International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 6 (Nov-Dec 2016), PP.151-156

A ROBUST APPROACH FOR SECURING LTE SYSTEM TRANSMISSION USING KEY SECURITY

[1] Lakhbir Kaur, [2] Chitender Kaur
[1,] Student, [2] Assistant Professor
[1,2] Department of Computer Science and Engineering, CEC College, Landran, Mohali - 140413, Punjab, India.
[1] lakhbir.kaur1991@gmail.com, [2] chitender.cse@cgc.edu.in

***Abstract*— The new cellular technology 4G LTE has been attracting several novel users. However, the communications amongst applications, system transfer rule the radio level still stay new. In this work, we perform an in deep study of these communications, their impact on performance, using a grouping of passive active measurements. We recognized that LTE has importantly smaller position support delays less RTT than those systems of 3G. We portray abundant inefficiencies in convey manage procedure over LTE such as undesired begin. We implement small fry new inactive bandwidth opinion move towards for LTE systems. Present commencement of 4G LTE system, there has been mounting concentration authority kind to improved appreciate the presentation, compared with 3G or Wi-Fi systems. We described one of the original steps in the way. We learn the system presentation of LTE system evaluates with previous types of mobile system. We examine LTE normally has importantly upper uplink downlink throughput than 3G yet Wi-Fi, with a average assessment of 6Mbps and 13 Mbps, in that order. We implement the first empirically copied complete authority replica of the inexpensive LTE system with smaller than 7% condition transition corresponding the stipulation state transitions matching. With recent year, quick progress in wireless interaction, elevated stress for broadband moveable wireless communications, the development of novel wireless multimedia applications have represented the incentive to the growth of broadband wireless contact technology. In this document, many safety issues of the LTE and LTE-A system has been discussed. First we show an impression of the LTE system structural design, Second arrangement is exposed as fit In proposed work, we developed the LTE system, Detect the Sybil Attack, Prevention perform through hybridization Approach (RSA DES).**

***Keywords*— LTE system, Sybil attack, Hybrid Approach using RSA, DES encryption algorithm and 4G Technology.**

I. INTRODUCTION

LTE defines for extended expression development [1] is not a lot knowledge as it is the way followed to attain 4G speeds. Like it defines, mainly of the occasion while your mobile display the 4G figure in the better right spot, it doesn't actually signify it. An instantly system begin advertising their connections as 4G LTE, a marketing approach that allowed them to claim next generation connectivity without having to reach the original need number first; it would be like U.S declaring they had landed on the high peak since they got pretty close.

The quick implement of multi-media applications wireless interaction such as Interactive game, Mobile, TV, Internet browser the mobile interaction technology required to meet dissimilar needs of mobile data multimedia operations etc. In direct to put up the adding [2] movable data use the novel multi-media applications, LTE and LTE-A technology have been particular by the 3GPP as the developing movable interaction technology for the further production broadband movable wireless systems. The LTE system is planned to be a package based arrangement containing a smaller amount system basics, which enhances elevated presentation in conditions of elevated data charge, less latency, suppleness bandwidth process by previous swirled interaction system [3]. The LTE-A scheme particular by the 3GPP LTE liberate 11 augments the previous LTE schemes to maintain a lot upper data use, minor time's improved ethereal competence. Together LTE and LTE-A system maintain level internet protocol connectivity, filled inter-working by dissimilar wireless contact system several novel kinds of bottom positions such as femto [4] bottom stations communicate knobs in a overall cellular system.

Due to this summary of that novel features, it acquires a set of latest safety defies in the propose of the protection structure of the LTE-A and LTE systems. 4G LTE is the newest deploy cellular system knowledge that provides fast speed data package for movable apparatus with advertises bandwidth similar still more than the residence broadband system speeds. Current work has demonstrated the power model of the LTE system. Compare 3G, LTE gives the undertake of [5] the higher energy efficient as a consequence of a new resource management higher achievable throughput policy. But the new technology has not been extensively studied empirically in a developed business system.

To mitigates effects of more than one trail diminishing accessible in UMTS, LTE uses OFDM for the downlink, i.e. as of the bottom position to the finish to broadcast the data more than a lot of contracted group careers of 180KHz every in its place of dispersal 1 indication more than the absolute 5MHz vocation bandwidth that is OFDM uses a great figure of thin subordinate carriers for multi transporter broadcast to take information. OFDM is a incidence separation multiplexing scheme used as a digital multi transporter intonation technique. OFDM assembles the LTE [6] obligation for range suppleness allows rate competent explanation for extremely broad

transporters with elevated peak rates. The usual LTE downlink corporeal distance can be seen as a moment occurrence system.

