (PHICH). The PHICH uses BPSK with repetition-3 coding [9]. This physical channel is fairly sparse, and thus PHICH Jamming is a threat worth considering.

F. Downlink and Uplink User Data

The Physical Downlink Shared Channel (PDSCH) and Physical Uplink Shared Channel (PUSCH) are used to transmit user data from the eNodeB to the UE and vice versa. While surgically jamming these channels is possible, the adversary might as well jam the entire LTE signal. Thus, PDSCH and PUSCH jamming are two of the least important threats to consider.

However, it is possible to jam a specific user's uplink transmissions. Doing so would require extensive decoding of control information and knowledge of the user's temporary mobile identity number. This makes it an extremely complex attack that might be considered a combination of jamming and cyber-attack. We, therefore, do not include it in the vulnerability assessment.

G. Uplink Control Channel

The UE uses the Physical Uplink Control Channel (PUCCH) to send a variety of uplink control information (UCI) to the eNodeB, including scheduling requests, Hybrid Automatic Repeat Request (HARQ) acknowledgments, and channel quality indicators. The UCI is mapped to the resource blocks on the edges of the system bandwidth, as shown in Figure 3. This allows PUCCH jamming to be possible when the jammer only knows the LTE system bandwidth and center frequency. For an uplink bandwidth of 10 MHz, roughly 16 resource blocks (or 192 subcarriers) are allocated to the PUCCH [9]. Therefore, PUCCH jamming requires jamming about 25% - 30% of the uplink system bandwidth. The PUCCH is modulated with a combination of BPSK and QPSK, and uses $1/3$ rate convolutional coding. Because of its low complexity, PUCCH jamming is an important threat to consider. Also, note that uplink jamming has an impact on the entire cell as opposed to locally around the jammer.

TABLE I

PHYSICAL CHANNEL AND SIGNAL MODULATION SCHEME, CODING TYPE AND RATE, SPARSITY, SYNCHRONIZATION REQUIREMENT, AND MINIMUM J/S TO CAUSE DOS

Channel/Signal	Modulation	Coding	Coding Rate	% of REs	Synch. Required	J/S_{CH}	J/S_F
PDSCH	{4,16,64}-QAM	Turbo	Adaptive	85%	No	0 dB	-1 dB
PBCH	QPSK	Convolutional	1/48	0.3%	Yes	0 dB	-25 dB
PCFICH	QPSK	Block	1/16	0.2%	Yes	0 dB	-27 dB
PDCCH	QPSK	Convolutional	1/3	7%	Yes	-5 dB	-16.5 dB
PHICH	BPSK	Repetition	1/3	1.5%	Yes	3 dB	-15 dB
PUSCH	{4,16,64}-QAM	Turbo	Adaptive	$\sim$ 75%	No	0 dB	-1 dB
PUCCH	BPSK, QPSK	Convolutional	1/3	$\sim$ 25%	No	-5 dB	-11 dB
PRACH	Zadoff-Chu Sequence	N/A	N/A	$\sim$ 2%	Yes	10 dB	-7 dB
PSS (Spoofing)	Zadoff-Chu Sequence	N/A	N/A	0.45%	No	3 dB	-20.5 dB
SSS	M-sequences	N/A	N/A	0.2%	Yes	15 dB	-12 dB
CRS	QPSK	N/A	N/A	5%	Yes	5 dB	-8 dB

H. Random Access Channel

After the initial cell search, the UE initiates the random access procedure with the objective to establish a RRC connection with the network. By transmitting the random access preamble on the PRACH, a UE lets the eNodeB know of its presence and that it wants to connect to the cell. The specific location of the PRACH is conveyed to the UE in the SIB2 message, which is carried over the PDCCH. Therefore, to effectively jam the PRACH, the jammer must decode the SIB2 message fields. It is important to note that a successful jamming attack against the PRACH will prevent new UEs from accessing a base station, but will not cause immediate DoS for active UEs. However, any active UE transitioning between idle and connected RRC states will be blocked, resulting in all devices within a cell being blocked within a rather short period of time.

