LTE PHY Layer Vulnerability Analysis and Testing Using Open-Source SDR Tools

Raghunandan M. Rao*, Sean Ha*, Vuk Marojevic*, Jeffrey H. Reed*
*Bradley Department of Electrical and Computer Engineering
Virginia Tech, Blacksburg, Virginia, USA
Email: {raghumr, seanha65, maroje, reedjh}@vt.edu

***Abstract*—This paper provides a methodology to study the PHY layer vulnerability of wireless protocols in hostile radio environments. Our approach is based on testing the vulnerabilities of a system by analyzing the individual subsystems. By targeting an individual subsystem or a combination of subsystems at a time, we can infer the weakest part and revise it to improve the overall system performance. We apply our methodology to 4G LTE downlink by considering each control channel as a subsystem. We also develop open-source software enabling research and education using software-defined radios. We present experimental results with open-source LTE systems and shows how the different subsystems behave under targeted interference. The analysis for the LTE downlink shows that the synchronization signals (PSS/SSS) are very resilient to interference, whereas the downlink pilots or Cell-Specific Reference signals (CRS) are the most susceptible to a synchronized protocol-aware interferer. We also analyze the severity of control channel attacks for different LTE configurations. Our methodology and tools allow rapid evaluation of the PHY layer reliability in harsh signaling environments, which is an asset to improve current standards and develop new robust wireless protocols.**

***Index Terms* – Long-term Evolution (LTE); Methodology; Protocol-aware Jamming; Software-Defined Radio (SDR); Open source tools.**

I. Introduction

Wireless infrastructure and technology is a vital resource to the economy and defense of the nation, and its protection is becoming increasingly important. While the commercial sector continues to increase the use of cellular networks for Internet access, public safety networks and the military plan to leverage commercial 4G cellular technology for their communication needs in emergency situations. The Internet of Things (IoT) will also impact the number of devices connecting to the cellular network. Even though the architecture of 5G is still an open question, there will be key differences with regards to many characteristics of 4G technology such as the ability to flexibly use spectrum; order of magnitude reduction in latency; and, perhaps most importantly, improved security and privacy [1].

Wireless communication networks provide a multitude of critical and commercial services and serve an ever increasing number of users. Ultra-reliable and secure wireless networks are necessary for national security and public safety, in order to provide efficient situation assessment, time-critical assistance and swift response to potential threats. This is also crucial for autonomous vehicular networks and unmanned aerial systems, where even a partial breakdown can have disastrous consequences.

Security and privacy has always been an evolving problem in the area of wireless communications since the days of analog 1G cellular networks. Each cellular generation has undergone its share of research and development related to wireless network attacks and countermeasures because each new feature introduced can have a potential vulnerability that can be exploited by an attacker. Different types of attacks to wireless networks have been the topic of research for several years [2]-[3].

Lazos et al. [4] propose a randomized distributed channel establishment scheme based on frequency hopping to address the problem of control channel jamming in ad-hoc networks. Bicakci et al. [5] focus on combating Denial of Service (DoS) attacks in 802.11 devices using practical hardware, software and firmware solutions. Liu et al. [6] develop a time-delayed broadcast scheme that partitions the broadcast operation into a series of unicast transmissions for spread spectrum systems with insider threats. Chiang et al. [7] introduce a code-tree system for circumventing cross-layer jamming attacks in wireless broadcast networks. Hidden Markov Models (HMMs) are adopted in [8] to characterize the sensing behaviors of legitimate and malicious users in collaborative spectrum sensing settings.

LTE is prone to protocol-aware interference, since the standards documentation is openly available. There has been prior work related to RF Jamming of LTE signals. Kakar et al. [9] investigate the performance of the Physical Control Format Indicator Channel (PCFICH) under harsh wireless conditions and propose strategies to mitigate interference on the PCFICH. Lichtman et al. [10] consider the problem of targeted interference on the Physical Uplink Control Channel (PUCCH) and propose detection and mitigation strategies to counter protocol-aware jammers. Labib et al. [11] introduce and demonstrate *LTE control channel spoofing*, which refers to spoofing by a fake eNodeB by transmission of a partial LTE downlink frame. Denial of Service (DoS) was found to be the result of transmission of the partial LTE downlink frames containing only the fake control channels, at a relatively higher