II. LTE ARCHITECTURE

LTE system is contained of the developed package centre [7] the E-UTRAN. The EPC is an all IP completely packets wrapped strength of character system in the LTE scheme. Voice check, which is conventionally a route switch system overhaul, will be switch by the IP compact disc subsystem system. The EPC include of a MME a portion entryway, a Packet Data system doorway jointly among house Subscriber Server. When a UE attach to the EPC, the MME indicate the EPC to execute a common verification through the UE. E-UTRAN comprises the Evolved Universal Terrestrial Radio Access system Base Stations, called eNodeB, which transport by UEs.

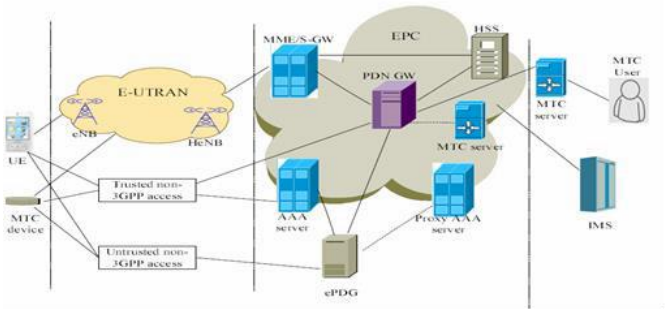

Figure no: 1 Long Team Architecture

The original declaration of LTE has been consistent by 3GPP with end 2008; as division of the 3GPP let go 8 conditions. As talk about earlier, LTE is the 4G technology designated by mainly movable worker as a development of their breathing 3G cellular system will as a result proffer worldwide wandering approximately the sphere for IP-based say data military. LTE provide some profits for profit worker that is as well of high alertness for primary responders.

First, LTE is based on high-tech technology:

1. OFDMA (Orthogonal Frequency Division Multiple Access) if at the similar occasion healthy broadcast over great bandwidth in multi-path radio circumstances [8] supply competent reserve stipulation to user in time occurrence fields.
2. MIMO (Multiple Input Multiple Output)antenna dispensation that takes advantage of the spatial variety to augment heftiness of the indication and/or add to the ability; in downlink, 2x2 and 4x2 systems are generally utilize in uplink, multi-user variety MIMO is used since station have nowadays a single transmitter.
3. AMC (Adaptive Modulation Coding) H-ARQ (Hybrid Automatic Repeat Request) devices to get a feel for to every consumer the transmit [6] style to their person radio excellence for quick retransmission of mistaken packages; in downlink QPSK, 16QAM, 64-QAM modulations can be new in uplink the intonation is nowadays incomplete to 16-QAM (future submission of terminal will as well in take in 64-QAM).

III. BACKGROUND

This section studies the survey of extended expression development the wireless skill criterion that offer as the source for the 4G wireless broadband system. The information described here will assist the person who convert appreciate the transformation development take on obtainable by extended term development. Dynamic the development of wireless broadband skill is clients growing prospect for bandwidth, speed universal access. User current day is linked 24/7 via their wireless instrument want exactly admission to the submission satisfied they use mainly market production tools, torrent video social system. The wish for instant access produce a required for superior bandwidth, enhanced receptiveness and speedy upload downloads rapidly than was agreed by past creation of wireless technologies. Wireless transporters system require to purpose additional like home line internet protocol based systems are to realize the associated [7] speeds client have approach to be expecting.

LTE technology emerges assist the corporation transfer better wireless internet connectivity mobility to its clients. LTE enhanced swiftness, higher bandwidth, less time assist redefine the conventional place of work with improved efficiency for movable employees by contribution in place of work commerce submission services. LTE permits enhanced interaction characteristics such as a real time video calling, direct connect access powerful wireless applications [8] client requirement applications employees need, while they require them as a rule.

LTE defines the conclusion of decades of expertise development, with every novel creation creating ahead the past to enhance clients in general wireless experience get together clients wireless associatively required for years to come.

Wireless mechanism enable single multi devices to interact with a real wired associated. Radio incidence is second-hand to broadcast the information. Such expertise are quickly developing to get together still the mainly difficult interactions required. Wireless interaction skill can all be confidential in 1 of the 3 ways, based in the detachment they are supposed to wrap. These comprise wireless individual region system, wireless local area system, world's area system. Wireless systems form the convey device between procedure conventional wired systems. Wireless Personal area system is incomplete to distance below concerning 10 m contain skills such as infrared, Bluetooth equipment, ultra-wide band.

