Futo Journal Series (FUTOJNLS)
e-ISSN : 2476-8456 p-ISSN : 2467-8325
Volume-4, Issue-2, pp- 84 - 93
www.futojnls.org

Research Paper December 2018

5G Wireless Network Mobility Management and Security Issues: An Overview of Existing Technologies

*Agubor C. K., Atimati E. E. and Akande A. O.
Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Nigeria
Corresponding Author's email: kemdirim2014@gmail.com

Abstract

Mobility management and security issues in 5G mobile wireless network are presented in this paper. Mobility and security issues are great concerns in mobile communications that improve as technology evolves from one generation to another. It is expected that for improved quality of service (QoS), 5G network will incorporate high, better mobility and security requirements compared to 4G. For better understanding of this, it is desirable to have a look at the mobility and security mechanisms of existing technologies. To achieve this purpose, recent scholarly and related articles bordering on the subject matter covering 2G to 4G were reviewed. Some of the mobility and security challenges inherent in these technologies were identified, two of which are the 3G's Authentication and Key Agreement (AKA); and the 4G's decentralized accountability for security. These challenges in both security and mobility management are seen as possible areas for improvement that 5G networks can leverage on. For this to be achieved, it is recommended that 5G mobile wireless should be implemented using network visualization technology (NVT) and software define networking (SDN), which will result to a more robust network with tougher security mechanism.

Keywords: 5G mobile wireless, mobility challenge, mobility communication, mobility management, security management

1. Introduction

Mobile wireless communication technology has evolved over the years. Globally, there are different generations of wireless communication technologies that are in existence. The most recent is the 4th generation Long Term Evolution (4G LTE) wireless network. Before the emergence of 4G LTE, the 3G (3rd generation) wireless network has been an active player in the industry. It has been a technology that is known for achieving higher speed tasks.

The 4G technology was designed to leverage on the performance of 3G technology. It has come with improved wireless capabilities, higher network speeds compared to 3G and visual technologies. The 4G technology is one that stands out based on its capability such as global roaming, accessing the internet anytime from anywhere and wider support for multimedia services. The 4G network came at a period when the 3G technology has started showing limitations in areas like spectrum allocation, bandwidth availability, and lack of seamless interconnectivity across heterogeneous networks. By design and mode of operation the 4G network is meant to cover wider geographical areas in which there are existing different operating networks. It merges all the other existing heterogeneous technologies and has the potential to effectively support triple-play (voice, video and data). It does this with a natural progression to support seamless, cost effective high data rates, global roaming, efficient personalized services, typical user centric integrated service model, high quality of service (QoS) and overall stable system performance (Sayan & Ray, 2006).

This paper presents both mobility and security issues in 4G LTE technologies through a review of recent research works. The aim is to highlight areas in 4G in terms of mobility management and security challenges which will need attention for future work by the research community as the industry gradually migrates from 4G to 5G (5th generation). Arrangement of the article starts with introduction in section 1, section 2 dwells on the evolution of mobile wireless technologies from first generation analogue to fourth generation digital systems. Section 3 discusses mobility and security issues in 4G (LTE) while solutions to 4G's mobility management and security challenges as a way forward for next generation wireless network (5G) is discussed in section 4. The conclusion is presented in section 5.

2. Evolution of Mobile Wireless Technologies

The 1G (1st generation) network was wholly analogue cellular systems and was a circuit switched based technology which came into operations in the early 1980s. The standards for the 1G cellular network included Advanced Mobile Phone System (AMPS) and Total Access Communication System (TACS). It was specifically meant for voice and text messages. The network had limited coverage area, capacity problems, poor quality of transmissions, security and inefficient utilization of the available spectrum.

2G (2nd generation) wireless technology was launched in the 1990s to meet the ever growing demand for voice and data applications. The system is purely digital which enables signal compression and thus uses the spectrum in a more efficient way compared to AMPS and TACS analogue systems. The standards for 2G network are:

(i) GSM (Global System for Mobile communication) which uses TDMA (Time Division Multiple Access) and FDD (Frequency Division Duplex).

