ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering
(IJERCSE)
Vol 5, Issue 1, January 2018

Review on Security for 5G Network

[1] Shagufta Khan
[1] Department Of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] shagufta.khan@Galgotiasuniversity.edu.in

Abstract:The advanced features of 5 G mobile wireless network networks bring new criteria and challenges for security. Compared to traditional cellular networks, this paper provides a comprehensive survey on 5G wireless network systems reliability. The paper begins with a study of the particularities of 5G wireless networks as well as the new requirements and reasons of 5G wireless securities. The potential attacks and security services in 5G wireless networks are then summarized with the consideration of new service requirements and new use cases. The recent development and existing 5G wireless security schemes are presented based on the appropriate security services including authentication, availability, confidentiality of data, key management and privacy The paper also addresses the new security innovations that include various technologies introduced to 5G such as heterogeneous networks, device-to-device networking, large multiple-input multiple-output, software-defined networks, and the Internet of Things Motivated by these research and development activities on security, we are proposing a new 5G wireless security architecture, based on which identity management analysis and flexible authentication are offered. As a case study, we are exploring a handover procedure and a signaling load scheme to show the advantage of the security architecture that is proposed. The challenges of 5G wireless security and its future directions are finally summarized.

Keywords: Authentication, 5G Wireless network, Security architecture, Attacks, Mobile communication.

INTRODUCTION

Today, as anticipated, the trend towards an omnipresent computing environment has led to mobile networks characterized by continuously increasing demand for high data rates and mobility. The most popular technology that has emerged to address these issues is 5G mobile, and the possibility of it being deployed by 2020 and beyond has put a lot of effort into developing it in the last few years [1]. 5G Communications seek to provide the bandwidth of big data; infinite networking capability and extensive signal coverage to support a rich range of high-quality customized services to end users. To this end, 5 G networks will use innovative new approaches to combine several different advanced technologies. This incorporation, however, would bring enormous security challenges to potential 5G mobile networks.

In particular, a wide range of security issues is likely to be posed in 5G mobile networks due to a number of factors, including: (i) the 5G system's IP-based open architecture, (ii) the complexity of the 5G system's underlying access network technologies(iii) a proliferation of highly mobile and complex interconnected interacting devices, (iv) the variety of device types with respect to their computational, battery power and memory storage capabilities; (v) open computer operating systems, and (vi) the possibility that the interconnected devices would usually be run by non-professional security users. Accordingly, 5G communications systems will need to address more and more threats than current mobile communications systems.

Although the upcoming 5G communications systems will be the target of many known and unknown security threats, it is not clear which threats will be the most serious and which network elements will most often be targeted. Since such information is of utmost importance for providing guidance in ensuring security for mobile communications systems[2] of the next decade, the goal of this chapter is to identify potential security issues and challenges for the emerging 5G communications systems. This paper is structured as follows after the introduction. They give an overview of a potential 5G communications system architecture based on the current work related to 5G systems in the first section; the next segment provides representative examples of potential threats and attacks on the main components of the new 5G networks to shed light on their potential security problems and challenges. In addition, literature-derived mitigation techniques are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

discussed for example attacks; finally, this chapter is concluded in the last section.

OVERVIEW OF 5G COMMUNICATIONS SYSTEM ARCHITECTURE

The adoption of a dense heterogeneous architecture in 5G communications, comprising macro-cells and small cells. It is one of the most promising low-cost solutions enabling 5G networks to meet the capacity growth needs of the industry and provide a consistent end-user connectivity experience [3]. Based on most recent literature they consider that a potential 5G macro-cell-scale communications architecture as shown in figure 1 will include a base station (BS), equipped with large antenna arrays, as well as additional large BS antenna arrays geographically distributed across the macro-cell network [4].

