Journal of Engineering and Applied Sciences 12 (Special Issue 2): 6252-6259, 2017
ISSN: 1816-949X

Analysis of Different Security and Vulnerability in Cellular Networks

Anu Ahlawat and Suresh Kumar
Department of ECE, University Institute of Engineering and Technology,
Maharshi Dayanand University, Rohtak Haryana, India

Abstract: During the past decades, infrastructure of wireless communication and the services being offered by the wireless networks have been proliferating in order to meet the rapidly increasing demands. In <30 years, Mobile technology has come a long way or in layman's words we have seen transition from bulky mobile phones and a budding internet to a world of super-slim smart phones that can transmit and store data as well as provides us facility of internet with a simple tap. Today, the world is so much dependent on mobile technology that it is being used for online banking which involves password sharing and much more confidential data is transmitted through these wireless links. Therefore, maintaining security of the information being shared through mobile phones is of paramount importance. Although, mobile phones offers better internet connectivity and numerous other advantages but on the other hand there are lots of security risks which are matter of concern for both users as well as service providers. This study, investigates various vulnerabilities and security threats in mobile communications (2-4G) and presents proficient defense mechanisms to improve the security of wireless networks.

Key words: GSM security architecture, UMTS, LTE, DoS, WEP, MIMA, IP address, MAC address, COMP128, OTA, SS7, FEC, 3GPP, WGN, QoS

INTRODUCTION

Wireless mobile communication has been flourishing since the last decades. And the mobile technology is an evolving concept. The world has seen various generations of mobile technology, i.e., 1-4G or in other words wireless mobile communication has experienced phenomenal growth, i.e., initially entire wireless system was based on circuit switching but today all the voice and messaging services are based on packet switching using Internet Protocol (IP) (Barakovic and Kapov, 2013). Because of easy availability and vast coverage area, mobile communication attracted many users as well as service providers. However, despite several advantages, owing to broadcast nature the information is transmitted through air as a transmission medium as a result the information transmitted through radio propagation is accessible to both authorized and unauthorized users because of this open architecture mobile communication has been facing various security issues. Moreover, the wireless communication is more vulnerable to malicious attacks than wired communication.

The usage of cellular mobile networks and communication in our everyday life is increasing day by day. These day people are using their smart phones as well as the high speed internet facilities to carry out e-Commerce as well as share their confidential information like their passwords and many other personal mails over the air. This sharing of personal information attracts the hackers as well as eavesdroppers to commit various cybercriminal activities.

Hence, paramount attention should be paid to fight against such illicit activities and make the cellular network more robust and reliable. This study, presents various security issues existing in the various cellular generations, i.e., from 2-4G.

MATERIALS AND METHODS

Security requirement in wireless networks: It is very much essential to provide reliable communication. To increase reliability and provide robustness there is need to highlight various requirements for enhancing the quality of service and providing better security (Fig. 1).

Authenticity: In simple words, it involves proof of identity in order to distinguish between authorized user and illegitimate user. Before any user is granted access to the channels, the credentials provided at the time of request for accessing channel are compared with those of stored at the database. If the credentials match, the access is granted otherwise denied.

Corresponding Author: Anu Ahlawat, Department of ECE, University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak Haryana, India