(ii) IS-136 known as Digital Advanced Mobile Phone System (D-AMPS) which uses TDMA and TDD (Time Division Duplex)

(iii) CDMA-one which uses CDMA (Code Division Multiple Access).

2.5G is a mid-generation and an upgrade of 2G. It is an enhanced data service network with standards as:

(i) GPRS (General Packet Radio Service)
(ii) EDGE (Enhanced Data rates for GSM Evolution)
(iii) IS-95B.
GPRS is an enhanced mobile data service for users of GSM and IS-136 (Quoc-Thinh, 2008). 2.5G network offered a higher data rate than 2G technology and enabled the delivery of

basic data services like text messaging but not enough to download an image or browse a website with data rate up to 144 kbps (Tripathi, Kumar & Maurya , 2014).

3G was designed to overcome all the limitations of the above technologies, and is characterized by higher data rates than the 2G, greater system capacity, and improved spectrum efficiency. The 3G has a range of technologies which are all based on CDMA. This include UMTS (Universal Mobile Telecommunication Services), CDMA 2000 (a direct successor to 2G CDMA-one), and TD-SCDMA (Time Division-Synchronous Code Division Multiple Access). The air radio interface for UTMS is WCDMA (Wideband Code Division Multiple Access). UMTS, sometimes marketed as 3GSM, using WCDMA was standardized by 3GPP (Third Generation Partnership Project). UMTS is the 3G technology chosen by most GSM/GPRS mobile operators (Quoc-Thinh, 2008). The dominant generation today is the 3G technology.

4G LTE implemented worldwide is meant to overcome the limitations of 3G. As specified by the International Telecommunication Union’s Recommendation (ITU-R), 4G provides very high speed connections such as 100 Mbps for outdoor environments and 1Gbps for indoor environments (Alquhayz, Al-Bayatti & Platt, 2012). LTE uses OFDMA (Orthogonal Frequency Division Multiple Access), designed to be all-IP and to support mobility and service continuity between heterogeneous access networks.

Figure 1 shows 4G as a technology that is completely standardized and equipped with multiple interfaces that will facilitate seamless handover between heterogeneous networks for the continuity of an ongoing service. Heterogeneous network presents different challenges because of the different technologies involved. These systems were designed independently to handle different services, data rates and users with different level of handover procedure and security management. The 4G technology has improved mobile management and security aspects than the 3G technology. However, some weaknesses in 4G’s performance in terms of mobility and security issues do exist.

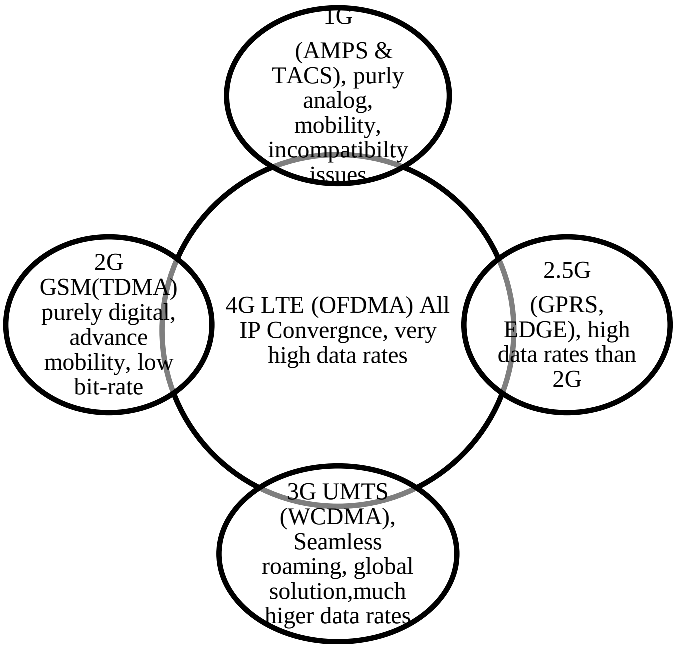
1G
(AMPS & TACS), purly analog, mobility, incompatibilty issues
2G GSM(TDMA) purely digital, advance mobility, low bit-rate
4G LTE (OFDMA) All IP Convergnce, very high data rates
2.5G
(GPRS, EDGE), high data rates than 2G
3G UMTS (WCDMA), Seamless roaming, global solution,much higer data rates

