A Countermeasure against Smart Jamming Attacks on LTE Synchronization Signals

Mert Eygi[1, 2] and Gunes Karabulut Kurt[1]
[1] Wireless Communication Research Laboratory (WCRL), Istanbul Technical University, Istanbul and 34469, Turkey
[2] TURKCELL Iletisim Hizmetleri A.S. ¸Istanbul, Turkey
Email: {eygi17, gkurt}@itu.edu.tr

Abstract —Long-Term Evolution (LTE) is one of the most frequently used wireless communication technology. As every wireless network, LTE is vulnerable to physical layer (PHY) jamming attacks due to the broadcast nature of channels. Since the jammer attacks are getting smarter and energy efficient, they can target a specific region or physical channel instead of entire band. Targeting the physical LTE downlink Synchronization Signals (SS) could be the most dangerous objective. In this paper, we investigate LTE PHY jamming attack against only primary and secondary synchronization signals. Jammer detection is performed by using Neyman-Pearson theorem. Then, a countermeasure method is proposed. Simulation results show that the proposed countermeasure can achieve lower pollution and better correct cell id performances during smart jamming attack against SS.

Index Terms—LTE, physical layer, jamming attack, primary synchronization signals, secondary synchronization signals

I. Introduction

To establish the downlink (DL) access, a User Equipment (UE) performs the cell search procedure, which includes achieving the initial synchronization and searching a base station (eNB) by using Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS). In this paper, we investigate the jamming of these Synchronization Signals (SS). A proposed method against this type of jammer is also explained.

In literature, some works on PSS and SSS are about modifying their existing algorithms. For example, [1] and [2] focus on the algorithms of SS to improve or reduce their complexity. Nevertheless, such algorithm improvements are not the subject of this publication. [3] and [4] state that since PSS and SSS are detectable at low SNR, jamming them needs fairly high power and synchronization, then the PSS or SSS spoofing could be efficient as well as jamming. According to these two papers, although PSS spoofing impacts very low amount RE (0.45%) and lowest radio frame jammer-to-signal value (-20dB) and its impact causes denial-of-service (DoS). Also, [5] denotes that the easiest way of control channel spoofing is PSS and SSS. A test-bed for synchronization spoofing is constructed and a UE cannot camp on the eNB while the received power of fake PSS is higher than the legitimate one. Likewise, [6] considers LTE initial synchronization and spoofing SS offers as a jamming method. [7] points out that jamming SS and physical broadcast channel (PBCH) are efficient and easy way to cause DoS. When the jammer is active, throughput, received SINR and block error rate of physical DL shared channel (PDSCH) and PBCH are sharply degraded. Similarly, in [8], our previous work, we perform a jamming attack on a commercial LTE network in both DL and UL transmission. Jamming the whole DL control signals including SS causes more negative results than UL control signals in terms of real network performance metrics such as SINR and throughput. Furthermore, [9] express a pulsed jammer synchronized on PSS and SSS is one of the most effective jammer type.

Despite all these valuable studies, there is no suggested method to prevent or to reduce the effect of only SS jamming. Our main contribution with this publication addresses this gap. Although jamming SS requires a high synchronization, the jammer attacks are getting smarter with of time. This study aims to shed light on what if the jammer attacks only SS and provides a countermeasure method for this type of jammer. Furthermore, we present a new performance metric called *Cell ID Correction Percentage* to support our results.

The reminder of this paper is organized as follow: Section II introduces a brief overview about LTE synchronization process and signals. Session III explains the three system models. Section IV describes the simulation environment including simulation details and performance metrics. The simulation results and their discussions are carried out in Section V, while the conclusion is presented in Section VI.