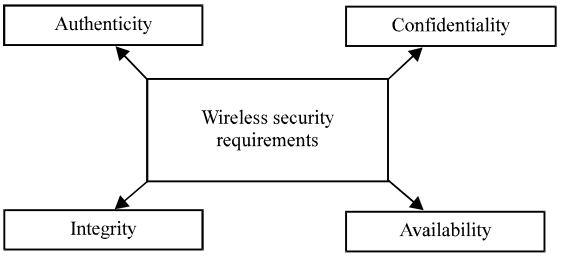

Fig. 1: Security requirements

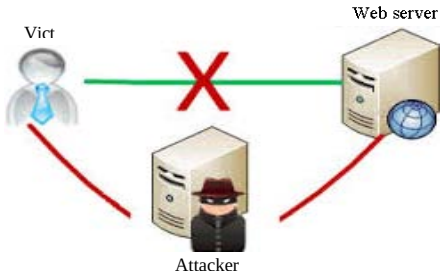

Fig. 2: MIMA attack scenario

Confidentiality: It basically can be said to be roughly equivalent to privacy. It ensures that the sensitive data should be disclosed only to authorized users while preventing information disclosure to unauthorized users. A very key component for protecting the confidentiality of information is encryption of data before it is transmitted. In recent times, physical-layer security is used as means to protect the data against attacks like eavesdropping (Wyner, 1975; Chen *et al*., 2009).

Integrity: As the information has its value only when it is correctly transmitted or in other words tampered information could prove more costly. Therefore, integrity refers to protecting information from any distortion or alteration by unauthorized users. It involves maintaining consistency, accuracy and trustworthiness of data. Cryptographic checksums are used for verification of integrity of data.

Availability: It refers to the ability of user to access resources anytime and anywhere without any interruption. The defiance of availability, also known as DoS. DoS is a type of active attack in which any authorized user is denied to access the resources resulting in unsatisfactory user experience (Wood and Stankovic, 2002; Huang *et al*., 2011; He *et al*., 2008).

RESULTS AND DISCUSSION

Types of attacks: The open environment of wireless communication system makes it prone to various attacks. The attacks can be broadly classified in two types. Active and passive attacks. Each of these attacks is briefly explained below.

Passive attack: A passive attack is a kind of attack in which the attacker continuously monitors the system in order to check out open ports and susceptibilities. Such, attacks are carried out with a sole aim of information gathering. To carry out such attacks; malicious user continuously listens to all the traffic flowing through a wireless network. Although, nature of these attacks is silent and are hard to detect but these attacks can be used for active attacks.

Active attacks: Active attack is a network exploit in which attacker not only listens to the information being shared between authorized users but also harms the integrity of the system, i.e., it attempts to make changes on the data being transmitted. The different types of active attacks are explained below.

Man-In-Middle Attack (MIMA): This attack allows remote attackers to spoof/replicate a base station. MIMA is an active attack here the attacker eavesdrops over the independent connection of the victims and relays messages between them. Let us consider that a user is having a TCP connection, the attacker then bifurcates this connection and the attacker will act as common node for both the connections. Therefore, two connections will be established; the first connection will be from first user to attacker and the second from attacker to other user. So, every information which will be shared between the two users will pass through the attacker. Therefore, attacker can easily steal the information passing between them. The MIMA scenario is depicted in Fig. 2.

DoS: This attack is an explicit attempt by the attacker and is carried out in order to prevent the legitimate users from using the services. DoS attacks can be mainly classified in two types: jamming and flooding.

Jamming: In wireless network, this attack is carried with an aim to cause disruptions in the transmissions between authorized users. A jamming attack is carried out by emitting unnecessary radio signals. In order to interrupt the transmission the jammer continuously transmits signals over a shared wireless channel and this continuous transmission causes lots of energy wastage therefore we can conclude jamming to be energy-inefficient. Therefore, in order to enhance its efficiency, a jammer transmits an interfering signal only

when it detects an authorized active transmitter. Depending upon the working of the jammers the jammers can be classified in five types (Pelechrinis *et al*., 2011).

Reactive jammer: In such type of jammer whenever legitimate transmission is detected a jamming signal is only imposed.

Constant jammer: In this type of jammer, a jamming signal is constantly transmitted.

Adaptive jammer: In this type of jammer, jamming signal is attuned to the level of received power at the legitimate receiver.

Intermittent jammer: In such type of a jamming signal is emitted from time to time.

Intelligent jammer: Such type of jammer exploits weaknesses of protocols of upper-layer for blocking.

Flooding attack: Here, an attacker sends enormous amount of packets with an aim to disrupt network communication with other nodes. The sole aim of the attacker is to drain out the resources on the victim's machine.