Figure 1: Wireless technology evolution

3. 4G LTE Network

3.1. Mobility Issues

Mobility management is the fundamental technology used to automatically support mobile terminals enjoying their services while simultaneously roaming freely without the disruption of communications (Jun-Zhao, Howie, & Sauvola, 2017). Mobility management was stated by Payaswini and Manjaiah (2013), as very crucial in 4G-Networks which is a heterogeneous network and more complex to handle. This can take place in different layers of the OSI (open system interconnection) model including network layer. These layers were given in Akyildiz, McNair, Ho, Uzunalioglu and Wang (1999) as layer-3 (L3), link layer-2 (L2) and cross-layer (L3 + L2). The L2 mobility refers to the case where the Mobile Node (MN) roams among different access nodes while the point of attachment to IP network remains the same. The L3 mobility involves the change of IP addresses (Payaswini & Manjaiah, 2013). Mobility wireless network refers to the MN remaining connected as it changes same network location or between different networks. It is a case of stay connected while on the move. Poor mobility management affects the quality of service (QoS). It is a case of experiencing a disconnection as movement progresses between locations or networks.

Connectivity problem was identified in Tripathi, Kumar and Manrya (2014) to be either due to triggering or handover issues. Triggering occurs when different kinds of events trigger mobility actions leading to some conflicts. Handover or Handoff management is a process by which a MN keeps its connection active when it moves from one access point to another (Chinwetalu & Nwachi-Akpor, 2014). The process as shown in Figure 2 focuses mostly on the control of the change of a mobile node's access point during active data transmission (Jun-Zhao, *et al*, 2017). 4G networks are both multi-domain and multi-technology which present different challenges because the different technologies involved were designed with different level of handover procedures.

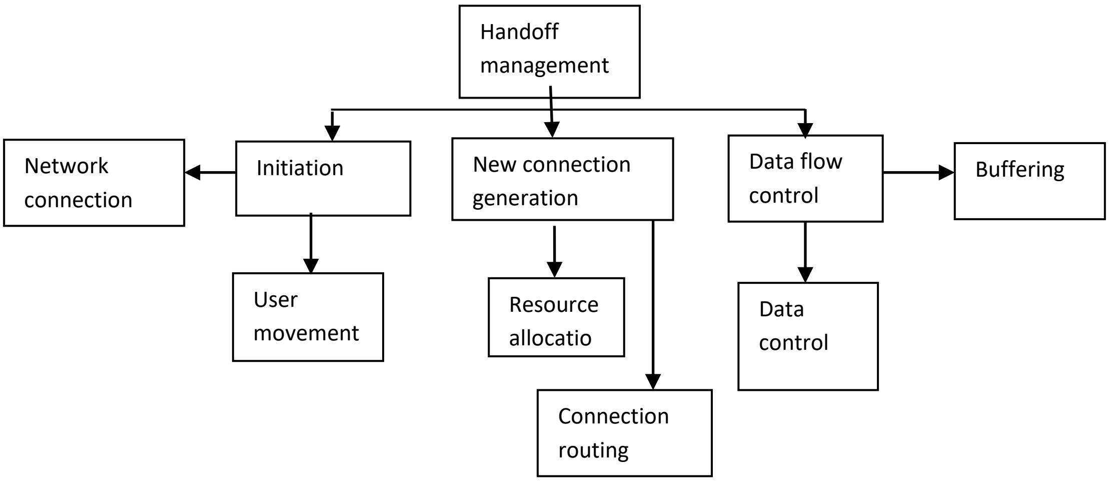

Figure 2: Handoff management process

There are two levels of handoff which are vertical and horizontal handoffs. Horizontal handoff deals with intrasystem handoffs while vertical handoff deals with intersystem handoffs. Both levels of handoff are supported by 4G system (Payaswini & Manjaiah, 2013). Intrasystem handoffs are when MN moves between two different cells or access points within the same network. In this case, mobility issues are confined within the same network. Vertical handoff takes place when more than one network is involved such as when MN migrates from one network to a different network. Payaswini and Manjaiah, (2013), concluded that it is difficult to realize the vertical handoff among different wireless communication systems while meeting appropriate level of QoS. This is because prolong handoff time will result to loss of packets or disconnections. The effect of handoff delay in 4G wireless network was also highlighted in Rakesh, (2016) where it was expressed as a service challenge. They stated that the user may experience a drop in QoS which will affect the service performance.