II. A Brief Overview of LTE Sychronization Signals

When the power of a UE is turned on, that UE needs to find an LTE cell for tuning. This process is called cell search and during this process, the UE gets a carrier frequency, cyclic prefix (CP) length, subframe and frame timing and physical layer (PHY) cell id. After that, the UE can get broadcast system information from the network. First of all, public land mobile network (PLMN) is selected, and then the cell search procedure starts. In that process, all supported LTE frequency bands are scanned by the UE. After finding the active channel, the UE selects the strongest cell in that RF channel. Thanks to SS, the UE completes the time and frequency

Manuscript received October 5, 2019; revised July 1, 2020.
This work is supported by the framework of ITU-AYP-2017-2.
Corresponding author email: eygi17@itu.edu.tr.
doi:10.12720/jcm.15.8.626-632

synchronization. SS play vital role on cell search procedure. Then, by using reference signal (RS), UE performs RF condition measurements for channel equalization to solve master information block (MIB) to access critical parameters for LTE DL systems.

PSS are mainly responsible for detection of carrier frequency, SS symbol timing and sub cell id called N_{subCI} whereas SSS are in charge of radio frame timing, PHY cell id group, N_{subCI} whereas SSS are in charge of detection of radio frame timing, PHY cell id group, N_{CIG} , and CP configurations. In LTE, there are 504 PHY cell identities (N_{ID}^{CELL}). Each identity consists of 168 unique N_{CIG} from 0 to 167 and each group differentiates with 3 unique N_{subCI} identities such as 0, 1 and 2. PHY cell id is calculated as;

$$N_{ID}^{CELL} = 3N_{CIG} + N_{subCI} \tag{1}$$

As mentioned before, to complete the cell search procedure, correct detection of the PHY cell id is very critical. In commercial LTE networks, N_{ID}^{CELL} planning requires to prevent N_{ID}^{CELL} conflict in a region. If there is conflict, the UE could camp on the wrong cell that is the far away, the UE does not service from the network, packet fails are increases and some network KPIs (key performance indicators) are reduces. That is why we are focusing on detection of correct cell id as a performance metric.

Frequency-domain Zadoff-Chu sequences are used to generate PSS. In [10], D. Chu described the Zadoff-Chu sequences from Frank-Zadoff sequences. They are very suitable for using these codes as a synchronization code because of zero cyclic autocorrelation feature for all nonzero lags. This feature provides to get maximum correlation between ideal and a received sequence when there is no lag. If the lag is not zero, the correlation becomes zero. The root indices 25, 29 and 34 are used to generate PSS. Besides, three Maximum Length Sequences (MLS) synchronization sequences play role to generate SSS. MLS is the subset of pseudo-random binary sequence and it is generated using maximal linear feedback shift registers. The SSS are scrambled but PSS are not scrambled. The 3rd Generation Partnership Project (3GPP) document [11] explains how to generate PSS and SSS sequences in detail.

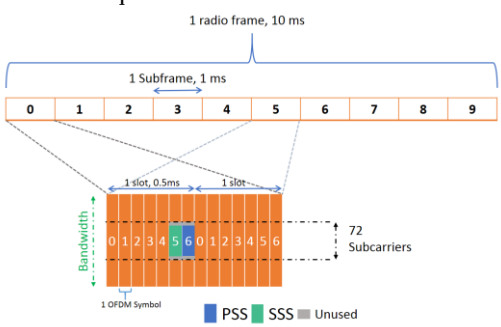

Fig. 1. Radio frame structure including PSS and SSS locations for normal cyclic prefix in frequency division duplex mode.

In PHY radio frame structure, CP length type (normal or extended) and duplex mode (frequency division duplex or time division duplex) determine the position of the PSS or SSS sequences. In FDD with normal CP length, the SSS and PSS are both respectively located at one after the other in the subframe 0 and 5. Within these subframes, both SSS and PSS are located at the end of the OFDM symbol. In addition to that, the PSS and SSS are located at the center 72 subcarriers with 1.08 MHz bandwidth. LTE FDD DL frame structure and the location of PSS and SSS are shown in Fig. 1.

III. System Model

During analysis, we have three system models. In the first case, we do not have any smart jamming attack to the system. Therefore, it is named as *Standard Transmission*. In the second model, called *Under Jammer Attack*, we have smart jammer that aims to destroy the synchronization signals but any countermeasure is not applied. A countermeasure is applied to the second model and it is called *Proposed Countermeasure*, which is the third system model.

