Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference

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

Abstract—**Mission-critical wireless networks are being upgraded to 4G long-term evolution (LTE). These networks require very high reliability and security as well as easy deployment and operation in the field. Wireless communications systems have been vulnerable to jamming, spoofing and other radio frequency (RF) attacks since the early days of analog systems. Although wireless systems have evolved, important security and reliability concerns still exist. This paper presents our methodology for testing 4G LTE operating in harsh signaling environments. We use software-defined radio technology and open-source software to develop a fully configurable protocol-aware interference waveform. We define several test cases that target the entire LTE signal or part of it and evaluate the performance of a mission-critical production LTE system. Our RF experiments show that LTE synchronization signal interference causes significant throughput degradation at low interference power. By dynamically evaluating the performance measurement counters, the k-nearest neighbor classification method can detect the specific RF signaling attack to aid in effective mitigation.**

Keywords—Long-term evolution; mission-critical networks; jamming; spoofing; software-defined radio; testbed; testing.

I. Introduction

Wireless infrastructure and technology add to the well-being of society by providing communications and multimedia services at affordable costs. While the commercial sector continues to expand its service diversity, mission-critical networks and, in particular, public safety and military networks are looking to leverage advances in cellular communications technology and fully adopt both the 4G long-term evolution (LTE) protocol, as well as the significant performance enhancing features developed by the commercial LTE-A equipment manufacturers.

Public safety units use wireless communications to effectively coordinate and provide assistance in time [1]. National security relies on wireless sensors and communications to efficiently assess and quickly respond to potential threats. The increasing number of unmanned vehicles poses more stress on reliable radio communications, where even a partial breakdown can have catastrophic consequences. Mission-critical systems, moreover, need to be quickly deployable and operated in non-ideal and potentially harsh radio frequency (RF) environments.

Wireless communications systems have been vulnerable to jamming, spoofing and other attacks since the early days of analog systems. Although wireless systems have evolved, important security and reliability concerns still exist. Different types of attacks to wireless networks have been the topic of research for several years [2], [3].

Lazos et al. [4] address the problem of control channel jamming in multi-channel ad-hoc networks and propose a randomized distributed channel establishment scheme that allows nodes to select a new control channel using frequency hopping. Bicakci et al. [5] target practical hardware, software, and firmware solutions for 802.11 devices to efficiently combat Denial of Service (DoS) attacks. Chiang et al. [6] introduce a code-tree system for circumventing jamming signals. He et al. [7] show that controlled node mobility can be exploited for increasing the resilience against jamming.

References [8]–[11] investigate different types of RF attacks on LTE networks. Since LTE is an open standard, an adversary can generate a protocol-aware attack, where the interfering signal is overlaid over a specific physical channel to degrade the system performance at low probability of being detected. Above papers conclude that relatively little energy is needed to cause major system performance degradation. Labib et al. [12] coin the term *LTE control channel spoofing*, which refers to transmitting a partial LTE downlink (DL) control frame from a fake eNodeB (eNB), and show that such an attack can cause DoS.

This paper analyzes the vulnerabilities of a mission-critical and commercially based portable LTE system. We introduce a software-defined radio (SDR) testbed and methodology for evaluating the impact of targeted RF interference on a production LTE system that is meant for mission-critical deployment in the field. We provide experimental results and compare the effect of protocol-aware and unaware interference on LTE system performance. Taking advantage of the system's performance measurement (PM) counters, a k-nearest neighbor (k-NN) classification method is proposed to detect the type of interference that the system experiences.

The rest of the paper is organized as follows. Section II presents the LTE system under test and briefly reviews the LTE control channels. Section III introduces our testbed and testing methodology. Section IV provides the performance results and analyses, Section V discusses the proposed detection mechanism, and Section VI concludes the paper.

II. Mission-Critical LTE System Under Test

The system that we analyze is a production LTE system built for military missions and next generation public safety network

This is the author's version of the work. For citation purposes, the definitive Version of Record of this work is: V. Marojevic, R. Rao, S. Ha, J.H. Reed, "Performance analysis of a mission-critical portable LTE system in targeted RF interference," *IEEE VTC Fall 2017*, 24-27 Sept. 2017, to appear on IEEExplore digital library.

trials. The system is embedded in a small form factor with the radio unit, the main unit and the power unit. The main unit features the Evolved Packet Core (EPC). This allows for rapid deployment in the field, needing only a power generator and an antenna mounted on a mast to establish a fully functional cell and offer LTE network access. If backhaul is available, external networks can be accessed.

