International Journal of Future Generation Communication and Networking
Vol. 10, No. 1 (2017), pp. 15-24
http://dx.doi.org/10.14257/ijfgcn.2017.10.1.02

4G Wireless Networks Architecture an Overview and Security Issues On 4G

Javed Ahmad Shaheen

Virtual University of Pakistan, Lahore
javedmatyana@yahoo.com

Abstract

In this paper comprehensive study on current proceeds in wireless network security problems or issues for 4G are being presented. Mobility is the most invigorating character, and it has a vast impact as how communication is embryonic into the future 4G long term Evolution networks and the mobility in 4G networks demands new mobility support. LTE is designed with strong cryptographic techniques, mutual authentication between LTE network elements with security mechanisms built into its architecture. The paper has a lot of contribution in different field of wireless network as in current era wireless network technologies have expanded rapidly and the emergence of novel applications such as tablet, Smartphone, mobile TV, web 2.0 and streaming contents such as videos, games and more, led to the demand of a faster network of next generation technology, the fourth Generation (4G) the new technology or generation of mobile communication standards in telecommunication emerging from future wireless networks which works under LTE (Long Term Evolution) and WiMAX (Worldwide Interoperability for Microwave Access). 4G provides five times faster mobile broadband internet access of discussed devices and Security is considered as the most important aspect in 4G LTE and WiMAX technologies, in these two standards a significant amount of attention has been given for the security design architecture. First the paper, presents the 4G architecture and its technical description and 4G wireless security with network security of upcoming generation. Second it discussed some security issues and possible threats on 4G. Third the paper proposed security model of 4 layers which ensures secure transmission of packets by adopting several compulsory security measures.

Keywords: *4G description, Security for Network, Architecture of Security, 4G Architecture and 3GPP, Wi-Max, Wireless security*

1. Introduction

Mobility is the most stimulating nature, and it has a vast impact as how communication is embryonic into the future 4G networks and the mobility in 4G networks demands new mobility support. If we compared it to usual mobility especially in wireless network, it has severe and vigorous security risks. In recent there is many advancements in wireless network. The wireless network technologies have included many rising applications like mobile television, web2-0 and streaming contents which is standardization feature of 3GPP (3^{rd} generation partnership project). The 4G is a completely new fully IPbased incorporated system of systems and also network of networks accomplished following junction of wired and wireless networks. It includes computers, electronics and communication technology for their consumer and many other convergences which give it capacity to provide 100 Mbps and 1 Gbps respectively in external and internal surroundings with uninterrupted Quality of Service (QoS) and high security. It is also offering many services of different kind at any moment of any time according to requirements of user and also anywhere and seamless interoperability always on at affordable cost.

ISSN: 2233-7857 IJFGCN

As the 4G is the next generation wireless communication systems of worldwide and it also has to become standardized as it has increased. security and too much trustworthy communication. The architectural design of 4G is very interoperability across the HetNet environments and it is also operate on the TCP/IP architecture procedure [3,].As the 3rd generation communication is going to shift to the.4th generation communication (4G) and many organizations like IEEE802.16m, International Telecommunication union (ITU), Vodafone, China mobile communications as well a lot of next generation mobile network vendors like Motorola and Samsung.[2,] are all repairing for their 4G technology. Now many definitions of 4G developed. which provide bandwidth of 1000Mbps in mobile devices and in normal 1Gbps. It is adjoining with heterogeneous networks which have number of Radio Access Technology and Radio Access network (RAN) [1,]. The enabling technologies interconnected for 4G are OFDM (orthogonal, frequency division multiplexing), vertical handover protocols, and in advance multiple input & multiple output and cognitive radio network is also added in 4G technology.

Different security issues problems and challenges in 4G technologies described in 4th section of this paper are being studied in this paper. The rest of, this paper is structured as, the section 2 consist of 4G technical overview and in Section 3 I, discuss, 4G network technology architecture [7,]. In Section 5 I have to studied proposed, four-layer security model which supervises and ensure more secure packet transmission by taking all necessary security procedures like taking the, form of interference, detection systems, Firewalls, and IPSec, and operating network resources in an intellectual way by using refined and authentication protocols.