A. Standard LTE DL Transmission

In the OFDM modulation the transmitted data stream symbols, $\mathbf{S}$, are divided into N_{sc} by using Serial-to-Parallel (S/P) converter, inverse discrete Fourier Transform (IDFT) operation is applied for all subcarriers. The dimension of the Fourier transform is N and it is equal to the N_{SC}^{DL} . Next cyclic prefix is adding to eliminate inter symbol interference, they are multiplexed and converted to analog by using digital-to-analog converter (DAC). After passing though fading channel, which impulse response is $g(t)$, and adding white complex Gaussian noise vector $n(t)$, the time domain signals reach to receiver. At the receiver, the reverse operation is performed to get received symbols matrix $\mathbf{Y}$. By using the (2) in [12] the mathematical expression in terms of N-point DFT;

$$\mathbf{Y} = DFT_N(IDFT_N(\mathbf{S}) \odot \frac{\mathbf{g}}{\sqrt{N}} + \mathbf{n}) \tag{2}$$

where $\mathbf{g} = [g_0, g_1, \dots, g_{N-1}]$ is a vector that is the frequency response of the channel $\mathbf{n} = [n_0, n_1, \dots, n_{N-1}]$ is complex zero mean i.i.d Gaussian noise vector and $\odot$ is cyclic convolution operator. By modelling the channel as N independent Gaussian channels, the system is modelled for the kth subcarrier;

$$\mathbf{y}_k = \mathbf{s}_k \mathbf{h}_k + \mathbf{n}' \tag{3}$$

where $\mathbf{h} = DFT(\mathbf{g})$, $\mathbf{n}' = DFT(\mathbf{n})$ and $k \in N_{SC}^{DL}$.

After OFDM demodulation, the channel estimation and equalization operations are applied. The reference symbols (RS) are used to estimate the channel. Then we can write;

$$\mathbf{Y}_{RS} = \mathbf{S}_{RS}\mathbf{H}_{RS} + \mathbf{n}'_{RS} \tag{4}$$

where $\mathbf{S}_{RS}$ is a diagonal matrix, $\mathbf{H} = \mathbf{Fg}$, where $\mathbf{H}$ is the impulse response of the channel and $\mathbf{F}$ represents the DFT operation matrix.

If the channel vector is Gaussian and uncorrelated with the channel noise, the minimum mean square estimator (MMSE), $\hat{\mathbf{g}}$, consists of cross-correlation matrix between $\mathbf{g}$ and $\mathbf{y}$, $\mathbf{R}_{gy}$ and the auto-covariance matrix of $\mathbf{y}$, $\mathbf{R}_{yy}$;

$$\hat{\mathbf{g}} = \mathbf{R}_{gy}\mathbf{R}_{yy}^{-1}\mathbf{y} \tag{5}$$

Due to multi-path environment of the system, amplitude distortion and shifted phase occurs in OFDM data. According to the [13], by using the estimated channel impulse response, the received data could be equalized. Therefore, the estimated form of the received data on the kth subcarrier is;

$$\hat{S}_k = \left(\frac{\hat{H}_k^*}{\| H_k \|^2} + \sigma_k^2\right) Y_k \tag{6}$$

where $\hat{\mathbf{H}} = \mathbf{F}\hat{\mathbf{g}}$ and $(\cdot)^*$ is the complex conjugate.

B. *Standard LTE DL Transmission with Jammer: "Under Jammer Attack"*

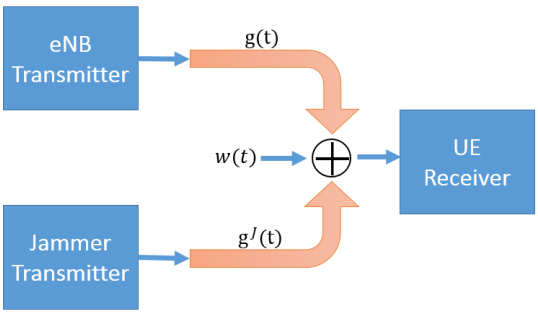

Fig. 2. The system model of the under jammer attack.