This is the author's version of the work. For citation purposes, the definitive version of record of this work is: R. Rao, S. Ha, V. Marojevic, J.H. Reed, "LTE PHY Layer Vulnerability Analysis and Testing Using Open-Source SDR Tools", IEEE MILCOM 2017, 23-25 Oct. 2017.

power level w.r.t. the legitimate eNodeB. The authors also propose mitigation strategies that required simple modification to the cell selection process of LTE. In [12], a comprehensive threat assessment of LTE/LTE-A is provided, highlighting the vulnerabilities of various LTE physical channels and signals. A survey of mitigation techniques against various jamming/spoofing attacks is also provided.

This paper provides a methodology for assessing the PHY layer vulnerabilities of cellular networks. Our analysis uses LTE as an example, but the methodology applies to many other present and future protocols. The contribution of paper is threefold: we provide

1) a methodology for PHY layer testing of wireless protocols,
2) open-source software enabling research and education using software-defined radios (SDRs), and
3) empirical results with open-source SDR-based 4G LTE systems.

The rest of the paper is organized as follows: Section II reviews the related work on PHY layer vulnerability and provides background on LTE control channels. Section III introduces our methodology, Section IV provides experimental results and analysis for LTE. Section V concludes the paper.

II. Control Channels in the LTE Downlink

Control channels in wireless networks are essential for providing the capability for the system to operate properly and efficiently. Using LTE as an example below we briefly review some of the important Downlink (DL) LTE physical control channels that are relevant for the experimental analysis discussed in this work. Note that in LTE the Base Station is referred to as the evolved NodeB (eNB) and the user terminal is referred to as the user equipment (UE).

Primary and Secondary Synchronization Signals (PSS/SSS): LTE uses two synchronization signals: the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS). The PSS and SSS are broadcast by the eNB for slot and frame synchronization. The PSS is constructed from Zadoff-Chu sequences due to the strong Constant Amplitude Zero Autocorrelation (CAZAC) properties.

The SSS is constructed from two maximal length sequences (M-sequences). As all communication between the UE and eNB requires time synchronization, disrupting the PSS or SSS will not cause an immediate Denial of Service (DoS), but will instead prevent new UEs from accessing the cell and idle UEs from re-synchronizing with the cell.

Physical Broadcast Channel (PBCH): The PBCH contains the Master Information Block (MIB) which informs the UE about the downlink bandwidth, resource length of the Hybrid ARQ (HARQ) Indicator Channel (PHICH), and the System Frame Number (SFN) for frame synchronization. The PBCH is mapped to the central 72 subcarriers of four consecutive OFDM symbols per frame. It is QPSK modulated with a 16-bit CRC, but with an effective coding rate of $1/48$.

Physical Downlink Control Channel (PDCCH): The PDCCH carries critical control information, such as UE resource allocation, modulation and coding scheme (MCS) of user data, information about the HARQ parameters and precoding matrices for MIMO. It is QPSK modulated with rate-$1/3$ convolutional coding and occupies the first few OFDM symbols of each subframe. During the initial cell access procedure, it informs the UE of the first System Information Block (SIB1), without which the UE will be unable to complete the cell attachment process. Additionally, after cell attachment, it would be impossible for the UE to obtain service and decode its data if the PDCCH is improperly decoded.

Physical Control Format Indicator Channel (PCFICH): The PCFICH contains information regarding the size of the PDCCH and is sent at the beginning of each subframe. It contains the Control Format Indicator (CFI) which is 2 bits in length, and is encoded using a code rate of $1/16$. Therefore corrupting the PCFICH will also corrupt detection of the PDCCH at the UE.

Cell-Specific Reference Signals (CRS): The CRS carries downlink pilot symbols that are used or channel estimation and quality assessment as well as equalization. CRS are QPSK-modulated and use a Gold sequence of length 31, which is initialized using the cell ID value. The CRS symbols are distributed sparsely in time and frequency, occupying about 5% of the Resource Elements (REs). The first position k_0 of the CRS in the LTE DL grid is determined by the Physical Cell Identity (PCI) $N_{c,ID} \in \{0, 1, \cdots, 503\}$, by the relation $k_0 = N_{c,ID} \bmod 6$ (assuming the range of $k_0 \in \{0, 1, \cdots, 5\}$).

