Universal Journal of Electrical and Electronic Engineering 7(6): 315-319, 2020 http://www.hrpub.org
DOI: 10.13189/ujeee.2020.070603

A Survey on Different Attacks in LTE/LTE-A Networks

K. Venkata Pavan*, S. Shanthi

Department of Electronics and Communication Engineering, Saveetha School of Engineering, Chennai-602105, India

Received April 8, 2020; Revised June 6, 2020; Accepted June 12, 2020

Cite This Paper in the following Citation Styles

(a): *[1] K. Venkata Pavan, S. Shanthi , "A Survey on Different Attacks in LTE/LTE-A Networks," Universal Journal of Electrical and Electronic Engineering, Vol. 7, No. 6, pp. 315 - 319, 2020. DOI: 10.13189/ujeee.2020.070603.*

(b): *K. Venkata Pavan, S. Shanthi (2020). A Survey on Different Attacks in LTE/LTE-A Networks. Universal Journal of Electrical and Electronic Engineering, 7(6), 315 - 319. DOI: 10.13189/ujeee.2020.070603.*

Abstract This paper is about security assaults in LTE/LTE-A Systems. The Long haul Development (LTE)/LTE-Progressed (LTE-An) arrange gives propelled administrations to billions of clients with its higher transfer speeds, better range effectiveness, and lower dormancy than heritage cell systems. Be that as it may, regardless of whether it experiences new security dangers because of its everything IP-based heterogeneous design. Accordingly, there is a basic need to play out a fast and precise system security estimation in LTE/LTE-A system. To accomplish LTE/LTE-A system security estimation, security-applicable information (in short security information) assortment and information examination for assault discovery are required as essentials. Be that as it may, the majority of the current work just spotlights on information assortment and examination for a specific sort of LTE/LTE-An assaults. Little work has been done to exhaustively perform information assortment and examination for identifying different assaults on LTE/LTE-A system. Not quite the same as past work, In this paper we focused on DOS, DDOS Man-in-the-Center (MitM) assaults, rebel base station assaults and the answers for such assaults were broken down to secure LTE and LTE-A systems

Keywords LTE, LTE-A, DOS, DDOS, Man in the Center Attacks

1. Introduction

Present day cell systems bolster an enormous number of administrations that go past conventional voice and short informing traffic to incorporate high transmission capacity information correspondences. These systems depend on 3GPP guidelines for remote correspondences, for example, the Universal Mobile Telecommunication System (UMTS) for current 3G get to systems. Discharge 8 of the 3GPP benchmarks brought about the organization of Long Term Evolution (LTE). This new innovation is portrayed by extraordinary upgrades in the Radio Access Network (RAN) for limit improvement as far as bits every second per Hertz (bps/Hz) just as an update of the cell center system (Enhanced Packet Core - EPC), moving towards an all-IP framework. Regardless of the colossal limit and framework upgrades executed by LTE, when all is said in done, cell systems are known to be powerless against security assaults [1], [2].

With the rapid development of wireless communication and multi-media applications such as Internet browsing, interactive gaming, mobile TV, video and audio streaming, the mobile communication technology needs to meet different requirements of mobile data, mobile calculations and mobile multi-media operations. In order to accommodate the increasing mobile data usage and the new multimedia applications, LTE and LTE-A technologies have been specified by the 3GPP as the emerging mobile communication technologies for the next generation broadband mobile wireless networks. The LTE system is designed to be a packet-based system containing less network elements, which improves the system capacity and coverage, and provides high performance in terms of high data rates, low access latency, flexible bandwidth operation and seamless integration with other existing wireless communication systems.

2. Literature Survey

Wei Cao(1) et, al recommended that as indicated by the

numerous past investigates, cell phones stay helpless against numerous sorts of assaults. Particularly, it is known to have a few vulnerabilities in mid 2G framework. For instance, the absence of shared validation in 2G framework makes it conceivable to assault by counterfeit base stations. Despite the fact that the encryption and verification calculations are suitably upgraded in LTE-A framework. Be that as it may, it is likewise helpless against aggressors. For instance, Jill Jermyn outlined past DoS assault models and exhibited botnets can cause a DoS by depleting client traffic limit over the air interface. Furthermore, the consequences of the paper show that a solitary assailant can radically diminish the QoS of real gadgets in a similar cell. LTE-A system comprises of the Developed Parcel Center (EPC) and the E-UTRAN. The EPC is an all-IP arrange in the LTE-A frameworks and comprises of a Portability The board Element (MME) and a Serving Entryway (SGW), E-UTRAN incorporates the Advanced All inclusive Earthly Radio Access System Base Stations, called eNodeB (eNB), which speaks with UEs legitimately. The entrance organize and the center system are associated through the S1 interface, and the eNodeBs is associated by means of the X2 interface [3], [4].