Since LTE DL control signals are not encrypted to all UEs and eavesdroppers, unauthorized sniffers can conveniently take the required information for blocking the services or damaging transmission. In our situation, the jammer sniffs the LTE DL transmission to synchronize the subframe and frame timing. To reveal the most dangerous SS signals attack, it is assumed that the jammer transmits its signals with the same SS indices as eNB. Fig. 2 shows the system model of the *Under Jammer Attack*. The g(t) and $g^j(t)$ denote the fading channels that effect eNB and jammer transmitted waveforms, respectively. The $w(t)$ represents the AWGN Noise. The jammer transmits only REs that contains malicious SS, all other REs are empty to minimize its power. The jammer SS signals are generated randomly with that property;

$$|\mathbf{SS}_{eNB}| = |\mathbf{SS}_{jammer}| \tag{7}$$

where the size of $\mathbf{SS}_{jammer}$ and $\mathbf{SS}_{eNB}$ are 62 (subcarrier)-by-4(OFDM symbols) complex signals.

C. *A Mitigation Method during SS Jamming: "*Proposed Countermeasure*"*

When SS jamming occurs, we perform a countermeasure method that eNB replaces the location of synchronization signals. In other words, PSS and SSS are replaced in OFDM Symbols. To detect SS jamming, a binary hypothesis testing problem for the received signal is defined;

$$\begin{aligned} H_0 &: \mathbf{Y}_{SS} = \mathbf{S}_{SS}\mathbf{H}_{SS} + \mathbf{w}_{ss} \\ H_1 &: \mathbf{Y}_{SS} = \mathbf{S}_{SS}\mathbf{H}_{SS} + \mathbf{J}_{SS}\mathbf{H}_{SS}^J + \mathbf{w}_{ss} \end{aligned} \tag{8}$$

where $\mathbf{Y}_{SS}$, $\mathbf{S}_{SS}$ and $\mathbf{J}_{SS}$ are the received SS at UE, transmitted SS from eNB and transmitted signals from Jammer, respectively. $\mathbf{H}_{SS}$ states the SS channel frequency responses between eNB and UE whereas $\mathbf{H}_{SS}^J$ denotes the SS channel frequency responses between jammer and UE. $\mathbf{w}_{SS} \sim \mathcal{CN}(0, \sigma_w^2\mathbf{I})$ is circular symmetric complex Gaussian noise for SS transmission.

The system model of this case is shown in Fig. 3 where λ the detection threshold is. If the SS jammer is detected, the UE informs the base station for replacing SS to save jammer attack. Else, there is no need to indices replacement in SS.

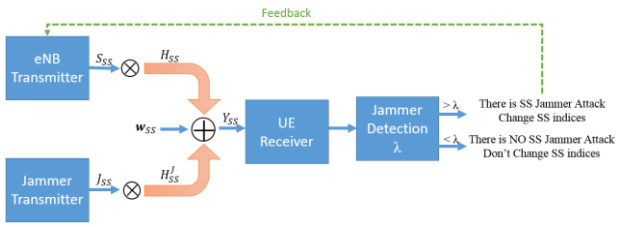

Fig. 3. The system model of the proposed countermeasure.

IV. Description of Simulation Environment

Our LTE DL transmission tests are realized in MATLAB®. In this section, simulation parameters details are described. Subsequently, performance metrics used in next section are explained in detail. Our performance metrics are error vector magnitude and Cell ID correction percentage.

A. *Simulation Descriptions*

During all simulations, SISO transmission is performed for simplicity. In other words, eNB, UE and Jammer have an antenna. However, MIMO transmission could be performed easily because it does not affect length or positions of SS Signals. Then, our simulations proposed solution can be applied. eNB transmitted waveform and grid are generated by using reference measurement channel (RMC) tool to realize LTE transmission. This tool has two inputs. The first one is cell-wide settings to have eNB configuration. This cell-wide settings are shown in the Table I. The second one is information bits vector to transport data. If the information bits remains empty, the transmission of PDSCH and its corresponding PDCCH are skipped in the transmitted waveform.

