ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 7, Oct 2022

Analysis of Privacy Preserving methods in 4G and 5G Cellular Networks

Dr. Poonam
ECE, MSIT
New Delhi, India
poonam.dahiya@msit.in

Dr Shaifali M. Arora
ECE, MSIT
New Delhi, India
shaifali04@msit.in

Dr Anshul Pareek
ECE, MSIT
New Delhi, India
er.anshulpareek@msit.in

***Abstract*—This paper intends to present a survey of privacy preserving methods that are available to provide data security in 4G and 5G mobile networks. A brief classification of threat models such as attacks on privacy, availability, privacy, and integrity has been provided. Then, based on the various categories of authentication and privacy saving methods the techniques are classified in categories like- handover authentication, deniable authentication, key agreement, three factor authentication, RFID authentication.**

Keywords—4G, 5G, security, authentication, cellular communication.

I. INTRODUCTION

The 5G mobile networks are superseding 4G around the world. The advancements in wireless communication and networking methods has converged 5G such that it is able to offer very high data rates, higher capacity, lower latency, and improvised security among other advantages. Telecommunication industry is targeting for a fully interconnected mobile society by merging 5G technology with IoT (Internet of Things). It is proposed to provide network services such as inter vehicular communication [1], smart electric grids [2], unmanned aerial vehicle [3], smart parking [4] etc. using this advanced technology. Fig. 1 demonstrates the services that will be enabled using 5G. Some leading telecommunication companies that are working on 5G technology are- NOKIA, ERICSSON with TELEFONICA & SOFTBANK, HUAWEI, VODAFONE, VERIZON COMMUNICATIONS, AT&T INC. across the world, and RELAINCE JIO, AIRTEL among others in India.

5G will be a blend of advanced wireless methods and IP based networks as provided by service provider companies that would offer high Quality of Service to the end user. This openness of mobile networks makes the devices more prone to various susceptibilities such as security while communicating, data privacy etc. [4]. Moreover, since it is IP based environment, the network may also suffer with the vulnerabilities related to IP. Hence, the security and privacy is an important aspect for the successful deployment of 5G technology.

This paper presents a comprehensive study of classification of attacks with authentication and privacy conserving techniques available for 4G and 5 G networks. These methods are categorized as- cryptographic methods, intrusion detection methods, and human factors.

II. ATTACKS IN 4G AND 5G NETWORKS

In this section various threats to 4G and 5G networks has been discussed. There are thirty-five identified attacks as shown in fig.2. broadly these attacks can be classified as attacks to privacy, attacks on integrity, attacks to availability and attacks to authentication. This classification has been made based upon the nature of the attack.

Z. Li et al (2013) proposed a method to detect and avoid replay attack wherein the illegal user pretends to be a legal user by logging the server by sending the messages a sent by valid user. The authors used hash function along with a timestamp. In 2015, Haddad et al proposed a solution to the issue of data packets replay by attacker or by external factors. The authors used a message in pairing that has been used as an authentication code. Cao et al in 2016 offered a method using Next hop chaining method to count values and by updating the value. They solved the issue of replaying the messages between the communication devices and the server via 3GPP network. Tian Liu et al (2021) [5] offered an authentication & key agreement protocol to overcome number de-synchronization issues. The authors used challenge response technique using random numbers to overcome replay attacks.

For the detection and prevention of the Denial of services attack Kumari et al [6] and Chaudhary et al [7] resolved the issues intended with the smart card by following the same approach of verifying the correctness of identity and its password. Liao and Hsiao [8] offered the solution to issue of jamming of the readers with blocker's tag by using elliptic curve cryptosystem method.

To detect and prevent forgery attacks [9-13] offered solutions using biometrics, CRC check, passwords for smart cards and some cryptographic approaches.

