SoK: Jamming of LTE

1st Eva Zinn
Technical University of Munich
Munich, Germany
eva.zinn@tum.de

***Abstract*—Long Term Evolution network is widely used in human everyday life but also for mission-critical applications of public security and military communications. Therefore, ensuring its security is crucial. However, studies of the past decades have found multiple denial-of-service (DOS) and loss-of-service attacks in the LTE network. Especially there are many reports on diverse types of jamming attacks. This might be the simplest form of network disruption due to the open nature of wireless channels.**

In this paper, we aimed to provide an easy-to-understand overview of different jamming types and their functionality. We systematized attacks according to their jamming type and functionality and provide categorization of surveys to this topic.

***Index Terms*—LTE, jamming, wireless security**

I. Introduction

LTE networks are among the most commonly used wireless networks. It is used in everyday life and even for mission-critical applications. As the use of LTE networks grows, so does the risk of jamming attacks that can disrupt or degrade the quality of the network. Such disruptions can be used for terrorist attacks. Therefore, it is crucial to ensure their security to prevent life-threatening situations.

details?

One of the reasons, therefore, is the broadcast nature of channels. This is the reason for its vulnerability against physical jamming attacks. Additionally, while the network is developing the attacks are improving too. Jamming attacks are becoming increasingly sophisticated, with improved energy efficiency, and the ability to target specific regions rather than the entire band. Our goal was to create a new perspective on jamming attacks in LTE networks and to identify the most serious threats. The new view is based on the knowledge of existing papers. Systematization and categorization provide an overview of LTE vulnerabilities and the efficiency of different jamming types. We present attack detection and mitigation strategies and point the way for future research.

First, we started with an explanation of the basics of LTE and jamming. This information is to be found in Section II. It starts with the basic knowledge of LTE followed by its physical structure. Finally, the jamming attack is defined, and diverse types are presented.

In Section III Systematization we identify questions and problem statements to the topic and present the tables created for an overview of various aspects of the papers.

The categorization provides an overview of papers, their content, and results. This overview is especially helpful for researchers to identify papers dealing with specific jamming types or to find research gaps for new and further research. After the overview of jammer types strategies for their detection and mitigation are presented. As a result, the reader can use the categorization together with the systematizing tables to understand the current state of research and continue the research on the papers containing specific results or working on the specific problem and save time reading through all the articles to find key points.

The process of writing this paper was challenging, particularly due to finding comparable metrics in different works. It was especially complicated to find a categorization since we had to go through many different articles with different categorizations and identify some similarities between the presented results. The creation of an overview table helped to simplify the process, serving as a prototype for systematizing the study on jamming attacks in LTE networks.

II. Background

A. LTE basics

In LTE the User Devices are called User Equipment (UE). They are constantly monitoring for LTE base stations called evolved NodeB (NodeB) to connect or assist the network. UE has two states: the RRC Connected state used to send or receive data and the RRC Idle state. It cannot remain in RRC Connected state to prevent wasting battery and resources and is predominantly in the RRC Idle state. Depending on the network policies the UE can connect to the earlier network generations if the home LTE network is unavailable. There is 2-way communication between cell phones and mobile networks in LTE. Downlink is the transmission of a cell tower to the cell phone, and uplink is the transmission from the phone to the network.

duh

To connect to the LTE network the UE needs to search and select a node. Then the user receives the system information to learn the up and downlink schedule and frame. After applying the system access protocol the nodes can exchange information.

4G LTE network uses Orthogonal frequency-division multiple access (OFDMA) as a transmission scheme. It allows simultaneous communication of different users in downlink communication. OFDMA splits the wide-band frequency carrier into smaller sub-carriers of 15kHz each. The sub-carriers consist of different information blocks. As a result, the information is mapped to the time and frequency domain. The simultaneous transmission of multiple subcarriers makes the transmission very effective. There are various channels and signals used for transmission.

whats a carrier?
schedule?

B. LTE – Physical structure: channels and signals

Following the main physical channels and signals of LTE will be presented and described.