2. Technical Description

The standard for 4G constituted of set of requirements has been specified by ITUR (International Telecomm Union Radio communication sector in March 2008 which are further named as ITM-A (International mobile Telecommunications advanced specification for $g standards. It has also specified peak speed for 4G Service 1Gbps to 100Mbps. [1]

As the first version of mobile Wi-Max and LTE is having very low bit rate rather than 1Gbps peak rate and not fully compatible with IMT-Advanced but many services provider branded it. Later on, in December 2010, ITU-R accepted, the said two technologies could still be considered as 4G, provided they represent ancestor to IMT-Advanced compliant versions. Later on WiMAX for has released its version for mobile called mobile Wi-Max released 2 also known as Wireless MAN Advanced or IEEE 802.16m and LTE has also released LTE Advanced called LTE-A. These are the diffident compatible versions for IMTAdvanced acquiescent for these two systems, and they have been promising speeds of 1 Gbit ps. It should also in our mind that 4G system does not support circuit switch telephony service. It provides only Internet Protocol (IP) based communication *e.g.* IP telephony. In 3G the previous technology used spread spectrum radio technology is dumped in all 4G systems and it is replaced by OFDMA which is multicarrier transmission and also replaced with frequency domain equalization (FDE) schemes, which consequently transfer very high bit rates regardless of extensive multi path radio propagation. So the peak bit rate is more enhanced through smart antenna arrays for multiple input multiple output (MIMO) communication.

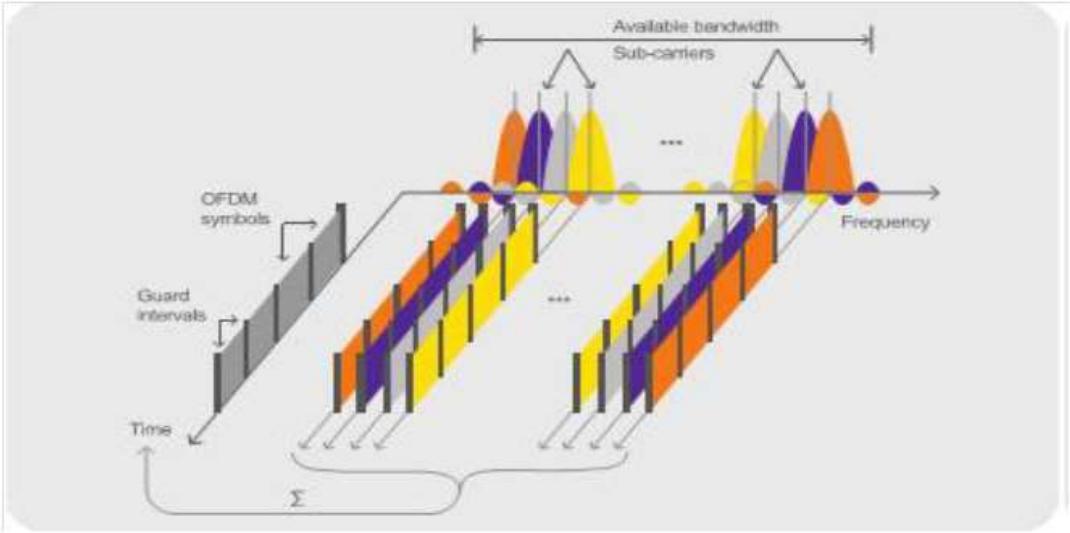

Figure 2.1.

As we have discussed 4G is based on packet switching only rather than circuit switching and it will require low latency for data transmission. When the 4G was deployed, the IPv4 address overtiredness was probable in its final stages. Therefore, for 4G IPv6 is necessary for supporting a huge number of wireless permitted devices. IPv6 has the capability to remove the need for network address translation (NAT) if there is availability for increasing the number of IP addresses available, IPv6 is a method of sharing a few number of addresses between bigger groups of devices, although NAT will require communicating with devices which are using existing IPv4 networks.

3. 4G, Network Architecture

The 4G network architecture constitute of multiple varied networks, such as Wimax and 3G [, 8]. In between the multiple access networks, anyone can use through the service subscriber and it also supports services from the same service unit like IP Multimedia subsystems. The Wimax architecture has an access serving network which has responsibility to provide access to the service stations or mobile stations which has a connection to network service provider. But the 3GPP LTE architecture has two core networks that is GPRS and EPC network. The GPRS core network provide network connections for existing RANs and Evolved packet core network (EPC) provide network connections to evolved RAN and 3 GPP, IP Access.

