Asia-Pacific J. Mgmt. Tech. Volume 1(2) 08 - 12
https://doi.org/10.46977/apjmt.2020v01i02.002

AJMT

Asia-Pacific Journal of Management and Technology

Online ISSN: 2652-6840

journal homepage www.ajmt.org

ReviewArticle

A Review on Future Security Challenges in 5G

Harish Muthuveeran Shanmugam*; Supraja Srinivasan

Lecturer, Department of Electrical and Electronics, Faculty of Engineering and Built Environment, Lincoln University College, Malaysia.

Correspondence E-mail:harish@lincoln.edu.my; supraja@lincoln.edu.my*

Abstract

The 5th Generation Mobile Technology will provide broadband internet access anywhere enabling users to connect with multiple devices on the go with Internet of Things (IoT). Technological enablers such as fog and cloud computing with Software defined Networking and Network function Virtualization. With the evolution from 4G to 5G there are many security challenges to be investigated for growing demands of user privacy. In this paper we provide an overview of different cryptographic attacks that can take place inside a 5G mobile network. Furthermore, we present the countermeasures for all the possible attacks and analyze future security challenges.

Keywords: *Security, 5G mobile Technology, Botnet.*

Introduction

The introduction of 5G mobile communication standard (test version) in most of the well-developed economies of the world, the evolution from 4G to 5G will be the most powerful workhorse for the Internet of things which will be the basis for smart city development especially for developing nations like India. The replacement of new networking technologies viz software defined network (SDN) and network function virtualization (NFV) will be the main backbone for 5G networks for faster access and reducing the latency compared to 4G networks. (Ahmad *et al,* 2017). Security aspects of 5G networks are to be well researched before the commercial deployment of the new mobile standard. As the 5G systems are mainly service-oriented, the analysis of threats in and outside the 5G networks are to be well analyzed in-terms of both passive and active cryptographic attacks

All the mobile networks from 3G to 4G will have the following security features in common as follows:

i) Secure-software management of SIM card (USIM)
ii) Mutual authentication between BTS and UE
iii) Communication links between different UE

All the above stated security features will not be sufficient for vertical service industries which may employ internet of things (IoT), as the individual networking elements will be based on cloud computing infrastructure. Privacy is an important security issue in 5G networks, that will be the most vital security concern to be addressed (5G PPP), (Huawei, 2016). Figure 1 shows the evolution secured trust model from 4G to 5G.

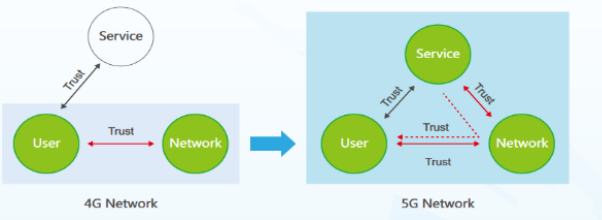

Figure 1: 4G to 5G Trust Model

Traditional mobile communication networks will provide authentication between network and end user. In the 4G standard the authentication between the user and the services are not provided. In 5G standard we are going to provide additional security element between the user-service-network (Huawei, 2019). There are a huge number of IoT devices that are not maintained by human beings, this result in new security challenges to be encountered and solved in the future IoT era. Therefore, we need a more secure 5G infrastructure which may support the development of cryptographically enhanced new IoT devices.

The paper organization is as follows: Part I describes the various security threats in 5G networks; Part II investigates the possible counter-measures, the conclusion and future work which should be implemented in real-world applications to have more secure communications in 5G related mobile networks.

Review of Literature:

I. Cryptographic Attacks in 5g:

While comparing with 4G, 5G communication networks will face more security attacks as it will be connected to outdoors involving IoT devices. There are many attacks that can be done in and out the 5G networks both active and passive nature. Existing security mechanisms available 4G are slow to defend and the cost of security infrastructure deployed are very high.

This section mainly focused on the possible cryptographic attacks in 5G networks.

The most suitable targets for mobile communication intruders in 5G networks will be User Equipment, network access, service-provider core network and IP networks that are externally available.

A. Attack on User Equipment

User equipment's can be 5G deployed smart-phones and tablets. They may provide high end new services to mobile users, so UE will be very prone to attackers. In the 2G, 3G and 4G mobile communication standard the traditional attacks were based on SMS and MMS based DOS attacks. In future 5G networks will be more vulnerable to attacks based on Trojan, worms and malware were both the User equipment and 5G core network services will be significantly affected. The open operating systems like the android and the iOS will serve the mobile users in downloading apps and games from both trusted and third-party. The mobile-malware thus installed in the User equipment Consume all the Central Processing Unit operation cycles in the mobile system on chip which may result in large power consumption and cause the depletion of battery power charge in the user equipment. Artificial intelligence also paves the way for the creation of mobile botnet which can be used for attacking many mobile users in parallel fashion (Rodriguez, 2015).