Uplink channels:

- Primary Uplink Shared Channel***(PUSCH)*** transfers user data
- Primary Uplink Control Channel ***(PUCCH)*** transmits Uplink Control Information (UCI)
- Physical Random Access Channel ***(PRACH)*** transmits Preamble for initial access

Downlink channels:

- Physical downlink shared channel ***(PDSCH)*** transmits user data and system information blocks (SIBs) for random access procedures.
- Physical Downlink Control Channel ***(PDCCH)*** transmits the Downlink Control Information(DCI) containing scheduling information. It is mapped to the first n symbols of OFDM in each of the downlink sub-frame. The amount of symbols is specified in PCFICH and can be from 1 to 4.
- Physical Hybrid ARQ Indicator Channel ***(PHICH)*** notifies about the success of an uploaded package.
- Physical Broadcast Channel ***(PBCH)*** periodically informs UE about the system information: operating parameters and synchronization signals. This information is required to register into the network
- Physical Control Format Indicator Channel ***(PCFICH)*** transfers the Control Frame Indicator (CFI) carrying information about frame structure and identifying the position of the PDCCH resource elements within the downlink frame.
- Physical Multicast Channel ***(PMCH)*** carriers MBMS user data

Uplink signals:

- Demodulation Ref Signal ***(DRS)*** is sent by the UE to the NodeB to enable channel estimation and data demodulation.
- Sounding Ref Signal ***(SRS)*** is configurated by the NodeB as a power reference for support frequency-dependent scheduling enabling uplink channel quality evaluation.

Downlink signals:

- Secondary Synchronization Signal ***(SSS)*** and Primary Synchronization Signal (PSS) contain information on physical layer identity and needs to be regularly tracked by the UE to maintain the connection with the eNodeB
- Cell-Specific Reference Signal ***(C-RS)*** support for channel estimation at the UE by eNodeB.

Other important terms:

- Master Information Block ***(MIB)*** contains the most frequent parameters significant for the initial access to the cell: downlink bandwidth, system frame number (SFN) and PHICH. SFN is required on the user side to receive packets and extract data.

will we need all of these?

C. Jamming

Jamming is a Denial of Service attack. A jammer occupies channels or sends signals to prevent communication between nodes or disrupt the connection. We classify 2 jamming types depending on the used technique: physical jamming and intelligent jamming.

While physical jamming refers to taking advantage of vulnerabilities of physical channels and signals, intelligent jamming takes advantage of the vulnerabilities of the upper-layer protocol e.g., network, transport and application layers [15]. Intelligent jamming requires an understanding of the upper-layer protocols to target the network control packets instead of data packets. In this work, we concentrate on physical jamming and advanced intellectual jamming attack - Smart Jamming.

Following we present a classification of physical jamming types adopted from [15].

Physical jamming refers to the use of radio frequency (RF) signals, however, there are different types of jamming based on their jamming technique e.g., jamming of a specific frequency or subcarrier. In the following diverse types of RF jamming will be presented. not in 15

Noise Jamming is based on transmitting noise or random signals on the same frequency as the target signal to interfere with or disrupt communication. This type of jamming does not require knowledge of the specific protocol or signal and simply aims to overpower it with noise. There are various subtypes of noise jamming e.g. barrage jamming. Barrage jamming refers to the simultaneous transmission of a large number of radio-frequency signals on the same frequency as the LTE network. Gaussian noise jamming uses a Gaussian-distributed noise signal to jam the targeted RF signal. Partial band jamming uses the transmission of additive white Gaussian noise (AWGN) over a specific band of subcarriers to jam the target. Single- and Multi-tone jamming uses high-power single or multiple impulses of AWGN noise to jam single or multiple subcarriers of the targeted signal. details?

Intellectual jamming types:

There are many different types of intellectual jamming and each of them aims to disrupt or degrade the normal operation of the network. The main methods used in this attack type are making use of protocol exploits, launching denial-of-service attacks, manipulating traffic or impersonating legitimate network components. In this work, we concentrate on a specific subtype of protocol exploit – Smart jamming.

Smart jamming is an adaptive jamming algorithm that dynamically adjusts the jamming signal in response to changes in network communication patterns. It can manipulate the information in the LTE network in ways that appear to be normal communication making it difficult for the network to distinguish the jamming from legitimate communication. For example, Smart Jamming can be a collision between an LTE UE and a simple reconfigurable narrowband jammer [1]. The attacker learns the schedule and physical layer parameters and uses the jamming device to deliberately jam signals

too vague

not sure what smart jamming is now?

and channels. Smart jamming is more difficult to detect and mitigate than physical jamming due to its adaptivity.

III. Systematisation

To systematize related surveys, we created a table marking the key aspects the papers deal with. Following we explain what the table represents and what were the ideas behind this systematization.

