Intrusion Detection System and Bandwidth Spoofing for Multi Stage 5G Wireless Networks

[1] Shivtanya Shivhar Nirmale, [2] Prof.V.V.Yerigeri
[1]M.Tech Student, [2]Designation of 2nd Author
Department of PG
MBESs College of Engineering, Ambajogai, MS, India

Abstract: The next decade which will be driven by the expected 50 billion connected devices connected to the cloud by 2020 and all need to access and share data, anywhere and anytime. With a rapid increase in the number of connected devices, some challenges appear which will be responded by increasing capacity and by improving energy efficiency, cost and spectrum utilization as well as providing better scalability for handling the increasing number of the connected devices. Apart from all these challenges the security remains a vital concern in 5G technology. In this paper, the security issues of future wireless communication networks have been discussed upon, with the game theoretic analysis of bandwidth spoofing attack on the future multi stage 5G wireless communication network. The intrusion on the relay, dense small cell access point and service provider base stations, which are forming a future multi-stage 5G wireless communication network, is detected using a intelligence based adaptive intrusion detection system.

Index Terms **- 5G Technology, Bandwidth Spoofing Attack, Intrusion Detection System**

I. INTRODUCTION

With the evolving technologies, wireless communication has also evolved through generations. Evolution is the need of the hour. With the increasing user demands, wireless communication has to evolve to meet these demands. Our wireless network architecture and equipment's are changing, to meet the demands of the user. From closed hierarchical networks, we have shifted towards the flat networks which are more porous and easier to penetrate. Thus developing technologies paved the way for the wireless network attacks. Now irrespective of using expensive Radio Access Network (RAN) equipment's, we make use of femto - cells, small cells and Wi-Fi hot spots for reaching to the end user with better quality of service [1-4]. But these act as an entry point in to the mobile networks, providing an intrusion site for the attacker. Wireless network attacks are classified and explained in detail on the basis of access control, authentication, availability, confidentiality and integrity in [5]. Evolution in the wireless communication industry has also forced the attackers or intruders to evolve for intruding in to the network. Now the intruders are finding new ways to intrude into the evolved wireless network architecture as given in [6]. These attacks are somewhere came in to existence in 4G and are still vulnerable.

While data transmission in network and storage in the cloud offers several advantages in terms of data storage, availability, scalability and processing, it increases the chance of malicious attacks, that in addition to potential privacy invasion by cloud operators who can have access to sensitive data. All this puts a question mark whether cloud data storage is feasible, especially for governmental agencies and financial industries. Several works have attempted to solve the security challenges of cloud storage. For instance, Gai et al. proposed a method that splits files into encrypted parts and store them in distributed cloud servers without users' data being directly reached by cloud service operators [7]. In [8], the authors optimized the data placement on cloud servers that minimizes retrieval time of data files while guaranteeing their security based on the distance between nodes that store the data chunks, such that the malicious attacker cannot guess the locations of all the data chunks. In [9], the authors suggested that data to be encrypted and decrypted before sending it to clouds.

The basic theory of security includes maintenance of confidentiality and integrity of communication by securing the individuality and privacy of mobile subscribers within the network. The communication networks are more largely vulnerable to cyber-attacks. In the last decade, hackers have grabbed the attention towards the wireless mobile network, resulting in a surge of security breaches [10-15]. The liability of being attacked by the hackers is further increased in the 5G future networks with the introduction of IP-based flat architectures and extensive cloud involvements for network computing and communication [16]. Thus, for incorporating security an aspect within a future network is must and should. Hence, mobile users' secrecy traits should now be the part of 5G architectural designs. The development of security in 5G networks has an immense scope. This paper presents a minor step towards securing the 5G Wireless Communication Networks (WCN's). In order to focus towards security, a heterogeneous 5G cellular network architecture as proposed in [17], need to be addressed. Relays, macro-cells, microcells and small cells, are considered as an important component of the proposed architecture. Such a division of architecture supports enhanced coverage and thus overcomes the low signal problem. But, in return they are creating a dynamic spot for the intrusion to happen. Since, unauthorized users can easily access relays and small cell access points, so these two locations are highly susceptible to attacks.

II. RELATED WORK

Wireless communication has evolved from analog voice calls to high quality broadband services with high speed data. With the rapid increase in the demand of the users in the near future, a wireless network has to come up with new technologies. In the next generation networks i.e. 5G, introduction of Flat IP architecture and extensive involvement of cloud in the network processing and communication increases the vulnerability to hackers. Hence, it has become obvious that in 5G networks, security must be built-in and the security aspects must be accompanied with the architectural design, while designing 5G networks [5-9].

To overcome these challenges, the performance criteria in terms of throughput, latency, and connectivity density needs to be raised, while ensuring the security. The main ideology of the security is to protect the identity and privacy of the subscribers, while maintaining the confidentiality and integrity of their communication. In the recent times, communication networks are becoming the prime objectives of the cyber-attacks because of their high vulnerability.