IV. VULNERABILITY ASSESSMENT

We have discussed several jamming and spoofing attacks against LTE. This section compares these attacks in terms of efficiency and complexity to quantify the vulnerability of LTE and determine its weakest links. First, we need to introduce two different ways of measuring the received jammer-to-signal ratio (J/S), that is, the ratio of the received jamming signal power to the received LTE signal power. Two different J/S metrics are required because there are two different ways to observe J/S.

We will define J/S_{CH} as the J/S that only takes into account the specific subcarriers and OFDM symbols (a.k.a. REs) of the channel or signal being jammed. For example, when jamming the broadcast channel (the light blue region in Figure 2), it is assumed the jammer will place its energy on top of the broadcast channel in time and frequency, and not transmit on any other REs. Thus, J/S_{CH} corresponds to the received power from the jammer divided by the received power of only the broadcast channel, not the entire downlink signal.

J/S averaged over an entire frame will be referred to as J/S_F. Using the previous example of jamming the broadcast channel, J/S_F corresponds to the received power from the jammer divided by the received power of the accumulated signal power over the entire 10 ms LTE uplink or downlink frame. The J/S_F metric provides a convenient way to compare each jamming attack against the baseline attack, which is jamming the entire downlink or uplink signal.

Note that J/S alone does not given enough information to determine how large an area around the jammer is jammed (i.e., the radius of effect). Link budgets, which take into account factors like the jammer's transmit power and channel attenuation, are needed to determine such information.

The vulnerability of each channel or signal is based primarily on three factors:

1) The sparsity of the channel with respect to the entire downlink or uplink frame, i.e. the percent of REs used for the channel.
2) The jamming power needed to significantly corrupt the channel or signal, which we measure using the metric J/S_{CH}.
3) The complexity of the jammer required to perform such an attack, mostly based on whether synchronization to the cell is needed or not.

This information for each channel and signal is summarized in Table I. The sparsity can be combined with the minimum J/S_{CH} needed to cause immediate denial of the channel or signal to find an approximation for the corresponding J/S_F. This is an approximation because it assumes a uniform power spectral density across the LTE downlink or uplink signal, which is not the case in real world deployments. From the perspective of a jammer trying to minimize its power consumption and be more difficult to detect, a lower J/S_F is better.

The jamming portion of the vulnerability assessment involved a series of experiments using both simulation and tests with commercial LTE equipment [10]. These experiments were meant to determine the approximate J/S_{CH} needed for each attack to cause DoS. First, we developed each of the downlink jamming attacks using a system bandwidth of 10 MHz and one UE. We used the open-source, 3GPP compliant LTE emulation library known as srsLTE, a library that provides a full physical layer software

radio implementation for both the LTE downlink and uplink. It allows full operation of a software-radio-based eNodeB, with ability to transmit and receive on all physical channels. We define the minimum J/S_{CH} needed for a successful attack as causing either an error rate of 10%, or a failed detection rate of 90%. At these failure rates, DoS is achieved in most cases, making them fairly conservative figures. In addition to using open-source software, we used commercial LTE (test) equipment for certain experiments. The specific eNodeB will not be disclosed due to the sensitive nature of jamming. Throughput was measured for each experiment, and the minimum J/S_{CH} was measured when throughput reached 10% relative to the baseline (no jammer) scenario. Results of these experiments are summarized in the J/S_{CH} column of Table I.

To analyze the effect of RF spoofing, we built a testbed using Rohde & Schwarz's CMW-500 as the legitimate eNodeB. To emulate PSS and SSS spoofing we used srsLTE, along with commercial-off-the shelf software-defined radio hardware. A commercial LTE dongle was connected to a 2nd laptop, which monitored the UE state. For both cases of spoofing, either through PSS or through PSS and SSS, we observed that the UE was not able to camp (i.e., maintain a connection on) the legitimate eNodeB while the spoofing attack occurred at a higher power level. This resulted in the UE being denied LTE service. Even though this corresponds with a J/S_{CH} of 0 dB, a 3 dB "safety-margin" from the perspective of the jammer was added, as seen in Table I. Note that in the comparison we only include PSS spoofing. Performing PSS and SSS spoofing combined requires 3 dB more power in terms of J/S_F. PSS and SSS jamming are not included in the comparison because they require considerably more power and are not efficient attacks.