The next generation public safety network, known as FirstNet in the US, requires compliance with 3GPP LTE Release 8 or higher. The system that we analyze is a 10 MHz frequency-division duplex LTE system that adheres to the Release 8 specifications. That is, it creates LTE frames using the same set of control channels and signals as commercial LTE networks. Commercial LTE user equipment (UEs) can attach to this network. This leverages competitive R&D innovations, industry leading performance enhancements, and sophisticated handheld devices produced for the mass market and available at competitive prices. Note that the specifications for public safety LTE UEs differ from those of commercial UEs, allowing higher transmission power, among others. Our analysis does not assume any specific type of UE. We analyze the LTE system performance. Our results are generalizable across 3GPP compliant LTE networks and UEs since we do not assume any specific LTE-Advanced (Rel. 10 or higher) or LTE-Pro (Rel. 12 or higher) features.

The control channels of the LTE radio access network are essential for providing effective communications capabilities for the users of the system. Without control channels and signals, the rest of the network is unusable. We briefly review some of the fundamental LTE downlink (DL) and uplink (UL) control channels that are relevant for the experiments and analyses of this paper. These channels are available in all releases of LTE. Additional control channels or control information are needed for some of the more advanced LTE features, such as carrier aggregation and use of unlicensed spectrum.

Primary and Secondary Synchronization Signals (PSS/SSS)— The PSS and SSS need to be regularly tracked by the UE in order to maintain synchronization with the eNB of the cell.

Physical Broadcast Channel (PBCH)—The PBCH contains the Master Information Block (MIB) which provides details about the downlink bandwidth, resource length of the Hybrid ARQ (HARQ) Indicator Channel (PHICH), and the System Frame Number (SFN) to aid the UE in frame synchronization. The PBCH is mapped to the central 72 subcarriers of the OFDM symbol and is spread over four frames. It is QPSK modulated with a 16-bit CRC, but with an aggregate coding rate of 1/48.

Physical Downlink Control Channel (PDCCH)—The PDCCH carries critical control information, such as UE resource allocation, the Modulation and Coding Scheme (MCS) of user data, and information about retransmission and MIMO operation. It is QPSK-modulated with rate 1/3 convolutional coding. During initial cell access, it informs the UE of the first System Information Block (SIB1). Without the SIB1, the UE will be unable to complete the cell attachment process. Additionally, after cell attachment, it would be impossible for the UE to decode its data if the PDCCH is improperly decoded.

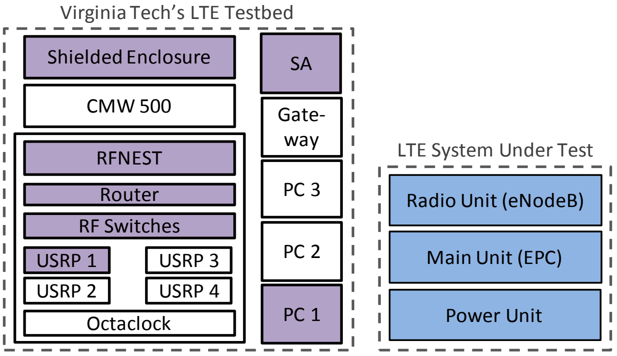


Fig. 1. Testbed hardware (shaded blocks are used in the experiments, SA: signal and spectrum analyzer).

Physical Control Format Indicator Channel (PCFICH)—The PCFICH contains information regarding the size of the PDCCH. It contains the Control Format Indicator (CFI), which is 2 bits, and is encoded using a block code rate of 1/16.

Cell-Specific Reference Signal (CRS)—The CRS carries DL pilot symbols that are used for coherent detection of the digitally modulated data. It is QPSK-modulated and uses a Gold sequence of length 31, which is initialized using the cell ID. The signal occupies about 5% of the LTE DL frame and is distributed across the LTE time-frequency resource grid.

