ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 12, December 2017

# 4G Wireless Security Threats Due To the Interference

[1] Nagesha A. G., [2] Dr. Gowrishankar S. S.
[1] Acharya Institute of Technology, [2] BMS College of Engineering

***Abstract:*** **- The 4G wireless network standards are motivated to frequency reuse, where it will raise the system capacity and normalize the planning of radio networks. As the system capacity increases, the signal to noise (SNR) ratio will be degraded due to the interference in the cells. The present security will not suitable for the physical layer of Long Term Evolution (LTE) networks. The key characteristics of the channels of wireless networks are open and broadcasting. As these networks can be attacked easily through interference, signal jamming and eavesdropping. Hence the security issues in physical design will be considered as the critical issues in LTE networks. So, before discussing security issues, we should identify the threats and vulnerabilities raised in the low-level layer of wireless networks. Later in this paper, the secure schemes and other procedures will be explained where that can be adopted in the physical layer.**

***Index Terms:*** **Interference, Physical layer, Security, Spectrum.**

## I. INTRODUCTION

In the present generation, the expectations are high with respect to the support provided by the mobile networks towards the data applications and spectral efficiencies. To attain these two parameters the orthogonal frequency division multiplexing (OFDM) (1) has been introduced. And this will mainly work with 4g based networks like Long Term Evolution (LTE) and WiMAX, the main reason to adopt the OFDM is to achieve frequency reuse. The frequency reuse factor ideally equals to unity (i.e., N = 1), practically it will vary. To achieve this requirement, few of the changes have to be made w.r.to the base station and also with the users. And these changes are essential because of the power limitations. To achieve the frequency reuse factor, N = 1,(1) this update will result in interference in the signals. This will result in the loss of data, and also duplication of data sometimes further it will be vulnerable to the external attack.

To overcome this threat and vulnerability, the system has to incorporate few of the interference cancellation techniques as well as the mitigation techniques. In early days to overcome these type of issues, the people normally use the encryption/decryption process, authentication and few more techniques. But when it comes to 4G wireless networks, it will not be sufficient to follow these traditional procedures to achieve the data security. If we consider an example, these methods cannot eliminate the issues raised by the interference and eavesdropping. As the new trends in the technologies, we can rectify the drawbacks that are raised in the physical layer with the help of structured signaling schemes and co-operative techniques. The high computational complexity is adopted for the data transmission over the wireless channel where it will use the full bandwidth usage.

## II. NETWORK ARCHITECTURE OF 4G LTE

The Third Generation Project (3GPP) developed the broadband technology called LTE for the 4G wireless network. The main reason for the adoption of LTE network is to achieve the high-speed internet for the mobile devices and LTE will be used as a channel for reaching the high data transfer rate in the mobile devices.

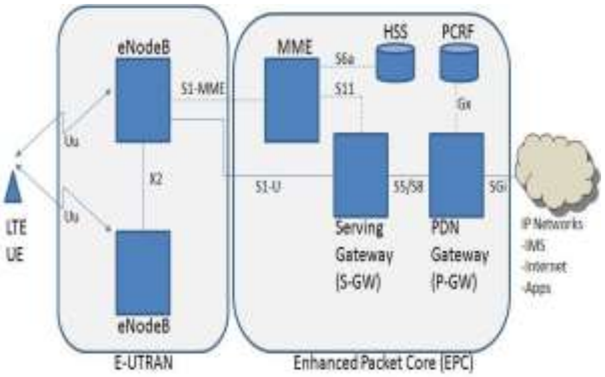

***Figure 1: LTE Network Architecture***

The LTE will make use of the IP technology to the highest rate for data transfer and voice calls. Nowadays the wireless network providers are changing rapidly to adopt for the LTE network to achieve the improved efficiency, less latency time and the capability to handle the high data traffic. To achieve all these parameters the wireless network operators are moved to IP based network. Initially, they all are working with circuit switched networks (4). In circuit-switched networks, the time division multiple access (TDMA) is used for the data access but in the IP based network the orthogonal frequency division multiple access (OFDMA) has to be used, where it will be used to achieve the improved efficiency(2), less latency time and the capability to handle the high data traffic.