Replay/playback attack: It is a type of active attack in which the data transmitted is repeated maliciously. An attacker intercepts the data transmitted in order to resend it further. This repetition is done in order to exhaust out the energy of the network (Feng *et al*., 2011).

Impersonate attack and sybil attack: In this the attacker obtains the IP address or MAC (Media Access Control) address of any authorized user and then makes this identity as it own. This attack is very well known. Then this stolen identity may be used by the attacker to do various other attacks. The advanced version of impersonate attack is termed as Sybil attack in such type of attack the attacker steals multiple identities (Fig. 3).

Vulnerabilities in GSM: GSM is a digital cellular system; it was introduced in Europe in 1991.The GSM network architecture was designed initially by laying stress on authentication of user, maintain user anonymity and keeping the confidentiality of user in mind. However, integrity of the network was ignored (Lo and Chen, 1999).

The services provided by GSM network cannot be accessed by any subscriber prior to authentication, i.e., he must be first authenticated for authentication of the user

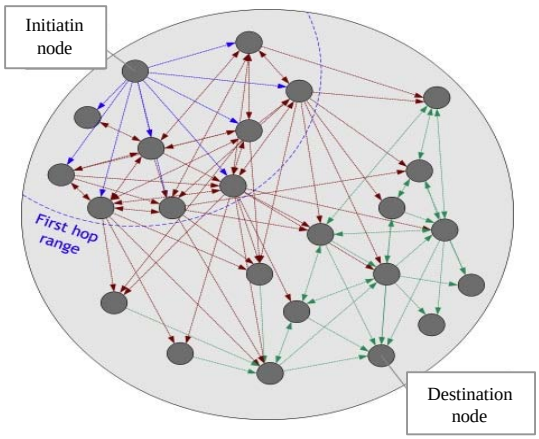

Fig. 3: Flooding scenario; Oberg and Xu (2007)

the GSM network uses A3 algorithm. The authentication uses a challenge-response mechanism. And A5 algorithm is used for the purpose of encryption (Chandra, 2005).

There are various security vulnerabilities found in GSM. Some of these issues are resolved in higher cellular network generations. Some of the challenges faced by the GSM networks are mentioned below.

Unilateral authentication: GSM network authenticates the users but the users do not authenticate the network, due to this the attacker uses a forged Base Transreceiver System (BTS) with the same mobile network code as that of legitimate subscriber network to masquerade himself and performs MIMT attack (Siddique and Amir, 2006; Niemi and Nyberg, 2003).

Flaws in implementation of A3/A8 algorithms: The A3 and A8 algorithm resides in the SIM which can cause security issues by cloning the SIM it is possible to get all the call and messages traced from the respective SIM number. Also by using the technology of mobile, attacker can decode the algorithm's and can attack on provider's network. Although, in the GSM security architecture, the operator can choose any of the algorithm for authentication, i.e., either A3 or A8 but some operators uses COMP128 and this algorithm was developed by the GSM association. Later on, many security flaws were found in the structure of COMP128 (Lo and Chen, 1999; Rankl and Effing, 2003).

SIM card cloning: This attack is well-known for >25 years and when this attack is performed various secure values that are stored in SIM are extracted and are programmed into another chip card, creating a replica of the original SIM. Cloning is feasible by both physical and Over-The-Air (OTA) methods (Gonzalez-Castano *et al*., 2002).

Physical cloning: In physical cloning duplicate SIM is created by gaining access to the target SIM and extracting its unique identifiers using a card reader and then a card writer is utilized to replicate the SIM values into new SIM card. In order to perform physical cloning the attacker should possess following things (Rao *et al*., 2002; Biryukov *et al*., 2000):

- A programmer (Super sim, Sim Max) for reading the SIM
- Also a blank SIM is necessary, on which data can be copied
- Silver SIM Wafer Cards are generally utilized for this purpose
- And lastly a program is required to readout the identifiers like Ki, IMSI (International Mobile Subscriber Identity) and ICCID (ID of the SIM-card)

OTA: It is also possible to extract the unique identifiers of the SIM like Ki, IMSI without any physical access. For this purpose several challenges are sent to the SIM over the air and then these challenges are analyzed. However, this is a time consuming approach (Barkan *et al*., 2003).