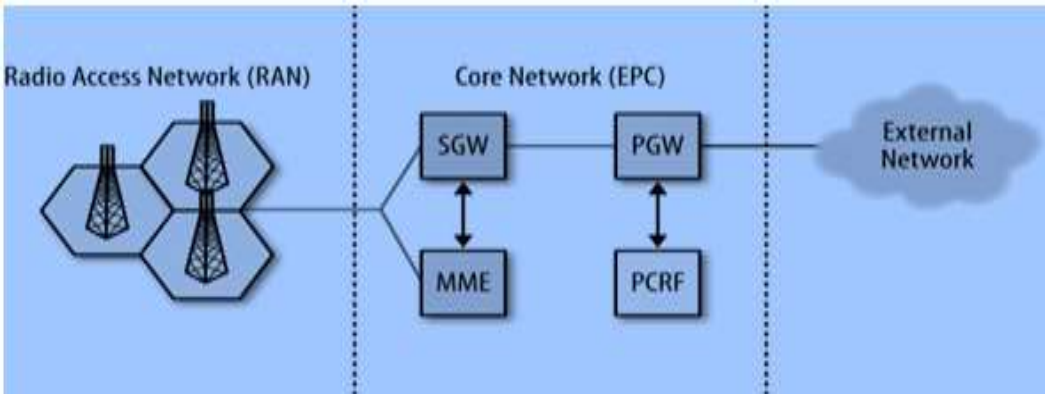

Figure 3.1. It is Showing Communication /Access of RAN with EPC

The basic network architecture for 4G is clearly elaborated as well explained in this figure 3.2

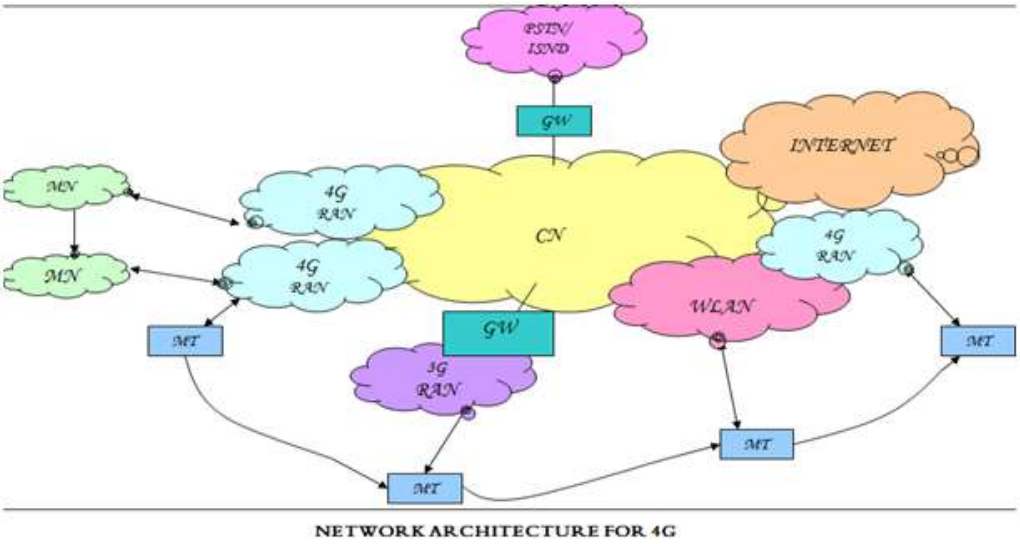

Figure 3.2.

3.1. IP Multimedia Subsystem Security Architecture

The IMS (IP Multimedia, subsystems) is an overlie on top of the network infrastructure like 3 GPP overlay on IMP. It wants to defend the all IMS sessions in between the end-users and IMS servers. It is also offering its authenticated and authorized mechanisms. There are two parts of IMS security and are described below.

3.1.1. First-hop Security: First Hop security secures the first hop from the end user to the proxy call session control function.

3.1.2. Network Domain Security: Network domain security protects the rest of hops between call session control functions inside IME core.

