A CRITICAL REVIEW ON 5G NETWORKS

Dhruv Kumar, Assistant Professor, Department of Computer Science & Engineering, Galgotias University

ABSTRACT

New security needs and problems are created when the characteristics of 5G mobile wireless network systems move into the next generation. This article offers a deep examination of 5G wireless network system security, which was made possible thanks to a complete analysis. The introduction begins with a look at 5G wireless network details, such as their special needs and motives, followed by a study of 5G wireless security's overall concepts. With the consideration of new service needs and new use cases, prospective threats and security services are detailed in 5G wireless networks. For reference, 5G wireless security service features, such authentication, availability, data confidentiality, key management, and privacy, are provided below with their current and recent developments. This article addresses the novel security characteristics, including heterogeneous networks, device-to-device communications, enormous multiple-input multiple-output, software-defined networks, and the Internet of Things, that are applied to 5G. We offer a novel 5G wireless security architecture based on which identity management and flexible authentication are performed. To illustrate the architecture's capabilities, we discuss a handover method and a signalling load scheme. 5G wireless security is coming to a head and being explained.

KEYWORDS: 5G Network, WSN, IOT

INTRODUCTION

The next generation of wireless technology beyond existing 4G/IMT-Advanced Systems (or the 5th generation of wireless systems) is known as 5G. Not only does 5G cellular systems carry on the tradition of 4G networks, but it also provides several more services. As part of their 5G research and development efforts, phone manufacturers and carriers are shooting for a variety of additional capabilities, such as more capacity than the existing 4G standard, bigger numbers of Internet users, and D2D compatibility. To achieve low latency and reduced energy consumption, 5G cellular network planning likewise emphasises reduced latency and lower energy consumption. Many 5G wireless systems, which connect devices to end points in the field, can reach speeds of 1-10 Gbps, connect with 1 millisecond of latency, and provide 1,000 times more bandwidth per unit area than current systems. They can support a greater number of connected devices, can be reliable and support up to ten years of battery life for low power devices. As part of meeting the performance requirements, several technologies including HetNet, MIMO, mmWave, D2D communications, SDN, NFV, and networking slicing are used to develop 5G systems. 5G wireless standards is merely in the early stages of development. This depicts a general design of 5G wireless systems. The wide availability of 5G wireless technologies allows new uses in both voice and data transmission, as well as countless gadgets and applications for connecting society at large. Vehicle-to-vehicle (V2V) communications and vehicle-to-

infrastructure (V2I) communications are all outlined as 5G use cases. However, it is conceivable but challenging to include security features such as authentication, integrity, and secrecy due to the broadcast nature and restricted bandwidth of wireless communications. Network security threats such assaults, vulnerabilities, and privacy problems exist in the present cellular networks, especially with regard to media access control (MAC) and physical (PHY) layers. Using established security architectures with user identity management, mutual authentication between the network and user equipment (UE), secure communication channels, and so on, we've implemented security features for voice and data communications. In legacy cellular networks, Long Term Evolution (LTE), providing users and network operators with a high degree of security and trustworthiness is the goal. Mutual authentication is also performed between a mobile unit and a base station. In addition, key management ensures security of the network's access and mobility. Studies are also being done on security issues connected to the use of LTE technology. However, in order to support new use cases and the new networking paradigms, new security criteria are required. For overall 5G advanced characteristics such as reduced latency and great energy efficiency (EE), security methods are required.

SECURITY ISSUE IN 5G

In order to overcome these concerns, security must be included into the system's design from the outset. To meet varied use cases and trust models, security solutions must be adaptable. Figure 3 illustrates the different trust models supported by the legacy cellular networks and 5G wireless networks. 5G-wireless networks need authentications for service parties on both the serving and home networks, as well as those in the service area. The security requirements for vertical industries use cases may vary greatly across various applications. Additionally, mobile devices have an acute battery constraint and hence demand lightweight security methods. High-speed services, on the other hand, need effective security methods with minimal latency. As a result, providing more freedom for 5G security solutions is another important demand. Because there are several device kinds and a large number of them, authentication management in 5G is more complicated. Each application may use a different authentication strategy, depending on the requirements. Study shows that network provider authentication can be implemented, or service provider authentication can be implemented, or both. Additionally, 5G security requires flexibility, but security automation is critical too. This management approach is automated, comprehensive, and intelligent, all at once. More personal information is utilised in a variety of applications, such surveillance using 5G wireless networks, and this has lead to an increase in privacy issues. Even more importantly, the range of services provided in 5G will be closer than previously. An example of this is a large network disruption which allows for termination of the fixed telephone connection, internet connection, and TV service simultaneously. To maintain the security of the 5G system, security automation is required.