A. Attacks against Privacy

There are fourteen listed attacks in this category like parallel session, replay, MITM (Man in the middle), eavesdropping, collaborated, tracing, spoofing, privacy, stalking, cipher-text, plain-text, and disclosure. MITM is the most severe attack among all these attacks. Conti et al [14] described this attack as FBS (False Base Station Attack). This attack occurs when invalid third party tricks its BTS (Base

ISSN PRINT 2319 1775 Online 2320 7876

Research paper **© 2012 IJFANS. All Rights Reserved, UGC CARE Listed (Group -I) Journal Volume 11,Iss 7, Oct 2022**

Transceiver Station) as a real BTS of the network. Chen et al [15] proposed a solution to MITM attack by

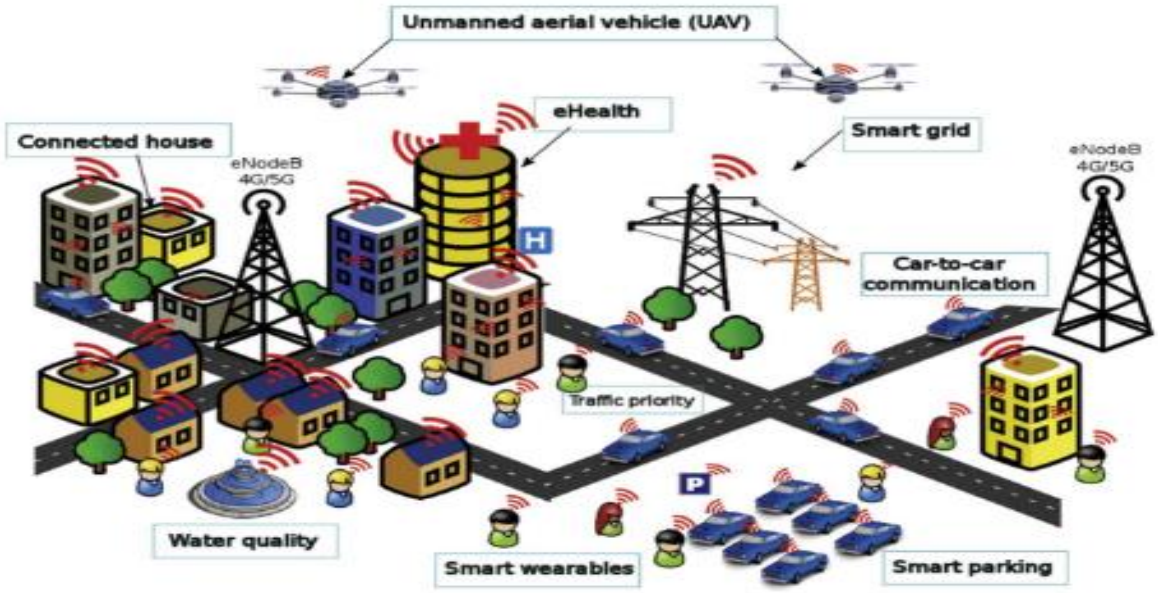

Fig.1. Services of 5G network.

using a temporary secret channel. This technique worked on minimizing the human interactions in the network. To identify MITM attack, Mayrhofer et al [16] offered a method using arbitrary supporting channel approach. Yao et al [17] introduced a highly secure authentication method known as GBS-AKA which can detect MITM attack by using timestamp and session key. This approach is applied during the authentication process. With MITM attack, the attackers can also impose other attacks like eavesdropping to intercept messages and keys.

B. Attacks on Integrity

This category of attacks includes the attacks that are intended to modify the data communicated between network and end user. Cloning, spam, message modification, insertion of message, tampering attacks lie in this category.

The cloning attack, as described by Hasan et al [18], is a man in the middle rouge rouge Base Transceiver Station having access of cross layer facts. To perform such an attack following steps are followed- first of all indirect sniffing of the uplink and downlink channels is done, in the second step 5G control signals are parsed and after getting the cross layer data attack vectors are created. For the detection of cloning attacks Dong et al [19] proposed a protocol named LSCD. This protocol offers protection against cloning by building witnesses and provides high probability of detection of attacks. Along with these methods hash functions such as SHA-1 and MD5 are also used by researchers for the detection of attacks by checking for a correct hash value.

C. Attacks on Availability

The motive behind availability attack is to make any service unavailable to the user. There are six attacks that lie in this category of attacks, namely, physical attack, First In First Out attack, skimming attack, redirection attack, and free riding attack. The issue of redirection attack has been addressed by Saxena et al [20]. This attack is very easy to impose if the attacker gets to know valid user's information. The attacker can increase its signal power or by implicating a BTS in the mobile network. MAC protocol has been used by the authors to deal with the attack. Li et al [21] offered a solution to the same problem by merging MAC and local area identifier.