Based on the information gathered in Table I, we can form an initial threat assessment of the vulnerability of LTE to jamming and RF spoofing. We compare the attacks against a baseline attack, which we define as barrage jamming over the entire LTE system bandwidth on either the downlink or uplink frame. Barrage jamming simply involves transmitting noise (typically Gaussian) over the entire LTE frame. Because there is an efficiency and complexity aspect to each attack, instead of simply ranking them, we have assembled the attacks into a two-dimensional map, shown in Figure 5. From the perspective of a jammer, the most effective attacks are towards the bottom-right. Specifically, we believe that efforts toward hardening LTE for critical communications should focus on addressing possible PSS spoofing, PUCCH jamming, PCFICH jamming, and PBCH jamming attacks.

It is also important to note that, even the most complex attacks can be easily implemented with widely available open-source libraries, low-cost software radio hardware with a budget under $1500 and basic Linux programming skills.

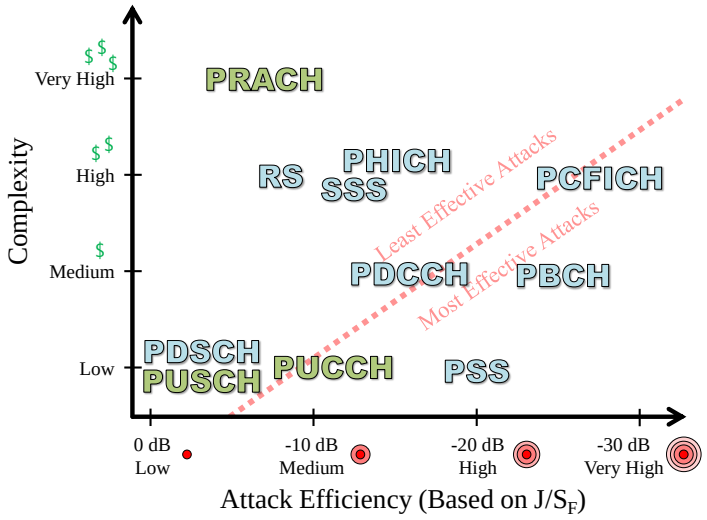

Fig. 5. Ranking of Attacks Based on Jamming Efficiency and Complexity

V. Survey of Mitigation Techniques

Before we discuss methods for mitigating jamming and RF spoofing attacks to LTE, it is important to understand the implications of the changes needed to harden LTE. The cellular technology inside of modern cellphones and other UEs resides in an application-specific integrated circuit (ASIC), sometimes referred to as a system-on-chip or the chipset. On the other side of the link, the eNodeBs typically use a baseband unit that does most of the processing in software, and an RF module handles the RF chain. Thus, changes to the behavior in the eNodeB likely only require a firmware update, whereas changes to the UE require a new chipset to be designed and manufactured.

There is little openly available literature related to LTE jamming attacks, and even less on mitigation of attacks. The authors of [11] propose various methods for enhancing the security of LTE networks against jamming attacks. This includes spread-spectrum modulation of the downlink broadcast channels. This strategy is meant to mitigate a jammer that targets the center 1 MHz of the downlink signal, where many important signals and channels are located. By using direct-sequence spread spectrum (DSSS), the important signals and channels can be spread across the entire available downlink bandwidth, which in most cases is 10 MHz. The authors also propose scrambling the radio resource allocation for the PUCCH with an encrypted sequence, whereby the allocation of the PUCCH is no longer on the band edges of the uplink band, but instead can appear anywhere in the uplink frame. Only legitimate users connected to the cell would know how to decrypt the scrambled sequence. Lastly, the authors of [11] propose a system in

which the MIB and SIBs would be encrypted so that essential network configuration parameters are not transmitted in the clear. All three of these anti-jamming strategies require changes to the UE chipset as well as changes to the eNodeB because of the extensive modifications to the LTE protocol and signaling.

PSS spoofing can be mitigated by creating a timer for receiving the SSS. If this timer expires, the UE should blacklist the PSS and choose the second strongest cell within the same frequency. PSS and SSS spoofing attacks can be mitigated by having the UE create a list of all available cells in the given frequency channel along with their received power levels. The UE could then search for the PBCH of the strongest cell and have another timer for decoding the MIB. If this timer expires, the UE would look for the PBCH of the next strongest cell, and so forth [12].