Physical Uplink Control Channel (PUCCH)—The PUCCH is a dedicated control channel that UEs use to request resources and provide related control information to the eNB.

Physical Downlink and Uplink Shared Channels (PDSCH and PUSCH)—These two channels carry the user data on the DL and UL along with certain control information. Note that when a user has an active data session, UL control information is mapped to the PUSCH as opposed to the PUCCH.

III. LTE Testbed and Testing Methodology

A. LTE Testbed: Hardware

Virginia Tech built an LTE testbed using SDRs, LTE test instruments, and emulated and real over-the-air LTE channels [13]. The rackmount testbed includes RF ports for attaching external RF signals. We use one of these ports to attach the mission-critical LTE system to the commercial UE, which is placed in the shielded box. The UE transmits and receives over-the-air over a short distance inside the shielded box. The remaining signal path is guided through RF cables with controlled attenuation. Fig. 1 shows the test setup.

A computer (PC1) generates the interference waveform in software. The samples are passed to an Ettus Universal Software Radio Peripheral (USRP1) via the Ethernet router. USRP1 creates the RF signal that goes through an RF switch into the RFNEST analog channel emulator. The purpose of the RF switch is to enable switching between channel emulation (RFNEST) and antenna (not shown here, see [13] for details). The interference RF signal is combined with the LTE signal from the eNB in RFNEST, which allows selecting independent signal attenuations to obtain the desired signal to interference ratio (ISR). The spectrum analyzer is used to empirically adjust power levels as well as to ensure time synchronization, which is needed only for some of the test cases. Finally the combined signal is passed to an antenna mounted inside the shielded enclosure. Note that the interferer also receives the eNB downlink signal, through USRP1, and uses the PSS and SSS for synchronizing to the cell.

B. LTE Testbed: Software

Our methodology 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, we can evaluate the system performance and determine the weakest component in the system and revise it to improve the overall system robustness. We therefore propose a parametric framework for interference generation, using the same waveform as the target system. In the case of LTE, individual subcarriers and OFDM symbols can be toggled to rapidly generate wideband, narrowband, and protocol-aware interference over any section of the LTE signal. We used the open-source software library srsLTE [16] and developed LTE protocol-aware interference waveforms that target specific subcarriers and OFDM symbols. The srsLTE library implements the LTE uplink and downlink waveforms and readily supports commercial off-the-shelf SDR hardware.

Asynchronous Interference Waveforms—The asynchronous interference waveform generates interference on specific subcarriers. This type of interference can be of certain duration or continuous or discontinuous in time. We can use this setup to generate any interference to LTE that does not need time alignment with the LTE radio frame. In particular, we use it for generating full-band, partial-band, and PUCCH interference, but can also generate a bogus PSS and/or SSS signal (PSS/SSS spoofing) by replacing OFDM symbols with valid synchronization sequences. Fig. 2 shows an example 1.4 MHz interference waveform with three discontinuous blocks of active subcarriers.

Synchronous Interference Waveforms—Transmitting on top of specific physical channels requires synchronization with the network to determine the channel location. Consequently, we use a setup where the interferer (1) acts as a receiver and synchronizes with the eNB, in this case, through LTE's PSS and SSS, and (2) synchronously transmits its interference signal. 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 and SSS.

C. Performance Evaluation Metrics

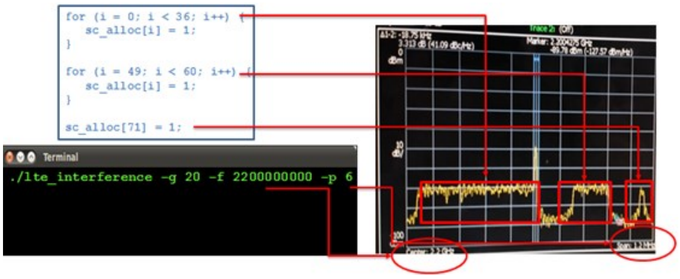
In order to compare the vulnerabilities of different control channels, we define a uniform metric based on ISR, control channel resource occupancy fraction in the LTE signaling frame, and its relative power w.r.t. the data channels. In this regard, we define the following metrics: (a) Interference to Signal Ratio per Resource Element (ISR_{RE}), (b) Interference to Signal Ratio per Frame (ISR_F).