Short range of protection: In GSM networks confidentiality is provided through encryption but the information is encrypted on when it is passed over the air interface, i.e., between Mobile Station (MS) and BTS. This clearly indicates that whenever the information is passed over the fixed parts that information can be easily eavesdropped by the attackers because it is transmitted without being encrypted. Moreover, the air interface is considered to be weakest for the hackers. Security for SS7 (Signaling system No. 7) part was not provided as SS7 was used for few of the institutions (Lorenz *et al*., 2001).

Leaking the user anonymity: The GSM network requests the user to transmit its IMSI visibly through the air interface whenever a user enters the location area for the first time or when the mapping between the user's TMSI (Temporary Mobile Subscriber Identity) and IMSI is lost. This information can be missed used by the attackers (Bocan and Cretu, 2006).

No provision for integrity: The GSM security architecture provided provision for authentication and confidentiality however, the security requirement mandates the provision of integrity to be included in the architecture of any network in order to prevent the information from being tampered. But the integrity protection has been ignored in the GSM security architecture.

Vulnerabilities in cryptographic algorithms: The two algorithms, i.e., A5/1 and A5/2 were used for encryption of GSM but the main flow found in these algorithms was that the algorithms were confidentially developed. So when the A5 algorithms were realized in public and analyzed by the cryptanalysts it was apparent that encryption can be easily attacked and broken by relatively easy methods. The main vulnerability found in these algorithms was the generated key (Kc). The algorithms (A5/1, A5/2) were not designed with modern cryptographical knowledge (Katugampala *et al*., 2005; Rekha *et al*., 2005).

Solutions to vulnerabilties of GSM

Use of safe algorithms for authentication: It can help in thwarting the perilous SIM cloning attacks. However, to implement this solution it is essential to disturb new SIM cards and modify the software of HLR (Home Location Register). At present, in order to thwart OTA cracking of Ki; GSM uses both COMP128-2 and COMP128-3 Moreover, in COMP128-3 algorithms the effective key length of session key has been increased by 10 bits which further enhances the security of GSM networks.

Using secure ciphering algorithms: By implementation of secure ciphering algorithms and modification of the authentication protocols the safety of GSM consortium can be improved. It will help in securing the backbone traffic from the problem of eavesdropping from the hackers and modification of transmitted data can be prevented.

End-to-end encryption: Another, way to secure GSM communication is to deploy the end-to-end security or security at the application layer. End-to-End Encryption (E2EE) crypts sensitive data. This information securely travels over the vulnerable channels to its destination where it is decrypted (Rekha *et al*., 2005).

Improvements in umts over GSM: UMTS security was built by retaining strong security features and advantages of GSM and addressing the vulnerabilities of GSM security architecture. The 3G introduced entirely packet based networks whereas the earlier mobile generations were based on circuit switching. The various other improvements over GSM include.

Mutual authentication: The term mutual authentication means that both user as well as network has to authenticate each other. In GSM, the authentication was done only one way, i.e., only from user to network which makes GSM vulnerable to many attacks in order to counter those attacks UMTS uses mutual authentication there by providing security against rogue base station.

Integrity protection: UMTS also provides provision of integrity mechanism which protects the messages from any alteration. Hence, integrity mechanism with improved authentication provides protection against active attacks.

Enhanced encryption: UMTS provides enhanced encryption to ensure that the messages are available only to authorized users. In case of GSM, the encryption is performed at BS whereas in UMTS encryption is employed in the Radio Network Controller (RNC). UMTS uses longer encryption key lengths which further ruggedized the confidentiality.

Quality of service: Quality of service was not fully addressed by GSM security architecture. In UMTS QoS was incorporated in order to maximize the user experience and also to ensure that spectrum is optimally allocated for a particular type of data service.