### A. RAN for LTE

The authors of the accepted manuscripts will be given a copyright form and the form should accompany your final submission. To establish the wireless radio connection between the mobile operator and the smart devices the radio access network (RAN) will be used and this is also termed as Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network (E-UTRAN). The System Architecture Evolution will consider the non-radio factors and this also adds the network called as an Evolved Packet Core (EPC) Network. The combination of these two like LTE and SAE forms the Evolved Packet System (EPS) (5). The main advantage of EPS is it provides the internet for the end users by establishing the IP connectivity with the Packet Data Network (PDN).Each EPS will have the EPS bearers where these bearers will be used to channelize the IP traffic with PDN gateway to the User Equipment (UE). The EPS also provides the Voice over IP (VoIP) services. Each EPS bearer is closely monitored with the QoS, where this will be used to measure few of the LTE parameters.

### B. Types of LTE Categories

The LTE technology was basically conceived and developed by 3GPP. The main advantage of the LTE is to enhance the capacity and to increase the speed of the data transfer over the mobile networks where the data communication is mainly considered.

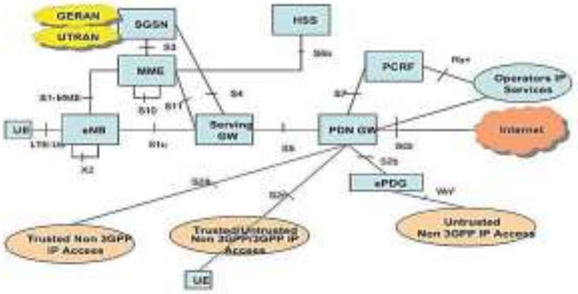

*Figure 2: LTE System*

The LTE system mainly consists of two parts one is user equipment (UE) and the other is Base station is eNB. The base station uses the service gateway (SGW) to connect to the internet backbone.

| UE Category | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| Downlink rate (Mbit/s) | 1 | 10 | 50 | 100 | 150 | 300 | 300 | 300 | 3000 |
| Uplink rate (Mbit/s) | 1 | 5 | 25 | 50 | 50 | 75 | 50 | 150 | 1500 |

### III. TYPES OF INTERFERENCES IN LTE

Interference will occur due to the influence caused by one radio signal to the other. And these interferences are mainly classified as

i. Inter-symbol interference
ii. Co-channel Interference
iii. Adjacent channel Interference

**i. Inter-Symbol Interference**

The Inter-symbol interference will occur due to the distortion of the signal in telecommunication. In radio frequency, one or more signals may collide with other radio frequency signals which lead to producing the noise and sometimes we can't rely on the signal. And this will be caused due to the non-linear frequency or multipath propagation (6) and results in poor signal clarity. This type of interference rose within the system and then the output will be manipulated in the decision device. This outcome will not be accepted in the real-time environment.

**Multipath Propagation**

Multipath propagation is one of the reasons for inter-symbol interference and this will occur when the transmitted signal takes different paths to reach the receiver. Normally these situations will rise when the reflected signals rebounded from the surfaces, and the signal passed through the obstruction, due to the atmospheric conditions. The paths to the receiver will have distinctive lengths to reach the receiver, and enable multiple versions to reach the destination in the different time period. The extra time taken for the symbol transmission is to identify the appropriate symbols.

How to avoid Inter-symbol Interference (5)

Communication systems are intended to create the small impulse responses which are sufficiently short to lessen the likelihood of signals to pass the other signals within the transmission. The energy will be stored in each signal and without extra information from different signals in the bandwidth.

Making transmissions with back to back raised-cosine impulses will avoid inter-symbol interference.
Guard periods will be stored in different symbols. This will avoid the symbols to get out of order, and avoids the inter-symbol interference.

**ii. Co-Channel Interference**
Co-channel interference is one of the obstructions that rose between two cells of the 4G-LTE networks and this will happen because of channel sharing. And this will reduce the overall performance of the system when it comes to spectral efficiency and data rarely. To enhance the effectiveness of spectrum, few of the frequency reuse methods are used. In any case, this technique prompts co-channel interference as a similar arrangement of frequencies that are utilized by a few cells in the system.
Present Techniques to avoid Co-Channel Interference
i. User-centric coordinated scheduling
ii. Power Control Mechanism
iii. Spectrum Management
In User-centric scheduling, the interference is taken care by the central resource manager that will be located in macro base station center. In this technique, the central resource manager will have the list of dominant interferers. The conditional channel quality information (CQI) defines the signal to interference ratio.
In power control mechanism, the power supplied to the transmitter will be taken control to overcome the co-channel interference. In many of the femtocell base stations the power setting scheme is fixed and here it will have the preconfigured power. The only disadvantage is it is not suitable for macro cell and creates large interference throughout the network.
The interference will normally occur between the femtocells and macrocells and this is due to the poor spectrum management in the network. In this scheme, if the interference level is reached above the threshold level then the fractional frequency reuse (FFR) used to perform over the neighboring base station with the limited set of subcarriers to identify the cell edge and also to reduce the radius of the cell.