Interference to Signal Ratio per Resource Element—ISR_{RE} is defined as the ratio of the interference signal power to that of the LTE signal, assuming that all the Resource Elements (REs) have the same transmit power.

Interference to Signal Ratio per Frame—When the interferer targets a specific control channel, it occupies a specific fraction of the total number of REs in the LTE DL frame. To account for this, we define it as

$$ISR_F = \frac{ISR_{RE} \times N_{T,F}}{N_{tot,F}},$$

where $N_{T,F}$ denotes the number of targeted REs per frame and $N_{tot,F}$ the total number of REs per frame. We use this metric to compare the effects of different interference strategies on system performance.



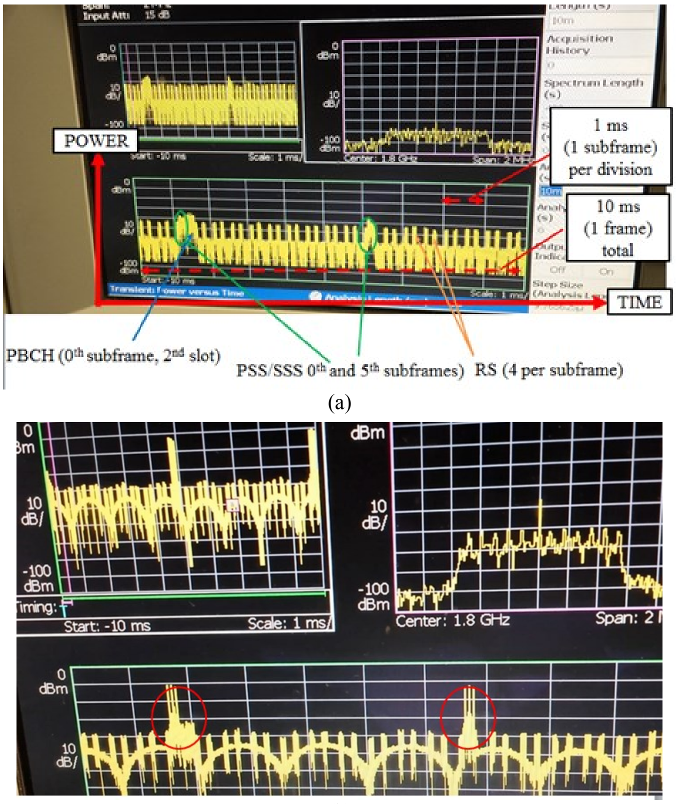
```
for (i = 0; i < 36; i++) {
   sc_alloc[i] = 1;
}

for (i = 49; i < 60; i++) {
   sc_alloc[i] = 1;
}

sc_alloc[71] = 1;
```

```
./lte_interference -g 20 -f 2200000000 -p 6
```

Fig. 2. Asynchronous interference waveform generation.



(a)

(b)

Fig. 3. Partial LTE DL signal which, for illustration purposes, consist of the PSS/SSS, PBCH, and CRS only (a). Partial LTE DL signal with synchronous PSS/SSS interference (b).

D. Test Cases

Table I presents the interference scenarios. The difference between PSS/SSS spoofing and interference is the following: In the case of spoofing, a fake, but legitimate PSS/SSS is transmitted asynchronously to the legitimate PSS/SSS. PSS/SSS interference, on the other hand, implies transmitting interference on top of the eNB's synchronization signals, i.e. synchronously.

The interference node (PC1 with USRP1 in Fig. 1) uses the PSS/SSS from the LTE system under test to synchronize the

TABLE I. TEST CASES (INTERFERENCE SCENARIOS).

	Interference Scenario	Direction	Synchronous
0	No interference	-	-
1	Full-band interference	UL/DL	No
2	Half-band interference	UL/DL	No
3	PUCCH interference	UL	No
4	PUSCH interference	UL	No
5	PSS/SSS spoofing	DL	No
6	PSS/SSS interference	DL	Yes

interference signal with the LTE frame at the UE. This is needed only for the test case 6. The RF signal attenuators are electronically adjusted to achieve the desired ISR. For this we use RFview, the graphical user interface allowing digital control over all 8 signal paths of RFNEST [13]. The controlled test setup ensures a low-noise RF environment such that the LTE system performance becomes interference-limited.