D. Attacks against Authenticity

The attacks that disrupts bi directional authentication (client to server or server to client) are known as attacks on authentication in the mobile network. There are ten attacks, namely, password stealing, brute force, dictionary, password reuse, forgery, leak of verifier, stolen smart card, and collision attacks listed under this category.

The oPass (One-time password) approach has been adopted by Sun et al [22]. The authors prevented password reuse as well as password stealing problem at the same time. In this approach a new password is generated for every session of activity that

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 7, Oct 2022

gets expired as soon as the session gets over. The oPass approach can be adopted in 4G and 5G cellular networks.

III. PRIVACY PRESERVING METHODS

In this section, the countermeasures adopted by the privacy preserving methods for 4G and 5G networks has been presented. These methods can broadly be categorized into three-

1. Cryptographic Methods
2. Human Factors
3. Intrusion Detection Techniques

Fig.3 shows the classification of the methods used for privacy saving methods. Table 1 lists the methods used by the authors for privacy protection in 4G and 5G mobile networks.

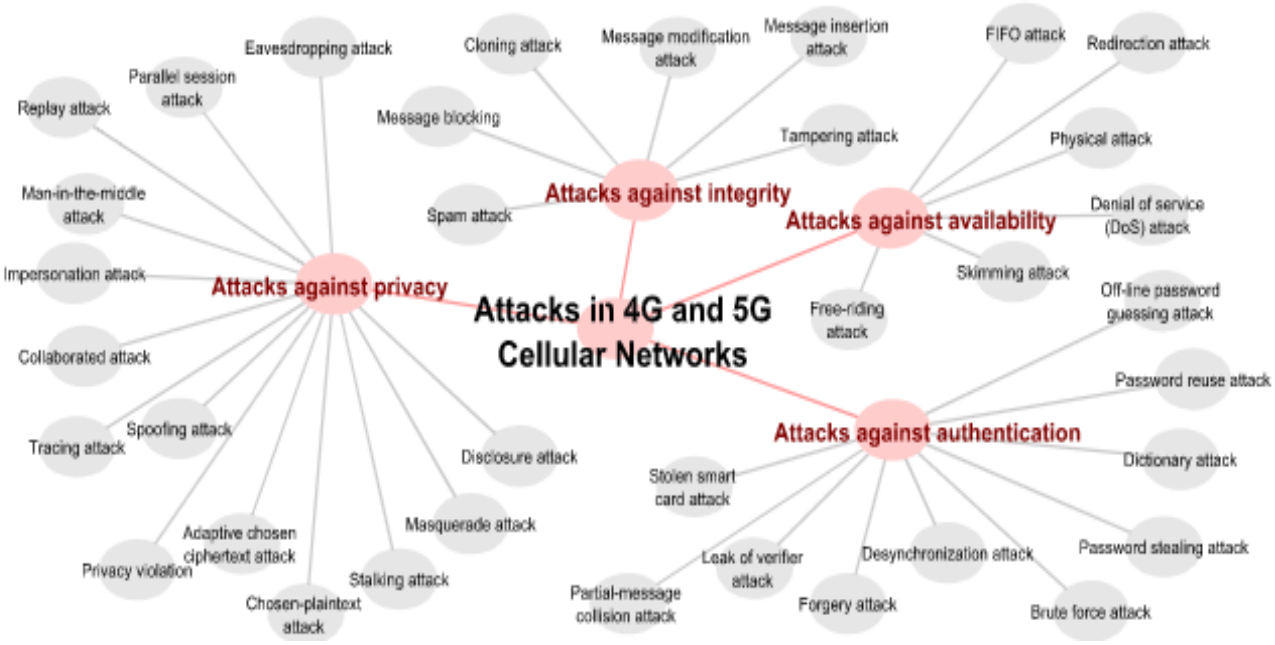

Fig. 2. Attacks in 4G & 5G network.

A. *Cryptographic Methods*

Cryptographic approach is the most widely used approach for authentication and privacy securing in 4G and 5G networks, that can further be classified as Public key, symmetric key, and without key cryptography as shown in fig 3.

The authors [23-25] used the public key cryptography method to identify actual base station or the actual access point. Zhu et al [23] combined blind signature method and Rabin's public key method. This method includes three algorithms namely- key generation, encryption, and decryption. There are two entities in blind signature method: 1. Signer, 2. Signature requester. This method involves very high computational cost and is needs more efforts. Conditional anonymity has been provided by Gisdasik et al [24] by using group signature technique. The authors developed their technique by using local revocation by the verifier. This method used RSA that are very long for many applications. This limitation has been addressed by Bonch et al [25] that used short group signatures.