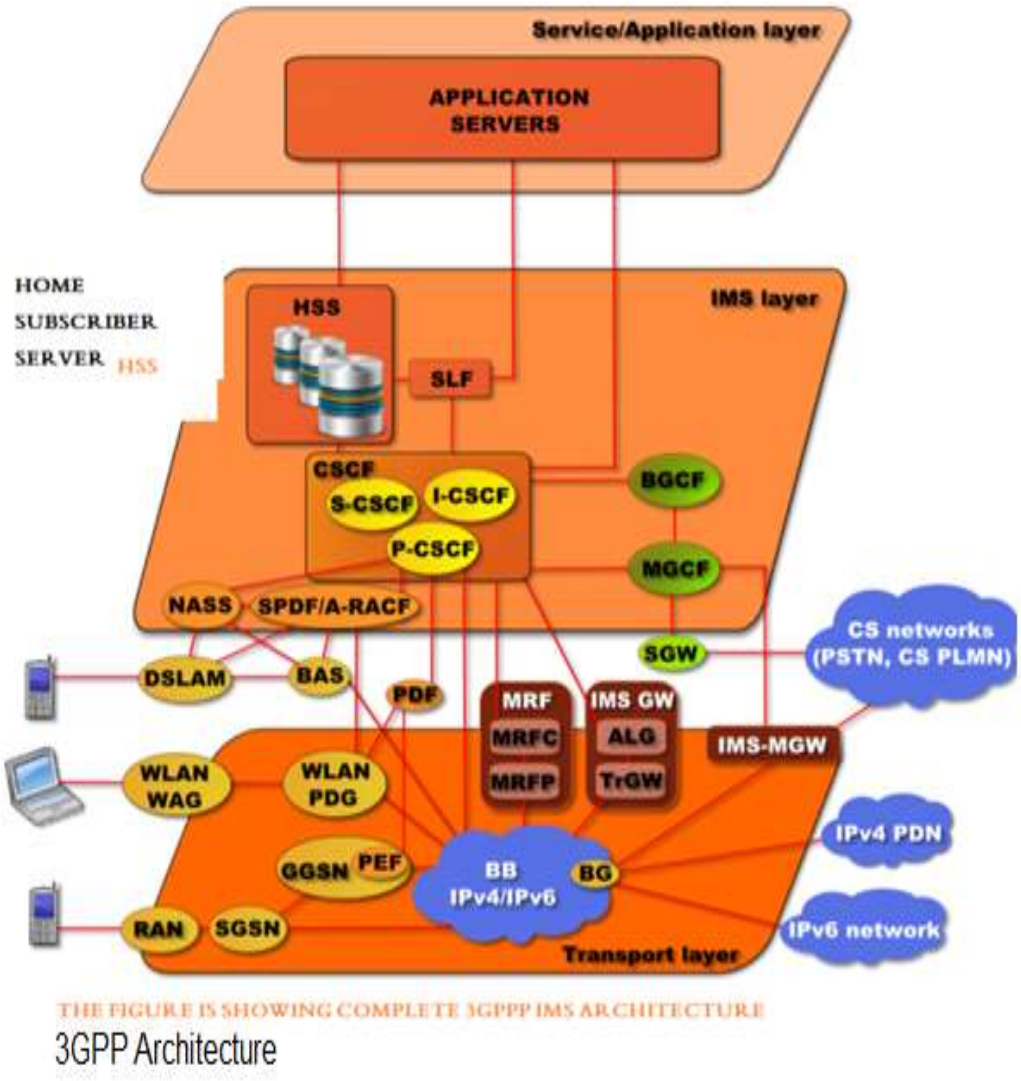

Figure 3.3.

3.2. Next Generation Network Security Architecture

The network security for next generation mostly secures the IMS security and it has two security domains.

Access view security: this view secures the first hop for end user device to access the network.

- The Core view security: the core view covers security within intra operated domain.

3.3. The 8 Security Dimensions for 4G

The dimensions of 8-security are used in 4G to take care and to measures applied counter threats and attacks some of them are describe as under

i. Access controls: it controls and measures protection level against unauthorized use of network resources.

ii. Authentication: this is used to measure confirmation level for uniqueness of each entity using the network.

iii. Nonrepudiation: it is used to demonstrate the data from its origin or recognizes the grounds of an event or action.

iv. Data confidentiality: it is major security dimension which is used for ensuring that data is not exposed to prohibited users.
v. Communication security: Communication in security is used to allow information flow only between permitted end points.
vi. Data integrity: it is used to ensure the correctness of data in such as, data can be tailored, erased, created or simulated without authorization and it also provides a intimation if unauthorized effort has put forward for the data change.
vii. Availability: it is also used to ensure that there is no denial of authorized access to elements of network, information that is stored, Information flows, services and applications suitable for network impacting events.
viii. Privacy: in the last the privacy is the main security dimension for providing the protection of derived information from the examination of network actions.