III. PHY Layer Vulnerability Assessment Methodology

The methodology that we develop is based on testing the vulnerabilities of a system by analyzing the individual subsystems. By targeting a specific subsystem or a specific combination of subsystems at a time, we can infer the weakest component and revise it to improve the overall system robustness. Hence, we propose tools for assessing the individual system components and metrics for evaluation. Here, we regard the LTE control channel(s) to be the subsystem(s), for the purpose of analysis. Although we present the tools and metrics for LTE, rather than in an abstract way, the concepts are applicable for other wireless protocols as well.

A. Open-Source Software Tools

We propose a parametric framework for interference generation by using the same waveform as the target system. This ensures that there is high correlation in the protocol signaling between the interference and the target waveform(s). In the case of LTE, individual subcarriers and OFDM symbols can be allocated/blanked to rapidly generate wideband, narrowband, and protocol-aware interference over any portion of the DL LTE time-frequency grid. Note that other wireless standards, including IEEE 802.11xx and emerging IoT standards, use OFDM. Fig. 1 illustrates the general framework for OFDM-based parametric interference generation. It allows generating

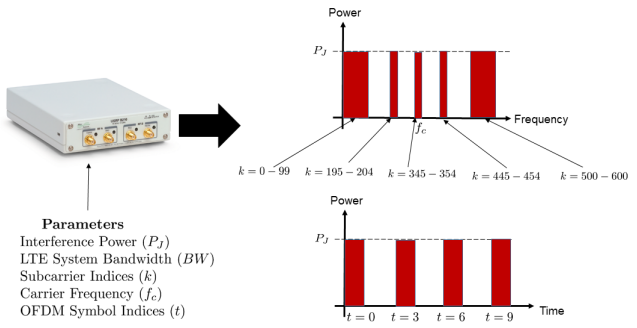

Fig. 1. OFDM-based parametric interference generation.

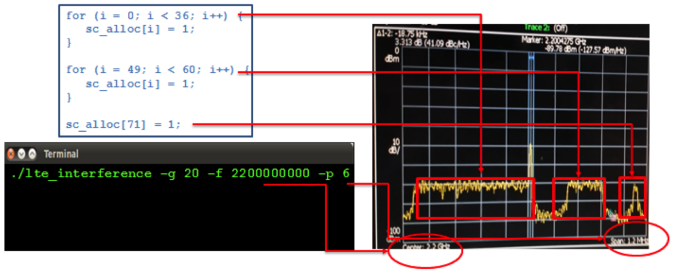

Fig. 2. Asynchronous interference waveform generation.