The symmetric key method has been incorporated by Chen et al [26], Weng et al [27], and Saxena et al [28], that provided user confidentiality. AES has been used by Chen et al as the symmetric key for data privacy. Considering the fact that symmetric methods of encryption are faster than asymmetric methods Saxena et al offered a method based for IoT based LTE mobile networks comprising symmetric key cryptography method. In almost all methods hash key functions are used to gain data integrity of the encrypted data.

B. *Human factors*

To be sure about authentication, countermeasures for human factors has been proposed in the literature. The researchers have divide human factors into three categories; 1. Passwords and PIN number that anyone can know, 2. Passcodes, Tokens, RFID, and Token that one can have, 3. Identification of someone such as biometric traits, voice, and signature of a person.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11,Iss 7, Oct 2022

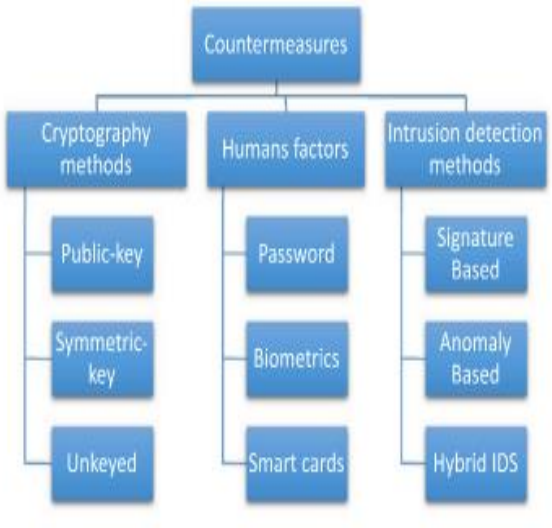

Fig. 3. Classification of the methods used for privacy saving methods.

The above listed factors can be either forgotten, stolen by someone to forge, shared, or lost.

C. Intrusion detection

The IDS known as intrusion detection scheme is the second level of privacy persevering. When the intruder is able to take over the entity in the network by surpassing every safety measure, the IDS must be able enough to identify the malicious attack and stop it further. Several methods have been proposed

in the literature to perform this task for the 4G and 5G mobile networks. BRPCA (the Bayesian robust principal component analysis) method has been adopted by Papadopoulos et al [29]. Kang and Kang [30] used Deep Neural Networks to detect if the attacker has entered the mobile network or not. This method provided very high accuracy rate and it is a real time system. Random packet inspection method for LTE mobile networks has been proposed by Sou and Lin [31].

IV. CONCLUSION

State of the art techniques for privacy preservation for 4G and 5G mobile networks has been provided in this study. Threat model and attacks against privacy of user has been discussed. In addition, a classification of the countermeasures has also been studied.

REFERENCES

[1] Sun, J., Zhang, C., Zhang, Y., & Fang, Y. (2018). An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Transactions on Parallel and Distributed Systems, 21(9), 1227-1239.

[2] Ferrag, M.A., Ahmim, A., (Eds.), 2017. Security Solutions and Applied Cryptography in Smart Grid Communications, Advances in Information Security, Privacy, and Ethics, IGI Global.

[3] Niu, Y., Gao, C., Li, Y., Su, L., Jin, D., & Vasilakos, A. V. (2019). Exploiting device-to-device communications in joint scheduling of access and backhaul for mmWave small cells. IEEE Journal on Selected Areas in Communications, 33(10), 2052-2069.

[4] A. Zhang, J. Chen, R. Q. Hu and Y. Qian, "SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2659-2672, April 2019.

[5] Gandotra, P., Jha, R.K., 2016. Device-to-device communication in cellular networks: a survey. J. Netw. Comput. Appl. 71, 99–117

[6] Kumari, S., Gupta, M.K., Khan, M.K., Li, X., 2014b. An improved timestamp-based password authentication scheme: comments, cryptanalysis, and improvement. Secur. Commun. Netw. 7 (11), 1921–1932.