Table I: eNB Cell-Wide Settings

Parameters	Value	Description
N_{RB}^{DL}	50	DL resource blocks number

CellRefP	1	Reference Signal antenna ports number
N_{ID}^{CELL}	17	Physical layer cell identity
CP	'Normal'	Cyclic Prefix length
DuplexMode	'FDD'	Duplexing mode
CFI	2	Control format indicator
Ng	'sixth'	HICH group multiplier
PHICHDuration	'Normal'	PHICH Duration
N_{FFT}	1024	FFT size

B. Performance Metrics

The definitions and calculations of Error vector magnitude and cell id, N_{ID}^{CELL}, correction are introduced as performance metrics. The main results of the simulations to be shown in the next section are examined according to these performance metrics.

The whole signal quality can be indicated by error vector magnitude (EVM). In [14], [15] The EVM is identified as the square root of the average power of the error vector divided by average power of the reference signal. In some sort, RMS (Root-mean-squared) value between measured and ideal symbols is calculated in EVM, this EVM is called as RMS EVM.

Let the received symbol at the lth resource element is $\hat{a}_l + j\hat{b}_l$ and the reference or transmitted symbol is $a_l + jb_l$. Then the EVM can be expressed as;

$$EVM_{RMS} = 100\sqrt{\frac{\frac{1}{L}\sum_{l=1}^{L}(a_l - \hat{a}_l)^2 + (b_l - \hat{b}_l)^2}{\frac{1}{L}\sum_{l=1}^{L}(a_l + b_l)^2}} \quad (9)$$

where L is the total number of RE, a_l and $\hat{a}_l$ are in-phase measurement of the l th RE whereas b_l and $\hat{b}_l$ are quadrature-phase measurement of the lth RE. We always perform post-equalized signals EVM RMS measurement for RE that has PSS and SSS complex signals.

The second performance metric is cell ID correction percentage. This metric is generated by comparing the identified cell identity at the UE, called N_{CID}^{UE} versus determined cell identity in the, called N_{CID}^{eNB}. To obtain N_{CID}^{UE}, *ltecellsearch* function of the MATLAB® is used. The function gives the cell identity carried by SS signals in the received waveform. Time-domain and frequency-domain correlations are used to detect PSS and SSS, respectively. To have reliable results, monte-carlo simulation method is performed with trial number, N_{Tr}. In each trial, tr, N_{CID}^{eNB} and N_{CID}^{UE} are compared. If they are equal, the *counter* is incremented by 1. Then the cell id correction percentage, CID_{Corr}, is defined as;

$$CID_{Corr} = 100 \times \frac{count(N_{CID}^{UE} == N_{CID}^{eNB})_{tr}}{N_{Tr}} \quad (10)$$

V. Numerical Results and Discussions

During all analysis, we assumed that the jammer's objective is blocking only DL Synchronization Signals. Therefore, we start with the detection of SS Jammer. When SS Jammer is present, to minimize the damage, SS block replacement solution is applied. In that case, the question is how many OFDM symbols the SS should replace and it is answered. Finally, it is examined what happens if the power of jammer is increased.

Before applying proposed mitigation method, detection of SS jammer should be done. In literature, jammer detection methods are proposed such as simple energy detector or interference identification with classification. While our analysis, by using the definitions and equations in [16], we perform a binary hypothesis-testing problem for expressed in (8). H_0 refers *Standard Transmission* and there is no jammer attack to SS during transmission whereas H_1 denotes *Under Jammer Attack* case and in that case, the SS jammer is active. The EVM of SS of the received signal are used for benchmarking of two cases. Since the noise assumed circularly symmetric complex Gaussian, the histograms of the EVM of SS block becomes Gaussian. In addition to that, adding the jammer signal to the eNB signal shifts the EVM histogram for the H_1. In other words, the hypothesis-testing problem is considered as a mean-shifted Gaussian problem as shown in the Fig. 4. During analysis, SNR range is from -10 to 4 dB and Fig. 4. shows only four of them. It is obviously seen that the EVM performance is decreases while SNR decreases.

