TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

A Survey on Security and Authentication Issues and Future Trends in Next Generation Networks

[1]Ravindra .S B.E. M.Tech, [2]Dr.Shankaraiah B.E. M.Tech Ph.D (IISc)
[1]Senior Assistant Professor, Department of ECE, City Engineering College, Bangalore
ravindraa.s@gmail.com
[2]Professor and Head, Department of ECE, JSS Science & Technology University, Mysore
shankarsjce@gmail.com

Article Info
Volume 83
Page Number: 35 - 44
Publication Issue:
May - June 2020

Article History
Article Received*: 11August 2019*
Revised*: 18November 2019*
Accepted*: 23January 2020*
Publication*: 07May2020*

Abstract:
With an increasing number of mobile devices, large amounts of data and higher data rates, the current generation of the mobile network is being reconsidered. The next generation networks (NGN) are expected to fulfill high-end requirements, with three features: pervasive connectivity, extreme low latency, and high-speed data transmission across broad areas. This article presents an extensive analysis of current 4 G and next generation network authentication and security systems. We first offer an overview of existing 4 G and next-generation network surveys. We then describe multiple threats in 4 G networks and next-generation networks, including privacy attacks, integrity attacks, availability attacks and authentication attacks. We also provide security services, including authentication (authentication entity, message authentication), confidentiality and integrity. We are also providing authentication and security solutions for networks of next generation. By knowing the drawbacks to IKEV1, as well as the future direction, we identify challenges in new generation networks by supportingIKEV2 re-authentication and re-using new hash signature algorithms.

Keywords: *NGN, Security, Authentication, Availability, Confidentiality, Key Management, Privacy, IPsec, IKEV1, IKEV2.*

I. INTRODUCTION

With the increasing threats from the Internet and computer networks and the relative rate of safety needed, addressing security issues and creating an application security model for next-generation networks is important. Based on these three features, the next-generation network services are 1. Awareness of Service 2. Richness Product 3. Flexibility of service. Application potential for these services is high through the convergence of such services into a broadband infrastructure [1].

The vision of the next 5 G wireless communication networks consists in providing extremely high data rates, low latency, increased base station capacity, and significant enhancement in service quality (QoS) recognized by users compared to current 4 G LTE networks[2].

High-end requirements are to be met for the next or 5th generation (5 G) mobile networks. Three unique features characterize the 5 G networks: ubiquitous connectivity, extremely low latency and high-speed transfer of information. In addition to state-of - the-art infrastructure, the5 G networks will provide new architectures and technologies [3].

Figure1 demonstrates the common architecture of 5 G wireless networks. 5 G Wireless systems not only offer traditional voice and data communication, but also support new applications in the industry and many other devices .Wireless systems are also available. [4].

The combination of different wireless technologies

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

and communications providers in a 5 G world, which share an IP based core network, will provide mobile devices with the option of switching between providers and technologies so that high quality of service (QoS) is preserved. Quick vertical transmission and network transparency make currencies susceptible to a range of liabilities, such as access control, protection of communication, data confidentiality, availability, and privacy [5].

The remainder of the paper is sorted out as pursues: Section II exhibits the related work; Section III depicts attacks and security services in next generation networks; Section IV presents security services in next generation networks V includes solutions for security and authentication; Section VI clarifies challenges and future directions lastly, Section VII Presents conclusions.

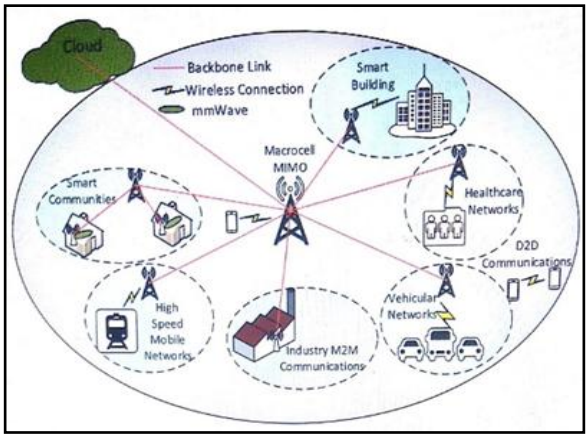

Figure1. 5G Cellular Networks General Architecture

II. Related Work

Our intention is to find a reply: "What is 5 G going to do and how?"We analyze and address significant drawbacks of cellular networks in fourth (4 G) generation as well as related new 5 G network technologies. In 5 G networks, the new technology for 5 G nets, we identify challenges and present a comparative study of the architectures proposed that can be categorized based on energy efficiency, network hierarchy and network types. Particularly relevant are the issues related to implementation (e.g. disruption, QoS, handoff, security-privacy, channel access, and load balancing) [3].