A simple way of mitigating PUCCH jamming would be to provide periodic PUSCH resources to UEs, even if not requested [13]. This way, the UE will send its uplink control information on the PUSCH instead of the PUCCH. Since the downlink resources are typically the bottleneck, the overhead associated with such periodic assignment of PUSCH resources might not be as critical.

The authors of [14] investigate the PCFICH jamming attack and propose a mitigation strategy called "extra-blind PDCCH decoding". This strategy suggests that the UE decodes each PDCCH block with all three possible CFI values, instead of extracting it directly from the PCFICH. Another option is using a fixed CFI for mission-critical LTE networks or operational modes. Unfortunately both of these strategies require modifications to the UE chipset, making them unlikely to be implemented unless they are added to the 3GPP specifications.

These mitigation strategies only address a few of the attacks that we discussed in this article. Further research on mitigation techniques that require minimal changes to the UE, and the LTE standard itself, is needed.

VI. Conclusion

In this article we analyzed the vulnerability of LTE to jamming, spoofing, and sniffing by looking at each of the physical channels and signals of LTE. Using barrage jamming as a baseline, we have shown that more effective jamming methods can be realized by exploiting the specific protocol features of LTE. We derived metrics related to the efficiency and complexity of each method to compare them and conclude that the PSS, PUCCH, PCFICH, and PBCH are the weakest subsystems and should, therefore, be addressed first. When considering how many forms of jamming are more efficient than barrage jamming (PCFICH jamming, for instance, provides a 27 dB jamming advantage), it is clear that LTE is highly vulnerable to adversarial jamming. This high level of vulnerability is not surprising given that LTE was

not designed to become a mission-critical communications technology. However, with the rapid adoption of mobile devices and networks, LTE is going to be highly relied-upon during the next decade. We therefore recommend that the identified vulnerabilities be seriously considered and mitigation techniques integrated into future 3GPP releases and LTE network deployments, especially for critical communication systems. Backward compatible solutions, such as [1], would ensure a gradual evolution to more robust LTE/LTE-A networks.

VII. Acknowledgment

We would like to thank Oceus Networks, Inc. and Vencore, Inc. for funding parts of this research. This work was also supported by the Defense University Research Instrumentation Program (DURIP) contract number W911NF-14-1-0553 through the Army Research Laboratory (ARL). Lastly, we would like to thank Sanjole, Inc. for providing the LTE network captures and software to analyze them.

References

[1] 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.

[2] 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.

[3] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode (Release 12)," 3rd Generation Partnership Project (3GPP), TS 36.304, Mar. 2015. [Online]. Available: http://www.3gpp.org/dynareport/36304.htm

[4] ——, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) (Release 12)," 3rd Generation Partnership Project (3GPP), TS 36.331, Mar. 2015. [Online]. Available: http://www.3gpp.org/dynareport/36331.htm

[5] C. S. Patel, G. L. Stüber, 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.

[6] T. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *IEEE International Conference on Communications (ICC)*, June 2011.

[7] M. Baker and T. Moulsley, "Downlink physical data and control channels," in *LTE, The UMTS Long Term Evolution: From Theory to Practice*, 2nd ed., S. Sesia, I. Toufik, and M. Baker, Eds. Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd, 2011, ch. 9.

[8] G. Gorbil, O. H. Abdelrahman, and E. Gelenbe, "Storms in mobile networks," in *Proceedings of the 10th ACM symposium on QoS and security for wireless and mobile networks*. ACM, 2014, pp. 119–126.

[9] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation (Release 8)," 3rd Generation Partnership Project (3GPP), TS 36.211, Dec. 2009. [Online]. Available: http://www.3gpp.org/dynareport/36211.htm

[10] T. Newman, A. He, J. Gaeddert, B. Hilburn, T. Bose, and J. Reed, "Virginia tech cognitive radio network testbed and open source cognitive radio framework," in *International Conference on Testbeds and Research Infrastructures for the Development of Networks Communities and Workshops*, April 2009, pp. 1–3.

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

[12] M. Labib, V. Marojevic, J. H. Reed, and A. 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, to be published.