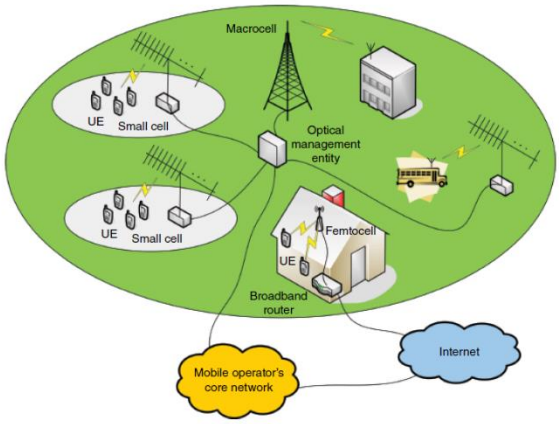


Fig.1Typical 5G Communications Systems Architecture

The distributed large antenna arrays will play the role of small-cell access points that support multiple Radio Access Network (RAN) protocols for a wide range of underlying access network (2G/3G/4G) technologies [5]. In addition, mobile users work with each other in the outdoor environment to shape virtual large antenna arrays. Together with the BS' distributed large antenna arrays (i.e. small-cell access points), the virtual large antenna arrays can create virtual, massive MIMO (Multiple-Input Multiple-Output) links in the small cells [6]. The access points for the small cells depend on robust backhaul communication over optical fibers.

SECURITY ISSUES AND CHALLENGES IN 5G COMMUNICATIONS SYSTEMS

The consumer infrastructure, access networks, the central network of mobile operators and the external IP networks will be the most enticing targets for potential attackers in emerging 5 G communications systems to help understand the future security issues and challenges affecting these components of the 5G system, we present representative examples of potential threats and specific attacks for these components. To derive such examples, they are exploring threats and attacks on legacy mobile systems (i.e. 2G/3G/4G) that could affect upcoming 5G communications systems by exploiting specific features of this new communication platform. For example attacks, we also discuss potential literature-derived mitigation techniques to provide a roadmap for more enhanced countermeasures to be deployed.

1. User Equipment:

The widespread adoption of open operating systems and the fact that the future EU will support a wide range of connectivity options (e.g. 2G/3G/4G, IEEE 802.11, Bluetooth) are factors that make the future EU a top cybercrime target. User Equipment (UE), such as strong smartphones and tablets, will become a very significant part of our daily lives in the 5G communications era. Such equipment will provide a wide range of attractive features to enable end users to access a variety of personalized services of high quality. However, the expected increasing popularity of the future EU, combined with the increased capacity of 5G networks for data transmission The widespread adoption of open operating systems and the fact that the future EU will support a wide range of connectivity options (e.g. 2G/3G/4G, IEEE 802.11, Bluetooth) are factors that make the future EU a top cybercrime targets. In addition to the conventional Denial of Service (DoS)-based SMS / MMS attacks, the potential UE will also be exposed to more advanced attacks from mobile malware (e.g. worms, viruses, trojans) targeting both the UE and the 5G cellular network. The open operating systems will enable end users to install applications on their devices, not only from trusted sources, but also from untrusted sources (i.e. markets of third parties). So the mobile malware, It will be included in applications that look like harmless apps (e.g. games, utilities), and will be downloaded and installed on mobile end-user devices that expose them to many attacks. Mobile malware can be designed to allow attackers to access the personal data stored on the device, or to launch

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

attacks (e.g. DoS attacks) on other organizations, such as other UE, The mobile access networks, the core network of mobile operators and other external networks connected to the core mobile network. Consequently, infected potential mobile devices would pose a threat not only to their users but also to the entire 5 G mobile network that supports them.

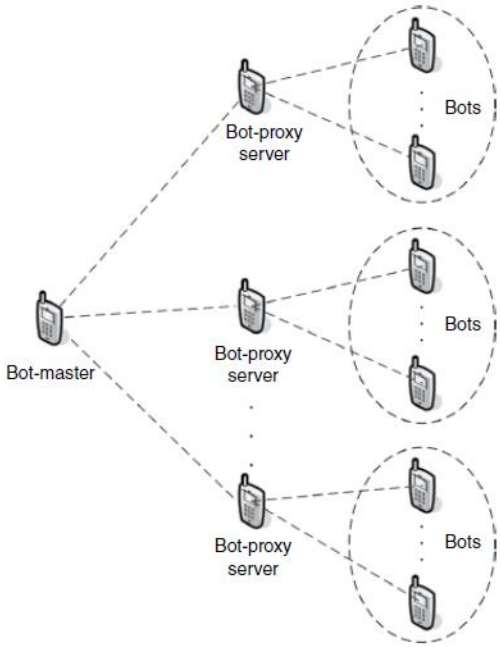
1.1 Mobile Malware Attacks Targeting UE:

As the future UE in the 5G era will be a personal device that stores everything from phone contacts to banking information, and is carried by the end user almost everywhere, it will function as a single portal to the digital identity and activities of the end user As the future UE in the 5G era will be a personal device that holds everything from phone contacts to banking information, and is carried virtually everywhere by the end user, it will serve as a single portal for the end user's digital identity[7] and activities.. The malicious software gains unauthorized access to the stored information of the end user gathers it and transmits it to the malware owner through all communication channels of the EU.