Terminal mobility which allows mobile users to freely roam across geographical boundaries of wireless networks is also an aspect of mobility challenge in 4G (Akyildiz *et al*., 1999). Terminal mobility can be in form of location or handoff management. Unlike the location management which involves QoS issues such as authentication information, information regarding original and new cells, the handoff management ensures communication is ongoing when the terminal roams from a local network to a visited network (Chawan & Mane, 2013; Tripathi, *et al,* 2014). The mobile Ipv6 address changes as the mobile terminal leaves one network to another and so causes an increase in system load, high handover latency and packet losses (Chawan & Mane, 2013). This result to system degrades and the QoS performance is affected.

In the design of handoff management techniques, the following challenges were listed in (Akyildiz , Xie & Mohantya , 2004):

(i) Reduction of both signaling and power overheads.

(ii) QoS guarantees during the handoff process – extreme low intra and intersystem handoff latency, which includes signaling message processing time, resources and routes setup delay, format transformation time, limited disruption to user traffic, near-zero handoff failure and packet loss rate.

(iii) Efficient use of network resources.

(iv) Enhance scalability, reliability, and robustness.

3.2. Security Issues

Security schemes in wireless communication have evolved in line with the evolution of wireless technologies. The different technologies have had their security systems evolving from one stage to a higher level. In 1G wireless, it was possible for intruders or a third party to gain fraudulent access to the network. 2G GSM had an improved security system over 1G but with a weak improved security authentication algorithm. The master security key could be disclosed by having a million interactions with a SIM card (Kakesh, 2016).

In 3G wireless network an enhanced process of a two-way authentication mechanism was adopted. Mutual authentication was achieved by the mobile device and network. For stronger security, 128-bit encryption and integrity keys were utilized (Spatz & Schmitz, 2000). Security was further enhanced by introducing some mechanisms to ensure freshness of the cipher keys. It was demonstrated by Horncand and Howard, (2000) that if a security key is compromised, the damage is limited for that period of validity of the key resulting to a short rather than long lasting effect.

Significant advances have been made to improve security issues from 1G through to 4G LTE wireless networks. The 4G system is an IP-base infrastructure and has an open nature. It has improved security mechanism compared to 3G. A detailed report in Seddigh *et al*, (2010) showed that 4G uses temporary identifiers just like the 3G but further abstraction was used to narrow the opportunity for intruders to steal identifiers compared to 3G.

By design and mode of operation the 4G networks is meant to cover a wider geographical area in which there are different operating networks with their specific security schemes. It is expected that the 4G will offer seamless service to these heterogeneous networks. However, the heterogeneity of these wireless networks lead to complications in security and privacy (Shin, Ma, Mishra & Arbangh, 2006). Vulnerabilities at either the physical or MAC (multiple access control) layers of the network may be attributed to the challenges presented by these heterogeneous networks.

In another report, Barbeau (2005) mentioned interference and scrambling attacks as the two key vulnerabilities at the physical layer. Interference can result to communication system failure as a result of a high SNR (signal-to-noise ratio) caused by interfering signals in the form of white Gaussian Noise (WGN) and multicarrier (narrow band signal), that are deliberately inserted into the system (Ravishankar & Harishankar, 2008). Scrambling is a more difficult form of attack to implement. This is because a particular or part of the frames is the target. To be successful, the attacker must be knowledgeable and sophisticated to be able to identify particular frames and time slots.