Limei He(5) et.al suggested that the third Era Association Task (3GPP) reported the 3GPP R8 form as the primary specialized standard for The Long haul Advancement (LTE) in 2008, which offers higher transmission capacities, better range productivity, and lower dormancy than heritage cell systems. Therefore, LTE organize is broadly sent by portable administrators around the globe. The R10 variant of 3GPP brought the LTE-Progressed (LTE-An) organize that expands LTE, and acquainted new innovations with improve framework execution. The standard rendition has now been refreshed to R14, and 3GPP has begun exchange and investigation of 5G advances. The LTE/LTE-A system is progressively defenseless against different security dangers, offering ascend to a basic need to perform extensive system security estimations, which contemplates different security assaults and dangers, just as their location and investigation techniques. Security estimation is an ongoing procedure that can distinguish existing assaults on organize and assess the level of system security. Effective related information assortment and information investigation can guarantee the fast and exact discovery of security assaults and give the premise to organize security estimation. We utilize the expression "information assortment" to allude to the methodology that catches security-applicable data in arrange gadgets. In our specific situation, we audit the first information and acquired highlights in information assortment strategies. We utilize the expression "information investigation" to allude to the technique that breaks down the gathered information to accomplish assault identification. In our specific situation, we audit the information investigation calculations and systems in existing writing. The majority of existing work centers around information assortment and examination for a specific kind of LTE/LTE-An assaults (e.g., RF sticking assaults [6], [7], [8], flagging assaults [9], [10], [11], strange Taste assaults [12], [13], etc), little work has been done as far as exhaustive information assortment and investigation for security estimation in LTE/LTE-A. As far as we could possibly know, this is one of the primary papers that give a far reaching rundown of assaults on the LTE/LTE-A system and give an exhaustive study on security information assortment and information investigation strategies for LTE/LTE-An assault identification.

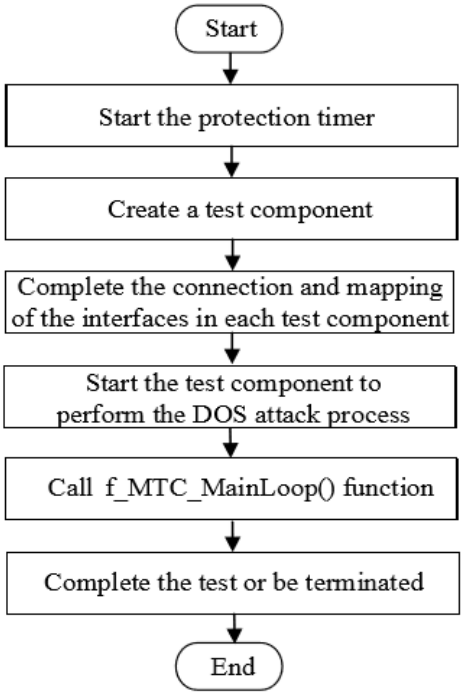
Roger Piqueraslover[14] et.al suggested that the intermingling of the Web and cell versatility systems is empowering new M2M correspondence frameworks as a feature of the Web of Things [16]. The business agreement is that there will be extreme development in portable cell availability due to M2M and implanted versatile applications. Most of M2M frameworks as of now work on 2G and 3G arranges in any case, in the long haul, everything is relied upon to change to LTE. Some anticipate that 50 billion non-individual information just cell phones will be on existing systems sooner rather than later [15]. The rise of the Parcel and the spike in the quantity of associated gadgets could have flagging burden suggestions on the cell center system [17]. It will be important to enhance how M2M hubs use organize assets. Indeed, even with the upgrades made to LTE, Machine-to-Machine traffic is relied upon to altogether influence the system [18]. The normal number of gadgets attempting to associate remotely might be adequate to overpower the system because of high flagging traffic volume.

Mina Labib(19) et.al recommended that information traffic request in cell systems has been becoming immensely because of the ubiquity of brilliant hand-held gadgets. These gadgets offer a wide assortment of utilizations that require high information throughputs, for example, video and sound spilling, video conferencing, and intelligent gaming [20]. The Long haul Advancement (LTE) and LTEAdvanced (LTE-An) are institutionalized by the third Era Association Undertaking (3GPP) to turn into an exceptionally flexible 4G radio framework that empowers cell arrange administrators to satisfy such high needs in information traffic [21]. LTE offers better inclusion, improved framework limit, high ghostly efficiency, low dormancy, and high pinnacle information rates in a savvy way [22]. Business LTE administrations have been propelled in excess of 130 nations as of now [23]. LTE is unarguably turning into the essential standard for 4G cell innovation.