Nevertheless, mobile botnets can also perform the above attacks to hit several mobile end-users simultaneously and in an automated manner. Therefore, it is expected that mobile botnets will be a major means for attackers to gain financial benefits in the 5G period on a greater scale.

1.2 5G Mobile Botnets:

Mobile botnetsare expected to be widely used by attackers in the 5G communications environment, as future mobile devices are ideally suited for remote controlled machines due to their specific features5G mobile devices in particular would support various connectivity options and increased uplink bandwidth, and will tend to always be turned on and connected to the Internet [8]. Future attackers will thus be able to deploy mobile botnets in many effective ways for 5G communications networks.Unlike mobile botnets in legacy mobile networks, potential mobile botnets for 5G networks will be networks of compromised mobile devices operated by malicious actors commonly known as bot-masters. For example, a centralized 5G mobile botnet, where the attacker controls the compromised mobile devices through central Command and Control (C&C) servers, is illustrated in figure 2.



.

Fig.2Centralized 5G Mobile Botnet

2. Access Networks:

Service networks are supposed to be extremely heterogeneous and diverse in 5G communications, including several different radio service systems (e.g. 2G/3G/4 G) and other innovative connectivity schemes such as femtocells[9]. So that the quality of service is guaranteed. For example, the EU should be able to establish a link over 2G or 3G networks, in the absence of 4G network coverage. The fact that 5G mobile services will support several different access networks, however, allows them to inherit all the security issues they must support from the underlying access networks.Improved security measures should be put in place during the transition from 4G communications to 5G communications to combat emerging security threats on 5G access networks. Potential security risks to potential 5G access networks should be identified first to address this problem. Therefore, we concentrate on actual attacks on current 4 G access networks and HeNB femtocells in this segment, which could also be potential attacks on 5 G access networks.

3. Mobile Operator's Core Network:

Because of their open architecture based on an IP, 5G mobile systems will be vulnerable to common Internet IP attacks. DoS attacks, which today represent a major threat on the Internet, The new 5G communications systems targeting companies on the core network of the mobile operator will be available. Nevertheless, the main network of the 5G mobile operator may also be impacted by DDoS attacks targeting outside organizations while passing their malicious traffic over it.

3.1 DDoS Attacks Targeting the Mobile Operator's Core Network:

DDoS attacks[10] will be very serious incidents impacting the functionality of the potential targeted 5 G core mobile network. Considering that millions of users will be using 5G mobile networks, the effects of DoS and DDoS attacks on the core network will be serious. A botnet can launch DDoS attacks in the communications environment of 5 G, including a large number of infected mobile devices. Two representative DDoS attacks against the core network of a 4 G mobile operator are featured in this subsection. Also, these two examples of attacks can be extended to the core 5G network.

- Signal Amplification
- HSS Saturation

3.2 DDoS Attacks Targeting External Entities over a Mobile Operator's Core Network:

The new 5G mobile networks may also act as a conduit for DDoS attacks on targets in other external networks (e.g. business networks) linked to the mobile core network in future. In this case, a mobile device botnet can be used to produce a large volume of traffic and to transmit it over the mobile core network to the victim, located within the networks of the external network. Although the core network itself will not be the object of these attacks, the fact that they inject massive traffic loads into the core network will affect its performance. The recent Internet-based DDoS attacks on Spamhaus have shown how the high volume of attack traffic can affect the availability of the underlying communication network used to transmit it to the particular target.

4. External IP Networks:

External IP networks can also be the object of DDoS attacks on 5G communications systems, where mobile botnets produce a large volume of traffic and send it over the mobile core network to the target. Furthermore, external IP networks, such as enterprise networks, can be a soft target to be exploited by malware through accessing infected mobile devices.