LTE-security evolution: As the security architecture of cellular networks has evolved continuously. In 1G (first Generation) wireless it was very easy for intruders to eavesdrop and gain access to the network using fraudulent means (Zhang and Fang, 2005). In 2G GSM, the algorithms used for authentication were easy to decode. Moreover, the master security keys were easy to disclose with a few interactions with a SIM card (Shin *et al*., 2005). In 3G wireless, the authentication process was strengthened by using mutual authentication. In addition, security in 3G was further increased by using 128-bit encryption and integrity keys (Putz and Schmitz, 2000). Then the next generation, i.e., the 4G or LTE system showed a transition from circuit switched to packet was designed to be a packet based system that offers many advantages as compared to previous networks.

Vulnerabilties in LTE: Due to the introduction of new radio access technologies and movement towards IP-based architecture, new vulnerabilities have aroused, given below is the classification and categorization of various threats to LTE security architecture (Fig. 4).

Physical layer issues: There are basically two types of vulnerabilities at physical layer in LTE system-interference and scrambling attacks (Putz and Schmitz, 2000). Interference causes interruption in smooth functioning of a communication system due to high signal-to-noise ratio. Interference in any communication system can be carried out in two ways: noise, multicarrier (Husso, 2006). Noise interference can be performed using White Gaussian Noise (WGN). In the case of multi-carrier interference, the attacker identifies carriers used by the

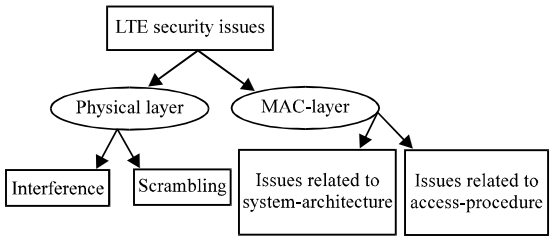

Fig. 4: Types of attacks in LTE

system and injects a very narrowband signal onto those carriers. Scrambling is also a type of interference which is inserted for small intervals of time. In this type of attacks specific frames are targeted. In order to disrupt the services of a particular user, the attacker targets control and management information. However, the attacker has to be sophisticated and knowledgeable. Because, specific frames and time slots must be identified for the attack to be successful. As a result, scrambling is difficult to implement successfully. Therefore, it represents least security concern.

MAC layer issues

Open architecture issues: Transition to open set of communication protocols, i.e., TCP/IP suite anticipated increase of issues in LTE such as the vulnerability to the injection, modification, eavesdropping attacks and more privacy risks than those in the GSM and the UMTS networks (Al-Humaigani *et al*., 2009; Aiash *et al*., 2010). LTE architecture becomes more vulnerable to the traditional malicious attacks such as IP address spoofing, DoS attacks, spam mails and calls and so on (Park and Park, 2007).

Issues related to access procedure: In order to achieve a mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME) through the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN), the LTE architecture has enhanced the UMTS-Authentication and Key Agreement (UMTS-AKA) and presented the new access security approach, Evolved Packet System AKA (EPS AKA) and the J-PAKE (Password Authenticated Key Exchange by Juggling) mechanism. However, these authentication protocols too suffer from various vulnerabilities like leakage of IMSI, leakage of key, traffic redirection, tracking of temporary identity, i.e., GUTI (Xiehua and Yongjun, 2011; Vintila *et al*., 2011; Deng *et al*., 2009; Abdo *et al*., 2012). These vulnerabilities need to be addressed to bring robustness in the security architecture.

Solutions to lTE vulnerabilities: Various solutions have been proposed by various researchers in order to cater the vulnerabilities of LTE. A few of them are given below by Zheng *et al.* (2005), hybrid authentication, authorization and key agreement has been proposed which is based on Trust Model Platform (TMP) and Public Key Infrastructure (PKI). With an aim to achieve mutual authentication between user equipment and hybrid node passwords are linked with finger prints and public key. This proposed scheme provided robustness to users so that they can access sensitive services and data.