Passive attacks and active attacks are two different forms of security assaults. A passive attack is conducted by an attacker in order to learn or make use of information that is already present on the legitimate user's computer, but the attacker does not seek to attack the network itself. Passive surveillance is made up of two sub- categories, namely, surreptitious surveillance and traffic analysis. Passive assaults attempt to invade the

privacy of users and their personal data. The main difference between passive attacks and active attacks is that the former is less likely to alter or stop lawful communications. MITM, replay attack, denial of service (DoS) assault, and distributed denial of service (DDoS) assault are typical of an active assault.

TRAFFIC ANALYSIS

Spying is a technique that is often employed by someone who is unaware to intercept the communications of others. While active wiretapping is an assault on communication, passive eavesdropping is ineffective since communication does not change with passive eavesdropping, as demonstrated. Eavesdropping is difficult to see since it is a passive process. the use of encryption to radio link transmissions is widely used to combat eavesdropping Due to encryption, the eavesdropper will not be able to intercept the signal the receiver has received. Another kind of passive assault is a traffic analysis, which is performed without the sender's knowledge. Traffic analysis intercepts the position and identity of communication parties, such as parties using a communication network, by observing the traffic on the received signal. In other words, even encrypted communication can be cracked, even if traffic analysis may be utilised to expose the communication patterns of the parties. Even when used to genuine communications, the traffic analysis attack is ineffective.

CONCLUSION

On top of providing a number of new features, 5G wireless networks provide new services, such smart grid, smart home, vehicular networks, and m-health networks, as well. User terminals, the home, and the serving network are all elements of the trust model in the legacy cellular networks. The trust models varies depending on the use cases in which they are used, which may include new participants in 5G wireless networks. Authentication is required across numerous actors with varying degrees of confidence.

The work that has been done in this area includes studies on trust models that focus on different scenarios. To allow safe data transfer across 5G wireless networks for vehicle communications, Eiza et al. developed a system model. All state and local government vehicles, together with the Department of Motor Vehicles, are part of the proposed system model. It is more sophisticated than in the traditional cellular networks since the trust mechanism is set up differently. New trust models are required to enhance the overall performance of security services such as IoT user cases authentication in the presence of an increase in the number of devices equipped with 5G wireless network technology. This fusion centre, however, lacks a trust model between the devices and itself.

REFERENCES

1. Bashir, U., Jha, K. R., Mishra, G., Singh, G., & Sharma, S. K. (2017). Octahedron-Shaped Linearly Polarized Antenna for Multistandard Services Including RFID and IoT. *IEEE Transactions on Antennas and Propagation*, *65*(7), 3364–3373. https://doi.org/10.1109/TAP.2017.2705097
2. Fan, K., Gong, Y., Du, Z., Li, H., & Yang, Y. (2015). RFID secure application revocation for IoT in 5G. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 175–181. https://doi.org/10.1109/Trustcom.2015.372

3. Fan, K., Gong, Y., Liang, C., Li, H., & Yang, Y. (2016). Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. *Security and Communication Networks*, *9*(16), 3095–3104. https://doi.org/10.1002/sec.1314
4. Hester, J. G. D., & Tentzeris, M. M. (2017). A Mm-wave ultra-long-range energy-autonomous printed RFID-enabled van-atta wireless sensor: At the crossroads of 5G and IoT. *IEEE MTT-S International Microwave Symposium Digest*, 1557–1560. https://doi.org/10.1109/MWSYM.2017.8058927
5. Kumar, A., & Kaur, R. (2016). PSO-Based NBI resistant asynchronous MC-CDMA multiuser detector. *International Journal of Intelligent Systems and Applications*, *8*(10), 60–67. https://doi.org/10.5815/ijisa.2016.10.07
6. Kwan, J. C., & Fapojuwo, A. O. (2016). Measurement and analysis of available ambient radio frequency energy for wireless energy harvesting. *IEEE Vehicular Technology Conference*, *0*. https://doi.org/10.1109/VTCFall.2016.7881084
7. Narottama, B., Fahmi, A., & Syihabuddin, B. (2016). Impact of number of devices and data rate variation in clustering method on device-to-device communication. *APWiMob 2015 - IEEE Asia Pacific Conference on Wireless and Mobile*, 233–238. https://doi.org/10.1109/APWiMob.2015.7374966
8. Fortino, G., & Trunfio, P. (2014). Internet of things based on smart objects: Technology, middleware and applications. In *Internet of Things Based on Smart Objects: Technology, Middleware and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-319-00491-4
9. Geller, J., Grudzinskas Jr., A. J., McDermeit, M., Fisher, W. H., & Lawlor, T. (1998). The efficacy of involuntary outpatient treatment in Massachusetts. *Administration and Policy in Mental Health*, *25*(3), 271–285. https://doi.org/10.1023/A:1022239322212
10. Gope, P., & Hwang, T. (2015). Untraceable Sensor Movement in Distributed IoT Infrastructure. *IEEE Sensors Journal*, *15*(9), 5340–5348. https://doi.org/10.1109/JSEN.2015.2441113
11. Gupta, P., Agrawal, D., Chhabra, J., & Dhir, P. K. (2016). IoT based smart healthcare kit. *2016 International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings*, 237–242. https://doi.org/10.1109/ICCTICT.2016.7514585
12. Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of empowered IoT users. *Proceedings - 2016 IEEE 1st International Conference on Internet-of-Things Design and Implementation, IoTDI 2016*, 13–24. https://doi.org/10.1109/IoTDI.2015.39
13. Jalali, R., El-Khatib, K., & McGregor, C. (2015). Smart city architecture for community level services through the internet of things. *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, 108–113. https://doi.org/10.1109/ICIN.2015.7073815