3G and 4G networks are securely layered, but some prominent types of attacks are still possible. A survey of all possible attacks in current and future scenarios was conducted in this paper. Access control, authentication, availability and confidentiality, as attacks can be made in the form, channel assignment and source end, are classified as attacks on the Wireless network [6].

The vulnerabilities and threats of security in wireless communication have been explored, with a focus on physically secure, new paradigms for effective defense mechanisms for improving the security of the wireless networks [7].

A detailed analysis of existing networks 4G and 5G authentication and privacy schemes, as well as the taxonomy and contrast of 4G and 5G cellular network authentication and privacy protection schemes [8].

An insight into the security challenges, networking software, virtualization and user privacy issues in clouds and network functions. Solutions and protocols for protected 5 G systems are now available [9].

Comparing conventional cellular networks with a thorough study on the safety of 5 G wireless network systems. In the light of new service requirements, the potential attacks and security services under 5Gwireless networks are summarized. The new security features include various technologies for 5 G, including heterogeneous networks, device-to-device communications, multi-output massive inputs, networks with software, the Internet of Things. The main concern for the continuity of corporate security and privacy is the continuity of security research and development activities [10] in 5 G business environment.

In the long term, the quality and strength of the security mechanisms offered are assumed to contribute, at least in the long term, to the perceived level of security. Perception is closely related to confidence; therefore, very rapid negative changes could occur [11].

Safety research, study of exploitation and design of

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

prevention safety protocol for communication– including anonymity, authentication and scalability of mobile network [12].

Some of the common security risks to the- delivery of services and business continuity, details the protection of Cisco IP NGN. A model operating process for a end-to-end security analysis, design and implementation is included in the Cisco IP NGN security architecture. This model also helps to establish the economic and operational value of security services and can be used to promote the introduction of managed safety services through technology that incorporates network safety capabilities and systems-built solutions for integrated, collaborative and adaptive safety [13].

III. Attacks And Security Services In Next Generation Networks

Thirty-five attacks have been found to examine and avoid the protection of security and privacy for cellular networks including 4 G and 5G.

1. Attacks against privacy:

The MITM attack [8], MITM targets the real data flowing between endpoints, as well as confident and integral data itself, is the most serious attack of these attacks.

The reference model, such as the OSI versions, as well as two different network architectures, i.e. GSM and UMTS, is taken into consideration. In particular, we categorize MITM attacks based on several parameters such as network location of an attacker, communication channel nature and impersonation techniques. Based on a classification of impersonation techniques, we then give each MITM class implementation steps [14].

The man-in-the-middle (MITM) attack is the significant danger for hand held gadgets to concede to a session key in which they don't share any earlier mystery ahead of time, regardless of whether these gadgets are physically situated in a similar spot, a bipartite and a tripartite confirmation convention utilizing an impermanent private channel, Besides, we further stretch out the framework in to a transitive authentication convention that permits numerous hand held gadgets to set up a meeting key safely and efficiently[15] we study empowering secure and protection saving AMI-UC correspondences by means of LTE-A systems.

By trusting the LTE-A networks, the proposed system aims to achieve critical specifications of protection such as authentication, confidence, and key agreements and data integrity. In addition, a method of aggregation is used to secure energy customers ' confidentiality. The required bandwidth can also be reduced, which can reduce connectivity costs.

Our analyses have shown that our proposals are protected and require low overhead communication [16]. The opponent invites the victim MS to use a weak or non encrypted serving network during this assault. When a network is targeted an intruder hidden between the MS and the SGSN tries to bypass UMTS encryption, induces a dual purpose UMTS / GSM system to use less reliable GSM authentication, and receives AUTN. The assailant can then wake up the Victim's MS [4] session.

It enables insecure communications and sessions easily altered and eavesdropped. The Universal Mobile Telecommunications System Protocol, Authentication and key agreement (AKA) proposes the resolution of vulnerability in the GSM system; the S-AKA protocol may reduce bandwidth consumption; and the number of messages required by authenticating mobile subscribers [17]. Authenticating mobile subscribers is the most common agreement.