B. *Attacks using 5G mobile Botnet*

The compromised mobile users will be controlled by the centralized Command and Control server; it is one among the bot-proxy servers possessed by an attacker. The bot-master can use SMS services to distribute their attacking commands to other mobile users in the network which will initiate the DDoS attack inside the 5G network. Figure 2 shows the pictorial description of mobile-botnet attack and centralized bot-net infrastructure (Mantas *et al*, 2015)

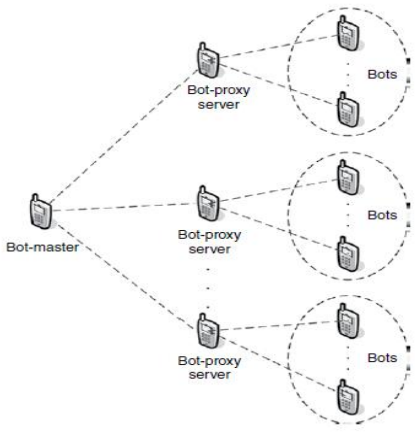

Figure 2: Centralized Bot-net Infrastructure

C. *Attacks on 5G access networks*

The 5G mobile communication standard will support variety of access networks from 2G to LTE (Long term Evolution). In the absence of 5G network coverage, it should seamlessly support the other access technologies to maintain Quality of Service (QoS). The attacks on 4G networks will be performed inside a 5G infrastructure in the initial stage.

Mobile Equipment location tracking by attackers is one of the major attacks inside a 5G network. The attackers use two techniques to identify the location of the mobile equipment. They are the cell radio network temporary identifier (C-RNTI) and packet sequence numbers (Horn *et al*, 2015).

The main work of C-RNTI is to provide a unique and time-based Identifier at the particular cell site. It is assigned by the 5G network core via s special type of control signal while the mobile user is present at the particular cell site. The C-RNTI is transmitted as plain-text, so the attacker easily knows the user location.

D. *Bandwidth Stealing attack*

In 4G networks, the attacker can create false buffer status reports which can modify the packet scheduling algorithm used by the e-NodeB. Once the behavior of the entire scheduling algorithm is changed, the attacker may obtain the C-RNTI from the other mobile users and false status reports.

The e-NodeB will think that there will be no messages/ commands to be transmitted or received by the mobile users and it may allocate the maximum resources to the attacker and the other real mobile users will be starved of resources thus resulting in bandwidth stealing and creating Denial of Service attacks.

E. *HeNB Physical attacks*

Physical tampering of RF components is a possible attack in future 5G networks. This attack is too risky when it is executed inside a telemetry hospital management system. If malicious RF components are used by the intruder the HeNB will interfere with other wireless communication systems monitoring health-care to patients which may result health loss and lives in hospitals. A specific Intrusion detection system is to be designed in-order to mitigate these types of physical attacks on HeNB nodes in the future 5G networks. With the help of malicious codes the attacker can also gain access to HeNB through wires of the HeNB node and steal away the access credential details of the HeNB

F. *Attacks on 5G mobile core networks*

Malicious traffic can be used to create DoS attacks with the use of compromised HeNBs which can affect the core network elements. Internet key exchange version 2 attacks and flood attacks based IKEV2 can be used to un-tunnel the secured pathway between the HeNB and the security gateway which will connect the other elements of the core network. Such attacks can compromise the HeNB nodes and modifies the location of it, thus it will create the formation false emergency SMS centers which will seriously attack the law and order situation of a country.

II. Countermeasures for Attacks In 5g:

In this subsection, we discuss the countermeasures used for authentication and user privacy securing schemes in 5G mobile networks.

A. Target User Equipment Counter-Attack

User Equipment's viz. Laptops and mobile phones can be given security against Denial of Service attacks by using Anti-Malware software that can be installed in the user device which gives an ample protection against the DoS, SMS and MMS based attacks. Mobile equipment manufacturer Nokia has launched a security portfolio "NetGuard" to address these challenges.

Other Mobile-Internet security providers such as McAfee, Norton and Kaspersky also deliver Anti-malware software to protect our data stored in User equipment's and cloud.

B. Mobile Bot-net Counter-Attack

Intrusion made by Mobile Bot-net can be effectively detected using machine learning and artificial intelligence techniques. Machine learning algorithms such as Random Forest RF and K-Means++ will be able to classify the mobile data traffic signals normal or intrusion.

These algorithms will behave as intrusion detection system for software defined networking and network function virtualization architecture which gives 5G networks with enhanced security features (Li *et al,* 2018).

C.*User-Equipment Location Tracking Counter-Attack*

The user equipment location can be tracked with handover signals obtained by the intruder eNode-B. Encryption of Handover signals using advanced encryption standard (AES 128-bit) will be useful to encrypt the C-RNTI assignment signal, so the intruder will not be able to track the user equipment sessions (Fang *et al,* 2017).

The Rogue e-NodeB will not be able to capture the IMSI number of the user equipment thus encryption of handover signals may provide counter-attack solution for the User equipment Tracking attack.