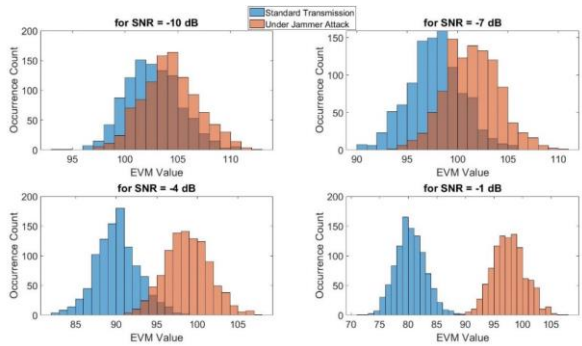

Fig. 4. EVM Histograms corresponding four SNR values.

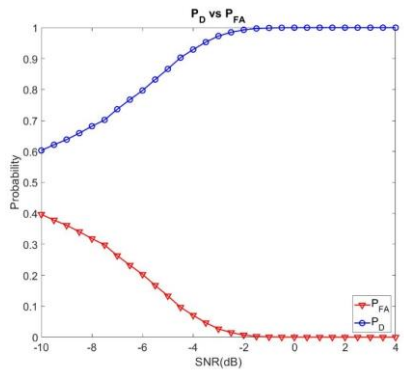

Fig. 5. Probability of Detection (P_D) and False Alarm (P_{FA}) values corresponding to each SNR.

After obtaining SS EVMs for each SNR value, the threshold of the detector is considered as the middle point of the EVMs. Subsequently, the detection probability, P_D versus probability of false alarm, P_{FA} for each SNR value is obtained and the performance of the detector is shown in Fig. 5. It can easily say that, low SNR values sharply reduces the detection performance. For examples, the P_D

becomes 62.17% at SNR 9.5 dB or when the SNR is equal to 7.5dB the P_{FA} is 29.80% for a determined threshold λ.

While SS Jammer is present, our recommended mitigation method is implemented to switch the case from *Under Jammer Attack* to *Proposed Countermeasure*. In this situation, the "new" position of the SS block should be determined. According to the 3GPP specifications, the synchronization signals are expected on the subframe 0 and 5. Therefore, we are looking forward to a place for SS

FDD Frame structure, the first right 4 OFDM symbols of SS block are reserved for PBCH in subframe 0. In addition to that, the other downlink control channels are placed mostly at first two symbols in each subframe and it means that left 4 or 5 symbol of SS block are reserved for these channel signals. Consequently, we have only four options for determining how many symbol should be replaced the SS block;

Option #1: replace the SS block symbol numbers by -3.
Option #2: replace the SS block symbol numbers by -2.
Option #3: replace the SS block symbol numbers by 6.
Option #4: replace the SS block symbol numbers by 7.

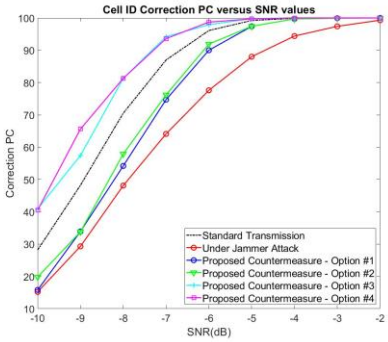

Fig. 6. Cell id correction percentage for all possible cases and options.