[7] Chaudhry, S.A., Farash, M.S., Naqvi, H., Kumari, S., Khan, M.K., 2015. An enhanced privacy preserving remote user authentication scheme with provable security. Secur.Commun. Netw. 8 (18), 3782–3795.

[8] Liao, Y.-P., Hsiao, C.-M., 2014. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Netw. 18, 133–146

[9] Laya, A., Alonso, L., Alonso-Zarate, J., 2014. Is the random access channel of LTE and LTE-A suitable for M2M communications? A survey of alternatives. IEEE Commun.Surv. Tutor. 16 (1), 4–16

[10] Li, J., Wen, M., Zhang, T., 2016. Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. IEEE Internet Things J. 3 (3), 408–417

[11] Hoare, C.A.R., Communicating Sequential Processes. In: Orig. Concurr. Program., Springer New York, New York, NY, 1978, pp. 413–443

[12] Kulseng, L., Yu, Z., Wei, Y., Guan, Y., 2010. Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. In: Proceedings of IEEE INFOCOM, IEEE, pp. 1–5

[13] Liu, T., Wu, F., Li, X., & Chen, C. (2021). A new authentication and key agreement protocol for 5G wireless networks. Telecommunication Systems, 78(3), 317-329.

[14] Kormann, D.P., Rubin, A.D., 2000. Risks of the passport single signon protocol. Comput. Netw. 33 (1–6), 51–58.

[15] Krawczyk, H., Bellare, M., Canetti, R., 1997. RFC2104 - HMAC: Keyed-hashing for message authentication, Tech. rep..

[16] Ku, Y.-J., Lin, D.-Y., Lee, C.-F., Hsieh, P.-J., Wei, H.-Y., Chou, C.-T., Pang, A.-C., 2017.

[17] 5g radio access network design with the fog paradigm: confluence of communications and computing. IEEE Commun. Mag. 55 (4), 46–52.

[18] Kulseng, L., Yu, Z., Wei, Y., Guan, Y., 2010. Lightweight Mutual Authentication and Ownership Transfer for RFID Systems. In: Proceedings of IEEE INFOCOM, IEEE, pp. 1–5.

[19] Kumari, S., Khan, M.K., Li, X., 2014a. An improved remote user authentication scheme with key agreement. Comput. Electr. Eng. 40 (6), 1997–2012.

[20] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, V. Kumar, Security and Privacy in Fog Computing: Challenges, IEEE Access (2017)

[21] 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.

[22] Madueno, G.C., Nielsen, J.J., Kim, D.M., Pratas, N.K., Stefanovic, C., Popovski, P., 2016.

[23] Assessment of LTE wireless access for monitoring of energy distribution in the smart grid. IEEE J. Sel. Areas Commun. 34 (3), 675–688.

ISSN PRINT 2319 1775 Online 2320 7876

UGC CARE Listed (Group -I) Journal Volume 11,Iss 7, Oct 2022

[24] Mahmoud, M., Saputro, N., Akula, P., Akkaya, K., 2016. Privacy-preserving power injection over a hybrid AMI/LTE smart grid network. IEEE Internet Things

[25] Manolopoulos, V., Papadimitratos, P., Tao, S., Rusu, A., 2011. Securing smartphone based ITS. In: Proceedings of the 11th International Conference on ITS Telecommunication, IEEE, pp. 201–206.

[26] Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.-P., 2013. Game theory meets network security and privacy. ACM Comput. Surv. 45 (3), 1–39.

[27] Mayrhofer, R., Fub, Ion, I., 2013. UACAP: a unified auxiliary channel authentication protocol. IEEE Trans. Mob. Comput. 12 (4), 710–721..

[28] Mayrhofer, R., 2007. Towards an Open Source Toolkit for Ubiquitous Device Authentication. In: Proceedings of Fifth Annual IEEE International Conference on Pervasive Computer Communication Workshop, IEEE, pp. 247–254

[29] Mehaseb, M.A., Gadallah, Y., Elhamy, A., Elhennawy, H., 2016. Classification of LTE uplink scheduling techniques: an M2M perspective. IEEE Commun. Surv. Tutor. 18(2), 1310–1335.

[30] MIT Kerberos Distribution, 2017. URL ⟨https://web.mit.edu/kerberos/⟩.

[31] Sou, S.-I., Lin, C.-S., 2017. Random packet inspection scheme for network intrusion prevention in LTE core networks. IEEE Trans. Veh. Technol.