Authentication, encryption and integrity protection are key security issues in 4G LTE with procedures listed as (Seddigh, Nandy, Makkar & Beauoront, 2010):

(i) Freshness – The authentication vector which is at the heart of the authentication procedure is guaranteed to be fresh. i.e not previously utilized. This is achieved via the sequence numbers exchanged in the messages that serve as input to the ciphering and integrity algorithms (Sankaran, 2009)

(ii) Security algorithms - The algorithms used in the HE (home environment) and USIM (Universal Subscriber Identity Module) to compute the authentication vectors are mostly one-way mathematical functions, where the output is obtained with a given set of inputs, using a pre-defined algorithm. Thus, as explain in Sankaran (2009), it is extremely complex for an attacker to try to obtain the inputs using the outputs.

The security requirements of 4G heterogeneous networks have been defined as having two levels. The first level is on mobile equipment and the second is on Operator networks. Mobile equipment requirements include protecting the device’s integrity, privacy and confidentiality, controlling access to data, and preventing the mobile equipment being stolen or compromised and the data being abused or used as an attack tool (Zheng, He,Yu & Tang, 2006).

Furthermore, the encryption and cryptography methods being used for 3G networks are not appropriate for 4G networks as new devices such as smart phones and other end-user equipment (UE) and services are introduced for the first time in 4G networks (Chavan & Mane, 2013). In this case the UE can also become a source of malicious attacks (Ku, Swain and Das, 2015). The application of the 3G’s Authentication and Key Agreement (AKA) to a

4G communication architecture was investigated by Aiash, Mapp, Lasebae and Phan, (2010) using X.805 standard. Their analysis showed many threats to the network's security. This indicated that the current security threats in 3G and other new threats were inherent to 4G technology. The progression to 4G which is a heterogeneous network, results in openness to not just cellular attacks but internet based attacks.

4. 5G Concerns

4.1. Mobility Management

The next generation network (5G) is one that should be able to achieve high QoS compared to 4G in terms of mobility management. It should, as a matter of importance, incorporate high and better mobility requirements compared to 4G, thus, providing satisfactory service to mobile users on the move. Therefore, a high mobility technique which incorporates mobility management is a future research direction for 5G systems.

Mobility management should take the form of intra-domain and inter-domain mobility management structure which describe the movement of MN within domains and between domains respectively. This scheme is similar to intrasystem and intersystem handover process obtained in 4G as earlier described. However, the intra-domain will focus mainly on a fast, reliable, seamless mobility support within a given area of coverage. The inter-domain on its own part will be a scheme that will provide global mobility solution with the advantages of flexibility, robustness, and scalability. The scheme should be flexible enough for users to join and leave any network without experiencing any service interruption and so enjoying transparent mobility support.

The inter-domain and intra-domain can use proposals of Internet Engineering Task Force (IETF) that outlines the routing strategy for IP based wireless networks (Jun-Zhao, *et al,* 2017),. These proposals are Mobile IP (MIP), Hierarchical Mobile IP (HMIP), Cellular IP (CIP) and HAWAII (Payaswini & Manjaiah, 2013). MIP is a macro mobility solution applicable for inter-domain roaming while HMIP, CIP and HAWAII are used as the micro mobility solutions for intra-domain migration.

The concepts highlighted above aims at designing a flat mobile architecture that enables enhanced access to IP services and built-in support for mobility and heterogeneous radio access technologies. This scheme is known as Distributed Mobility Management (DMM) (Zuniga *et al*, 2013; Chan *et al*, 2014; Liu *et al*, 2014). The DMM framework envisions an all-IP infrastructure where the flow of users' data routed through the optimal path, exploiting multiple anchor points and deployment of IP services are closer to the users.

4.2. Security Issues

The security risks in 4G networks as discussed previously are due to the fact that it is a distributed and open architecture network and has a decentralized accountability for security. A distributed and open architecture network entails one that is not physically segregated as it is with 2G and 3G networks. These networks are owned and operated by single Mobile Network Operators (MNO) that can enforce security policies on their respective platforms. The 4G is an all IP with infrastructures and services of MNO interconnected to form a single aggregated service providing network. This makes it possible for one compromised device to create access for potential attackers. There is also decentralized accountability for security resulting to lack of overall control of security in 4G LTE (Firdaus, (2016). This typical characteristic of 4G LTE allows seamless roaming across heterogeneous networks making it difficult for MNOs to present end-to-end security levels to their subscribers (Uma & Sumathi , 2016).