As you know from Section II there exist various jamming types. As a result, there are surveys dealing with one specific and others dealing with different jamming types. It is important to be able to sort out those dealing with the specific one. Additionally, it is helpful to know whether the paper deals with the vulnerability of specific physical channels and signals. We also noticed that every work related to the topic deals with one of the following questions: network vulnerability, attack detection, and anti-attack strategies. Those criteria are the basis for table 2.

why?

We aimed to create a comparison between different jamming types. Unfortunately, we cannot provide a metric to compare different smart jamming types however it is more effective compared to physical jamming since it can "learn" the network and uses knowledge of LTE protocols. unfounded

To compare the efficiency of different physical jamming types we adapted the metrics and results from surveys to create table 1 and fig. 1 . Table 1 concentrates on physical channels and signals and fig. 1 visualizes the effectiveness from the jammer perspective vs the complexity of exploiting vulnerabilities of the physical layer.

The effectiveness and complexity results were adapted from [5] and [6]. There were some slight differences in the results in this case we adopted the result from the later published work. Both papers use barrage jamming as a baseline and compare other attacks against the baseline. We were inspired by the idea of assembling the attacks into a two-dimensional map from [6]. This visualization method allows the identification of the most effective attacks from the jammer's perspective and those with a good price-quality ratio.

The above-mentioned papers base the efficiency on the jammer-to-signal ratio (J/S). Since the authors use similar calculations for the average J/S we only adopt the result for our comparison. This refers to J/S averaged over an entire frame.

what does that mean?

The complexity is mostly based on the necessity to synchronize to the cell. The authors of [6] are warning of low implementation costs for the most complex attacks. According to them, it is possible within a budget of $1500 by making use of widely available open-source libraries and low-cost software radio hardware.

IV. Categorization of other work

In this Section, we shortly introduce the ideas, methodology, and results of surveys. First, we introduce those papers dealing with the vulnerabilities of the physical layer, because some of the intellectual jamming attacks including some smart jamming subtypes make use of them.

There is no categorization done in this section!!

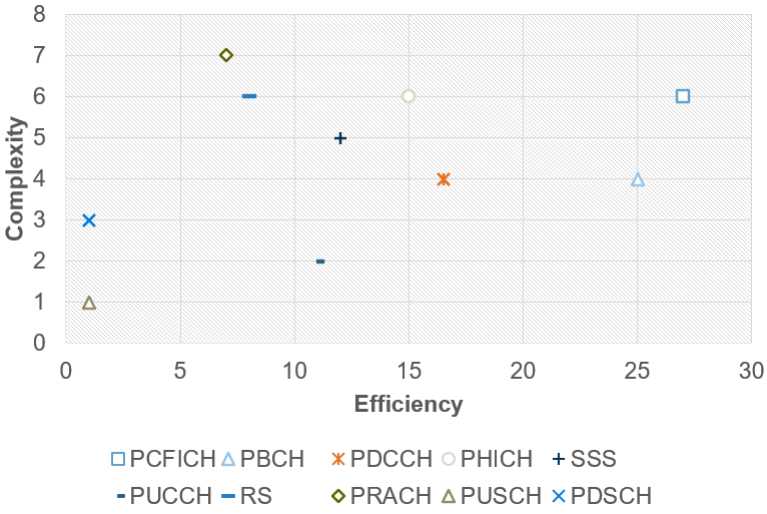

Fig. 1. Ranking of attacks based on efficiency and complexity from table 1.

attack types never explained?

Physical layer

In [5] and [6] the authors investigate the vulnerability extent of LTE physical layer components to intentional jamming. They provided jammer-to-signal ratio-based metrics after an analysis of the physical frame, modulation, and coding schemes. Table 1 was based on the adopted comparison values from these surveys. In case of slight differentiations between the results of surveys, we adopted the results from the later published paper [6]. The surveys focus exclusively on jamming attacks that are more efficient than barrage jamming. The graph 1 visualizes the complexity-efficiency ratio and helps to identify those with the best complexity-efficiency ratio. The most efficient from jammer's point of view are on the bottom right. Except for "the center 6 resource blocks" the jamming names refer to the jammed channel or signal. "Center 6 resource blocks" refers to jamming PBCH without synchronization by the constant waveform duty cycle.

According to [6] there are four main physical vulnerabilities: PCFICH, PBCH, PSS, and PUCCH.