Jérôme Brouet et al.,2011 [9] expand the operational efficiency, these organisations require wireless data broadcast capability to switch images, contact to databases or broadcast live video strains from the occurrence region. But, these requirements cannot be tacit with narrow-band expertise. However, LTE can bring these competences to primary responders with opportune disagreement of files program of live high description video torrent. Besides, future development of LTE, LTE- superior, will further get well the presentation not only to the profit of movable operational but also for first responders by as long as added treatment suppleness more skill particularly at the cell perimeter, two key performance sign of a radio safety system. Jin Cao et al.,2013 [10] paper varieties a digit of donations to the safety kind of the LTE LTE-A systems. First, they nearby an

indication of the safety functionality of the LTE and LTE-A systems. Second, the safety vulnerabilities active in the construction the propose of the LTE LTE-A systems were explore. Third, the present explanation to these difficulties was typically checked. Finally, they demonstrate the probable investigation matters for the prospect investigate workings. Hyoung-Kee Choi et al.,2015 [11]obtainable to improve safety outgoings in the radio admission system by make use of group-based confirmation. Evaluating to associated workings the planned procedure did not need a fundamental modify in the obligatory safety protocol. Advance, the planned procedure was established by presentation assessment that it produces less computational communiqué disbursement than the recent LTE-AKA. James Henrydoss et al., 2014 [12]in attendance a complete appraisal of safety structure confirmation process build into the LTE system planning development .A transient summary of DDoS attacks safety susceptibility in LTE system incorporated. This paper appraisal the distance border line connected safety glitches by it in LTE system. This paper accessible using palpable jamming announcement based method to talk to jamming matter in distance boundary. Ruei-Hau Hsu et al.,2015 [13]presented two authentic key exchange protocols for end-to-end security group unnamed protection in system sheltered system-absent D2D communications, separately. With group unnamed protection, users of Pro Se-enabled mobile devices can secrete their identity group information during D2D communications. The anonymous protection also provisions revocability traceability to revoke mobile users disclose the identity group information of mistrustful D2D communications in Prose. In terms of security, two future schemes were established by formal analyses. In terms of performance, they implement the group anonymous verification protocol on android devices to evaluate the feasibility. Younes El Hajjaji El Idrissi, et al.,2013 [14]optional a fresh immoral verification method which negotiator the customer substantiation to the WLAN on behalf of the 3G system. The new process was based on the Elliptic Curve Diffie-Hellman symmetric cryptosystem. The intended procedure realizes quick common verification with denotation of a new key structure. The safety possession of the new process was chequered by means of a official authentication which had proved a elevated aptitude in judgment possible attacks without thinking in safety procedures. Jill Jermyn et al.,2014 [15]recommended, the safety risk landscape next to communiqué schemes had rapidly developed over the previous few duration, with major disseminated contradiction of examination attacks the extensive dinner of mobile malware. In this paper they make familiar Fire cycle, a new modelling replication stage for next-generation LTE mobility system safety investigate. This principles agreeable stage is appropriate for immense scale safety examination of intimidation in disagreement of actual LTE movable system.

IV. PROBLEM FORMULATION OF LTE SYSTEM

Long Term Evolution (LTE) / Wimax are one of the emergent system skills which are helpful in increasing the capacity speed with different radio interfaces to improve the system performance. Its major aspire is to get better the system presentation with the help of digital signal processing modulation concepts which simplifies the system. Security is one of the main issues in 4G LTE systems. [16] The intruders could eavesdrop on conversations gain fraudulent access to the system easily. After looking at various authentications ciphering algorithms, Researchers finds the lot of vulnerability problem in security mechanism in LTE/ Wimax. There can be a lot of call dropping probability or handoff problems in these type of mobile communication standards. There can be multiple copies of enodeB which increases the unnecessary load on the system which will degrade the performance of the wireless system. So, these are some issues which should be resolved for the reliable communication of the system to increase the system security.

Open Issues OF Long Term Evolution

In this paper, we define a only some shows potential proposed instructions on the LTE safety as the possible further work, which are explained as go after. The protection mechanism to make sure dependable elevated speed associatively for responsive information is used. In this situation, the safety system for the sensory information should not reason huge functioning spending less time in command to function powerfully.