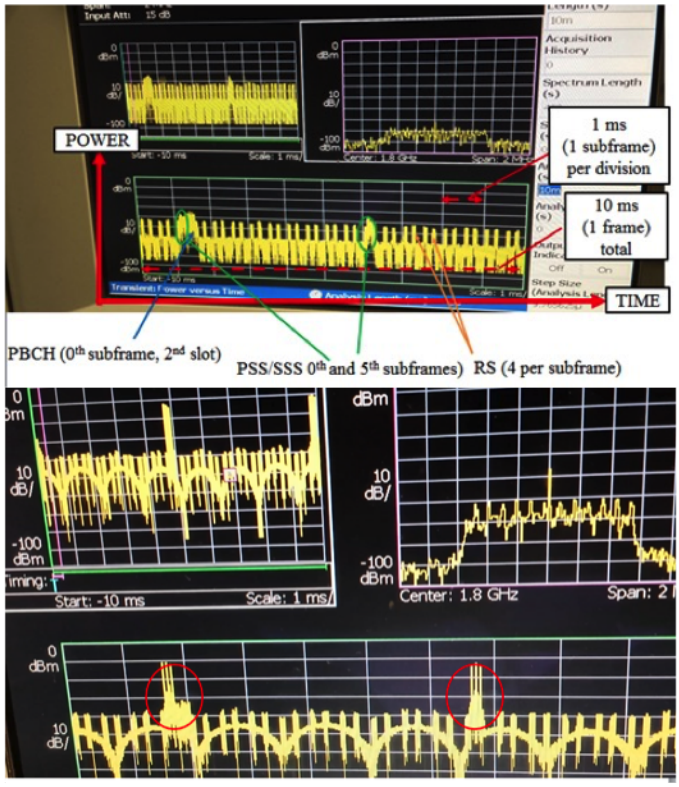

Fig. 3. Synchronous interference waveform: eNB signals which, for illustration purposes, consist of the PSS/SSS, the PBCH, and the CRS only (top and bottom) and synchronous PSS/SSS interference (bottom).

asynchronous and synchronous interference waveforms that we build from the open source LTE library srsLTE [13]. The srsLTE library implements the LTE uplink and downlink waveforms and supports commercial off-the shelf hardware such as Universal Software Radio Peripherals (USRPs). Broadly, we classify the interference waveforms based on the time-synchronization requirements of the jammer w.r.t. the target:

1) Asynchronous Interference Waveforms: The asynchronous interference waveform generates interference on specific subcarriers. This type of interference can be of certain duration/duty cycle or continuous or discontinuous in time. We can use this setup to generate any interference to LTE that does not need accurate time alignment with the LTE frame. We can also generate a fake PSS and/or SSS signal (for example, to execute PSS/SSS spoofing as in [11]) by replacing OFDM symbols with LTE synchronization sequences. As an example, the spectrum of a 1.4 MHz interference waveform with three blocks of active subcarriers is shown in Fig. 2. Assuming the subcarrier indices $k \in \{0, 1, \cdots, 71\}$, the jammer transmits only on subcarriers k_j such that $k_j \in \{0, 1, \cdots, 35\}$ (540 kHz wide), $k_j \in \{49, 50, \cdots, 59\}$ (165 kHz wide) and $k_j \in \{71\}$ (15 kHz wide).

2) Synchronous Interference Waveforms: Transmitting on top of specific physical channels requires synchronization with the network to determine where the physical channels exist in time. Therefore, we design an interferer that (1) acts as a receiver and synchronizes with the eNB, in this case by acquiring the legitimate PSS and SSS of the LTE cell and (2) synchronously transmits its interference waveform to the target. A configurable timing offset can be specified to account for transmission and other delays. Fig. 3 illustrates the synchronous interference waveform which targets the PSS/SSS.

B. Metrics for Performance Evaluation

In order to compare the impact of different control channel attacks, we need a uniform metric that captures the differences between the control channels. In this regard, we devise a metric based on the (a) Jammer to Signal power ratio (JSR) values, (b) control channel occupancy fraction in the LTE Frame, and (c) control channel relative power w.r.t. the data channel. Equivalent metrics apply for other wireless standards and additional metrics may need to be specified for the specific analysis. For LTE, we define the following quantities:

1) Jammer to Signal Ratio per resource element (JSR_{RE}),
2) Jammer to Signal Ratio per Frame (JSR_F), and
3) Relative power w.r.t. the Physical Downlink Shared Channel (PDSCH) (ρ_{PDSCH}).

1) JSR_{RE}: It is defined as the ratio of the jammer power to that of the LTE signal, assuming that all the LTE resource elements (REs) have the same transmit power. We also consider that the jammer allocates equal power on all subcarriers at all times.

TABLE I
INDICATORS OF ALL CONSIDERED JAMMER STRATEGIES.

Target	Periodicity	Error Flag
Barrage	Subframe	PDCCH error/PCFICH error/synch error/ PBCH error
PSS/SSS	Frame	If frame synchronized: sync loss. If frame does not synchronize: Unable to sync
PDCCH	Subframe	Decoded RNTI $\neq$ SENTVALUE
PBCH	Frame	Decoded MIB $\neq$ Default configuration
PCFICH	Subframe	Decoded CFI $\neq 2$
CRS	Subframe	PDCCH error/PCFICH error/synch error/ PBCH error

2) JSR_F: In our experiments, the jammer is targeting specific control channels, all of which occupy different fractions of the total number of REs per LTE DL frame. To account for this, we define JSR_F given by

$$JSR_F = JSR_{RE} \times \frac{N_{T,F}}{N_{tot,F}}, \tag{1}$$

where $N_{T,F}$ denotes (the number of REs allocated to the control channel per LTE frame, and $N_{tot,F}$ the total number of REs per LTE frame.