Zheng *et al.* (2015) an AKA which is based on the scheme called Self-certified Public Key (SPAKA) has been presented. In this scheme, a public key broadcast protocol is generated using probabilistic method. This method helps to distinguish between rogue and genuine base station this was one of the major shortcomings of the 3G AKA scheme as well.

Li and Wang (2011), AKA based on Wireless Public Key Infrastructure (WPKI) has been presented and this new AKA scheme is termed as A Security Enhanced Authentication and Key Agreement (SE-EPS AKA). This scheme provided robustness to the security of LTE by using Ellipse Curve Cipher (ECC) encryption. In this encryption scheme the messages exchanged as well as the identity of user are secured with limited energy consumption.

Abdo *et al.* (2013), various vulnerabilities including brute and intelligent forces were pointed out in SE-EPS AKA protocol. In this study another scheme has been presented in order to further enhanced the confidentiality of user which was matter of concern in the scheme presented in Li and Wang (2011) and this new approach is termed as authentication and key agreement (ECAKA).

Mun *et al.* (2009), various new approaches presented in the study by Zheng *et al.* (2005), Li and Wang (2011) and Abdo *et al.* (2012) in order to overcome vulnerabilities of LTE employ public-key based protection mechanisms and this study presented various limitations of using public key.

Kien (2009) this study proposed the solution to the problems mentioned by Mun *et al.* (2009). The solution provides the need to take large number of deployment overheads so as to establish public key infrastructure in LTE. But the solution proposed is very expensive to implement.

Shi *et al.* (2009), to provide access layer security in LTE networks an EAP Archie method has been proposed. This scheme uses AES ciphering in order to achieve mutual authentication and key agreement.

CONCLUSION

Wireless mobile communication has been rapidly growing and has experienced phenomenal growth. Since, it provides access to users at all time and everywhere, mobile communication attracted users as well as service providers across the world. However, mobile communication has been facing various security issues. In this present study, we have presented a detailed study of both the vulnerabilities and existing security measures available in various networks. However, the need to strengthen the security measure may also draw the attention of researchers to further hardening of mobile station user equipment, along with the network. This study will provide a good study material and a platform to motivate the researchers to work in this field and develop novel and hardened security measures.

REFERENCES

Abdo, J.B., J. Demerjian, H. Chaouchi and G. Pujolle, 2013. EC-AKA2 a revolutionary AKA protocol. Proceedings of the International Conference on Computer Applications Technology (ICCAT), January 20-22, 2013, IEEE, Sousse, Tunisia, ISBN:978-1-4673-5284-0, pp: 1-6.

Abdo, J.B.B., H. Chaouchi and M. Aoude, 2012. Ensured confidentiality authentication and key agreement protocol for EPS. Proceedings of the 2012 Symposium on Broadband Networks and Fast Internet (RELABIRA), May 28-29, 2012, IEEE, Baabda, Lebanon, ISBN:978-1-4673-2151-8, pp: 73-77.

Aiash, M., G. Mapp, A. Lasebae and R. Phan, 2010. Providing security in 4G systems: Unveiling the challenges. Proceedings of the 6th Advanced International Conference on Telecommunications (AICT), May 9-15, 2010, IEEE, Barcelona, Spain, ISBN: 978-1-4244-6748-8, pp: 439-444.

Al-Humaigani, M., D.B. Dunn and D. Brown, 2009. Security transition roadmap to 4G and future generations wireless networks. Proceedings of the 41st Southeastern Symposium on System Theory (SSST 2009), March 15-17, 2009, IEEE, Tullahoma, Tennessee, ISBN:978-1-4244-3324-7, pp: 94-97.

Barakovic, S. and L.S. Kapov, 2013. Survey and challenges of QoE management issues in wireless networks. J. Comput. Netw. Commun., 2013: 1-28.

Barkan, E., E. Biham and N. Keller, 2003. Instant ciphertext-only cryptanalysis of GSM encrypted communication. Proceedings of the 23rd Annual International Conference on Cryptology (Crypto 2003), August 17-21, 2003, Springer, Santa Barbara, California, pp: 600-616.