2. Attacks against integrity:

Six attacks in this group, i.e. spam attack, blocking of message, copying, attack alteration of message, attack insertion and tampering of message [8].

The cloning attack is based on a red man-in - the-middle BTS with access to information on the cross-layer. The adversary takes the following steps when performing a 5 G layer attack: 1) passive sniffing of

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

downlinks and uplink channels; 2) parsing 5 G control messages; 3) extracting cross layer information; 4). Cloning attack detection[18].

3. Attacks against availability:

Six attacks are graded as First Out, Redirector, Physical Attack, Skimming and Free-Riding Attack in that category. The object of an attack to make a service, for example the data routing service, unavailable [8].

A new secure and effective LTE network AKA protocol which supports safe and efficient communication between different IoT devices and between users. Analysis shows that our protocol is protected, efficient, and confidential and reduces authentication bandwidth consumption [19].

The authentication of data has become increasingly important to prevent the repeated establishment of authentication facilities for different applications. A group-based, protected authentication and key contract (GBS-AKA) scheme that enables the majority redundant signals to be reduced and core network congestion to be lightened. In addition, the authentication delay could be reduced significantly and multiple malware attacks could be prevented [20].

The TrPF trajectory for participatory sensing is a privacy-preserving framework. On the basis of this system, the theoretical model of mixed zones is strengthened by considering the time factor in the light of graphic theory [21].

4. Attacks against authentication:

We classify 10 attacks into this category: password reuse attack, password stealing attack, dictionary attack, brute force attack, desynchronization attack, forgery attack, verifier attack leak, partial message collision attack and a stolen smart-card attack [8].

Brute Force:

Makes an attacker by using an automated error and checking mechanism to guess a username, a password, a credit card number or a security key.

Insufficient Authentication:

Requires a website intruder to access sensitive content or functions without authentication of the website without authentication.

Weak Password Recovery Validation:

Requires an attacker to access a website which requires him or her to obtain, alter or retrieve another user's password illegally. The smart card attack and offline devaluation attack disrupt remote smart card user authentication schemes, which can be extracted from the attacker without knowing any passwords if an user's smart card is stolen.

A protocol called oPass user authentication that reuses a telephone and short message service to steal the password and recreate the password. OPass requires only one single telephone number for each participating website and includes a telecom service provider during phases of registration and recovery [22].

IV. Security services in next generation networks

In particular, we include four types of security services: authentication (authentication of person, authentication of message), confidentiality (confidentiality of data, data protection), access and completeness.

1. Authentication

Two types of authentications exist: authentication of the individual and authentication of document. Within 5 G wireless networks, both authentication of the entity and message authentication are crucial for tackling the above attacks. Authentication of an entity is used to make sure that the interacting party appears to be the same. 5 G networks are open platforms with a variety of services in the legacy of cellular networks. Some of them are intelligent transport, intelligent grid, industrial IoT. The access and service authentication system will be simpler and less costly for networks and service providers alike. In 5 G, three models of authentication that coexists to meet the needs of various enterprises.

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

Network authentication Only Authentication of service providers entails significant cost. Service providers can afford to pay for service authentication networks so that users can access several services once a single authentication has been completed. It frees consumers from the burden of having to obtain a service grant again and again when using various services. Authentication only on the other hand, networks can rely only on established vertical industry authentication capabilities and exclude devices from authentication by the radio network, thereby reducing operating costs for the networks. For some applications a proprietary model could be used in authentication by both networks and service providers. Networks are responsible for network access and service providers are responsible for internet access [23].

2. Confidentiality

Two aspects, i.e. confidentiality and privacy, are the confidentiality. Data protection safeguards data transfer from passive attacks, limits data access to intended users only and prohibits unauthorized users from accessing or revealing data. Server prohibits the tracking and manipulation of valid user information, for example, privacy protections traffic flows from an intruder analysis. Traffically, sensitive information, for example the location of the sender / receiver, etc, can be diagnosed [24].

In order to achieve smooth transitions between the HeNB and the eNB, stability in the LTE networks is important. A fast and stable authentication handover framework that suits all of the LTE network mobility scenarios. Our scheme does not only achieve a simple authentication process with a requested efficiency, compared with other transfer schemes, but also provides several safeguards, including Perfect Forward / Backward Secrecy (PBS / PFS), which has never been achieved through previous projects[25].