3) ρ_{PDSCH}: LTE allocates different power levels to different control channels. ρ_{PDSCH} is defined as $\rho_{PDSCH} = \frac{P_T}{P_{PDSCH}}$, where P_T is the power allocated by the LTE transmitter to the control channel, and P_{PDSCH} is the power allocated to the PDSCH in the same frame.

Therefore, these three factors determine the overall jammer to signal ratio JSR_N given by

$$JSR_N = JSR_{RE} \times \frac{N_{T,F}}{N_{tot,F}} \times \frac{P_T}{P_{PDSCH}}. \tag{2}$$

The above relation is adapted from [14] and is modified to account for the non-uniformity in power allocation for all control channels. Since JSR_N represents the overall power requirements of the jammer w.r.t. that of the LTE DL signal, we use it as the metric to compare the relative robustness of the control channels.

In order to compare the robustness of each control channel to targeted interference, we also need to define events at the receiver that constitute a successful jamming attack. In addition to this, we also need to set thresholds for the *probability of error* or *error rate* P_{err}, beyond which the control channel is said to be irreversibly corrupted. In essence, such a scenario will lead to the UE operating with corrupted control information that can cause severe system level issues, and in the worst case, DoS. Table I describes the event (i.e. error flag in libLTE) that indicates a successful LTE DL jamming attack.

IV. LTE EXPERIMENTAL RESULTS AND ANALYSES

A. Experimental Setup using Open-Source SDR Tools

Fig. 4 shows the experimental setup on the Virginia Tech LTE Testbed [15] which features three Universal Software Radio Peripherals (USRPs) to emulate the LTE eNB, UE and the protocol-aware jammer. The jammer was provided a

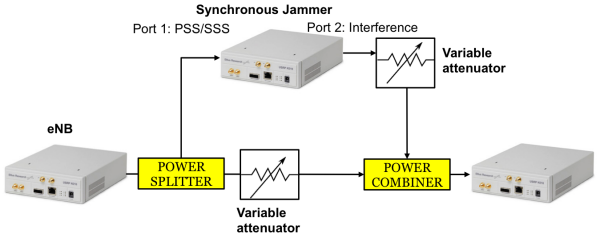

Fig. 4. Experimental setup of the jamming experiments.

PSS/SSS from the eNB in order to synchronize the jamming signal with the UE when needed. The LTE DL signal and the synchronous jamming signal are combined using radio frequency (RF) power combiners. Attenuators in each RF path provide a means to control the JSR. RF cables were used to connect the components and hence, the RF environment was low-noise. Therefore, the resulting LTE system performance is interference-limited.

For each value of JSR, the error rates were calculated after subjecting each considered DL physical control channel to 10^5 trials of targeted interference. Each trial composed of transmission of 1 subframe (for PCFICH, PDCCH, CRS and Barrage jamming schemes) and 1 frame (for PSS/SSS and PBCH jamming schemes). For each jamming scenario, the error event is defined in Table I. The error rate for each channel P_{err} is defined as the ratio of the the number of frames (or subframes) for which the error flag (defined in Table I) is active (N_{err}), to the total number of frames (or subframes) transmitted (N_{trial}). The error rate was calculated using the relation $P_{err} = N_{err}/N_{trial}$. The JSR was computed using (2), where the term ρ_{PDSCH} was computed for each jamming strategy experimentally, and is tabulated in Table II.

