Volume 6, Issue 1, January 2019 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Bandwidth Spoofing and Intrusion Detection System for Multi Stage 5G Wireless Communication Network: A Review

Shivtanya Shivhar Nirmale
M. Tech. Research Scholar,
Department of Post Graduation
MBES's College of Engineering,
Ambajogai, (M.S.) [INDIA]
Email: tanunirmale@gmail.com

Vaijanath V. Yerigeri
Head of the Department
Electrical and Instrumentation Engineering
MBES's College of Engineering,
Ambajogai, (M.S.) [INDIA]
Email: vaijanatha_y@rediffmail.com

ABSTRACT

Mobile data traffic has increased many folds in recent years and current cellular networks are un-deniably overloaded to meet the escalating user's demands for higher capacity, data rates, and higher security. To meet such demands, Device-to-Device (D2D) communication is regarded as a potential solution to solve the capacity bottleneck problem in future 5G wireless cellular networks. In this paper, the generalized architecture for 5G wireless networks and its features, issues are discussed. The most important, security issues of 5G wireless communication networks have been emphasized upon, with the game theoretic analysis of bandwidth spoofing attack on the multi stage 5G wireless communication network. The intrusion on the relay, small cell access point and base station, which are forming a multi stage 5G wireless communication network, is detected using an Adaptive Intrusion Detection System.

Keywords:—*Device-to-Device (D2D) communication, Bandwidth Spoofing Attack, Intrusion Detection System.*

I. INTRODUCTION

Device-to-Device (D2D) communication, Bandwidth Spoofing Attack, Intrusion Detection System. 5G wireless communication networks (WCN). This paper focuses on the security analysis of the 5G WCN and has analyzes the impact of bandwidth spoofing attack using game theory on the SCA in 5G WCN. This paper reviewed an Adaptive Intrusion Detection System (IDS) using Hidden Markov Model (HMM) for detecting an intrusion on SCA in 5G WCN [1]. In the end, conclude with contribution of this review paper, their overall impact on future research in terms of power optimization and security issue of 5G wireless communication networks.

II. LITERATURE SURVEY

P. Traynor, we characterize the impact of the large scale compromise and coordination of mobile phones in attacks against the core of these networks. Through a combination of measurement, simulation and analysis, we demonstrate the ability of a botnet composed of as few as 11,750 compromised mobile phones to degrade service to area-code sized regions by 93%. As such attacks are accomplished through the execution of network service requests and not a constant stream of phone calls, users are unlikely to be aware of their occurrence. We then investigate a number of significant network bottlenecks, their impact on the density of compromised nodes per base station and how they can be avoided. We conclude by discussing a number of

countermeasures that may help to partially mitigate the threats posed by such attacks [9].

M.Ye and G.Hu, proposed Nash equilibrium seeking algorithm includes the gradient estimation part and the gradient search. An example and numerical simulations are provided to demonstrate the performance of the designed Nash equilibrium seeking algorithm[17].

Jin Cao, concluded that, work could attack much more attentions from the academia and industry to promote the corresponding research activities and could provide helpful indications for the deployment of the LTE/ LTE-A 4G wireless networks[6].

P. Schneider and G. Horn, we propose a 5G vision based on softwareisation. We provide a non-exhaustive list of current security, trust and resilience issues that are critical to be explored in 5G. We finally give some directions to overcome these issues[2].

A. Gupta and R. K. Jha, survey will surely inspire next generation researchers to come up with intelligent and stronger security mechanisms and make a safer network[8].

A.Gupta and R.K.Jha, survey, the prime focus is on the 5G cellular network architecture, Massive MIMO technology, and Device to Device Communication (D2D). Along with this, some of the emerging technologies that are addressed in this paper include interference management, spectrum sharing with cognitive radio, ultra -dense networks, multi-radio access technology association, full duplex radios, millimeter wave solutions for 5G cellular networks, and Cloud Technologies for 5G Radio Access Networks and Software Defined Networks (SDN). a general probable 5G cellular network architecture is proposed which shows that D2D, small cell access points, Network Cloud, and the Internet of Things (IoT) can be a part of 5G cellular network architecture[1].

