International Journal of Intelligent Information Technologies
Volume 18 • Issue 3

Experimental Study of Location Spoofing and Identity Spoofing Attack in Internet of Things Network

Mihir Mehta, Gujarat Technological University, India*
Kajal Patel, Vishwakarma Government Engineering College, India

ABSTRACT

IoT devices are placed at open places, generally at where monitoring and controlling of devices from remote location is difficult. Location spoofing is a threat in which an intruder intentionally modifies the contextual information such as geolocation of a device. Location spoofed device will pass faulty data to the base station, and because of that, serious problems such as traffic jam in smart city application, machine malfunctioning in industry application can take place. So decision making in IoT applications to determine correctness of contextual information is a prime concern for smooth functioning of networks. Identity spoofing is a threat in which an attacker captures the identity information of a legal device and can misuse this stolen information for performing various cyber threats such as MITM, key stolen, and replay. The authors have simulated these attacks in Cooja simulator and investigated the performance of the network in the presence of these attacks. The conclusion is that these attacks affect network performance in an adverse way.

KEYWORDS

COAP, Context Validation, Delay, IP Spoofing, Location Spoofing Attack, Power Consumption, RPL, Throughput

INTRODUCTION

Security is a prime concern for Internet of Things networks. IoT is a collection of distinct types of connected devices; in which they can do exchange of the data as well as computational tasks. IoT networks have constraints of storage capacity, processing power and battery power. Because of that, conventional security explanations can not be applied to the IoT networks. IoT networks are always preferable to an intruder for performing various cyber-attacks as they lack standards, policies and are directly associated with the network. It is predicted in a recent Gartner report, almost 20 billion devices will be part of the IoT network in 2022. (H. Kim, 2017). This report signifies the usage of IoT networks into various applications. Currently, we can find out different applications of IoT in

DOI: 10.4018/IJIIT.309587 *Corresponding Author

the area of health monitoring, smart farming, environment monitoring and so on. So, if there is no proper security applied to the network; then it will be of no benefit to society.

Various researchers have studied in detail regarding the importance of IoT security and different security threats to an IoT Architecture. However; there is no significant work which focuses on the impact of Location Spoofing and Identity Spoofing attacks on the performance of the network. Location is a very important parameter for taking a decision into the IoT application like Military and Industry. When we deploy the devices into the network, they are open to all. Anyone can access that location or device. So, if an intruder intentionally captures an IoT device and changes its location; then the device will sense the wrong data and also transfer this wrong sensed information to the base station. In this way, an attacker can launch the Physical attack like location spoofing attack and changing the distance attack. So, when the device connects with the base station or server, before making any decision; it is very much necessary to verify its location related context information. Geolocation is a key feature in an IoT network, as based on that network can provide various services to the users. In many applications, IoT devices are a fixed part of the network and movement of that device by an intruder from one place to another place can launch the attack into the network. Example: If an intruder changes the sensors' location measuring speed at roadside beyond awareness of the base control station, the base control center will investigate statistics analogous to a dishonest location. Such kinds of planned or unplanned activity may launch the attack and can disturb the well-planned transits system by initiating traffic-jam and accidents. (M. Wazid, 2018). Identity Spoofing is an attack in which an intruder steals legal device's identity information and misuses that information for performing Man in the Middle attack or Masquerade attack. It has been observed in recent research work that an IP Spoofing attack is possible in the IoT network. IP address is the unique identity of the device when it connects to the network. To forward the data packets on the Physical link, MAC address is required. Because of that binding of IP address and MAC address is required. Both IP address and MAC address are very much important for identification purposes and for data delivery. Intruder can stick its own IP address to the victims' MAC address. In this way, an attacker can direct all the traffic towards itself. We have implemented these both attacks in Cooja simulator and measure the changes into the performance of the system in the presence of attacks.