IV. Experimental Results and Analyses

We measure the UL and DL LTE system throughput using iPerf to quantify the impact of interference. The results are shown in Figs. 4 and 5 for two ISR_{RE} vales.

The nominal LTE system throughput is around 12 and 8 mega-bits per second (Mbps) on the DL and UL, respectively. We observe that the throughput degrades as the interference covers more signal bandwidth. In other words, full-band interference is the most severe since all resource elements are affected. However, from Table II we see that this is not a power-efficient method since it requires high interference power.

PUSCH interference is the next most significant threat, but requires slightly less interference power, proportional to the span of the PUSCH w.r.t. the entire LTE system bandwidth. For 10 MHz LTE, PUSCH interference requires about 1.25 dB less power to cause the same degradation as full-band interference on the UL.

PSS/SSS spoofing does not have a significant effect on the throughput because, from the perspective of the receiver, the spoofing synchronization signals are simply asynchronous narrowband signals with a low duty cycle. However, synchronization signal spoofing impedes LTE network acquisition for UEs that are in the initial cell selection process, as demonstrated in [14] and [15]. Synchronous PSS/SSS interference does not cause synchronization loss, even at high ISR; however, there is noticeable degradation of throughput, which proves to be more serious than the potential loss of synchronization.

Because of the sparsity of resource elements that the PSS and SSS occupy in the LTE resource grid, synchronous PSS/SSS interference is a very energy-efficient interference strategy (Table II). PUCCH interference requires 20 times more energy to degrade the UL throughput just as much as PSS/SSS interference. However, the RF energy efficiency comes at the cost of higher complexity in the interference waveform generation because of tight synchronization requirements between the interferer and the UE. If synchronization can be achieved, PSS/SSS interference becomes the by far most serious threat when considering both impact and power efficiency. Imperfect synchronization can be overcome by extending the transmission over more than the two OFDM symbols per half frame of the PSS plus SSS without excessively sacrificing efficiency.

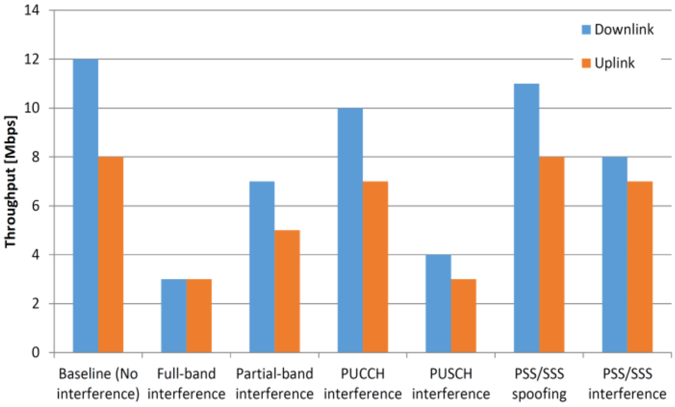


Fig. 4. Throughput results for ISR_{RE} = 0 dB.

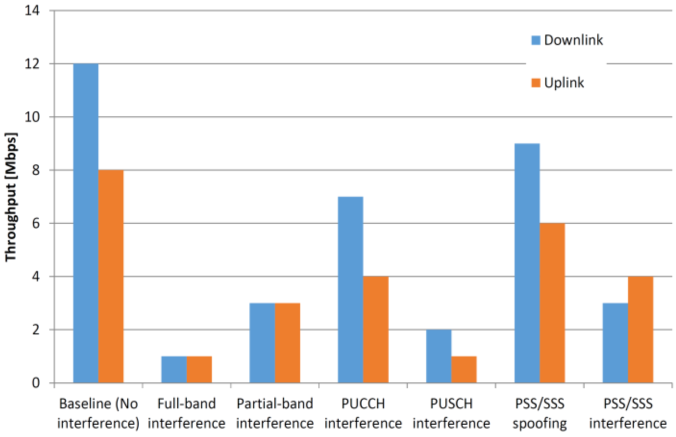


Fig. 5. Throughput results for ISR_{RE} = 5 dB.