**iii. Advanced Channel Interference (ACI)**
This type of interference is due to the high power residue of an adjacent channel signal. This will occur due to the inadequate filtering and lack of monitoring in frequency control. To avoid this interference, the telecommunication regulators have to look after about the spectrum.
The ACI ratio is used to identify the interference range which is used to affect the adjacent channels.

## IV. LTE SECURITY

The LTE Security is mainly categorized into three categories.
i. LTE Authentication
ii. NAS Security
iii. AS Security

**LTE Authentication**
This process executes the authentication process between the user equipment and the mobile network. The authentication process is used to identify the user profile as he is authorized or unauthorized to the specified network. If the user is authorized then the authentication will be successful otherwise not. The Authentication and key agreement (EPS AKA) protocol are used to authenticate the user of the specified network. The EPS AKA technique comprises two stages. Initially, an authentication vector (RAND, AUTN, XRES, KASME) was generated by HSS (Home Subscriber Server) and conveys the same to MME. In the next step, any one of the listed authentication vectors will be selected by the MME and the same vector is used for mutual authentication in the user equipment and the authentication key (KASME) will be shared with each other. The process of mutual authentication is used by the user and the network to authenticate each other.
The entity referred as Access Security Management Entity (ASME) is used to receive the top-level key and that will be used to access the network.

**NAS Security**
NAS security, intended to safely send the flagging messages through the radio links to UEs and MMEs, check the integrity and encrypting the signal messages of NAS. Multiple keys will be utilized for integrity check and as well as for cipher code. The major function of the NAS is integrity check and it has to process whereas the ciphering is the arbitrary process. The security keys like integrity key (KNASint) and cipher key (KNASenc), are determined from KASME.

**AS Security**
AS security is mainly designed to guarantee secured data delivery between a UE and an eNB through radio connections. The AS Security process both the checks like integrity check and ciphering for the control plane signaling messages, and applies ciphering only for the IP packets available in the user plane. Distinct keys are utilized for integrity check and as well as ciphering of signal messages and for IP packets the AS security will use the ciphering.

## V. CONCLUSION

In this paper, we discussed the threats that will be raised in the physical layer. And we mainly concentrated on the Interference factor where it affects the signal quality and also the eavesdropping where it will affect the security of the data where the data will be vulnerable to the attacks.

## REFERENCES

[1] Martin Sauter, From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband, ch.4, pp.450-205, John Wiley and Sons, Ltd, Feb.2011

[2] Dimitrios Bilios, Christos Bouras, Vasileios Kokkinos, Andreas Papazois, and Georgia Tseliou, "A Performance Study of Fractional Frequency Reuse in OFDMA Networks", IEEE Wireless and Mobile Networking Conference, pp.38-43, Sept. 2012.

[3] Christos Bouras, Georgios Kavourgias, Vasileios Kokkinos, Andreas Papazois, "Interference Management in LTE Femtocell Systems Using an Adaptive Frequency Reuse Scheme", IEEE conference, pp.1-7, April-2012.

[4] Seokhyun Yoon, Joonyoung Cho , " Interference mitigation in heterogeneous cellular networks of macro and femto cells", ICTC International conference , pp. 177-181, Sept. 2011.

[5] Motoki Morita, Yasuhiko Matsunaga, Kojiro Hamabe,"Adaptive Power Level Setting of Femtocell Base Stations for Mitigating Interference with Macrocells", IEEE Vehicular Technology Conference (VTC fall), pp. 1-5, Sept.2010.

[6] Avani Dalal, Hailong Li, and Dharma P. Agrawal, "Fractional Frequency Reuse to Mitigate Interference in Self-Configuring LTE-Femtocells Network", Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 49-54, Oct.2011.

[7] Feng-Seng Chu, Kwang-Cheng Chen, "Mitigation of Macro-Femto Co-channel Interference by Spatial Channel Separation", IEEE Vehicular Technology Conference (VTC spring), pp.1-5, May. 2011.

[8] Zubin Bharucha, Gunther Auer, Tetsushi Abe and Nobuhiko Miki, "Femto-to-Macro Control Channel Interference Mitigation via Cell ID Manipulation in LTE" IEEE Vehicular Technology Conference (VTC fall), pp.1-6, Sept.2011.