To determine the best replacement Option, N_{ID}^{CELL} correction percentile metric is investigated. In addition to the four options, the *Standard Transmission* and *Under Jammer Attack* are added for comparison. Please note that, In *Standard Transmission*, is there is no SS jammer whereas in the *Under Jammer Attack*, there is a jammer attack. However, the replacement solution is not applied. Fig. 6. states that, all possible replacement options have better N_{ID}^{CELL} correction percentage than the *Under Jammer Attack* at low SNR values. It is interesting that the Options #3 and #4 have better cell id correction percentage than *Standard Transmission*. To reveal the reason of that, we investigate EVM comparisons for slots from 0 to 19 within one radio frame. The fading channel models and doppler frequencies are changed for each slot comparison. It is interesting that, the odd numbered slots have better EVM results than the even numbered slots. Since options #3 and #4 are placed in slot number 1, their results are much better than the other cases including *Standard Transmission*. In addition to that, the (7) holds, which means that the SS Block power of jammer is equal to the eNB SS block power. Since the option #4 has the best correction performance, the SS block is replaced by 7 OFDM symbol in the *Proposed Countermeasure* for the next following analysis.

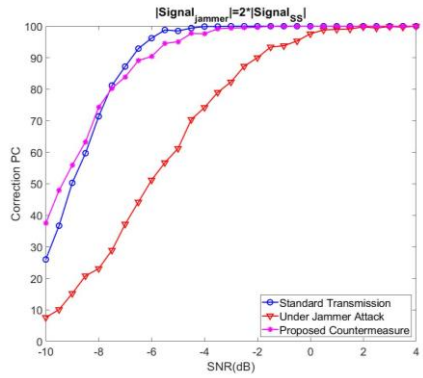

Fig. 7. Cell id correction percentage when the jammer doubles its SS signals magnitude.

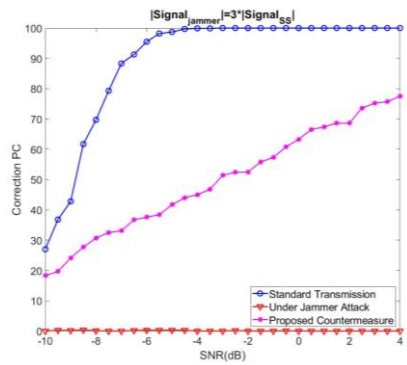

Fig. 8. Cell id correction percentage when the jammer triples its SS signals magnitude.

Further, we analyze what happens when the jammer increases its power. The Fig. 7 represents the correction percentiles if the jammer signal doubles the enB SS block magnitude whereas the Fig. 8. figure shows what if jammer signal triples. Cell id correction margin increases between *Under Jammer Attack* and others. For instance, at SNR -5 dB, the *Under Jammer Attack*, *Proposed Countermeasure* and *Standard Transmission* is equal to 61.2%, 94.5% and 98.5% correction percentile, respectively. The *Proposed Countermeasure* is effected partially while the increasing jammer power. In addition to that, only after 4 dB, the *Under Jammer Attack* has the 100% correction percentile. On the other hand, the Fig. 8. shows that how cruelly jammer power can affect the cell id correction. Even at high SNR values, *Under Jammer Attack* does not pass the 0.5%. Although our proposed solution is also effected sharply from the jammer, the correct cell id information can rescue. Numerically, *Under Jammer Attack*, *Proposed Countermeasure* and Standard *Transmission* is equal to 0%, 73.6% and 100% at SNR 2.5 dB, respectively.

VI. Conclusions

In this paper, we indicate that the SS jamming reduces the cell id correction percentage remarkably. When this

occurs, the UEs, which are under SS jamming, cannot access the LTE network, then this type of attack should be considered as DoS. In our work, to detect the jammer, EVM measurements are used by Neyman-Pearson analysis. Further, when the SS jammer is present, we put forward a countermeasure method that minimizes the jammer effect. The method is done by replacing the OFDM symbol of both PSS and SS. Moreover, we find out that the most optimal replacement is 7 symbols. Finally, we study what happens when the jammer increases its signal magnitude. In these cases, our mitigation method advantages much more remarkable and increases the cell is correct detection percentage sharply.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Both authors conceived of the presented idea. G,K developed the system design whereas M,E performed the derivations and simulations. The authors discussed the results and contributed. They had approved the final version.