TABLE II. RELATION BETWEEN ISR_F AND ISR_{RE} FOR 10 MHz LTE.

Interference Scenario	$\left(\frac{N_{T,F}}{N_{tot,F}}\right)$	$\frac{ISR_F}{ISR_{RE}}$ (dB)
Full-band interference	100%	0
Half-band interference	50%	-3.01
PUCCH interference	25%	-6.02
PUSCH interference	75%	-1.25
PSS/SSS spoofing	0.3%	-25.3
PSS/SSS interference	0.3%	-25.3

V. Interference Detection

The advantage of using mission-critical production LTE equipment is the ability to leverage sophisticated detection mechanisms to determine the presence of interference and determine the type of interference. The LTE test equipment that we used was equipped with a sophisticated performance measurement (PM) system, which includes PM counters that can be leveraged to detect abnormal RF behavior. As an example, we present the case of PUCCH interference detection using a k-NN classification algorithm shown below.

Figure 6 shows the 2-dimensional 3-NN algorithm by monitoring two PUCCH-related performance metrics from our production LTE equipment, which we refer to here as *PM_Counter1* and *PM_Counter2*. For classifying a data point, we examine *k*=3 nearest data points surrounding it. The "blue cluster" in Fig. 6 denotes a classification of "Interference", Algorithm 1: One iteration of k-NN classification

```
1. Initial inputs:
     $N$ metrics (PM Counters/ Key Performance Indicators) as feature-vector $[Metric_1, Metric_2, \ldots, Metric_N]$
     $n$ categories of classification $\{C_1, C_2, \ldots C_n\}$
     $M$ training samples as feature vectors: $\{m_1, \ldots m_N\}$, with each $m_i$ properly classified from one pf the $n$ possible categories.
2. Initialize training samples: $\{m_1, \ldots m_N\}$.
3. Input to current iteration of algorithm:
     Data point (as feature-vector) to classify $x = [Metric_1, Metric_2, \ldots, Metric_N]$
     For each $m_i$ in $\{m_1, \ldots m_N\}$
         Compute distance between $x$ and $m_i$: $d_i = distance(x, m_i)$.
4. Sort $\{d_1, \ldots d_N\}$ in order of increasing distance.
5. Select $\{m_1^*, \ldots, m_k^*\}$ as the $m_i$'s corresponding to the $k$ smallest entries of $\{d_1, \ldots d_N\}$.
6. Classify $x$ based on majority vote: $x$ belongs to the $C^*$corresponding to the category that the majority of the $k$ training samples $\{m_1^*, \ldots, m_k^*\}$ belong to.
```

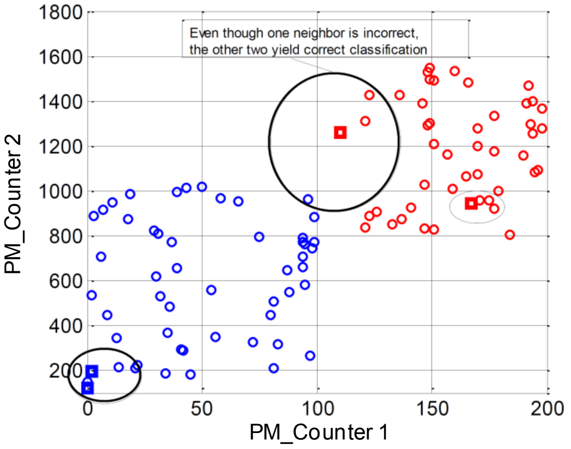


Fig. 6. Detection of PUCCH interference with a 3-NN classification algorithm, using two appropriate PM counters available in the production LTE eNB.

whereas the "red cluster" denotes "No Interference". The circles are dummy initialization points for the k-NN algorithm (may also represent training data) and the squares are actual data points gathered from our experiments. This example illustrates that k-NN is able to properly classify the given PM counter data, even though one data point deviates from the center of the pre-classified initialization points.