Throughout future research into the LTE-A defense, the development of MTC security mechanisms in the Long-Term Evaluation-Advanced (LTE-A) mobile environments is the main. We improve the current transmission mechanisms and offer an effective group anonymity transmission protocol, suitable for all mobility scenarios in the LTE-A networks, for a large number of mobile MTC devices. Reduce signage costs in the access network as well as in the core network, as well as preserve privacy [26].

3. Availability

Availability is a measure of how accessible and usable a service is to any legitimate user wherever and wherever it is requested. Display assesses the robustness of the network in various attacks and is an important performance metric in 5G. The availableness attack is a standard active attack.

DoS attack is one of the major attacks on availability, which may cause legitimate users to refuse access to the service. Connections between legal users by messing with the radio signals interrupt or interfere with communication. 5 G wireless networks face a major challenge with large unsecured IoT nodes in order to avoid jamming and the threat of DDoS in order to ensure the service available [10].

4. Integrity

Information consistency ensures that the data received by the recipient should be similar to that sent by the recipient. Data during transmission should not be changed. Data integrity type: integrity of connection to recovery, integrity of connection without recovery, integrity of the field selective connection, integrity of the field connection, integrity of the selective field connectionless.

V. Solutions For Security And Authentication

Here we learn about different solutions for next-generation networks using authentication and privacy schemes. These solutions can be classified in three kinds: encryption methods, factors for humans and detection methods for intrusion as shown in the Figure. 3.

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

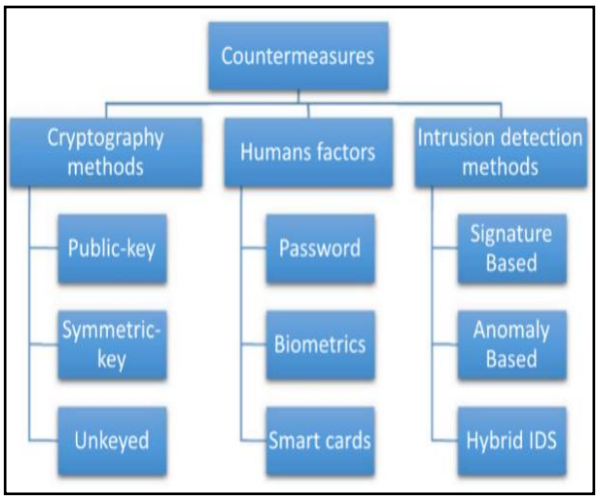

Figure3. Classification of countermeasures used by the authentication and privacy preserving schemes for 4G and 5G cellular networks

1. Cryptography methods

Cryptographical methods are the standard solution used by next-generation network authentication and protection schemes and are divided into three types, namely public key encryption, symmetric key cryptography and unkeyed cryptography. The schemes [27] managed by the open base station (BS) or access point (AP) with a public key infrastructure (PKI). In the schemes mentioned [28], Paillier cryptosystem is used based on three algorithms, namely key generation, encryption and decryption.

Two significant, unique and random prime numbers are used to generate keys: p and q. The encryption algorithm calculates $c = (1+N)^m r^N mod N^2$ m as a message to encrypt: 0=m < N, where, r is a random integer 0<r < N, with public key N = p.q. The decryption algorithm calculates the clear text m:

$$m = \frac{(c.r^{-N} mod\ N^2)-1}{N}$$

Four schemes use symmetric encryption[2] to provide user anonymity, as well as proposing an authentication protocol that is based fully on an IoT enabled LTE network symmetric key system. In addition to this, [5] is used as the symmetric data encryption algorithm for mobile devices by the Advanced Encryption Standard (AES). Based upon the principle of the symmetric key algorithms more quickly than asymmetric key algorithms. Almost all authentication and privacy protection systems use hash functions to provide encrypted messages with data integrity. We note that three popular methods are used in these systems, namely the Message Authentication Code (MAC), the Keyed-Hach Message Authentication Code (HMAC) and the AMAC [29].

A pre-shared key (PSK) method for mutual authentication and session key derivation is EAP-PSK (Extensible Authentication Protocol (EAP). When mutual authentication has successfully been accomplished by both parties, EAP-PSK offers a secure channel of communication. For authentication on insecure networks such as IEEE 802.11, EAP-PSK is built [30].

A privacy-conserving authentication system based on elliptical encryption curve is proposed to provide secure roaming services for mobile users in Global Mobility Networks. Under a formal model that meets any functional safety criterion, the proposed scheme is protected. The authentication scheme is equivalent to existing [31].