CONCLUSION

5G wireless networks are expected to deliver improved technology allowing numerous new applications. In this analysis, they provided representative examples of potential attacks on the main components of the forthcoming 5G communications systems to elucidate the future security problems and threats that are to be anticipated in the 5G period. They have based in particular on examples of potential attacks on the following components of the 5G system: the UE, access networks, core networks of mobile operators and external IP networks. To extract these examples, we analyzed threats and attacks against legacy 4G networks as a starting point and extended them to 5G communications systems of the next generation by taking into account their specific characteristics. Finally, we addressed possible mitigation strategies extracted from the literature for these cases, as our goal is to provide a roadmap for the implementation of more enhanced countermeasures to tackle the potential security concerns of the forthcoming 5G communications systems properly.

REFERENCES

[1] J. G. Andrews *et al.*, "What will 5G be?," *IEEE J. Sel. Areas Commun.*, 2014, doi: 10.1109/JSAC.2014.2328098.

[2] W. Xiang, K. Zheng, and X. S. Shen, *5G mobile communications*. 2016.

[3] R. Scott, "Base station," *IHS Jane's Def. Wkly.*, 2015, doi: 10.1007/978-3-642-41714-6_20809.

[4] J. Hoydis, C. Hoek, T. Wild, and S. Ten Brink, "Channel measurements for large antenna arrays," in *Proceedings of the International Symposium on Wireless Communication Systems*, 2012, doi: 10.1109/ISWCS.2012.6328480.

[5] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access*. 2015, doi: 10.1109/ACCESS.2015.2461602.

[6] D. Gesbert, S. Hanly, H. Huang, S. Shamai Shitz, O. Simeone, and W. Yu, "Multi-cell MIMO cooperative networks: A new look at interference," *IEEE J. Sel. Areas Commun.*, 2010,

doi: 10.1109/JSAC.2010.101202.

[7] J. L. Fenton *et al.*, "Digital Identity Guidelines," *NIST Spec. Publ. 800-63B*, 2017, doi: 10.6028/NIST.SP.800-63b.

[8] C. Xiang, F. Binxing, Y. Lihua, L. Xiaoyi, and Z. Tianning, "AndBot: Towards advanced mobile botnets," in *LEET 2011 - 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats: Botnets, spyware, Worms, and More*, 2011.

[9] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. C. Reed, "Femtocells: Past, present, and future," *IEEE Journal on Selected Areas in Communications*. 2012, doi: 10.1109/JSAC.2012.120401.

[10] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, 2013, doi: 10.1109/SURV.2013.031413.00127.

[11] Usha Yadav , Gagandeep Singh Narula, Neelam Duhan , Vishal Jain , B. K. Murthy, "Development and Visualization of Domain Specific Ontology using Protege ",Indian Journal of Science and Technology, Vol. 9, No. 16, April, 2016, page no. 1-7 having ISSN No. 0974-6846.

[12] Usha Yadav, B K Murthy, Gagandeep Singh Narula, Neelam Duhan and Vishal Jain, "EasyOnto: A Collaborative Semi Formal Ontology Development Platform", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under Nature Inspired Computing, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6746-4 page no. 1 to 11.

[13] Usha Yadav, Gagandeep Singh Narula, Neelam Duhan and Vishal Jain, "A Novel Approach for Precise Search Results Retrieval based on Semantic Web Technologies", 10th INDIACom; INDIACom-2016, 3rd 2016 International Conference on "Computing for Sustainable Global Development", 16th – 18th March, 2016 having ISBN No. 978-9-3805-4421-2/, page no. 1357 to 1362.

[14] Balamurugan S, Visalakshi P, "Hybrid Firefly Algorithm Harmony Search for Feature Selection with BCNF for Multiple Subtables and EM-GMM for Top Down Initial Partitioning", Asian Journal of Research in Social Sciences and Humanities Year : 2016, Volume : 6, Issue : 8, 2016

[15] Balamurugan S, Visalakshi P, "Privacy-Preserving Data Mining of Query Logs with Multiple Log Subtables in Conditional Functional Dependencies", Asian Journal of Research in Social Sciences and Humanities Year : 2016, Volume : 6, Issue : 8, 2016

[16] Balamurugan S, Visalakshi P, "Boyce-Codd Normal Form Based Privacy Preserving Multiple Subtables with Conditional Functional Dependencies", Asian Journal of Information Technology Vol 15, Issue : 12, 2016