VI. Conclusions

This paper has analyzed a mission-critical LTE system operating in a harsh signaling environment. The results have shown that PSS/SSS interference is a major threat to LTE performance after the UE attaches to a cell, and that full-band/half-band and PUSCH interference cause the most severe throughput degradation, but at the cost of higher power. We have also developed a k-NN clustering method that evaluates a subset of the available PM counters to detect the nature of interference. Typical commercial LTE systems have hundreds of PM counters, with many of them applied specifically to RF performance. This is therefore a ripe area for R&D and our results demonstrate how existing mechanisms can be leveraged to detect the presence of unusual interference in the network. This is a crucial step for effective deployment and operation of mission-critical 4G networks and for designing interference-aware systems on the road to 5G. No wireless system can be made 100% secure and, at the same time, efficient. Hence, tradeoffs will need to be made when developing effective interference mitigation techniques. This is an important area in R&D that can significantly contribute to the evolution of wireless protocols towards 5G and beyond.

Acknowledgment

This work was supported in part by Oceus Networks, DURIP contract numbers W911NF-14-1-0553/0554 through the Army Research Office, and the National Science Foundation (NSF) contract number CNS-1642873. The authors would also like to thank Vincent Horne and Amit Ganjoo for their reviews and valuable suggestions that improved the presentation of the work.

References

[1] M. Sohoul, et al., "Next generation public safety networks: a spectrum sharing approach," *IEEE Commun. Mag.*, Vol. 54, Iss. 3, March 2016.

[2] P. Konstantinos, M. Iliofotou, S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Commun. Surveys & Tutorials*, Vol. 13, No. 2, pp. 245-257, 2011.

[3] Y.-S. Shiu, Y. C. Shih, H.-C. Wu, S.C.-H. Huang, H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, Vol. 18, Iss. 2, pp. 66-74, April 2011.

[4] L. Lazos, Sisi Liu, M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," *Proc. 2nd ACM Conf. Wireless Network Security*, 2009, pp. 169-180.

[5] K. Bicakci, B. Tavli, "Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks," *ACM J. Computer Standards & Interfaces*, Vol. 31, Iss. 5, pp. 931-941, Sept. 2009.

[6] J. T. Chiang, Yih-Chun Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," *IEEE/ACM Trans. Networking (TON)*, Vol. 19, Iss. 1, pp. 286-298, Feb. 2011.

[7] X. He, H. Dai, P. Ning, "Dynamic adaptive anti-jamming via mobility control," *IEEE Trans. Wireless Communications*, Vol. 13, Iss. 8, pp. 4374-4388, Aug. 2014.

[8] S. Bhattarai, "On simulation studies of jamming threats against LTE networks", *Proc. IEEE Int. Conf. Computing, Networking and Comms. (ICNC 2015)*, Anaheim, CA, USA. 16-19 Feb., 2015, pp. 99-103.

[9] J. Kakar, et al., "Analysis and mitigation of interference to the LTE Physical Control Format Indicator Channel," *Proc. 2014 IEEE MILCOM*, Baltimore, MD, 6-8 Oct. 2014, pp. 228-234.

[10] F. Aziz, J. Shamma, G. Stuber, "Resilience of LTE networks against smart jamming attacks," *Proc. 2014 IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 734-739.

[11] M. Lichtman, et al., "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Commun. Mag.*, April 2016.

[12] M. Labib, V. Marojevic, J. Reed, "Analyzing and enhancing the resilience of LTE/LTE-A," *Proc. IEEE Conf. Standards for Communications and Networking (CSCN)*, Tokyo, Japan, 28-30 Oct. 2015, pp. 315-320.

[13] V. Marojevic, et al., "Software-defined testbed enabling rapid prototyping and controlled experiments for the LTE evolution," *IEEE WCNC*, 19-22 Mar. 2017.

[14] M. Labib, V. Marojevic, J. Reed, A. Zaghloul, "How to enhance the immunity of LTE systems against RF spoofing," *Proc. Int. Conf. Computing, Networking and Comms. (ICNC 2016)*, Kauai, HI, 15-18 Feb. 2016.

[15] M. Labib, V. Marojevic, J.H. Reed, A.I. Zaghloul, "Enhancing the robustness of LTE systems: analysis and evolution of the cell selection process," *IEEE Commun. Mag.*, Vol. 55, Iss. 2, Feb. 2017.

[16] srsLTE - Open Source LTE, https://github.com/srsLT