Acknowledgment

This work is mainly supported by the framework of ITU-AYP-2017-2. Also, the authors would like to thank Turkcell Iletisim Hizmetleri A.S. for collaborative approach and supports.

References

[1] C. Eric M. Silva, G. J. Dolecek, and F. J. Harris, "Cell search in long term evolution systems: Primary and secondary synchronization," in *Proc. IEEE 3rd Latin American Symposium on Circuits and Systems (LASCAS)*, 2012, pp. 1-4.

[2] B. Shoba and K. Jayanthi, "Low complex primary and secondary synchronization signal structure design for LTE systems," in *Proc. International Conference on Microwave, Optical and Communication Engineering (ICMOCE)*, IEEE, 2015, pp. 467-470.

[3] 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, 2016.

[4] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," in *Proc. IEEE Global Conference on Signal and Information Processing*, 2013, pp. 285-288.

[5] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "How to enhance the immunity of LTE systems against RF spoofing," in *Proc. International Conference on Computing, Networking and Communications (ICNC)*, IEEE, 2016, pp. 1-5.

[6] X. Li, X. Xie, J. Zeng, and Y. Wang, "Vulnerability analysis and verification for LTE initial synchronization mechanism," in *Proc. 36th IEEE Sarnoff Symposium*, IEEE, 2015, pp. 150-154.

[7] R. Krenz and S. Brahma, "Jamming LTE signals," in *Proc. IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2015, pp. 72-76.

[8] Y. Coskun, M. Eygi, G. Sezgin, and G. K. Kurt, "Jamming resilience of lte networks: A measurement study," in *Proc. International Telecommunications Conference*, Springer, 2019, pp. 151-162.

[9] G. Philippe, F. Montaigne, J. C. Schiel, E. Georgeaux, C. Gruet, Y. Roy, *et al*, "LTE resistance to jamming capability: To which extend a standard LTE system is able to resist to intentional jammers," in *Proc. Military Communications and Information Systems Conference*, 2013, pp. 1-4.

[10] D. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Transactions on Information Theory*, vol. 18, no. 4, pp. 531-532, 1972.

[11] Evolved Universal Terrestrial Radio Access, "Physical channels and modulation," 3GPP TS 36.211. V10.2, 2009.

[12] J. J. V. D. Beek, O. Edfors, M. Sandell, S. K. Wilson, and P. O. Borjesson, "On channel estimation in OFDM systems," in *Proc. IEEE 45th Vehicular Technology Conference*, 1995, pp. 815-819.

[13] A. Mehmood and W. A. Cheema, "Channel estimation for lte downlink," M.S. thesis, Dept. Electrical Eng., Blekinge Institute of Technology, Karlskrona, Sweden 2009.

[14] H. F. Wang, C. P. Hwang, and M. S Chen, "The error vector magnitude (EVM) performance in LTE downlink," in *Proc. Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC)*, IEEE, 2019, pp. 1-3.

[15] H. A. Mahmoud and H. Arslan, "Error vector magnitude to SNR conversion for nondata-aided receivers," *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2694-2704, 2009.

[16] S. M. Kay, *Fundamentals of Statistical Signal Processing*, Prentice Hall PTR, 1993.

Mert Eygi was born in Izmir Province, Turkey, in 1992. He received the B.S. degree from the Izmir Institute of Technology in 2015 in electrical and electronics engineering. He has received the MS degree in Telecommunications Engineering from Istanbul Technical University in 2020. His master thesis subject is about LTE physical layer jamming attacks and their mitigation methods. At the same time, he is currently working

for Turkcell Iletisim A.S. as an access network planning and optimization engineer.

Gunes Karabulut Kurt received the B.S. degree in electronics and electrical engineering from Bogazici University, Istanbul, Turkey, in 2000, the M.S. and Ph.D. degree from University of Ottawa, in 2002 and 2006, Ottawa, Canada, and both in electrical engineering. She is currently a professor of electronics and communication department at Istanbul Technical University in Istanbul, Turkey. Her research interests include wireless communications, network coding, communication testbed, localization and energy harvesting.