4. Wireless/4G Security Issues

4.1. Physical Layer Issue for 4G

Both WIMAX and LTE have focused on two key inclinations at the physical layer. By intentionally inserting manmade interference on a medium, the functioning of communication system can stop because of high signal to noise ratio.
There are two types of interference that can be carried out: Noise and multicarrier.

4.1.1. Noise Interference: It is performed using white Gaussian noise (WGN).

4.1.2. Multicarrier Interference: In it the attacker identifies carriers which are used by the system and then injects very narrowband signal on these carriers [4]. As the Interference attacks can easily be carried out as if the piece of equipment as well the knowledge to carry out such attacks is available without difficulty and widely. In this review on security, it indicates that interference is easy to detect using radio spectrum monitoring equipments. By using radio direction finding apparatus, the interfering source can be traced [1]. In addition, the power of the source signal has to increase and if spreading techniques are used, it may result to increase its resilience in opposition to interference. While the possibility of interference is significant, therefore it is easily being detected and addressed and we believe in its impact on the WIMAX/LTE network and users will also be limited [13].

4.2. Wimax MAC Security Issues

In WiMAX-MAC layer firstly it has to establish initial access with base station then to IEEE802.16 [11]. The Radio interface standard of WiMax describes several steps, if we say about a mobile station it includes seven steps. These are initial ranging and time synchronization, Upper level parameter acquisition, basic capabiliiities negotiation, scanning and synchronization, mobile station authorization and key exchange and registration with the serving base station is the last step by which connection established. Among these all steps five steps involved non secure traffic and other two steps involved secure traffic exchange based on the device authentication standards of WiMax [6].

4.3. DoS Security

The Denial-of-Service (DoS) is also a main security issue; it is attack which is a concern with WiMax network. These attacks are being initiated through simple flooding, attacking on authenticated management frames [2].

4.4. Security Issues for Wi-Fi, under 4G

Wireless LANs based, on WI-FI technology is available from a decade. However, the WIFi technology is, mostly used in homes and public places such as, airports, hostels, and, shopping malls and now in universities where security is seeming less critical, while the cost benefits of Wi-Fi could be attractive to enterprise environments thanks to improved mobility, costs for lower operational, and flexibility. Consequently, security researchers have focused on security threats and their solutions in Wi-Fi networks to make it applicable to the enterprise environments. The security mechanism for Wi-Fi so called wired equivalent privacy (WEP), had a number of security flaws arising from the misapplication of cryptography, *e.g.* the utilization of RC4 stream cipher and the authentication of CRC32 [3]. For this a comprehensive security assessment based on the ITU-T X.805 standard has been performed [9]. To remedies the security flaws of WIFi, there are many solutions have been proposed. The Robust Security Network (RSN) is used for the IEEE 802.Ix standard which is port based network access control that is a layer 2 authentication mechanism and it also specifies how EAP can be encapsulated in the Ethernet frames. RSA Laboratory and Cisco have developed TKIP to diminish the RC4 weakness through repeated replenishment of encryption key [5].

4.5. Potential Threats in 4G

The 4G technology may have to face many possible potential security Risks and threats. The various heterogeneous technologies have capability to access the infrastructure, so it must have needed potential security to secure technologies. 4G technology may also collapse to the entire network infrastructure when multiple service providers share the core network infrastructure. In 4G wireless technologies, end user equipments (either MS or any Wi-Fi routers) can also become a source of malicious attacks, malware, worms, viruses, calls and spam mails and so on. The spam over internet and the new spam for VoIP results a serious problem like the today's E-mail spam [2]. As like the above VoIP threats on the technology, 3 more VoIP Threats are:
(1) Spoofing that misdirects communications, modifies data, or transfers cash from a stolen credit card number,
(2) Standard input point, registration hijacking that, substitutes the IP address of packet, header with attacker's IP,
(3) Dropping of private, conversation that intercepts, and CRYPT arises, on IP packets,

5. Four Layer Security Model for 4G Networks

The 4 layer purposed security model integrated into two frameworks, peripheral and core which allow exploring new security concepts. In this model there are three separate security layers *i.e.* networking architecture security, network transport security & service and application security.