Biryukov, A., A. Shamir and D. Wagner, 2000. Real time cryptanalysis of A5/1 on a PC. Proceedings of the 2000 International Workshop on Fast Software Encryption (FSE), March 20-23, 2000, Springer, Berlin, Germany, pp: 1-18.

Bocan, V. and V. Cretu, 2006. Mitigating denial of service threats in GSM networks. Proceedings of the 1st International Conference on Availability, Reliability and Security (ARES 2006), April 20-22, 2006, IEEE, Vienna, Austria, ISBN: 0-7695-2567-9, pp: 1-6.

Chandra, P., 2005. Bulletproof Wireless Security, GSM, UMTS, 802.11 and Ad hoc Security. Newnes Publisher, Newnes, New South Wales, ISBN:9780750677462, Pages: 237.

Chen, X., K. Makki, K. Yen and N. Pissinou, 2009. Sensor network security: A survey. IEEE Commun. Surveys Tutorials, 11: 52-73.

Deng, Y., H. Fu, X. Xie, J. Zhou and Y. Zhang *et al*., 2009. A novel 3GPP SAE authentication and key agreement protocol. Proceedings of the IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC 2009), November 6-8, 2009, IEEE, Beijing, China, ISBN:978-1-4244-4898-2, pp: 557-561.

Feng, Z., J. Ning, I. Broustis, K. Pelechrinis and S.V. Krishnamurthy *et al*., 2011. Coping with packet replay attacks in wireless networks. Proceedings of the 8th Annual IEEE Conference on Communications Society on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 27-30, 2011, IEEE, Salt Lake City, Utah, ISBN:978-1-4577-0094-1, pp: 368-376.

Gonzalez-Castano, F.J., J. Vales-Alonso, J.M. Pousada-Carballo, F.I. de Vicente and M.J. Fernandez-Iglesias, 2002. Real-time interception systems for the GSM protocol. IEEE Trans. Veh. Technol., 51: 904-914.

He, D., J. Wang and Y. Zheng, 2008. User authentication scheme based on self-certified public-key for next generation wireless network. Proceedings of the 2008 International Symposium on Biometrics and Security Technologies (ISBAST 2008), April 23-24, 2008, IEEE, Islamabad, Pakistan, ISBN:978-1-4244-2427-6, pp: 1-8.

Huang, H., N. Ahmed and P. Karthik, 2011. On a new type of denial of service attack in wireless networks: The distributed jammer network. IEEE. Trans. Wirel. Commun., 10: 2316-2324.

Husso, M., 2006. Performance analysis of a WimAX system under jamming. MSc Thesis, Helsinki University of Technology, Espoo, Finland,

Katugampala, N.N., K.T. Al-Naimi, S. Villette and A.M. Kondoz, 2005. Real-time end-to-end secure voice communications over GSM voice channel. Proceedings of the 13th European Conference on Signal Processing, September 4-8, 2005, IEEE, Antalya, Turkey, ISBN:978-160-4238-21-1, pp: 1-4.

Kien, G.M., 2009. Entity Authentication and Personal Privacy in Future Cellular Systems. River Publisher, Aalborg Denmark, ISBN:978-87-92329-32-5, Pages: 243.

Li, X. and Y. Wang, 2011. Security enhanced authentication and key agreement protocol for LTE/SAE network. Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), September 23-25, 2011, IEEE, Wuhan, China, ISBN:978-1-4244-6250-6, pp: 1-4.

Lo, C.C. and Y.J. Chen, 1999. Secure communication mechanisms for GSM networks. IEEE. Trans. Consum. Electron., 45: 1074-1080.

Lorenz, G., T. Moore, G. Manes, J. Hale and S. Shenoi, 2001. Securing SS7 telecommunications networks. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security Vol. 2, June 5-6, 2001, Military Academy, West Point, New York, USA., pp: 273-278.