5G networks need to provide capabilities not only for voice and data communication but also for new services, new industries and for a multitude of devices and applications to connect society at large (Ericsson White Paper, 2017). Therefore, as a result new services, applications and security demands could vary significantly among services. For instance security demands for mobile Internet of Things (IoT) and high-speed mobile services will vary. This makes it technically necessary for the system to have a well-integrated security solution. Yang, *et al*, (2015), suggested that physical layer security and cryptography are two security measures that can efficiently safeguard devices and services. Physical layer security with proper planning and execution will protect the communication phase of the network while cryptography will protect the processed data after the communication phase.

The network infrastructure has to be robust enough to allow security to be built for 5G services. The robustness should enable 5G to provide more options beyond node-to-node and end-to-end security available in today's mobile systems (Schneider, 2016). It entails how well the physical entities of the network elements (NEs) are isolated from each other. This may be done based on network visualization technology (VNT) by which a network could build different network slices (Huawei White Paper, 2015). These slices can be seen as 5G small nodes. For each network slice, a different security protocol may be required for a particular service. Such network configuration can be provided through software defined networking (SDN) enabled solution. The capability of SDN was shown in Uma and Sumathi (2016), as an optimistic platform that can introduce intelligence into 5G and address the security challenges.

5. Conclusion

Mobile wireless communications technology have evolved from 1G through 4G and gradually approaching 5G to keep pace with the ever increasing bandwidth demands. Security techniques are in place to safeguard today's mobile communication systems, however tougher security mechanisms are still necessary for future networks. The 5G technology will have a high data rate compared to 4G (LTE) and is expected to be a combination of 2G, 3G and 4G (LTE) with greater coverage and high reliability. It is also expected to have a better QoS than 4G due to an improved reduction in end-to-end latency. Therefore, improved mobility management and tougher security mechanisms are required which will be an improvement on 4G systems. As a new network, 5G will experience new-use cases and thus will likely be exposed to new forms of threats. Such threats could be checked by having improved and robust built-in security mechanisms.

The concept of security automation should be considered. This will allow the network to be self-adaptive and self-healing using intelligent security controls. All of these could be provided on the platform of SDN. The SDN enabled solution is capable of not only providing a re-configurable network management platform, but also simplifies authentication handover in accomplishing reduced latency. With the implementation of VNT, appropriate flexibility will be provided in the selection of security for the different network slices thus having a network with enhanced flexibility security selection mechanism as compared to existing technologies.

References

5G Security: Forward Thinking, (2015). *Huawei white paper.* Available: www.huawei.com [Accessed: July, 12, 2017]

Aiash, M., Mapp, G., Lasebae, A. & Phan, R. (2010). Providing security in 4G systems: Unveiling the challenges in telecommunications. *Sixth Advanced International Conference (AICT)*. 439 – 444.

Akyildiz, I.F., Xie, J. & Mohantya, S. (2004). Survey of mobility management in next-generation all-Ip-based wireless systems, *IEEE Wireless Communications*, 17.

Akyildiz, I.F., McNair, J., Ho, J.S.M., Uzunalioglu, H. & Wang, W. (1999). Mobility management in next-generation wireless systems. In: *Proceedings of the IEEE,* 87(8), 1347-1384.

Alquhayz, H. Al-Bayatti, A. & Platt, A. (2012). Security Management System for 4G Heterogeneous Networks, *In Proceedings of the World Congress on Engineering (WCE)*, London, U.K..

Anonymous, (2017). *Ericsson White Paper*,Uen, 284, 23-3269.

Barbeau, M. (2005). Wimax/802.16 Threat Analysis. *In Proceedings of the 1st ACM International Conference on Quality of Service & Security in Wireless and Mobile Networks*.

Chan, *et al.,* (2014). Requirements for Distributed Mobility Management, *RFC 7333*.

Chavan, S. & Mane, V. (2013). 4G Wireless Networks Challenges and Benefits**.** *International Journal of Emerging Technology and Advanced Engineering,* 3(7).