- PCFICH is transmitted in the first OFSM symbol of each subframe and occupies 16Res and is therefore vulnerable to jamming
- PBCH mapped to the central subcarriers on the first 1ms sub-frame of every frame.
- Jamming the PSS or SSS is designed detectable at a low signal-to-noise ratio and requires a high amount of power.
- PUCCH transmited on the edges of the system bandwidth

[3] confirms jamming of synchronization signals as one of the most dangerous attacks as it decreases the cell id correction rate.

[8] confirms concerns about these signals once the user device connects to the cell. The control information of PUCCH is placed on the edges of the system bandwidth. Therefore, a jammer only needs information on LTE system bandwidth and centre frequency.

for what?

In [16] authors concentrated explicitly on PUCCH. The

Jamming type	Channel	Signal	Direction	Synch. Required	Complexity	J/SF
PCFICH	✓		d	+	High	-27 dB
PBCH	✓		d	+	Medium	-25 dB
PDCCH	✓		d	+	Medium	-16.5 dB
PHICH	✓		d	+	Hight	-15 dB
SSS		✓	d	+	Medium High	-12 dB
Center 6 Resource Blocks	✓		d	+	Very Low	-11 dB
PUCCH	✓		u	-	Low	-11 dB
RS		✓	d	+	High	-8 dB
PRACH	✓		u	+	Very High	-7 dB
Barrage jammer	n/a	n/a	n/a	-	Very Low	-2 dB
PUSCH	✓		u	+	Very Low	-1 dB
PDSCH	✓		d	-	Low Medium	-1 dB

what does this type mean ??

TABLE I
PHYSICAL JAMMING ATTACKS SORTED BY EFFICIENCY. ADAPTED FROM [5], [6].

jamming attack of this survey seeks to disrupt the connection by corrupting the control information transmitted by PUCCH. The authors admit that it is not the most advanced LTE jamming attack however it has a good complexity-efficient ratio, which is confirmed by fig. 1.

The survey [10] deals with the LTE vulnerability against intentional jamming on the Synchronisation Signals (P/SSS) and PBCH. As a test, files of several gigabytes were downloaded. At the same time, the connection was increasingly jammed until the connection dropped. According to the presented testing results a connection drop can be achieved if the jamming power is at least 3dB higher than the received power of the useful signals.

[11] dealt with vulnerabilities of mission-critical and commercially based portable LTE systems. According to [11] jamming of PUSCH leads to the strongest degradation of network performance at the cost of higher power consumption.

[13] dealt with the hopping jamming attack. This attack is based on continuous frequency change of the jamming signal. The aim is the disruption of LTE communication by creating high interference levels over a wide range of frequencies. First of all the functionality of the partial band jamming was verified for different power levels and bandwidths. Jamming of at least 28dB is successful in achieving DoS for the network.

Jamming Detection Mechanisms

[8] refers to a work dealing with machine learning methods for jamming detection in 5G and evaluating the accuracy of specific methods: neutral networks, super vector machine (SVM), and random forest algorithms.

A Jamming attack on PDCCH needs decoding the PCFICH to be more effective because the varying size of PDCCH is transmitted in PCFICH. According to [15] Jamming PDCCH is less sparse than the PCFICH and as a result less effective jamming attack.

[9] dealt with physical jammers on commercial LTE networks and compared chirp partial part to conventional partial band jammers. According to the results chirp partial jammer is more efficient. Generally, the jamming of the UL control channels was declared to be more effective due to the hardware limitations when compared to DL.

The k-Nearest Neighbors (k-NN) – classification algorithm is a machine learning technique to classify data points based on the surrounding data. Therefore, the performance of metrics is monitored. The algorithm examines k nearest data points surrounding a given data point to determine the classification. The algorithm can accurately classify data points e.g., ”interference” or ”no interference”, by identifying patterns in the data. [11] introduces the k-NN method analysing Performance metrics counters to identify the type the jammer.

Anti-Jamming pretty much reformulated from 8

[8] also deals with physical attacks and confirms the efficiency level of jamming attacks from [6] and [5]. In addition to jamming strategies, the survey introduces anti-jamming strategies of different categories.