V. GAP IN STUDY

The reasearchgap deals with the heavy user traffic amd as the number of users increases the load on the network also increases also the security threat for the secure communication of the frames for the successful transformation of the frames at the reciever end. There are lot of vulnerabilities in the network which requires more encryption of the frames to reduce the loss of frames in the network.

VI. OBJECTIVES

In this section, we explain the proposed work in key points:

- To study the basics of wireless technology trends and their pros and cons for the security threats.
- To implement the attack using LTE technology trends to analyse the performance in the presence of threat in the network. The implementation deals with the occurrence of the attack in the LTE network so that we will come to know about the performance in the presence of the attack on which we have to work on it.
- To implement Hybridization of RSA and DES key encryption algorithms for network security. This process deals with the implementation of the secure transmission of the packets.
- To evaluate the performance in terms of number of frames loss, Throughput and Latency to improve the Quality of service in LTE wireless standard technology. So these parameters will result in the evaluation of the system through which we will come to know the overall performance of the network.

VII. SIMULATION MODEL

In simulation Model, we in attendance the method for power measurement system, as well as trace-driven imitation examination genuine submission container learning.

The first step is the deployment of the eNodeB requires X locations Y locations because without locations it's not possible to deploy nodes in the LTE systems. Then we have to

initialize the specifications which are used in the configurations of the system. These specifications deals with the modulation orders, Input bit rate the input sampling rate which is used to provide the number of samples then these all things require the channel model which acts as a medium simulate the entire specification for the configuration.

In a Sybil attack the assailant undermines the standing system of a peer-to-peer network by produces a great figure of pseudonymous individuality, by means of them to increase a doubtfully large pressure. A standing system's vulnerability to a Sybil attack depends on how economically individuality can be reason, the degree to which the standing system believe inputs from entity that do not have a wire of belief between them to a trustworthy unit, whether the standing system treat all substance identically. Evidence shows important Sybil attack can be approved out in an extremely inexpensive ordered way in practical systems. A thing on a peer-to-peer system is a portion of software which has admission to local possessions. A unit promotes itself on the peer-to-peer system by present individuality. More than one individuality can be similar to a solitary thing. In previous language, the charting of identity to entity is a lot of to one. Entities in peer-to-peer systems use frequent individuality for force of unemployment, supply sharing, reliability, honesty. In peer-to-peer systems, the uniqueness is used as a notion so that a inaccessible body can be conscious of identity without of necessity meaningful the communication of individuality to restricted thing. By failure to pay, every different individuality is regularly whispered to be similar to a different local thing. In practicality many identity may communicate to the similar local article. A defective node or an challenger may current several individuality to a peer-to-peer system in command to emerge purpose as plentiful different knobs. After beautiful part of the peer-to-peer system, the opponent may then eavesdrop infrastructure or act unkindly. By hidden donation manifold individuality, the opponent can organize the system obviously.

Then the transfer the number of frames takes place which consists of the packets to be transferred. If the number of frames loss takes place in high manner then the implementation of the security algorithms are required that consists of hybridization of two key security algorithms. If the number of frames is not lost then the whole process will run smoothly the evaluation of the parameters will takes place in terms of packet delivery, bit error rate, throughput which are very helpful in estimation the lifespan of the LTE systems. If the frames or the necessary information drops then it will degrade our system performance which results in inefficient packet delivery will consume overall high energy consumption in the system results in the failure of enodeB which acts as a communicator to send packets to the packet gateway which will further communicate to the other gateways to reach to the destinations.