5G would require maximum bandwidth and energy efficiency. A modern authentication approach based on CRC offers a quantitative analysis of the protection achieved based on message and CRC sizes. It preserves conventional CRC except for re-programmable connections needed by the LFSR to enforce the encoding and decoding. The CRC enables random and malicious bandwidth detection to be combined. Its main benefit is the ability to detect all double-bit errors in a message, which is particularly important for Turbo code systems, including LTE [32].

2. Smart-card-based password authentication method

Wen –Li's protocol is vulnerable to offline attacks by a password and service denial, and it does not offer forward confidentiality and anonymity to users. We have also established three general principles, with the security analyze of these two schemes and our experience with protocol design, which are vital to

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

secure, smart card-based password authentication schemes: (i) Public-key techniques are invaluable for resisting offline password guessing attacks and for maintaining user confidentiality under the smart card's non-tamper resistance assumption; (ii) an inevitable trade-off arises while fulfilling the objectives of local password updating and resistance to smart card loss attacks; (iii) at least two exponentiation (respectively elliptic curve point multiplication) operations; server-side operations are necessary to achieve forward secr ecy [33].

3. Intrusion detection method

Securing information systems in no option nowadays is a must instead. The rising number of attacks on networks and systems has brought about the need for fast, simple and reliable IDS. Two detections used by IDS are available: anomaly-based detection and signature-based detection. Network-based Intrusion Detection System (NiDS) is the safety aspect of cloud computing services, which has become a preferred solution for new companies and corporations. NIDS identifies and monitors network attacks. NIDS's real-time alert is able to successfully identify the classified attacks via the network [34].

The large number of signatures contained in its database is suffering from IDS dependent on signatures. A proposed module with small databases and the most common signatures and an update agent. Parallel storage. For the host-based IDS and Network-based IDS [35] this module can be used.

VI. Challenges And Future Directions

1. Challenges

Some of the IKEV1 limitation are (i)IKEv1 Main Mode Reflection Attack with Digital Signatures or Pre-Shared Keys, (ii)IKEv1 Main Mode Reflection Attack with Public Key Encryption, (iii) IKEv1 Aggressive Mode Authentication Failure with Digital Signatures(iv) IKEv1 Main Mode Authentication Failure with Digital Signatures not needing self-communication [36].

IKE daemon does not currently support the authentication during IKE rekeying, since IKE rekey follows the "break-before-make" strategy, which is to tear up existing IKE / IPsec SAs and to create new IKE / IPsec SAs. When BTS remains unauthenticated and the peer certificate is corrupted, traffic to a non-secure entity will always be permitted. That does not mean that BTS offers secure transport in real time. The weakness is more evident considering future uses, such as MC / Native / Multi-tenancy. BTS, where the latest signature hash algorithms have to support IPsec, 3GPP Release 14 support is required.

2. Future Solution

IKE Re-Authentication with "Make-before-break" Approach:

Like IKEv1, IKEv2 has no clear re-authentication support when re-enabling. IKEv2 rekeying is currently based on CREATE CHILD SA (not causing re-authentication). Conversely, rekeying IKEv2 can be based on the exchange of IKE SA INIT. This method would lead to re-authentication (meaning a' break-before-making' approach), the development of a new IKE SA and packet loss for each rekeying process.

New Authentication Method Support:

A new method for the authentication of assisted hash algorithms for signature. It allows pairs to know and use the other end of which Hash algorithms are accepted (as long as one is expected to be allowed under regulation – right auth = rsa-4096-sha256 or right auth = rsa-2048-sha256).

VII. Conclusions

Enhanced performance is required for many new applications across Next Generation Networks. We presented a comprehensive study in this paper on recent privacy and authentication advances in networks of the next decade.

Current security solutions have been introduced, based mainly on the security services offered, such as authentication, availability, privacy, key

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

management. Solutions are outlined for different security entities. Finally, we presented the challenges and protocols for the security and authentication of the next generation networks.

We expect this to resolve security concerns in industry and academia in order to provide research directions in the near future for the implementation of safety and authentication in next generation networks.