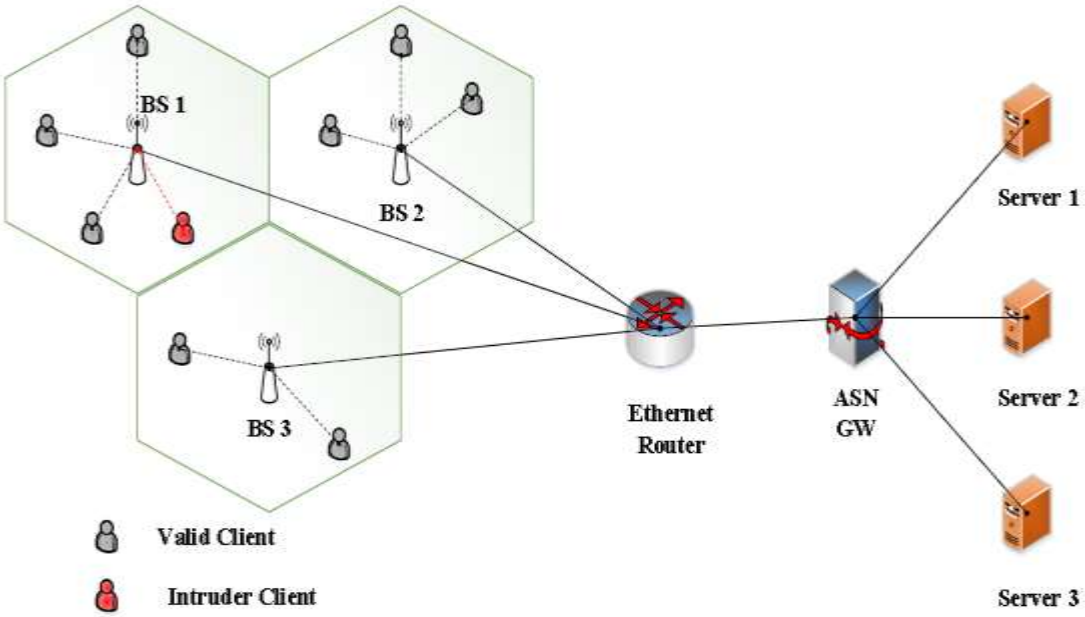

Figure 1: A General Wireless Network Scenario under threat.

A general 5G wireless Network under threat is depicted in Figure 1. It is showing that the different base stations are connected to the backbone network with the help of an Ethernet router and all the valid clients in a particular cell are reporting to a particular base station inside that cell. The security threat condition has arisen when an intruder client, who is behaving as a valid client, tries to capture the base station and intrude in to the network.

A. Probable Security Attacks for 5G Network Architecture

Among the attacks given in [13], Denial-of-Service (DoS) attack is the most common and dreadful attack which aims at exhausting the resources of the target. This attack generally targets the web services and is very common in today's internet. In the present generation, mobile networks are now becoming an integral part of day today life. But these networks are the most probable targets for the DoS attacks and mostly carried out by mobiles using a mobile botnet. They are targeting the control plane elements like Mobility Management Entity (MME) in 4G networks [14]. In [16], an attack against the Home Location Register (HLR) has been shown but by following the simple means. Security breach on 5G WCN can be minimized by implementing intrusion detection system (IDS) on the relay for the respective cases. The implementation of IDS as per the given cases, not only enhance the security of the network but also consume less power and helps in achieving power optimization in 5G WCN. According to the above discussion it is concluded that DoS attacks are posing major threat to the future 5G networks. Mitigating the threat will be one of the prime research areas during the next few years. Next section comprises of a mathematical analysis of bandwidth spoofing attack (a kind of DOS attack) using game theory in 5G WCN.

III. Attack Modeling 5G Wireless Communication Networks

In the previous section, it is clear that all security attacks are posing major threat to the 5G wireless communication 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

This section introduces game theory formation for Bandwidth attack which is one of the type 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 [1]. 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 [2, 5].

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 [7-10].

B. Intrusion Detection System in 5G wireless communication network

A Hidden Markova Model (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 [1].

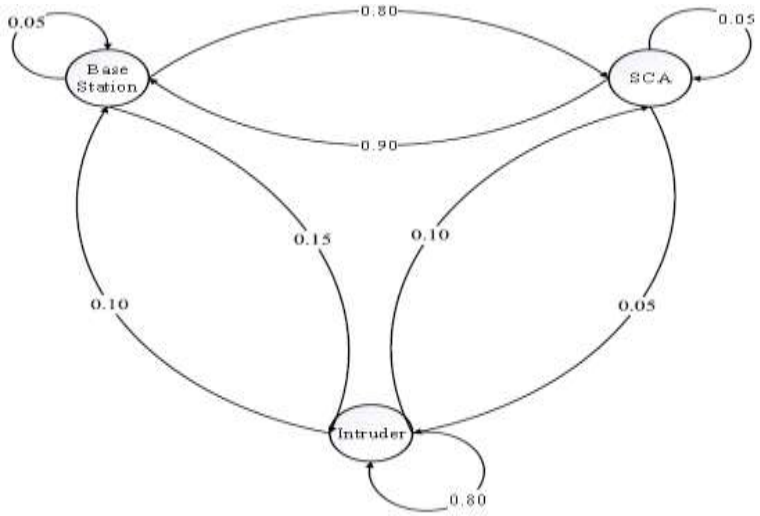

Figure 2: HMM for intruder detection with transition probabilities according to Table 1.