Chao Wang and H.M.Wang, the array pattern and intensity of eavesdroppers are very important system parameters for improving the secrecy performance of the mmWave communication. In particular, for the AN- assisted mmWave networks, the power allocated to AN depends on the array pattern and the intensity of eavesdroppers [3].

A. Gupta and R. K. Jha, concluded that, for the urban macro heterogeneous deployments in the 3GPP LTE standard, the optimal number of antennas at the SCA will be 3 because with the increase in the number of antennas at the SCA up to 5 antennas, total power per subcarrier will decrease but along with this the interference between the antennas of SCA will increase [10].

III. 5G Wireless Network Architecture

This section has shown the evolution of wireless technologies and has proposed a general 5G wireless network architecture which may provide a good platform for future 5G standardization network with issues and challenges. Security is the one of the important issue in 5G, which is discussed in detailed. Today and in the recent future, to fulfill the presumptions and challenges of the near future, the wireless based networks of today will have to advance in various ways. Recent technology constituent like high-speed packet access (HSPA) and long-term evolution (LTE) will be launched as a segment of the advancement of current wireless based technologies.

A. 5G Cellular Network Architecture

To contemplate 5G network in the market now, it is evident that the multiple access techniques in the network are almost at a

still and requires sudden improvement [1]. Current technologies like OFDMA will work at least for next 50 years. The wireless access points inside the building are connected with the large antenna arrays through cables for communicating with indoor users. This will significantly improves the energy efficiency, cell average throughput, data rate, and spectral efficiency of the cellular system but at the expense of increased infrastructure cost. With the introduction of such an architecture, the inside users will only have to connect or communicate with inside wireless access points while larger antenna arrays remained installed outside the buildings [2-6]. For indoor communication, certain technologies like WiFi, Small cell, ultra wideband, millimeter wave communications, and visible light communications [3] are useful for small range communications having large data rates. But technologies like millimeter wave and visible light communication are utilizing higher frequencies which are not conventionally used for cellular communications.

A general 5G cellular network architecture has been proposed as shown in Figure 1, which describes the interconnectivity among the different emerging technologies like Massive MIMO network, Cognitive Radio network, mobile and static small-cell networks. This architecture also explains the role of network function virtualization (NFV) cloud in the 5G cellular network architecture. The concept of Device to Device (D2D) communication, small cell access points and Internet of things (IoT) has also been incorporated in this proposed 5G cellular network architecture. In general, this 5G cellular network architecture may provide a good platform for future 5G standardization network.

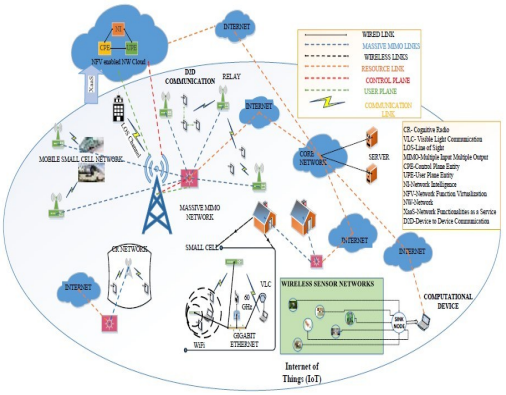

Figure 1 : A General 5G Cellular Network Architecture [1].