We define the error threshold $P_{err,th}$ to be the value beyond which Denial of Service (DoS) occurs, whose values are summarized in Table III. The reasons for the choice of $P_{err,th}$ for each strategy is given below:

1) PBCH has a very low coding rate of $1/48$, and is spread across 4 OFDM frames. Hence, it is robust against interference and we set a high error threshold of $P_{err,th} = 0.9$.
2) PSS/SSS is comprised of interference-resilient signals with very strong correlation properties [14]. Hence we set an error threshold value of $P_{err,th} = 0.5$.
3) PCFICH carries the locations of the PDCCH, and PDCCH has a fairly high code-rate of $1/3$. Hence, an error threshold of $P_{err,th} = 0.1$ is considered to be sufficient to disrupt these channels.
4) CRS is used for channel estimation and equalization which is crucial to decode all the other control channels. The aggregate $P_{err,th}$ cannot be greater than that of all other critical DL control channels and hence, we set $P_{err,th} = 0.1$. The same reasoning applies for barrage jamming as well.

The overall jammer to signal noise ratio ($JSR_{N,DoS}$) repre-

TABLE II
EMPIRICALLY MEASURED VALUES OF ρ_{PDSCH}.

Jamming Strategy	ρ_{PDSCH} (dB)
Barrage	0
PSS/SSS	-5
PDCCH	-5
PBCH	-2
PCFICH	-8
CRS	-10

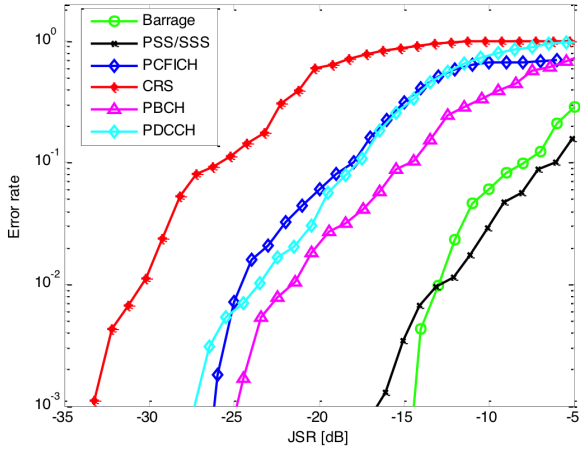

Fig. 5. Error rate as a function of JSR for the jamming experiments using open-source SDR tools for a 1.4 MHz FD LTE signal.

TABLE III
LTE DL PHYSICAL CHANNEL VULNERABILITIES FOR 1.4 MHZ FD-LTE.

Target	Fraction of REs	Complexity	$P_{err,th}$ to cause DoS	$JSR_{N,DoS}$ (dB)
Barrage	100 %	Very Low	0.1	-10
PSS/SSS	1.23 %	Medium	0.5	5
PDCCH	23.4 %	Medium	0.1	-16
PBCH	2.38 %	Low	0.9	-3
PCFICH	0.2 %	High	0.1	-19
CRS	4.76 %	High	0.1	-26

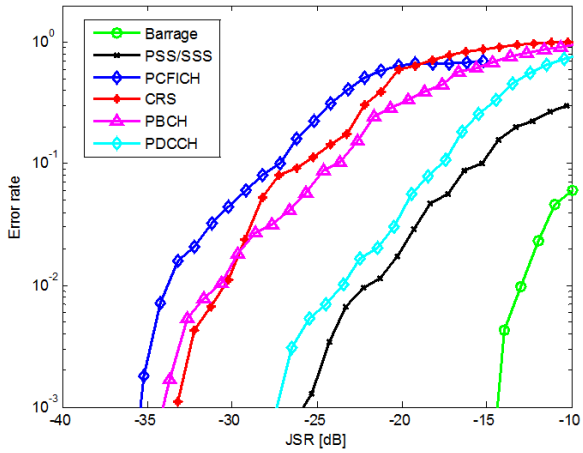

Fig. 6. Error rate as a function of JSR for the jamming experiments using open-source SDR tools for a 10 MHz FD LTE signal.

sents the JSR value that results in $P_{err} \geq P_{err,th}$, which in turn results in DoS.

B. Analysis of DL Jamming Results

The jamming experiments were performed for all six downlink jammer strategies and the results are shown in Fig. 5. The necessary JSR to jam each physical channel is summarized in Table III. We qualitatively comment on the complexity of the jamming attack for a 1.4 MHz FD LTE system, based on the degree of synchronization required to jam the subsystem and the contiguity of targeted REs comprising the subsystem. We see that the PSS/SSS is the least vulnerable DL physical channel. This is understandable since both the PSS and SSS use very strong correlation sequences (Zadoff-Chu and M-sequence respectively) that are inherently robust against noise and interference by design. Even though PSS and SSS are very sparse, the jammer needs more power than the LTE DL signal to corrupt them to the point of synchronization loss/inability to synchronize and therefore, DoS.