D. *Bandwidth Stealing Counter- Attack*

Bandwidth stealing is a very crucial problem for industries as software defined radio is becoming more prevalent. The University of Utah in USA is developing software “Kasera” to catch the bandwidth stealers that could tell whether the hackers use unauthorized bandwidth which is not licensed by the telecom authorities of the region, counter-attack scheme locally known as crowd-sourcing (Patrick, 2016).

E. *Counter-Attack for HeNB*

Intrusion detection systems based on trusted platform module (TPM) to be developed for mitigating physical attacks against HeNB. Trusted Platform module is a crypto processor which will be used to store encryption keys to authenticate the hardware of the HeNB. The chips are developed by trusted computing group (TCG) are based on Application Specific Integrated chip standard. However, the TPM will not be able to control the software running on the HeNB, it can give a more secure access to the Radio Frequency Hardware components present at the macro-cell site in 5G networks (*TPM* , 2018).

F. *Counter-Attack: Packet Sequence Numbers*

The packet sequence number over the radio channel should be discontinuous in nature during the handover process. This discontinuous nature will make the control and data plane using random offset procedure. Another approach is using fresh encryption keys for each HeNB which will make the packet sequence numbers to look more random in nature, thus provides software security for HeNB (Liyanage *et al*, 2018)

Table1: Counter Measures To be implemented in 5G networks

S. No	Name of the attack	Counter-measures
1	Target User Equipment	Installation of anti-malware software
2	Bot-Net Attack	Artificial Intelligence and Machine Learning
3	User Equipment Location Tracking	Dynamic CRNTI signaling, removing the plain message feature of CRNTI
4	User Equipment Location Tracking	Encryption of Handover/ Handoff commands
5	Packet sequence numbers	Making packet sequence numbers discontinuous
6	Bandwidth Stealing attack	Dynamic token passing mechanism by the UE to the HeNB
7	Physical Attacks on HeNB	Trusted Platform Module (TPM)

Conclusion:

This paper investigated the various future security challenges in 5G networks, the study of different attacks that is possible to be performed by the intruder in 5G networks were analyzed in detail. The countermeasures that can be used to mitigate the security breaches inside 5G mobile networks were reviewed and analyzed its future scope for the development new security tools exclusively to be used for IoT based 5G communications**.**

Future Work:

As the 5G network infrastructure will be the major horse power for the development of future IoT devices the security related to Physical layer, Cloud Infrastructure which includes software defined network (SDN) and Network function virtualization modules and employing end-to-end security infrastructure in

5G networks will be serious challengeable research work for research scholars and industries working on 5G network planning and Security infrastructure. Even the present LTE networks describe the usage of end-to-end security infrastructure, the existing security measures do not apply to virtualization functions which forms the main backbone for 5G cloud computing. The support for massive IoT devices can be enhanced by usage of 5G infrastructure for that the distributed authentication mechanism are needed to address the security issues of multiple IoT devices at the same time through distributed authenticated nodes. Distributed authentication will also be key future research work in 5G domain.

Moreover, the ransom-ware based attacks will be a very serious cyber-attack which will be the next attacking method for the hackers who may disrupt the IoT based 5G communications and make it to a national level threat.

Acknowledgments:

The authors are thankful to the Dean, and other faculty members of Faculty of Engineering and Built Environment, Lincoln University College, Malaysia for their enthusiastic encouragement and useful critiques of this research work.

Conflict of interest:

The authors declare no conflict of interest.

References

5G PPP. *The 5G Infrastructure Public Private Partnership*. Retrieved from http://5g-ppp.eu/.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G security: Analysis of threats and solutions", *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, 193-199.

Fang, D., Qian, Y., & Hu, R. Q. (2017). Security for 5G mobile wireless networks. *IEEE Access*, *6*, 4850-4874.

Horn, G., & Schneider, P. (2015, August). Towards 5G security. In *Proc. 4th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Helsinki, Finland*.

https://www.networkworld.com/article/3098351/security/how-bandwidth-thieves-will-be-nabbed-in-the-future.html

Huawei Technologies Co., Ltd. (2016). *White paper: 5G Network Architecture- A high level perspective.*

Huawei Technologies Co., Ltd. (2019). *Huawei 5 G security white paper*.

Li, J., Zhao, Z., & Li, R. (2017). Machine learning-based IDS for software-defined 5G network. *IET Networks*, *7*(2), 53-60.

Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2018). *Comprehensive Guide to 5G Security*. John Wiley & Sons, Incorporated.

Mantas, G., Komninos, N., Rodriuez, J., Logota, E. & Marques, H. (2015). Security for 5G Communications. *In: J. Rodriguez (Ed.), Fundamentals of 5G Mobile Networks.* (pp. 207-220). John Wiley & Sons, Ltd.

Patrick, N. (2016, July 21). *How bandwidth thieves will be nabbed in the future.*

Rodriguez, J. (2015). *Fundamentals of 5G mobile networks*. John Wiley & Sons.

TPM. (2018, June 13). *Trusted Platform Module*. Retrieved from https://www.techopedia.com/definition/4146/trusted-platform-module-tpm