Since the 5G cellular architecture is heterogeneous, so it must include macrocells, microcells, small cells, and relays. A mobile small cell concept is an integral part of 5G wireless cellular network and partially comprises of mobile relay and small cell concepts [7]. It is being introduced to put up high mobility users, which are inside the automobiles and high speed trains. Mobile small cells are positioned inside the moving automobiles to communicate with the users inside the automobile, while the massive MIMO unit consisting of large antenna arrays is placed outside the automobile to communicate with the outside base station. According to user's opinion, a mobile small cell is realized as a regular base station and its allied users are all observed as a single unit to the base station which proves the above idea of splitting indoor and outdoor setups. Mobile small cell users [8] have a high data rate for data rate services with considerably reduced signaling overhead, as shown in. As the 5G wireless cellular network architecture consists of only two logical layers: a radio network and a network cloud. Different types of components performing different functions constitute the radio network. The network function virtualization (NFV) cloud consists of a User plane entity (UPE) and a Control plane entity (CPE) that perform higher layer functionalities related to the User and Control plane, respectively. Special

network functionality as a service (XaaS) will provide service as per need; resource pooling is one of the examples. XaaS is the connection between a radio network and a network cloud [9]. The 5G cellular network architecture is explained in [10]. It has equal importance in terms of front end and backhaul network respectively.

B. Security Issues in 5G

Security is applied vertically that means at each layer security must be ensured. Security is a major concern in 5G, security issues can vary at each layer rising from simple beacon to complete message. The radio nature of 5G communications introduces various security threats [3-6]. The main threats are:

- ***Eavesdropping attack:*** an attacker passively listens to the radio channel between UE devices in order to get sensitive data. Data confidentiality in the cryptography approach can parry this threat.
- ***Impersonate attack:*** an attacker can pretend to be a legitimate UE device or eNB to get access to the traffic data. Authentication in the cryptography approach can parry this threat.
- ***Forge attack:*** an attacker may forge the content and send the fake data to the rest of UEs, which prejudices the system. Data integrity (digital signature) in the cryptography approach can parry this threat.
- ***Free-riding attack:*** in order to reduce system availability in D2D communications, an attacker may encourage selfish behavior of some UEs to preserve energy consumption so they may not be willing to send contents to others while receiving its demanding data from their peers. Such vulnerability may affect Quality of Experience (QoE) thus irritates user experiences and hinders the adoption of D2D communications. To resist such an attack, it is necessary to develop a cooperation stimulation mechanism [10, 11].
- ***Active attack on control data:*** an attacker tries to change the control data. Authentication, confidentiality and integrity in the cryptography approach can parry this threat.
- ***Privacy violation:*** some privacy-sensitive data such as identity, location, etc. are more concerned by D2D services functionalities, so this personal information must be concealed to non- authorized parties.
- Denial-of-Service (DoS) attack: it consists of rendering up unavailable a service in D2D communications. In [2], authors has shown via experimental study about exploration on characteristics of DoS attacks on Android devices in D2D underlying network environment that malicious devices can stealthily impair or even totally block the connection of legitimate devices in the underlying network.

IV. Attack Modelling For 5G Wireless Communication

In the previous section, it is clear that all security attacks are posing major threat to the 5G wireless networks. This section overviewed attack modeling for Bandwidth Spoofing and Intrusion Detection System in 5G wireless communication networks.

A. Bandwidth Spoofing Attack in 5G Wireless Communication Network

In the previous section, it is clear that DoS attacks are posing major threat to the 5G WCN. This section introduces game theory formation for Bandwidth attack which is

one of the types of DoS attack in 5G wireless communication networks. In this attack, the attacker has the knowledge about the traffic pattern of the network i.e. the Downlink/ Uplink (DL/UL) mapping of SCA with BS. The entire process of communication between BS and SCA is in three phase. In the first phase, BS performs the operation of ranging. In the second phase, once the ranging has been done, the SCA are able to send request to server from BS (UL). In the third phase, server responds the particular application from BS (DL) to SCAs. For this process, bandwidth is needed, so BS will now assign bandwidth to all the SCAs. In the third phase of assigning the bandwidth, the attacker has the chance to acquire the bandwidth that is going to be assigned to the SCA. In this section, the Bandwidth attack by attacker which is an un-Authorized client on SCA or defender using game theory is examined. This section helps in analyzing the way in which the attacker client wins the game by spoofing the bandwidth. This section also helps in analyzing the way in which SCA will protect the bandwidth by using Nash equilibrium.