Mun, H., K. Han and K. Kim, 2009. 3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA. Proceedings of the Wireless Telecommunications Symposium, April 22-24, 2009, Prague, Taiwan, pp: 1-8.

Niemi, V. and K. Nyberg, 2003. UMTS Security. John Wiley and Sons, Chichester, England, ISBN:0-470-85314-X, Pages: 283.

Oberg, L. and Y. Xu, 2007. Prioritizing bad links for fast and efficient flooding in wireless sensor networks. Proceeding of the International Conference on Sensor Technologies and Applications, October 14-20, 2007, Valencia, Spain, pp: 118-126.

Park, Y. and T. Park, 2007. A survey of security threats on 4G networks. Proceedings of the IEEE Workshops on Globecom, November 26-30, 2007, IEEE, Washington, DC., USA., ISBN:978-1-4244-2024-7, pp: 1-6.

Pelechrinis, K., M. Iliofotou and S.V. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of jammers. IEEE. Commun. Surv. Tutorials, 13: 245-257.

Putz, S. and R. Schmitz, 2000. Secure interoperation between 2G and 3G mobile radio networks. Proceedings of the 1st International Conference on 3G Mobile Communication Technologies, March 27-29, 2000, IET, London, UK., pp. 28-32.

Rankl, W. and W. Effing, 2004. Smart Card Handbook. 3rd Edn., John Wiley and Sons, Chichester, England, ISBN:9780470856680, Pages: 1120.

Rao, J.R., P. Rohatgi, H. Scherzer and S. Tinguely, 2002. Partitioning attacks: Or how to rapidly clone some GSM cards. Proceedings of the 2002 IEEE Symposium on Security and Privacy, May 12-15, 2002, IEEE, Berkeley, California, ISBN:0-7695-1543-6, pp: 31-41.

Rekha, A.B., B. Urnadevi, Y. Solanke and S.R. Kolli, 2005. End-to-end security for GSM users [speech coding method]. Proceedings of the IEEE International Conference on Personal Wireless Communications (ICPWC 2005), January 23-25, 2005, IEEE, New Delhi, India, ISBN:0-7803-8964-6, pp: 434-437.

Shi, Z., Z. Ji, Z. Gao and L. Huang, 2009. Layered security approach in LTE and simulation. Proceedings of the 3rd International Conference on Anti-counterfeiting, Security and Identification in Communication (ASID 2009), August 20-22, 2009, IEEE, Hong Kong, China, ISBN:978-1-4244-3883-9, pp: 171-173.

Shin, M., J. Ma, A. Mishra and W.A. Arbaugh, 2006. Wireless network security and interworking. Proc. IEEE, 94: 455-466.

Siddique, S.M. and M. Amir, 2006. GSM security issues and challenges. Proceedings of the 7th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, July 19-20, IEEE Computer Society, Washington DC, USA., pp: 413-418.

Vintila, C.E., V.V. Patriciu and I. Bica, 2011. A J-PAKE based solution for secure authentication in a 4G network. Proceeding of the 10th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications (NEHIPISIC'11), February 20-22, 2011, WSEAS, Cambridge, ISBN: 978-960-474-276-9, pp. 42-47.

Wood, A.D. and J.A. Stankovic, 2002. Denial of service in sensor networks. IEEE Comput. Mag., 35: 54-62.

Wyner, A.D., 1975. The wire-tap channel. Bell Syst. Technical J., 54: 1355-1387.

Zhang, M. and Y. Fang, 2005. Security analysis and enhancements of 3GPP authentication and key agreement protocol. IEEE. Trans. Wirel. Commun., 4: 734-742.

Zheng, Y., D. He, X. Tang and H. Wang, 2005. AKA and authorization scheme for 4G mobile networks based on trusted mobile platform. Proceedings of the 5th International Conference on Information, Communications and Signal Processing, December 6-9, 2005, IEEE, Bangkok, Thailand, ISBN:0-7803-9283-3, pp: 976-980.