- Multiple-Input Multiple-Output (MIMO) based Jamming Mitigation Techniques – technique can cancel out interference the more efficiently the more antennas are used. However, a high number of antennas need a lot of power and space so they can rather be used at the base station for uplink transmissions.
- Spectrum Spreading Technique – a technique used in wireless security to spread the energy of a signal across a wider bandwidth to reduce its power density in any frequency band. This method is especially effective when dealing with narrowband jamming signals. There are different methods including frequency hopping, direct frequency spreading, and time hopping.
- Multiple Base Stations Schemes – a technique based on switching to a different eNodeB. If the current node is not working or is under attack, the user can reconnect to another available one. Currently, the method is used in case the user is not able to read the information from the current base station and starts looking for the nearest one with the strongest signal.
- Coding and Scrambling Techniques – techniques aiming to hinder the interruption and disruption of normal connection. The authors of [4] suggest scrambled PRB allocation for PUCCH, a distributed encryption scheme for PDCCH coding and spreading for PBCH modulation to keep the transmissions safe.
- Dynamic Resource Allocation Schemes – a technique based on the usage of dynamic instead static resource allocation for transmissions to make them jamming sus-

tainable and prevent traffic congestion and resource waste e.g. PUCCH. [16] suggests a scheme including a jamming detection mechanism. It monitors the received PUCCH signal and compares it to the energy of other channels to detect unexpected behaviour and the number of consecutive decoding errors.

Smart Jamming

Results of [1] show that smart jamming attacks can cause DoS or loss-of-service in the LTE network. As a smart jammer was considered a collusion between a jamming device and a UE. There are two types of jammers: Cheater and Saboteur. The cheating UE is always connected to the network and aims to obtain more resources for itself by decreasing the competition among users. The Sabotaging UE may not be connected to the network. The research results that significant performance degradation can be caused by a widespread jamming attack. The authors used repeated Bayesian games to represent the interactions between a smart jammer and a network. Repeated Bayesian games are the types of game theory that consider repeated interactions between the attacker and the system. For each interaction, players have to make a decision based on their beliefs about each other's behaviour.

Smart jammers are more difficult to detect because of their dynamic character. However, despite the changing behaviour they cause failures. In [3] the researchers used the error vector magnitude to detect the jammer presence (EVM). These values are used for the analysis by Neyman-Pearson.

[7] present an algorithm for jamming type estimation with superior performance. The algorithm adjusts its estimation performance and balances error probabilities, without relying on network feedback.

Authors of [12] suggest the usage of artificial intelligence, specifically data mining and machine learning techniques, to increase LTE security. This way the network will be able to detect both large-scale and small threats. The resources therefore would be provided by the network and the cloud. Additionally, a local detection layer for low-traffic threats is recommended, which would constantly inform the global detection engine.

Smart jamming attacks are more sophisticated since they can "learn" and thus it is more difficult to organize suitable countermeasures because they should be dynamic. Following smart jamming countermeasures were mentioned in the studied surveys:

1) Increase Transmit Power (Pilot boosting) – increasing the transmitting power may help against some jamming attacks (CR-RS jamming).
2) Throttle All UEs' Throughput (threat mechanism) – a technique based on reducing throughput for active users. This might help against a user attempting to exploit the network for their advantage.
3) Change eNode B Frequency – a technique based on relocation of the centre frequency to different randomly chosen channels within the allocated spectrum. The reallocation includes the movement of all active users.

this is straight from 1

4) Change eNode B Timing – a technique based on change of the frame, slot and symbol timing. For this purpose, all the active users will be forced to a neighbouring cell. After the changes, users will reconnect back to the original node. and then?
In [3] 3 system models were developed to analyse the LTE vulnerability against the jamming attacks and the efficiency of countermeasures. As a countermeasure, the replacement of the OFDM frame for synchronization symbols was used. The result revealed the best replacement of 7 symbols. The percentage of correct cell detection increased with an increase in the jamming signal magnitude.
5) Change SIB 2 – technique able to prevent PRACH and PUCCH failures caused by jamming.

The authors of [7] use throttling and frequency change depending on the jammer type for their simulation. However, all five countermeasure types are presented.

In [1] against smart jamming attacks, the authors modulated an attacker jamming on CS-RS, PUCCH, PBCH, PRACH and PCFICH. As protection countermeasures, 1 to 5 were used.

[2] is the extension of the research in [1] under wideband multipath fading conditions. The estimation of the Signal-to-Interference-plus-Noise Ratio (SINR) in the frequency domain and computation of network utility based on observable parameters confirmed the network's vulnerability against smart jamming attacks. The demonstrated Repeated Game Learning and Strategy Algorithms can significantly improve performance by reducing performance loss and causing an adversary to withdraw their actions. The authors used the same countermeasure techniques as their previous survey [1].