References

1. Masoud Haveri Khyavi, Mina Rahimi" Conceptual model for security in next generation network"978-1-5090-2461-2/16 $31.00 © 2016 IEEE DOI 10.1109/WAINA.2016.12
2. M.Agiwal, A. Roy, and N. Saxena, ''Next generation 5G wireless networks: A comprehensive survey,'' IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.
3. N. Panwar, S. Sharma, and A. K. Singh, ''A survey on 5G: The next generation of mobile communication,'' Phys. Commun., vol. 18, pp. 64–84, Mar. 2016.
4. 5G security,'' Ericsson, Stockholm, Sweden, White Paper, Jun. 2015
5. Zhang, A., Chen, J., Hu, R.Q., Qian, Y., 2016. SeDS: secure data sharing strategy for D2D communication in LTE-advanced networks. IEEE Trans. Veh. Technol. 65 (4),2659–2672.http://dx.doi.org/10.1109/TVT.2015.2416002.
6. [Akil Gupta, Rajkumar Jha "Security Threats of Wireless Networks:ASurvey"ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE
7. Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo,"A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends "Vol. 104, No. 9, September 2016.
8. Mohamed Amine Ferraga, b, Leandrosaglarasc, AntoniosArgyrioud, DimitriosKosmanosd, Helge Janickec,''Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes''1084-8045/ © 2017 Elsevier Ltd. All rights reserved.
9. Ijaz Ahmad, Tanesh Kumar, MadhusankaLiyanage, Jude Okwuibe, and Mika Ylianttila."Overview of 5G Security ChallengesandSolutions"10.1109/MCOMSTD.2018.1700063.
10. D. Fang et al.: "Security for 5G Mobile Wireless Networks" volume 6, 2018,Digital Object Identifier 10.1109/ACCESS.2017.2779146.
11. 5G Security: Forward Thinking Huawei White Paper.
12. Roger PiquerasJover Bloomberg LP, New York, NY rpiquerasjov@bloomberg.net."Some key challenges in securing 5G wireless networks".
13. IP Next-Generation Network Security for Service Providers, white paper. http://www.cisco.com/go/nfp
14. Conti, M., Dragoni, N., Lesyk, V., 2016. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 18 (3), 2027–2051. http://dx.doi.org/10.1109/COMST.2016.2548426.
15. Chen, Chien-Ming, Wang, King-Hang, Wu, Tsu-Yang, Pan, Jeng-Shyang, Sun, HungMin, 2013. A scalable transitive human-verifiable authentication protocol for mobile devices. IEEE Trans. Inf. Forensics Secur. 8 (8), 1318–1330. http://dx.doi.org/10.1109/TIFS.2013.2270106.
16. Haddad, Z., Mahmoud, M., Taha, S., Saroit, I.A., 2015. Secure and privacy-preserving AMI-utility communications via LTE-A networks. In: Proceedings of the 11th International Conference on Wireless and Mobile Computing Networks Communication, IEEE, pp.748–755. http://dx.doi.org/10.1109/WiMOB.2015. 7348037.
17. Yao, J., Wang, T., Chen, M., Wang, L., Chen, G., 2016. GBS-AKA: Group-Based Secure Authentication and Key Agreement for M2M in 4G Network. In: proceedings of International Conference Cloud Computing and Research Innovation, IEEE, pp. 42– 48. http://dx.doi.org/10.1109/ICCCRI.2016.15.
18. Hasan, K., Shetty, S., Oyedare, T., 2017. Cross layer attacks on gsm mobile networks using software defined radios. In: Proceedings of 14th IEEE Annual