BACKGROUND

For the implementation of Location Spoofing attack, we have used COAP- Constrained Application protocol. It is designed for constrained networks to transfer the contents on the web. (N. Wang, 2017). It is widely used in applications in which machine to machine communication is required. COAP runs on the User Datagram Protocol. So, it is lightweight in nature and it is also interoperable with the HTTP. It is suitable for the IoT network as it can work on the microcontrollers having 10 KiB of RAM and 100 KiB of code space. (M. Naveed, 2019). It is based on the Client-Server communication paradigm. For the implementation of Identity Spoofing attack, we have used RPL- Routing Protocol for Low-Power and Lossy Network. RPL is a routing protocol established on IPv6. It is specially designed for low power wireless networks. It is a proactive routing protocol established on the distance vectors. (V. Haseeja, 2019). RPL creates a topology like a Tree topology. Network devices executing RPL protocol are organized in a manner that no cycle should be formed and this type of topology can be defined as a Destination Oriented Directed Acyclic Graph (DODAG). The RPL is prescribed by four types of control messages for topography preservation and message transfer. (1) DODAG Information Object (DIO) - It is the essential authority of routing control messages. It can store information such as the Rank of a node, the IPv6 address of the root, etc. (2) Destination Advertisement Object (DAO) - It provides the assistance for the down traffic and it is useful for forwarding the destination information upwards along the DODAG. (3) DODAG Information Solicitation (DIS) - It causes a potential for a node to demand DIO messages from a reachable neighbor. (4) DAO ACK – It is dispatched by a DAO subscribers in reply of a DAO message. (P. Gope, 2019).

Objective for this experimental research work is to analyze the impact of Location Spoofing and Identity Spoofing threat on the performance of IoT network. According to current CISCO report- almost 20 billion devices are associated with the Internet and IoT is currently introduced in Healthcare, defense, Agriculture, Industry, Smart City related applications. From all these applications, almost one third application depends on context related information for appropriate decision making process. In existing research work, consideration of context information especially geolocation data related information validation before analyses of data and decision making is missing. If we take simple example of sensor device placing at a junction on the roadside measuring number of vehicles passing in a fraction of time to take necessary decision for traffic management. If an Intruder captures this sensor device and intentionally deploy it at another junction of city, then sensor device will pass on the wrong data to the centrally command center. So, in this case device identity is legal but the context information of that device is manipulated. So, control center will analyze those false data and it will provide certain decision for traffic management. Now, that decision will not be effective for traffic management as it is based on spoofed context information. Because of that accident at junction can happen or also traffic jam can be happen. Also, because of this kind of malicious activity; network's throughput will be decreased and delay will be more as control center will be busy in entertaining of requests from this spoofed device.

Methodology and Experiments describes methodology for simulating Location Spoofing attack and Identity Spoofing attack in detail. It also describes simulation setup for attacks with necessary parameters- Number of motes, Protocol, Operating System. Authors have presented simulation results for measuring system performance in terms of power consumption, throughput and delay. At last authors have concludes the paper with direction of future work.

METHODOLOGY AND EXPERIMENTS

Location Spoofing Attack

Location spoofing is a physical kind of attack in which device's location related data is manipulated and then device tries to become a part of the network. In this kind of attack, devices will establish communication from the forged place/ location. It can affect the network's performance and also devices will generate fake data if its location information is spoofed. So, detection of this kind of attack is very important in mission-critical applications like the Military domain and Industry domain. It will improve Authentication service in the network. It will identify any suspicious activity in the network at an early stage.

By 2020, over and above 20 billion devices will be coupled with IoT, according to Machina Research. (Y. Wang, 2018). Of the billions of devices, more than half contain geographic location data, and about one-third rely heavily on specific appliances such as smart cities, asset detection, and agriculture. (Yan Zhao, 2018). Geo-positioning is desired for better understanding the demands of civilians, when and where they desire service, and the devices and physical geo-locations where they need service. Provide traffic related data and obstacles. Real-time traffic information. Planned road construction; parking spaces; schools, hospitals, emergency service locations: All these characteristics of smart cities depend on geographic location information. An attacker could swap the position of one IoT peripheral to simulate the geographic location of another IoT peripheral. Similarly, an attacker's shift in smart meters could allow distribution companies to expand power transfer in low-request domains and cut off power in high-use areas. To improve the resistance of the sensor to such attacks, we introduced the idea of geo-location using secret channel technology.

Identity Spoofing Attack

Attackers can make ridiculed RPL messages which bring about off-base IP-MAC restricting in Neighbor Cache. This is also known as neighbor reserve harming or assault on address enlistment.