14. Li, C., Hu, X., & Zhang, L. (2017). The IoT-based heart disease monitoring system for pervasive healthcare service. In H. R. J. Z.-M. C. T. C. F. C. J. L. C. J. L. C. Toro C. Hicks Y. (Ed.), *Procedia Computer Science* (Vol. 112, pp. 2328–2334). Elsevier B.V. https://doi.org/10.1016/j.procs.2017.08.265

15. Colella, R., Catarinucci, L., & Tarricone, L. (2016). Improved RFID tag characterization system: Use case in the IoT arena. *2016 IEEE International Conference on RFID Technology and Applications, RFID-TA 2016*, 172–176. https://doi.org/10.1109/RFID-TA.2016.7750760

16. Fan, C., Wen, Z., Wang, F., & Wu, Y. (2012). A middleware of internet of things(iot) based on Zigbee and RFID. *IET Conference Publications*, *2011*(586 CP), 732–736. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84864939256&partnerID=40&md5=48d6df2c9e0dd0aebcb7932fef789e55

17. Freidl, P. F., Gadringer, M. E., Amschl, D., & Bcosch, W. (2017). mm-Wave RFID for IoT applications. In P. T. (Ed.), *Proceedings of the 2017 International Workshop on Integrated Nonlinear Microwave and Millimetre-Wave Circuits, INMMiC 2017*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/INMMIC.2017.7927322

18. Hester, J. G. D., & Tentzeris, M. M. (2017). A Mm-wave ultra-long-range energy-autonomous printed RFID-enabled van-atta wireless sensor: At the crossroads of 5G and IoT. *IEEE MTT-S International Microwave Symposium Digest*, 1557–1560. https://doi.org/10.1109/MWSYM.2017.8058927

19. Kaur, M., Singh, U., & Singh, D. (2015). Design of FIR Filter Using Biogeography Based Optimization. *Proceedings - 2015 2nd IEEE International Conference on Advances in Computing and Communication Engineering, ICACCE 2015*, 312–317. https://doi.org/10.1109/ICACCE.2015.136

20. Kubo. (2015). The research of IoT based on RFID technology. *Proceedings - 7th International Conference on Intelligent Computation Technology and Automation, ICICTA 2014*, 832–835. https://doi.org/10.1109/ICICTA.2014.199

21. Mota, R. P. B., & Batista, D. M. (2013). A RFID QoS mechanism for IoT tracking applications. *2013 International Symposium on Wireless and Pervasive Computing, ISWPC 2013*. https://doi.org/10.1109/ISWPC.2013.6707429

22. Mainetti, L., Patrono, L., & Vilei, A. (2011). Evolution of wireless sensor networks towards the Internet of Things: A survey. *2011 International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2011*, 16–21. https://www.scopus.com/inward/record.uri?eid=2-s2.0-81455142290&partnerID=40&md5=8089ed723b1c1056c9a6ae8fa767fa4f

23. Nain, G., Fouquet, F., Morin, B., Barais, O., & Jézéquel, J.-M. (2010). Integrating IoT and IoS with a component-based approach. *Proceedings - 36th EUROMICRO Conference on Software Engineering and Advanced Applications, SEAA 2010*, 191–198. https://doi.org/10.1109/SEAA.2010.50

24. Pu, C. (2011). A world of opportunities: CPS, IOT, and beyond. *DEBS'11 - Proceedings of the 5th*

ACM International Conference on Distributed Event-Based Systems, 229. https://doi.org/10.1145/2002259.2002290

25. Rao, B. B. P., Saluia, P., Sharma, N., Mittal, A., & Sharma, S. V. (2012). Cloud computing for Internet of Things & sensing based applications. *Proceedings of the International Conference on Sensing Technology, ICST*, 374–380. https://doi.org/10.1109/ICSensT.2012.6461705