Game Theory: The game theory deals with the situation where, at least two entities interacting according to the rules of the game. In this theory, game is open, when each client has finite number of moves available but ends, when it has finite numbers of moves [6]. In this chapter, game theory is applied for analyzing the way in which the attacker client or intruder wins the game by spoofing the bandwidth.

Client A and B are playing a game with coin and both have decided that if both the faces are same i.e. (H, H) and (T, T) then B will pay i.e. A will win the game, and if both the faces of the coin are opposite, B will win and A will pay, remember toss is always unbiased [1].

$$Pay\ off\ A = \begin{matrix} \\ H \\ T \end{matrix} \begin{matrix} \begin{matrix} H & T \end{matrix} \\ \begin{bmatrix} +1 & -1 \\ -1 & +1 \end{bmatrix} \end{matrix}$$

Here H is Head and T is Tail. Since the above given matrix is the payoff matrix A, so payoff matrix B can easily be deducted from the above matrix. But while applying game theory, we came across two types of clients i.e. Intelligent and rational. The intelligent client means that they are able to take fruitful decision on the basis of their experience and think logically. While rational means that preferences are consistent with final outcomes of the decision- making process and are intended to maximize these preferences. The maximization is carried out by trying to achieve a certain gain, which is expressed through utility function. Hence both A and B being the intelligent client, B realizes after some time that A is playing the game and showing H continuously, so he adapts and show T. With the game progresses, both A and B will acts as an intelligent clients in a manner that A will Maximize the gain and B will Minimize the loss. So now the matrix will be

$$Max\ Min\ gain\ of\ A \begin{matrix} \begin{matrix} \text{Min Max loss for B} \end{matrix} \\ \begin{bmatrix} +1 & -1 \\ -1 & +1 \end{bmatrix} \end{matrix}$$

Here, A wants to maximize the Minimum gain and B wants to minimize the Maximum loss. Hence game is therefore the steps between multiple entities [1].

Nash Equilibrium: The games in the game theory are initially classified as Cooperative and Non-cooperative games. Cooperative games study the formation of coalitions with binding agreements that may be of benefit to the individual components, while the non- cooperative games are concerned with the mechanism of individual decisions, based on individual reasoning, in the absence of mandatory alliances. The formal discretion of a non-cooperative game takes

two forms and is classified as extended form and Strategic form. In the extended form, the description of game is made with a tree structure. While strategic form specifies the number of clients, the space of strategies and the utility function of each client.

B. Intrusion Detection System in 5G wireless communication network

The need to secure the 5G WCN has now become the prime concern. The most common method that came forward for detecting an intruder will be Intrusion detection system (IDS). Earlier, for maintaining the high security of the network an IDS runs at each BS. Each incoming request is submitted to the IDS for verification. It receives the client details in terms of MAC ID and BS ID to verify whether the request is genuine or not. But the types of services that are offered in that request are not known to the IDS. It tries to find out any anomaly in the request based on the spending profile of the requester. If the IDS confirm the request to be malicious, it raises an alarm, and the BS declines the request. The concerned client may then be contacted and alerted about the possibility that the security of BS is compromised [1-3].

The typical IDS need some additional features for better intrusion detection. Hence Hidden Markov Model (HMM) is introduced with the IDS to form an Adaptive IDS which can be used for the detection of an intruder. But for 5G WCN, IDS will run at the sites that are going to be attacked i.e. either at SCA or at relay. An HMM is capable of modeling more complicated stochastic processes than a traditional Markov model because it is a double embedded stochastic process which is having two hierarchy levels. An HMM has a limited set of states administered by a set of transition probabilities. An observation can be generated conferring to an associated probability distribution for a specific state. It is only the observation and not the state which is evident to a peripheral observer. Hence, IDS will be able to detect the intruder that is executing the bandwidth spoofing attack on the SCA in a 5G WCN [4 -8].