This model is designed to create available coherent heterogeneous communication on a global scale and it is also responsible to supply continuous connectivity through the seamless operation of multiple mobile networks which are accessible by mobile nodes, providing features like cognitive radio and vertical handover. Peripheral network and Core network proposed four layer, security models which, are integrated in to the two frameworks. This proposed, model has two frame works, which are used as:

- Peripheral frame: it can work on the mobile node and interacts with wireless access networks.
- Core framework: it can work in a, distributed fashion in the core infrastructure,

By this double, organized, frame work, a multi layer security, system arises that interacts, with these two, frameworks to provide, a secure environment.

6. Conclusion

For best perceptive, security of 4G networks, paper has represented different security aspects of 4G networks. This paper has also given some depiction on technical issues for 4G wireless network deployment and discussed physical layer issues, WiMAX_MAC layer, issues, DoS, issues and 4G WiFi security issue. As requirements apparently designates that there is a need for an integrated security model to protect data across different networks as well as the need to target the security models to protect different entities such as network infrastructures, servers and users. So far majority of research works have focused on studies or preliminary simulations. And they suggest that there is a vital need to expand researches with emulation and test-bed related studies to reveal further issues and challenges that needs to be addressed. Apparently there is still work to be completed; and researchers believe that there is a strong need for continuing studies on the fourth generation (4G) security threats and development of appropriate counter measures as in this paper 8security dimension for 4G networks are discussed and also discussed some possible potential threats, on 4G wireless networks but still there are new one exists. In the end paper has also proposed four layer 4G security model in which it they have to try to avoid unsecureness of 4G/ wireless and communication.

References

[1] N. Borisov, I. Goldberg and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", Proceedings of ACM MobiCom'2001, Rome, Italy, July 2001.
[2] T. Park, H. Wang, M. Cho and K. G. Shin, "Enhanced Wired Equivalent, Privacy for IEEE 802.11. Wireless LANs", CSE-TR-469-02, University of Michigan, **(2002)**.
[3] Bell Labs, "The Bell Labs Security, Framework: Making the Case for, End-to-End, Wi-Fi Security", **(2006)**.
[4] IEEE Draft 802.1x./D1., "Port Based Network Access Control", available from http://www.ieee802.org/1/mirror/8021/docs99/PortNACIEEE.pdf",.
[5] Z. Shietal, "Layered Security Approach in LTE and Sim-ulation", Proceedings 3rd Int'l Conference Anticounterfeiting, Security and Identification in Communication, (ASID 09), IEEE, **(2009)**, doi:10.1109/ICASID.2009.5276930.
[6] C. Vintila, V. Patriciu and I. Bica, "Security Analysis of ,LTE Access Network" Proceedings 10th Int'l Conf,. Networks (ICN 11), Intl Academy, Research, and ,Industry Assoc., **(2011)**, pp. 29-34.
[7] Network Architecture, tech,. specification 3GPP, TS 23.002, V9.1.0, ,3GPP, **(2009)**.
[8] L. Huang, "Performance of Authentication Protocols, ,in LTE_ Environments", Proceedings ,Int'l Conf,. Computational Intelligence and Security (CIS 09,), IEEE, 2009. doi:10.1109/CIS.2009.50
[9] L. Hui and B. Shuo, "Research and Implementation of LTE NAS Security", Proceedings Int'l . doi:10.1109/ICEIT.2010.5607551
[10] 4G Wireless Systems in Virtex-II by James A. Watson -- Manager, Applications Engineering, Xilinx, Inc. (7/1/01 -- Issue 40) jim.watson@xilinx.com
[11] Y. Raivio, "4G - Hype or Reality", IEE 3G Mobile Communication Technologies, Conference Publication, no. 477, **(2001)**, pp. 346-350.
[12] J. Hu and W. W. Lu, "Open Wireless Architecture - The Core to 4G Mobile Communications", In Proceedings of ICCT, **(2003)**.
[13] J. Pesola and S. Pönkänen, "Location-aided Handover in Heterogeneous Wireless Networks", In Wireless Personal Communications, vol. 30, iss. 2-4, **(2004)**.
[14] Technical Specification Group Services and System Aspects, IP Multimedia Subsystem (IMS), Stage 2, TS 23.228, 3rd Generation Partnership Project, **(2006)**.

Author

Javed Ahmad Shaheen, he has done his MSCS (Networking) from Virtual University of Pakistan Lahore. He has teaching experience in Islamia University of Bahawal Pur “Bahawal Nagar Campus” as “Visiting Lecturer”. He has practical experience of Networking.