V. Evaluation

As we explained at the very beginning, we found no SoK papers on jamming attacks in LTE networks during our research. However, some papers provided a categorization of attacks in mobile networks e.g. [15]. The categorizations presented in various surveys are not homogeneous. Some authors use made-up names for categories or concentrate on attack subtypes, which makes it difficult to identify the attack groups. As a result, it is difficult to understand what jamming types exist and analyse them. That was the TASK!

We present an overview of previous research on jamming attacks in the LTE network. We summarized the main ideas and findings of different papers and methodologies. We focused on accuracy and aimed to compare results from various surveys by using comparable metrics. Although we did not conduct any tests ourselves, we sought out comparable results from other researchers. We relied on measurements made by others and looked for indirect confirmations from various sources to ensure that our information was confirmed and non-controversial.

The concrete measures were especially important for us since they allow a precise comparison of how much more effective one is than the other. Since we did not implement

the testing environments ourselves, we have to rely on the measurements made by other researchers. Therefore, we looked for comparable results in different works and indirect confirmations in various surveys. By indirect confirmation, we mean a statement with a logical explanation but without specific measurements. We only used the information confirmed by various resources and if there was no controversial information found. To create a representative threat comparison we looked for as many confirmations as possible. For this reason, the amount of resources dealing with physical jamming is that high.

The provided comparison allows the identification of the most dangerous and eventually underestimated attack types. We consider this to be important for planning of future research areas in this field.

Due to resource limitations, we could not provide an overview and analysis of intellectual jamming attacks. This is open for further research.

VI. Discussion

According to the vulnerability analysis, physical jamming attacks should not be underestimated since they can cause significant interrupts and even denial of service. Additionally, they can be combined for more sophisticated attacks.

However intellectual attacks are more sophisticated and more difficult to detect. Implementation of a dynamic detection layer on the LTE network would provide effective protection. Analysis of the network connection would allow the identification of elemental and dynamic jamming strategies.

Future research should especially pay attention to the usage of machine learning for attack detection and mitigation. These techniques would make the network resistant to already existing jamming strategies and those to be developed in the future. On the other hand this might help to find existing hazards as it was in [17]. why here?

The authors of [17] applied natural language processing and machine learning techniques to analyse the LTE documentation to find existing hazards. This technique was effective in finding protocol vulnerabilities. The usage of this technique would help to identify existing network vulnerabilities mentioned in the LTE documentation. Combined with dynamical detection and protection strategies this method would increase the LTE jamming security level.

VII. Conclusion / Future Work

The study of various surveys on jamming attacks in LTE networks proves the network is highly vulnerable. This vulnerability can cause DoS, data loss, and loss of service. This is life-threatening since the LTE network is already used for some mission-critical tasks.

In this survey, we researched the vulnerability of the LTE network against jamming attacks. We concentrated on the physical jamming attacks as it is the classical method and is used as part of other more sophisticated attacks. Additionally, we concentrated on one type of intellectual jamming - smart jamming.

According to our research, the danger caused by physical jammer varies depending on the targeted channel or signal. We focus on jamming attacks that are more efficient than barrage jamming. Researchers highlight four main physical vulnerabilities: PCFICH, PBCH, PSS, and PUCCH. Smart jamming is more dangerous compared to physical jamming since it is more difficult to identify and fight. Although this attack is way more effective it is still of low complexity.

In our work, we mention some jamming detection and network protection strategies for LTE. Especially the machine learning detection and protection methods promise effective jamming protection.

References

[1] Aziz, F. M., Shamma, J. S., Stuber, G. L., "Resilience of LTE networks against smart jamming attacks," 2014 IEEE Global Communications Conference, 2014

[2] Farhan M. Aziz, Jeff S. Shamma and Gordon L. Stüber, "Resilience of LTE Networks Against Smart Jamming Attacks: Wideband Model," IEEE 26th International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): Mobile and Wireless Networks, 2015

[3] Mert Eygi, Gunes Karabulut Kurt, "A Countermeasure against Smart Jamming Attacks on LTE Synchronization Signals," Journal of Communications Vol. 15, No. 8, August 2020

[4] Roger Piqueras Jover, Joshua Lackey, Arvind Raghavan, "Enhancing the security of LTE networks against jamming attacks," Piqueras Jover et al. EURASIP Journal on Information Security, 2014