The PBCH is also resilient to jamming, since (a) it provides only basic initial information, and (b) it has a very low coding rate (cf. Section II). The PCFICH is robust to interference because of strong encoding, but its sparsity makes it susceptible to jamming relative to PDCCH. However, since jamming the PCFICH has the same outcome as jamming the PDCCH, the 3 dB gain of PCFICH w.r.t. PDCCH jamming is deemed infeasible for the jammer since the PCFICH's sparsity makes the jamming attack more complex and countermeasures have been proposed in the literature [9].

We see that CRS, in the case of a perfectly synchronized jamming attack, is highly vulnerable. This is due to (a) the sparsity of the CRS in terms of the fraction of REs per OFDM frame and (b) the dependence of all the other critical control channels on accurate channel estimates. In practice, perfect synchronization is difficult to achieve for a sparse and non-contiguously distributed signal such as the CRS. However, the jammer can target CRS subcarriers instead of CRS REs, which is a very simple strategy since the CRS subcarrier locations depend on the cell ID $N_{c,ID}$ and remains constant for all users of the cell. In this case the jammer need not synchronize with its target, thus reducing the complexity of the attack at the cost of a higher JSR.

It is clear that the PDCCH should have the highest priority for anti-jamming countermeasures because the PDCCH can be easily targeted with a relatively low JSR. CRS follows close behind, having by far the lowest required JSR to corrupt, but a much higher complexity. Similarly, the PBCH and, especially PSS/SSS are not high priority for anti-jamming; while an attack may theoretically cause complete DoS by targeting these subsystems, the attackers require nearly as much power as barrage jamming, making them less practical from an attacker's perspective.

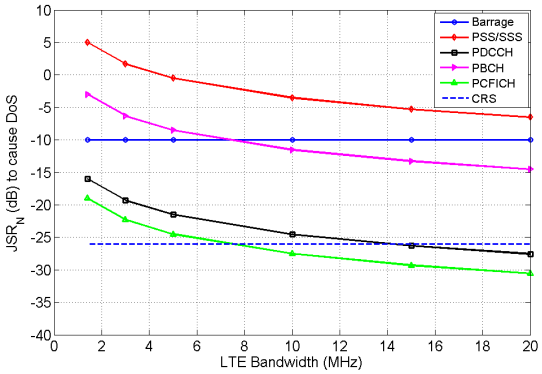

Fig. 7. JSR_N required versus LTE bandwidth to cause Denial of Service for all considered control channel attacks.

C. Vulnerability Analysis for Higher LTE Bandwidths

The results discussed so far apply only to a LTE bandwidth of 1.4 MHz. For higher LTE bandwidths, it is important to note that the following control channels lie within the central 72 subcarriers of the LTE frame for all bandwidths, (a) PSS/SSS, (b) PDCCH, (c) PBCH and (d) PCFICH. Hence, these control channels can be targeted by the jammer by confining its power within the central 72 subcarriers of the LTE signal. Hence, for cases (a)-(d) the required JSR ($JSR_{N,DoS}^{(BW)}$) to cause DoS for a LTE system bandwidth BW can be written as

$$JSR_{N,DoS}^{(BW)} = JSR_{N,DoS}^{(1.4\text{ MHz})} - 10\log_{10}\left(\frac{BW}{1.4\text{ MHz}}\right). \quad (3)$$

However, a jammer targeting the CRS will need to occupy the entire bandwidth, and the same is true for a barrage jammer as well. Therefore, the JSR_N requirements for all strategies except CRS and barrage jamming change as a function of the LTE bandwidth as described in equation (3). Fig. 6 shows the error rate as a function of the JSR for a 10 MHz FD-LTE system.