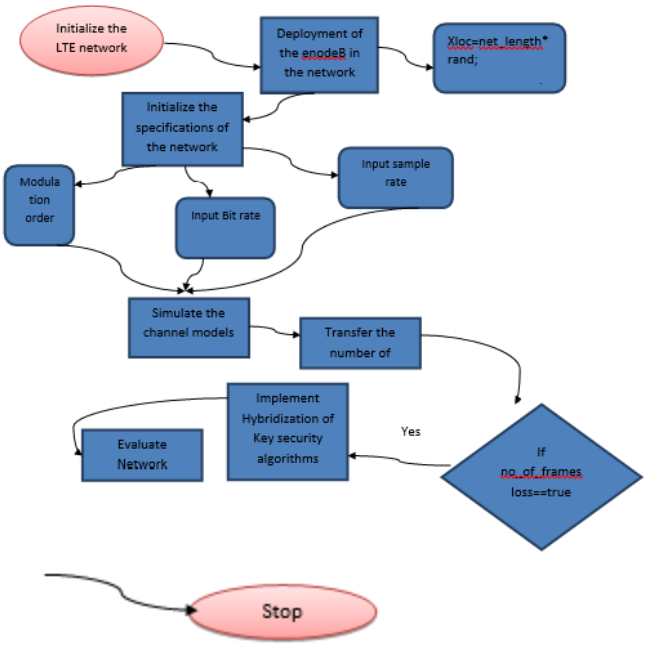

Figure no: 3 Simulation Model

VIII. SIMULATION RESULTS

The LTE network with eNodeB which will work as nodes and with mobile equipment which can also termed as users. The total network is covered by 1000 * 1000 meters. There are total 5 mobile equipment's which will communicate with the eNodeB and then it will communicate with the sending gateway through which the packets will be transferred and then it will move further to the Packet Delivery Gateway. RNC will control the structure of the network which will work as a radio network controller. The Sybil attack in which there are multiple copies of the Mobile equipment's which will increase the unwanted requests and will increase the loads on eNodeB. The yellow ones deals with the multiple copies and black ones deals with the original nodes of which multiple copies of the users generated. The Sybil node Id's at particular iterations i.e. which node is becoming malicious node at particular iterations.

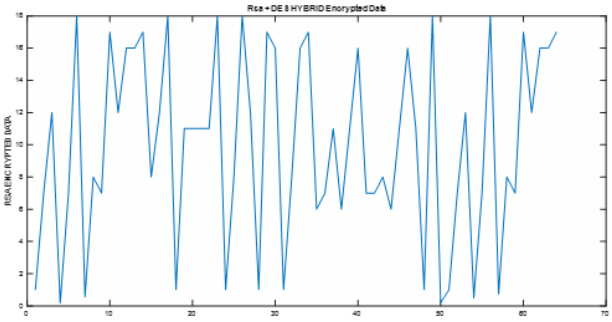

Figure no: 4 RSA+DES Hybrid Encrypted Data

The above figure shows the hybridization of RSA and Data Encryption scheme of the packets transfer through the gateways.

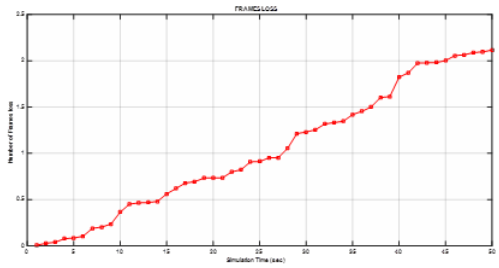

Figure 5: Frame Loss

From the figure we can see the number of frame loss with respect to the simulation time and shows that the number of frames losses after the hybridization scheme (RSA+DES) and shows that the how much securely the frames are transmitted with less number of frame losses which is one of our main motive. As the Frames losses are more then there are more chances to loose number of packets or we can say that more number of packets will drop and users are not able to accomplish their requests and gateways are not able to process the information.

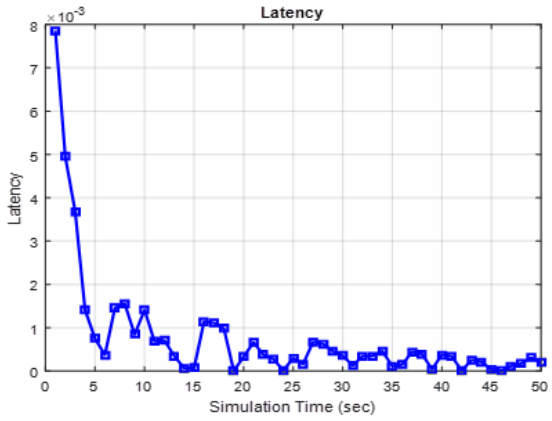

Figure 6: Latency

The above figure shows the latency with respect to the simulation time and shows that our proposed approach is working well as compared to the other traditional approaches. Latency is one of the main factors in packet delivery. If it is high then there is lot of chances of end to end delay which should be minimized for the successful delivery of packets at the receiver end. So this parameter should be less for the high packet delivery.