[5] Marc Lichtman, Jeffrey H. Reed, T. Charles Clancy, Mark Norton, "Vulnerability of LTE to Hostile Interference,", IEEE 978-1-4799-0248-4/13/$31.00, 2013

[6] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed, "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," IEEE Communications Magazine, April 2016

[7] Farhan M. Aziz, Member, Jeff S. Shamma and Gordon L. Stüber, "Jammer-Type Estimation in LTE With a Smart Jammer Repeated Game," IEEE Transactions on Vehicular Technology, Vol. 66, No. 8, August 2017

[8] Hossein Pirayesh and Huacheng Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey,", 2021

[9] Ya˘gmur Co¸skun, Mert Eygi, Gediz Sezgin and Güne¸s Karabulut Kurt, "Jamming Resilience of LTE Networks: A Measurement Study," Springer Nature Singapore Pte Ltd. 2019 A. Boyaci et al. (eds.), International Telecommunications Conference, Lecture Notes in Electrical Engineering 504, p.151

[10] Rafał Krenz, Soumya Brahma, "Jamming LTE signals," IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2015

[11] Vuk Marojevic, Raghunandan M. Rao, Sean Ha, Jeffrey H. Reed, "Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference," IEEE 86th Vehicular Technology Conference, 2017

[12] Roger Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions," 16th International Symposium on Wireless Personal Multimedia Communications (WPMC), 2013

[13] Teng, C. and Brown, Y. M., " LTE Frequency Hopping Jammer," retrieved from https://digitalcommons.wpi.edu/mqp-all/7264, 2019

[14] Youness Arjoune and Saleh Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," 2020

[15] Silvere Maviungou, Georges Kaddoum, Mostafa Taha and Georges Matar, "Survey on Threats and Attacks on Mobile Networks," 2016

[16] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, "Detection and mitigation of uplink control channel jamming in LTE," in Proc. IEEE Military Commun. Conf., Oct. 2014, pp. 1187-1194.

Papers	Year published	Smart jamming	Physical Jamming	Physical channels								Physical signals				Studied problems		
				Downlink channels					Uplink channels			Downlink signals		Uplink signals				
				Physical Downlink Shared Channel (PDSCH)	Physical Downlink Control Channel (PDCCH)	Physical HARQ Indicator Channel (PHICH)	Physical Control Format Indicator Channel (PCFICH)	Physical Broadcast Channel (PBCH)	Physical Uplink Shared Channel (PUSCH)	Physical Uplink Control Channel (PUCCH)	Physical Random Access Channel (PRACH)	Reference Signal (RS)	Synchronization Signal (P-SS and S-SS)	Demodulation Reference Signal (UL-RS) associated with transmission of PUSCH and PUCCH	Sounding Reference Signal (SRS) not associated with transmission of PUSCH and PUCCH	Attacks techniques and cellular networks resilience against them	Anti-attack strategies	Attack detection
[1]	2014	✓					✓	✓		✓	✓	CS-RS				✓	✓	
[2]	2015	✓					✓	✓		✓	✓	CS-RS				✓	✓	
[3]	2020	✓											✓			✓	✓	✓
[4]	2014	✓														✓	✓	
[5]	2013			✓	✓	✓	✓	✓	✓	✓	✓					✓		
[6]	2016			✓	✓	✓	✓	✓	✓	✓	✓		✓			✓		
[7]	2017			✓			✓		✓	✓	✓	CS-RS						
[8]	2021			✓	✓	✓		✓	✓	✓		CS-RS	✓			✓	✓	✓
[9]	2019			✓		✓		✓	✓		✓					✓	✓	
[10]	2015							✓		✓			✓	✓		✓		
[11]	2017								✓	✓		✓				✓		
[12]	2013	✓	✓		✓			✓		✓						✓		
[13]	2019		✓	✓	✓	✓	✓		✓	✓		C-RS	✓			✓		
[14]	2020															✓	✓	✓
[15]	2016			✓				✓		✓	✓	CS-RS				✓	✓	
[16]	2016									✓							✓	✓

TABLE II

OVERVIEW OVER PHYSICAL CHANNELS AND SIGNALS MENTIONED IN SURVEYS AND THE PROBLEMS THEY DEAL WITH.

[17] Yi Chen, Yepeng Yao, XiaoFeng Wang, Dandan Xu, Chang Yue, Xiaozhong Liu, Kai Chen, Haixu Tang, Baoxu Liu, "Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis," 2021