Jin Cao(24) et.al clarified that since there are a great deal of security vulnerabilities in the General Portable Media transmission Framework (UMTS) security instrument, for example, Man-in-the-Center (MitM) assaults [25], maverick base station assaults [26] and Preclude from

securing Administration (DoS) attacks [27], then extgeneration mobile communication systems need to give more security usefulness than the UMTS frameworks. To accomplish a common validation between the Client Hardware (UE) and the Portability Management Entity (MME) through the Advanced General Earthly Radio Access System (E-UTRAN), the SAE/LTE design improves the UMTS-Authentication and KeyAgreement (UMTS-AKA) and presents the new access security approach, Developed Bundle Framework Otherwise known as (EPS Otherwise known as) to evade the assaults existing in the UMTS frameworks. In addition, a new key hierarchy and handover key administration component has been acquainted all together with guarantee the security of the entrance and the versatility procedure in the LTE engineering [28]. Not with standing keep up the safe quality of the LTE frameworks, a LTE-A framework has presented some new substances and applications, for example, Machine Type Communication (MTC) [29], Home eNodeB (HeNB) [30], Transfer hubs [31] and specified the relating security vulnerabilities, prerequisites and arrangements [32]–[33]. In any case, there are still some security vulnerabilities in the current LTE/LTE-A systems, which should be additionally broke down.

3. Flow Diagram



4. Vulnerability in LTE Handover Procedure

To alleviate the security dangers presented by pernicious base stations, the LTE security component provides a handover key administration plan to invigorate the key materials between a UE and an eNB at whatever point the UE moves starting with one eNB then onto the next. Likewise, the 3GPP panel has specified the security prerequisites, dangers and answers for the security issues to help secure portability between heterogeneous access frameworks. Nonetheless, a ton of vulnerabilities have still been found in the LTE versatility the executives strategy and the handover key instrument.

5. LTE Handover Security

For the protected LTE handovers, a mixture confirmation and key understanding plan has been proposed to help globe versatility and secure correspondences in 4G remote frameworks. The plan connects a powerful secret key with an open key to give a lightweight verification and a non-renouncement administration. Also, by receiving people in general key communicate convention structured as a piece of the plan, a common confirmation between the UE and outside system (FN) can be accomplished without the utilization of certificate. Nonetheless, it might bring about a ton of computational expenses and capacity costs because of the utilization of open cryptography, and in this way brings a ton of difficulty to help the consistent handovers in 4G remote frameworks. A security meandering and vertical handover conspire among a few distinctive access advances in 4G remote systems has been proposed. The plan in structures a worldwide confirmation convention to empower a vertical handover between heterogeneous access frameworks including GSM, UMTS, WiFi and WiMAX without requiring an earlier membership to the visited systems. In any case, this plan focuses only on the handovers between WiMAX/WiFi and GSM/UMTS and spreads the security issues existing in the GSM frameworks. The handovers between the LTE/LTE-A frameworks and different access systems have not been tended to, where the LTE/LTE-A frameworks are entirely different from the GSM and the UMTS in the handover methodology and security vulnerabilities.

6. Conclusions

The 3GPP committee has motivated the LTE project in order to meet the requirements of increasing mobile data traffic and new multimedia applications. In this paper, we have overviewed the security issues in the LTE/LTE-A 4G wireless networks. We have first presented the security architectures and mechanisms specified by the 3GPP standard. We have further extensively discussed the vulnerabilities existing in the security architecture of the LTE/LTE-A wireless networks and reviewed the corresponding the state-of-the-art solutions proposed to

overcome those security flaws in the literature. Our survey has explored that there are still a lot of security issues in the current LTE/LTE-A networks. Finally, we have summarized potential open research issues as the suggestion for the future research activities on the security of LTE/LTE-A wireless networks. It is expected that our work could attack much more attentions from the academia and industry to promote the corresponding research activities and could provide helpful indications for the deployment of the LTE/LTE-A 4G wireless networks.

REFERENCES

[1] Wei Cao, Nan Ma, Ping Zhang," Security Analysis of DoS Attack against the LTE-A System", 2017 3rd IEEE International Conference on Computer and Communication s.

[2] Jill Jermyn, Gabriel Salles-Loustau, and SamanZonouz "An Analysis of DoS Attack Strategies Against the LTE RAN," Journal of Cyber Security, Vol.3 No.2, 159–180.

[3] 3GPP TS 36.401, "Evolved Universal Terrestrial Radio Access Network (EUTRAN), architecture description," Release 14, v14.0.0, 2017.

[4] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu and X. Fu, "On simulation studies of cyber attacks against LTE networks," 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, 2014, pp. 1-8.