May – June 2020
ISSN: 0193-4120 Page No. 35 - 44

Consumer Communications&Networking Conference (CCNC), IEEE, pp. 357–360.
19. Saxena, N., Grijalva, S., Chaudhari, N.S., 2016. Authentication Protocol for an IoTEnabled LTE Network. ACM Trans. Internet Technol. 16 (4), 1–20. http:// dx.doi.org/10.1145/2981547.
20. Yao, J., Wang, T., Chen, M., Wang, L., Chen, G., 2016. GBS-AKA: Group-Based Secure Authentication and Key Agreement for M2M in 4G Network. In: proceedings of International Conference Cloud Computing and Research Innovation, IEEE, pp. 42– 48. http://dx.doi.org/10.1109/ICCCRI.2016.15.
21. Gao, S., Ma, J., Shi, W., Zhan, G., Sun, C., 2013. TrPF: a trajectory privacy-preserving framework for participatorysensing.IEEETrans. Inf. Forensics Secur8(6),874-887. http://dx.doi.org/10.1109/TIFS.2013.2252618.
22. Sun, H.-M., Chen, Y.-H., Lin, Y.-H., 2012. oPass: a user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans. Inf. ForensicsSecur7(2), 651–663. http://dx.doi.org/10.1109/TIFS.2011.2169958.
23. ‘‘5Gsecurity:ForwardthinkingHuaweiwhitepaper,’’Huawei,Shenzhen, China, White Paper, 2015.
24. “Security for 5G Mobile Wireless Networks”Dongfeng Fang, Yi Qian , (Senior Member, IEEE), and Rose Qing yang hu,Digital Object Identifier 10.1109/ACCESS.2017.2779146.
25. [25]Cao, J., Li, H., Ma, M., Zhang, Y., Lai, C., 2012b. A simple and robust handover authentication between HeNB and eNB in LTE networks. Comput. Netw. 56 (8),2119–2131.http://dx.doi.org/10.1016/j.comnet.2012.02.012 .
26. Cao, J., Li, H., Ma, M., 2015. GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks. In: Proceedings of International Conference Communication, IEEE, pp. 3020–3025.http://dx.doi.org/10.1109/ICC. 2015.7248787.
27. Dake, Wang, Jianbo, Zheng, Yu, 2008. User authentication scheme based on selfcertified public-key for next generation wireless network. In: Proceedings of International Symposium on Biometrics Security and Technology, IEEE, pp. 1–8. http://dx.doi.org/10.1109/ISBAST.2008.4547638.
28. Mahmoud, M., Saputro, N., Akula, P., Akkaya, K., 2016. Privacy-preserving power injection over a hybrid AMI/LTE smart grid network. IEEE Internet Things.J.,1. http://dx.doi.org/10.1109/JIOT.2016.2593453.’
29. Katz, J., Lindell, A.Y., 2008. Aggregate Message Authentication Codes. In: Top. Cryptol. CT-RSA 2008, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 155–169. http:// dx.doi.org/10.1007/978-3-540-79263-5_10.
30. Bersani, F., Tschofenig, H, 2007. The EAP-PSK protocol: A pre-shared key extensible authentication protocol (EAP) method, RFC 4764.
31. Zhang, G., Fan, D., Zhang, Y., Li, X., Liu, X., 2015. A privacy preserving authentication scheme for roaming services in global mobility networks. Secur. Commun. Netw. 8 (16), 2850–2859. http://dx.doi.org/10.1002/sec.1209.
32. Dubrova, E., Naslund, M., Selander, G., 2015. CRC-based message authentication for 5G mobile technology. 2015 IEEE Trust., IEEE, 1186–1191. http://dx.doi.org/10.1109/ Trustcom.2015.503.
33. Ma, C.-G., Wang, D., Zhao, S.-D., 2014. Security flaws in two improved remote user authentication schemes using smart cards. Int. J. Commun. Syst. 27 (10), 2215–2227. http://dx.doi.org/10.1002/dac.2468.
34. Berkah I. Santoso, M. RienSuryatamaIdrus, IrwanPrasetyaGunawan”Designing Network Intrusion and Detection System using Signature-Based Method for Protecting OpenStack Private Cloud” 2016 6th International Annual Engineering Seminar (InAES),Year: 2016Page s: 61 – 66.
35. Abdullah H Almutairi, Dr. Nabih T Abdelmajeed,” Innovative Signature Based Intrusion Detection System Parallel Processing and Minimized Database” 2017 International Conference on the Frontiers and Advances in Data Science (FADS), 978-1-5386-3148-5/17/$31.00 © 2017 IEEE.

Authors Profile

Mr. Ravindra.S completed M.Tech in the year 2003 from NITK Surathkal and currently doing Ph.D under VTU in the field of Electronics and Communication Engineering. He has 16 years of rich experience in Academics.He has published many papers in National and International Journals. He holds lifetime ISTE membership. His research area includes Wireless Networking, Security in Mobile Communication.

Dr. Shankaraiah received his Ph.D. in the year of 2012 from IISc Bangalore and currently working as a Professor and Head in the Department of Electronics and Communication Engineering at JSS Science and Technology University (Formerly SJCE), Mysore. He has 23 years of rich experience in Academics. He has published more than 25 research articles in National and International Journals. His research area includes Wireless Networking, Hybrid wireless Networks, Context-Aware Computing, Ubiquitous Networks, Security in Mobile Communication, Privacy Issues in WSN.