Chinwetalu, B.N. & Nwachi-Akpor, J.O. (2014). Handoff Management: A critical Function in Mobility Management for Fourth Generation (4G) Wireless Networks, *Global Journal of Computer Science of Technology: E-Network, WEB and Security*, 14(2), 25.

Firdaus, H. (2016). 4G LTE Network Growth in India and Security Issue in Network, *International Journal of Computer Science and Network Security,* 16 (11).

Horncand, G. & Howard, P. (2000). An Introduction to the Security Features of 3GPP and Third Generation Mobile Communication Systems. *IEEE VTS 51st Vehicular Technology Cont.*

Jun-Zhao, S., Howie, D. & Sauvola, J. (2017). Mobility management techniques for the next generation, wireless networks, University of Oulu, Finland. Available: http://www.mediateam.oulu.fi/; [Accessed: July, 20, 2017].

Kakesh, K.R. (2016). A frame work for 4G wireless networks-overview and challenges. *Journal of Excellence in Computer Science and Engineering*, 2(1), 1-10.

Ku, M., Swain, B.R. & Das, P. (2015). Comprehensive Survey of Possible Security Issues on 4G Networks, *International Journal of Network Security & its Applications*, 7(2).

Liu, D., Zuniga, J., Seite, P., Chan, H. & Bernardos, C. (2014). Distributed mobility management: Current practices and gap analysis, IETF Tools.

Payaswini, P. & Manjaiah, D.H.(2013). Challenges and Issues in 4G Networks Mobility Management. *International Journal of Computer Trends and Technology*, 4(5).

Quoc-Thinh, N.V. (2008). Mobility Management in 4G Wireless Heterogeneous Network. Unpublished PhD thesis, Universite d'evry val-d'essonne.

Rakesh, K.R. (2016). A Framework of (4G) Wireless Networks-Overview and Challenges. *Journal of Excellence in Computer Science and Engineering*. 2(1), 3.

Ravishankar, B. & Harishankar, M. (2008). Roaming issues in 3GPP security architecture and solution using UMM architecture. *2nd Conf. on Mobile Ubiquitous Computing Systems, Services and Technologies.*

Sankaran, C.B. (2009). Network access security in next generation 3GPP systems: A Tutorial. *IEEE Communications Magazine.*

Sayan, A. & Ray, K. (2006). *IETE Technical Review,* 23(4), 253-265.

Schneider, P. (2016). 5G Security Research at Nokia Bell Labs, *Nokia Solutions and Networks.*

Seddigh, N., Nandy, B., Makkar, R. & Beauoront, J.F. (2010). Security advances and challenges in 4G wireless network, *8th Annual International Conference on Privacy, Security Trust.*

Shin, M., Ma, J., Mishra, A. & Arbangh, W.A. (2006). Wireless network security and interworking. *The Proceedings of IEEE in Cryptograph*.

Spatz, & Schmitz, R. (2000). Secure Interpretation Between 2G and 3G Mobile Radio Network. *First International Conference on 3G Mobile Communication Technologies*.

Tripathi, S., Kumar, R. & Maurya, D. (2014). Mobility Management Issues in 3G & 4G Network, *Journal of Advanced Computing and Communication Technologies,* 2(4), 17-19.

Uma, B. & Sumathi, S. (2016). High throughput, privacy and security for handover in 5G networks using software-defined networking. *International Journal of Innovative Research in Science, Engineering and Technology,* 5(2).

Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J. & Renzo, D. M. (2015). Safeguarding 5G Wireless Communication Networks Using Physical Layer Security, *Security And Privacy In Emerging Networks.*

Zheng, Y., He, D., Yu, W. & Tang, X. (2006). Trusted computing-based security architecture for 4G mobile networks. *In: Parallel and distributed computing, applications and technologies, (PDCAT)*, *Sixth International Conference,* Sichuan, 251 – 255.

Zuniga, J., Bernardos, C., De La Oliva, A., Melia, T., Costa, R. & Reznik, A. (2013). distributed mobility management: a standards landscape. *Communications Magazine, IEEE,* 51(3), 80–87.