[5] Limei He, Zheng Yan." LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey", IEEE-2018.

[6] W. Y. Xu, W. Trappe, Y. Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," ACM Int. Symp. Mob. Ad Hoc Netw. Comput., 2005, pp. 46–57.

[7] A. G. Fragkiadakis, V. A. Siris, and A. P. Traganitis, "Effective and Robust Detection of Jamming Attacks," Futur. Netw. Mob. Summit, 2011, pp. 1–8.

[8] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, "Detection and mitigation of uplink control channel jamming in LTE," MILCOM, 2014, pp. 1187–1194.

[9] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, "Signaling oriented denial of service on LTE networks," ACM Int. Symp. Mobil. Manag. Wirel. Access, 2012, pp. 153–158.

[10] A. Gupta, T. Verma, S. Bali, and S. Kaul, "Detecting MS initiated signaling DDoS attacks in 3G/4G wireless networks," Int. Conf. Commun. Syst. Netw., 2013, pp. 1-60.

[11] M. Pavloski, G. Görbil, and E. Gelenbe, "Bandwidth usage—based detection of signaling attacks," Information Sciences and Systems, vol.363, pp.105-114, Sep. 2015.

[12] S. Wahl, K. Rieck, P. Laskov, P. Domschitz, and K. R. Müller, "Securing IMS against novel threats," Bell Labs Technical Journal, vol. 14, no. 1, pp. 243–258, 2009.

[13] M. Nassar, R. State, and O. Festor, "Monitoring SIP traffic using support vector machines," Int. Symp. Recent Adv. Intrusion Detect., 2008, pp. 311–330.

[14] Roger Piqueras lover "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions", ISSN:1882-5621/13/ ©2013 NICT.

[15] "More than 50 billion connected devices," Ericsson, Ericsson White Paper, February 2011, http://goo.gl/KGaVg.

[16] A. lera, C. Floerkemeier, J. Mitsugi, and G. Morabito, "Special Issue on the Internet of Things," in IEEE Wireless Communications, vol. 17, December 2010, pp. 8-9.17.3rd.

[17] Generation Partnership Project: Technical Specification Group Services and Systems Aspects, "Study on Core Network overload solutions. 3GPP TR 23.843," vol. vO.7.0, 2012.

[18] A. Prasad, "3GPP SAE-LTE Security," in NIKSUN WWSMC, July 2011.

[19] Mina Labib, VukMarojevic, and Jeffrey H. Reed, "Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing",2015 IEEE Conference on Standards for Communications and Networking (CSCN).

[20] A. Damnjanovic, J. Montojo, Y. Wei, T. Ji, T. Luo, M. Vajapeyam, T. Yoo, O. Song, and D. Malladi, "A survey on 3gpp heterogeneous networks," Wireless Communications, IEEE, vol. 18, no. 3, pp. 10–21, June 2011.

[21] 3rd Generation Partnership Project (3GPP), "Technical Specifications; LTE (Evolved UTRA) and LTE-Advanced Radio Technology Series (Rel-12)," Tech. Rep. [Online]. Available: http://www.3gpp.org/dynareport/36300.htm.

[22] A. Khandekar, N. Bhushan, J. Tingfang, and V. Vanghi, "LTE-Advanced: Heterogeneous networks," in Wireless Conference (EW), 2010 European, April 2010, pp. 978–982.

[23] GSA, "Evolution to LTE Report," Global Mobile Suppliers Association (GSA), Tech. Rep., Apr. 2015. [Online]. Available:http://www.gsacom.com/gsm3g/infopapers.php4

[24] Jin Cao, Maode Ma. "A Survey on Security Aspects for LTE and LTE-A Networks",1553-877X/13/$31.00. 2013 IEEE.

[25] M. Zhang and Y. Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Commun., Vol.4, No.2, Mar. 2005, pp. 734- 742.

[26] C. Tang and D.O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," IEEE Trans. Wireless Commun., Vol.7, No.4, April 2008, pp.1408-1416.

[27] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Rel 12) 3GPP TS 33.401 V12.5.0, Sep. 2012.

[28] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC) (Rel 12), 3GPP TS 22.368 V12.0.0 Sep. 2012.

[29] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements

for Home Node B (HNB) and Home eNode B (HeNB) (Rel 11), 3GPP TS 22.220 V11.6.0 Sep. 2012.

[30] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects (Rel 9), 3GPP TR 36.814 V9.0.0 March 2010.

[31] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of Machine-Type Communications (Rel 12), 3GPP TR 33.868 V0.10.0, Sep. 2012.

[32] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB; (Rel 8), 3GPP TR 33.820 V8.3.0 November 2009

[33] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (Rel 11), 3GPP TS 33.320 V11.6.0 June 2012.