V. CONCLUSION

The key focus of this review paper is on the security in 5G Wireless networks, particularly, a general 5G cellular network architecture has been discussed. It has equal importance in terms of front end and backhaul network respectively. It describes the interconnectivity among the different emerging technologies like Massive MIMO network, Cognitive Radio network, and mobile and static small-cell networks. This architecture also explains the role of network function virtualization (NFV) cloud in the 5G cellular network architecture. The concept of Device to Device (D2D) communication, small cell access points and Internet of things (IoT) has also been incorporated in this 5G cellular network architecture.

The Game theory has proven to be a useful method in examining the bandwidth spoofing attack. In addition, with the use of prisoner's dilemma game theory, attacker is able to spoof the bandwidth from the defender and too with a significant winning percentage. This chapter has also proposed an adaptive intrusion detection system which is capable of detecting and removing the intruder which is executing the bandwidth spoofing attack on the SCA in a 5G WCN.

REFERENCES:

[1] Akhil Gupta, Rakesh Kumar Jha, Pimmy Gandotra, and Sanjeev Jain, "Bandwidth Spoofing and Intrusion Detection System for Multi Stage 5G Wireless Communication Network", IEEE Transactions on Vehicular

Technology, Volume: 67, Issue 1, pp no. 618 - 632, Jan. 2018.

[2] Gupta, Akhil; Jha, Rakesh Kumar, "Security threats of wireless networks: A survey," Computing, Communication & Automation (ICCCA), 2015 International Conference on, vol., no., pp.389, 395, 15-16 May 2015.

[3] Gupta, A.; Jha, R.K., "A Survey of 5G Network: Architecture and Emerging Technologies," in Access, IEEE, vol.3, no., pp.1206-1232, 2015.

[4] Schneider, P.; Horn, G., "Towards 5G Security," in Trustcom/Big DataSE/ ISPA, 2015 IEEE, vol.1, no., pp.1165 -1170, 20- 22 Aug. 2015.

[5] C. Wang and H. M. Wang, "Physical Layer Security in Millimeter Wave Cellular Networks," in IEEE Transactions on Wireless Communications, vol. 15, no. 8, pp. 5569-5585, Aug. 2016.

[6] HuiMing Wang, T.X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," IEEE Transactions on Communications, vol. 64, no. 3, pp. 12041219, Mar. 2016.

[7] Y. Zhang, H. M. Wang, Q. Yang and Z. Ding, "Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access," in IEEE Communications Letters, vol. 20, no. 5, pp. 930-933, May 2016.

[8] Jin Cao; Maode Ma; Hui Li; Yueyu Zhang; Zhenxing Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," in Communications Surveys & Tutorials, IEEE, vol.16, no.1, pp.283-302, First Quarter 2014.

[9] Monica Paolini, "Wireless security in LTE networks", White paper, 2012.

[10] Gupta, A.; Jha, R.K., "Security threats of wireless networks: A survey," in Computing, Communication & Automation (ICCCA), 2015 International Conference on, vol., no., pp.389-395, 15-16 May 2015.

[11] Patrick Traynor et al., "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core", Proceedings of the 16th ACM conference on Computer and communications security, 2009.

[12] Monica Paolini, "Wireless security in LTE networks", White paper, 2012.

[13] Gupta, Akhil, and Rakesh Kumar Jha. "Power optimization using massive MIMO and small cells approach in different deployment scenarios." Wireless Networks 23.3 (2017): 959-973.

[14] Gupta, Akhil, and Rakesh Kumar Jha. "Power optimization using optimal small cell arrangements in different deployment scenarios." International Journal of Communication Systems, 2017.

[15] Devi, Reeta, et al. "Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network." AEU-International Journal of Electronics and Communications 74 (2017): 94-106.

[16] Gupta, Akhil, Rakesh Kumar Jha, and Sanjeev Jain. "Attack modeling

and intrusion detection system for 5G wireless communication network." International Journal of Communication Systems 30.10, 2017.

[17] Geva, M.; Herzberg, A.; Gev, Y., "Bandwidth Distributed Denial of Service: Attacks and Defenses," in Security & Privacy, IEEE, vol.12, no.1, pp.54-61, Jan.-Feb. 2014.

* * * * *