Fig. 7 shows the variation of $JSR_{N,DoS}$ as a function of LTE system bandwidth (BW) for each jamming strategy. We see that (a) PSS/SSS will still be an inefficient attack for a system bandwidth of 20 MHz, (b) PBCH jamming performs better than barrage jamming only for $BW \geq 10$ MHz, (c) PCFICH jamming performs better than CRS jamming for $BW \geq 10$ MHz, and (d) PDCCH jamming, on the other hand performs better than CRS jamming for $BW \geq 15$ MHz. An obvious way to increase the resilience of the system would be to allocate the control channel REs (except the PSS/SSS) over the entire LTE bandwidth. This would ensure that the jammer would have to resort to wideband signaling to disrupt the LTE control channels.

V. Conclusions

This paper has introduced a methodology for analyzing the PHY layer vulnerability of wireless protocols. We have developed a software suite for introducing protocol-aware interference to a system. Our software is applicable to OFDM-based protocols. We applied it to target the LTE RF link and showed how different subsystems of LTE react differently to protocol-aware interference. We showed that the LTE synchronization signals (PSS/SSS) are the most resilient to synchronized jamming. We also saw that CRS, PCFICH and PDCCH are the most vulnerable to protocol-aware jamming. The results presented in this paper are based on open-source SDR-based LTE systems. Other systems will need different metrics and software for testing, but the proposed methodology can be applied for (1) methodical testing, (2) improving the robustness of the subsystem and hence the entire system and (3) designing of control channels to achieve a desired level of robustness.

As LTE evolves, these vulnerabilities will need to be taken into consideration while applying LTE for military and public safety networks, and for designing interference-resilient next-generation wireless protocols. Tradeoffs will be necessary to balance efficiency, system complexity and robustness to smart attackers. This will continue to be an important research area that will significantly contribute to the architecture of 5G wireless networks.

Acknowledgements

The authors would like to thank the the sponsors for their support. This work was funded by the National Science Foundation (NSF) under Grant CNS-1642873, and the Defense University Research Instrumentation Program (DURIP) contract numbers W911NF-14-1-0553/0554 through the Army Research Office.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, April 2015.

[2] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, pp. 245–257, Second 2011.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept 2016.

[4] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-channel Jamming Attacks in Multi-channel Ad Hoc Networks," in *Proceedings of the Second ACM Conference on Wireless Network Security*. ACM, 2009, pp. 169–180.

[5] K. Bicakci and B. Tavli, "Denial-of-Service Attacks and Countermeasures in IEEE 802.11 Wireless Networks," *Comput. Stand. Interfaces*, vol. 31, no. 5, pp. 931–941, Sept 2009.

[6] S. Liu, L. Lazos, and M. Krunz, "Thwarting Inside Jamming Attacks on Wireless Broadcast Communications," in *Proceedings of the Fourth ACM Conference on Wireless Network Security*. New York, NY, USA: ACM, 2011, pp. 29–40.

[7] J. T. Chiang and Y. C. Hu, "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 286–298, Feb 2011.

[8] X. He, H. Dai, and P. Ning, "A Byzantine Attack Defender in Cognitive Radio Networks: The Conditional Frequency Check," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2512–2523, May 2013.

[9] J. K. et al., "Analysis and Mitigation of Interference to the LTE Physical Control Format Indicator Channel," in *IEEE Military Communications Conference*, Oct 2014, pp. 228–234.

[10] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, "Detection and Mitigation of Uplink Control Channel Jamming in LTE," in *IEEE Military Communications Conference*, Oct 2014, pp. 1187–1194.

[11] M. Labib, V. Marojevic, and J. H. Reed, "Analyzing and enhancing the resilience of lte/lte-a systems to rf spoofing," in *Standards for Communications and Networking (CSCN), 2015 IEEE Conference on*.

[12] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, April 2016.

[13] "srsLTE - Open Source LTE," https://github.com/srsLTE, 2016, [Online; last accessed 23-October-2016].

[14] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to Hostile Interference," in *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, Dec 2013, pp. 285–288.

[15] V. Marojevic, D. J. Chheda, R. M. Rao, R. Nealy, J.-M. Park, and J. H. Reed, "Software-Defined Testbed enabling Rapid Prototyping and Controlled Experimentation for the LTE Evolution," in *Wireless Communications and Networking Conference (WCNC), IEEE*, March 2017.