[13] M. Lichtman, T. Czauski, S.-K. Ha, P. David, and J. H. Reed, "Detection and mitigation of uplink control channel jamming in LTE," in *IEEE Military Communications Conference (MILCOM)*, 2014, pp. 1187–1194.

[14] J. Kakar, K. McDermott, V. Garg, M. Lichtman, V. Marojevic, and J. H. Reed, "Analysis and mitigation of interference to the LTE physical control format indicator channel," in *IEEE Military Communications Conference (MILCOM)*, 2014, pp. 228–234.

BIOGRAPHIES

MARC LICHTMAN (marcll@vt.edu) received the B.S. and M.S. degrees in electrical engineering from Virginia Polytechnic Institute and State University, Blacksburg, VA, USA, in 2011 and 2012, respectively, where he is currently working toward the Ph.D. degree, under the advisement of Dr. Jeffrey H. Reed. His Ph.D. research is focused on introducing and developing the concept of Antifragile Electronic Warfare. His research interests include electronic warfare, machine learning, cognitive radio, and wireless communication system design.

ROGER PIQUERAS JOVER (rpiquerasjov@bloomberg.net) is a Wireless Security Research Scientist at the Security Architecture team of Bloomberg LP. Previous to that, he spent 5 years as Principal Member of Technical Staff at the AT&T Security Research Center. He graduated in 2006 with a Dipl.-Ing. in Telecommunications Engineering from the Universitat Politcnica de Catalunya (UPC). He also graduated with a MSc in Electrical and Computer Engineering from University of California Irvine and an MPhil. in Electrical Engineering from Columbia University, in 2008 and 2010 respectively. His work and research interests focus on wireless network security, LTE security and protocol exploits, IoT and embedded device security and new 5G mobile network architectures for control plane scalability.

MINA LABIB (mlabib@vt.edu) received his B.S. degree from Ain Shams University (Cairo, Egypt) in Electronics & Communications Engineering, and his M.Sc. degree from Carleton University (Ottawa, Ontario, Canada) in Systems and Computer Engineering. He is currently working toward the Ph.D. degree at the Bradley Department of Electrical and Computer Engineering at Virginia Tech within the Wireless@VirginiaTech research group. His current research interests are in the broad areas of

wireless communications, with a particular emphasis on LTE systems, enhancing the security of wireless communication systems, LTE-Unlicensed, spectrum sharing, and game theory.

RAGHUNANDAN M RAO (raghumr@vt.edu) received his Bachelor's degree in Telecommunication Engineering from R.V. College of Engineering, Bangalore, India in 2011, and his Master's degree in Laser Technology from the Indian Institute of Technology Kanpur in 2013. He is currently a graduate student at the Bradley Department of Electrical and Computer Engineering at Virginia Tech. His areas of interest include anti-jamming of LTE networks, mmWave communications, and software radios.

VUK MAROJEVIC (maroje@vt.edu) graduated from University of Hannover (M.S.), Germany, and Polytechnic University of Catalonia (Ph.D.), Spain, both in electrical engineering. He joined Wireless@Virginia Tech in 2013. His research interests are in software-defined radio, spectrum sharing, 4G/5G cellular technology and resource management with application to public safety and mission critical networks and unmanned aircraft systems.

JEFFREY H. REED (reedjh@vt.edu) is the founder of Wireless @ Virginia Tech, and served as its Director until 2014. He is the Founding Faculty member of the Ted and Karyn Hume Center for National Security and Technology and served as its interim Director when founded in 2010. In 2005, Dr. Reed became Fellow to the IEEE for contributions to software radio and communications signal processing and for leadership in engineering education. In 2012 he served on the Presidents Council of Advisors of Science and Technology Working Group that examine ways to transition federal spectrum to allow commercial use and improve economic activity.