Figure 2 depicts the special case of fully connected HMM in which every state of the model can be reached in a single step from every other state with transition probabilities as shown in Table 1. Here each client will be trained and maintained by HMM.

Table 1: Proposed HMM for intruder detection with transition probabilities

Demand	Response		
	Base Station (BS)	SCA (A)	Intruder (B)
Base Station (BS)	0.05	0.80	0.15
SCA (A)	0.90	0.05	0.05
Intruder (B)	0.10	0.10	0.80

IV. Simulation Results and Discussions

The bandwidth spoofing attack has been modeled using game theory and simulation has been performed for four rounds, involving 8 iterations. The results of the simulation are shown in Table II.

Table II: Results of the Game Theory for Bandwidth spoofing attack

	Round 1	Round 2	Round 3	Round 4	No. of Winning Round	Result
Iteration 1						
Player A Average Score	98	54	45	37	1	Player A wins with average score 22
Player B Average Score	84	33	44	55	2	
Iteration 2						
Player A Average Score	67	44	46	33	2	Player A wins with average score 28
Player B Average Score	85	65	64	55	1	
Iteration 3						
Player A Average Score	85	68	48	34	3	Player B wins with average score 23
Player B Average Score	67	56	49	42	1	
Iteration 4						
Player A Average Score	98	65	54	42	1	Player B wins with average score 27
Player B Average Score	86	58	76	48	2	

Here Player A is the genuine client and Player B is the attacker. The simulation has been performed in four rounds and the average score of each player coming after following the steps shown in the flowchart is recorded. Now the average score of each player is compared with its counterpart and the player who wins more number of rounds will be able to acquire the bandwidth. For the case of 4 iterations as in Table II, it is clear that Player A wins in the first two iteration with a fixed strategy. But in the therd iteration, player B understands the strategy of the player A and change its strategy accordingly which results in the win for player B. Now the bandwidth is with the player B. So for the next 2 iterations the bandwidth is with the player B. But when we run the simulation for different number of iterations, still the bandwidth acquiring percentage of the attacker is significant enough for the bandwidth spoofing attack to make an impact.

While the graph shown in Figure 3 clearly shows that the intruder probability is always less than the valid user probability. Hence it is easy to detect and remove the intruder from the model by using this proposed model of IDS.

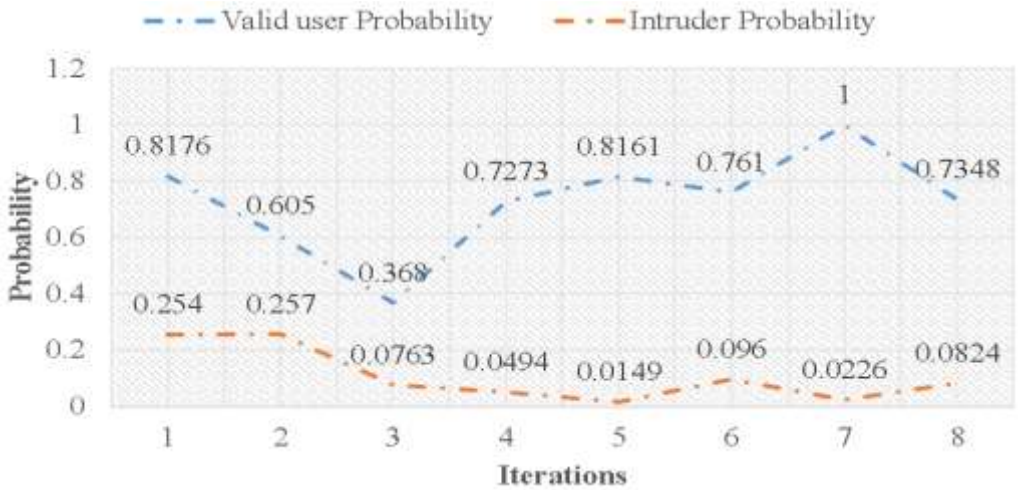

Figure 3: Valid User Probability v/s Intruder Probability.

V. CONCLUSION AND FUTURE WORK

In this paper, from the above results, it is concluded that the adaptive IDS will be able to detect the intruder that is executing the bandwidth spoofing attack on the SCA in a 5G WCN. Simulations have shown that in all the iterations, the probability assigned to the intruder is always less than the valid user probability. Hence, it has become easy for the adaptive model of IDS in the SCA to detect the intruder in the first step and remove it from the database in the next step. 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, 2018. "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.

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

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

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

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

[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.