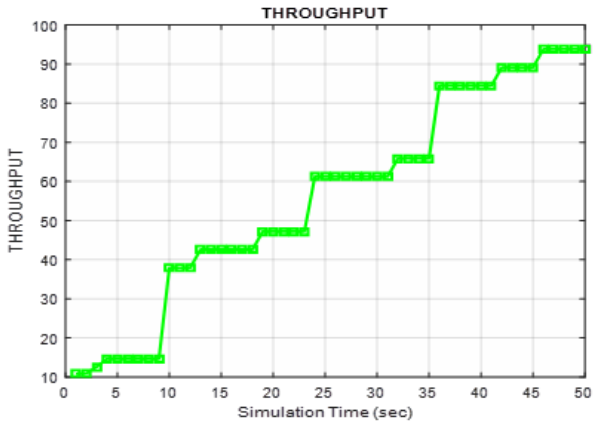

Figure 7: Throughput

The above figure shows the throughput of the long term evolution network with respect to the simulation time and shows that the throughput is coming 95 percent which is an appropriate outcome for the lifespan of the LTE network. Throughput is the term which implies that the total number of frames received at the receiver side through sender gateways with respect to the total number of frames sent and shows that our secure proposed hybrid approach is well efficient in increasing the lifespan of the network.

Table no: 1 Comparison Table

Parameters	Proposed Approach	Previous Approach
Frame Loss	2.34	650
Latency	0.03 sec	175 sec
Throughput	95 %	92 %

CONCLUSION

In this paper, we have primary demonstrated the safety architectures by the 3GPP pattern. We prospect talk about the trouble preceding in the safety structural design of the LTE wireless systems. Our preceding has exposed that there are at rest a set of safety effort in the current LTE systems. Ultimately, we have give details possible open planned struggle as the proposal for the next projected performance on the safety of LTE wireless systems. LTE system lacks necessary protections for the objects. This paper studies the protection of procedures, pointing out the protection vulnerability is lack of the security for delay in serving gateway designing a protection improvement structure. The structure is simple a great significant to LTE systems, especially when a high security standard is necessary.

REFERENCES

[1] Liu, Chin-Yu, et al. "The untrusted handover security of the S-PMIPv6 on LTE-A." Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on. IEEE, 2015.

[2] Liyanage, Madhusanka, et al. "Leveraging LTE Security with SDN and NFV." networks 2: 4.

[3] Qiang, Li, et al. "Security Analysis of TAU Procedure in LTE Network." P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on. IEEE, 2014.

[4] Rasheed, Iftikhar, et al. "Analysing the security techniques used in LTE Advanced and their evaluation." Digital Information Management (ICDIM), 2013 Eighth International Conference on. IEEE, 2013.

[5] Siwach, Gautam, and Amir Esmailpour. "LTE Security potential vulnerability and algorithm enhancements." Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on. IEEE, 2014.

[6] Taylor, Carol-Lyn, David Nolan, and Stan Wainberg. "Priority capabilities in LTE supporting national security and emergency preparedness next generation network priority services." Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE, 2013.

[7] Tu, Guan-Hua, et al. "How voice call technology poses security threats in 4G LTE networks." Communications and Network Security (CNS), 2015 IEEE Conference on. IEEE, 2015.

[8] Zhu, Li, et al. "Research on 3GPP LTE Security Architecture." 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing. 2012.

[9] Brouet, Jérôme, and She Feng. "LTE and future evolutions for the benefits of security wireless networks." Wireless Mobile and Computing (CCWMC 2011), IET International Communication Conference on. IET, 2011.

[10] Cao, Jin, et al. "A survey on security aspects for LTE and LTE-A networks". Communications Surveys & Tutorials, IEEE 16.1 (2014): 283-302.

[11] Choi, Hyoung-Kee, Chan-Kyu Han, and Dae-Sung Choi. "Improvement of security protocol for Machine Type Communications in LTE-advanced." Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International. IEEE, 2015.

[12] Henrydoss, James, and Terry Boult. "Critical security review and study of DDoS attacks on LTE mobile network." Wireless and Mobile, 2014 IEEE Asia Pacific Conference on. IEEE, 2014.

[13] Hsu, Ruei-Hau, and Jemin Lee. "Group anonymous D2D communication with end-to-end security in LTE-A." Communications and Network Security (CNS), 2015 IEEE Conference on. IEEE, 2015.

[14] Idrissi, Y. E. H. E., NoureddineZahid, and Mohamed Jedra. "Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA." Future Generation Communication Technology (FGCT), 2012 International Conference on. IEEE, 2012.

[15] Jermyn, Jill, et al. "Firecycle: A scalable test bed for large-scale LTE security research." Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014.