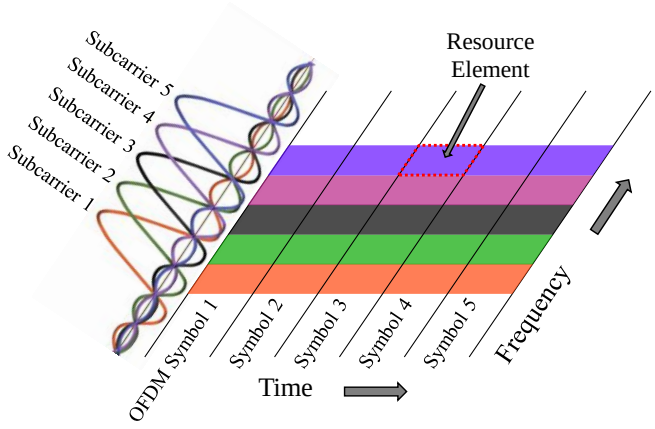

Fig. 1. Depiction of the OFDM time-frequency lattice

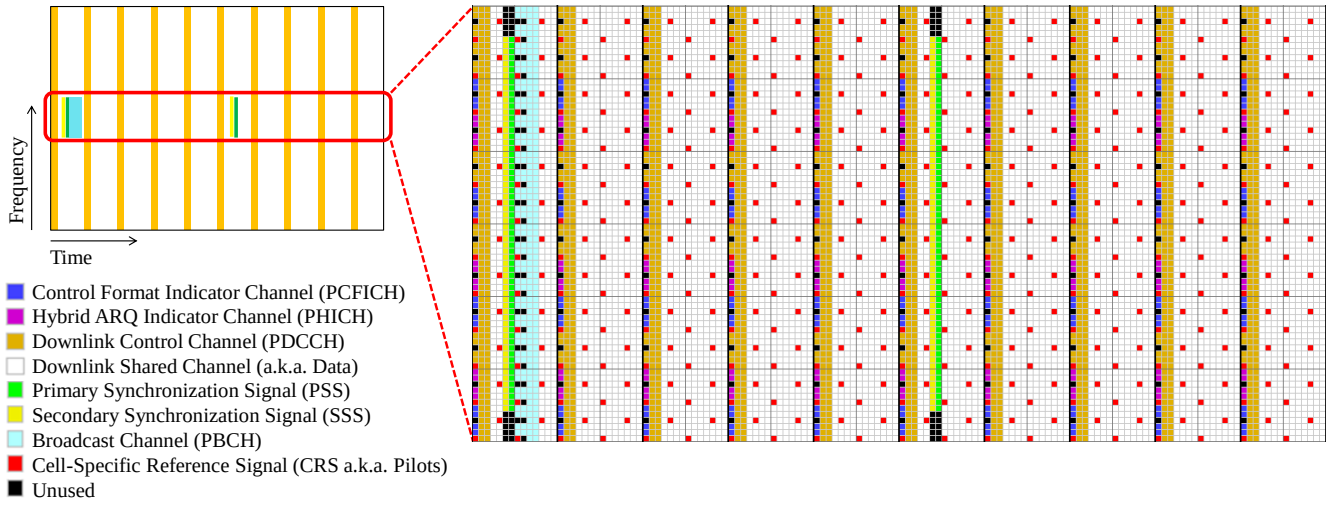

Fig. 2. The LTE Downlink Signal, showing one full 10 millisecond frame (left), and the central 1.4 MHz of the same frame (right)

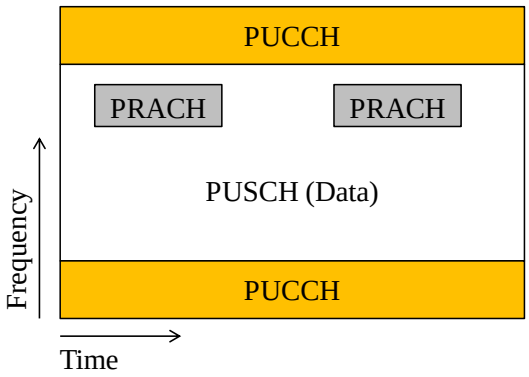

Fig. 3. The LTE Uplink Signal

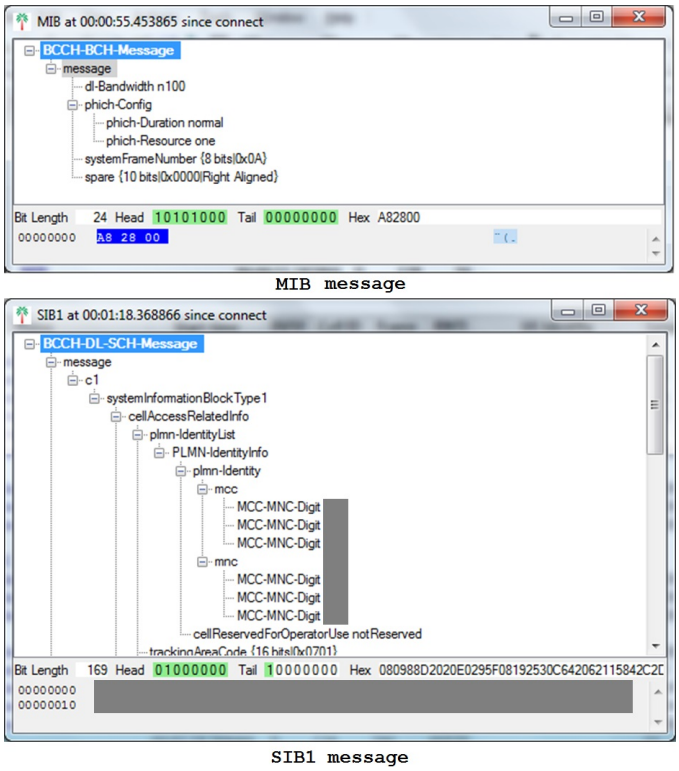

Fig. 4. Real MIB and SIB1 Messages Captured from a Production Network

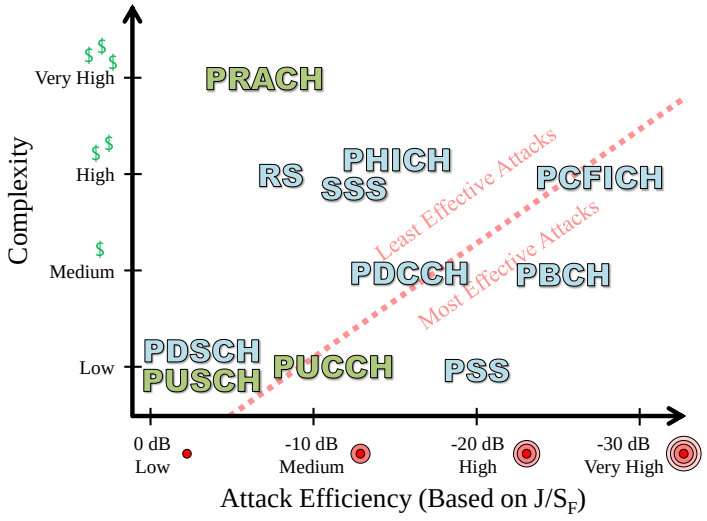

Fig. 5. Ranking of Attacks Based on Jamming Efficiency and Complexity

TABLE I

PHYSICAL CHANNEL AND SIGNAL MODULATION SCHEME, CODING TYPE AND RATE, SPARSITY, SYNCHRONIZATION REQUIREMENT, AND MINIMUM J/S TO CAUSE DOS

Channel/Signal	**Modulation**	**Coding**	**Coding Rate**	**% of REs**	**Synch. Required**	J/S_{CH}	J/S_F
PDSCH	{4,16,64}-QAM	Turbo	Adaptive	85%	No	0 dB	-1 dB
PBCH	QPSK	Convolutional	1/48	0.3%	Yes	0 dB	-25 dB
PCFICH	QPSK	Block	1/16	0.2%	Yes	0 dB	-27 dB
PDCCH	QPSK	Convolutional	1/3	7%	Yes	-5 dB	-16.5 dB
PHICH	BPSK	Repetition	1/3	1.5%	Yes	3 dB	-15 dB
PUSCH	{4,16,64}-QAM	Turbo	Adaptive	$\sim$ 75%	No	0 dB	-1 dB
PUCCH	BPSK, QPSK	Convolutional	1/3	$\sim$ 25%	No	-5 dB	-11 dB
PRACH	Zadoff-Chu Sequence	N/A	N/A	$\sim$ 2%	Yes	10 dB	-7 dB
PSS (Spoofing)	Zadoff-Chu Sequence	N/A	N/A	0.45%	No	3 dB	-20.5 dB
SSS	M-sequences	N/A	N/A	0.2%	Yes	15 dB	-12 dB
CRS	QPSK	N/A	N/A	5%	Yes	5 dB	-8 dB