The first attacker gets a DIO packet and grasps the IPv6 address of a node on the network. Then select the fatality node and submit a test package to investigate Victim during sleep mode or wake up. If the fatality node's radio is on, that is, in wake mode, the fatality node will confirm receipt of the test package. In this case, the attacker is waiting. Attackers can also efforts other IP addresses. If the fatality node is asleep, it will not provide the receipt of the test package. This time, the attacker sends a malicious DIS message, which is acknowledged by the border router. The edge router obsrves the IPv6 address and MAC address from the acknowledged malicious RPL message and modifies the routing table accordingly. Therefore, an incorrect entry is created in the router's grid table and all traffic is forwarded from the victim node to the attacking node.

Simulation Set Up

Experiments are done on Cooja Simulator for Location Spoofing and Identity Spoofing attacks. It permits the emulation of real time hardware platforms. It is especially planned for low power and resource constrained IoT devices. It works on the Contiki Operating system. Authors have used Sky Motes for the simulation purpose in both attacks.

Authors have considered the scenario of 6 motes in both attacks. For Location Spoofing attack; initially all six motes are placed at its genuine and legal location. Then an attacker captures the mote numbered as 1. He/ She forges the location related information for the mote 1. Intruder modifies context information of mote 1. After the relocation of mote 1, when it communicates with the command center or other motes, we can realize from the simulation readings that network performance attributes get effected because of such malicious activities. We have run the simulation for Location Spoofing attack for 15 minutes and have used the protocol CoAP for implementing Location Spoofing attack. Table 1 list out configuration settings authors have done for performing Location Spoofing attack in Cooja. Table 2 list out configuration settings authors have done for performing Identity Spoofing attack in Cooja.

Table 1. Configuration for Location Spoofing Attack in Cooja

Sr. No.	Parameter/ Property	Remarks
1	Number of Motes	6
2	OS	Contiki
3	Protocol	CoAP
4	Simulation Time	15 Minutes
5	Communication Range	50 m
6	Packet Size	127 bytes

Table 2. Configuration for Identity Spoofing Attack in Cooja

Sr. No.	Parameter/ Property	Remarks
1	Number of Motes	6
2	OS	Contiki
3	Protocol	RPL
4	Simulation Time	15 Minutes
5	Communication Range	50 m
6	Packet Size	127 bytes

Figure 1 represents screenshots of experiment performed by authors on Cooja simulator for implementing Location Spoofing Attack. It describes the behavior of motes before performing an attack and after the performing an attack.

For Identity Spoofing attack, Version IPv6 is considered of Internetworking Protocol. IPv6 has the address size of 128 bit. Because of this large address space more number of devices can become part of the network. We have considered mote 1 as an attacker mote, mote 6 as a border router mote and mote 2 as a victim mote. Mote 1 will send a spoofed DIS message to the Border router mote 6 and then the Border Router mote will modify its routing table. Mote 1 will bind its IP address with the MAC address of mote 2. Thus; it will attract all the traffic of Mote 2 towards itself by claiming illegal identity. Mote 1 will send probe message to remaining motes in the network and it will wait for the replay from other motes. If any other mote replay to mote 1, it signifies that mote which has passed replay message is in wake up mode. So, Mote 1 will leave that mote and will try for another mote. Mote 2 has not replied of probe message of Mote 1. It shows that Mote 2 is in sleeping mode currently. So, Mote 1 will spoof DIS message for this mote 2. And do the modification in IP-MAC address binding for this victim mote 2. After then, Mote 1 passes this spoofed DIS message to border router mote 6 for updating Neighbor Cache entry. So, all the traffic towards mote 2 now will be redirected towards mote 1. It means that Mote 1 will claim the identity of Mote 2. Figure 2 represents screenshots of experiment performed by authors on Cooja simulator for implementing Idenitty Spoofing Attack. It describes the behavior of motes before performing an attack and after the performing an attack.

RESULTS

Authors have considered the following three attributes for evaluation of performance results in the presence and absence of the Location Spoofing and Identity Spoofing attack: (1) Power Consumption (2) Throughput (3) Delay.

Figure 1. Screenshots for Location Spoofing Attack in Cooja

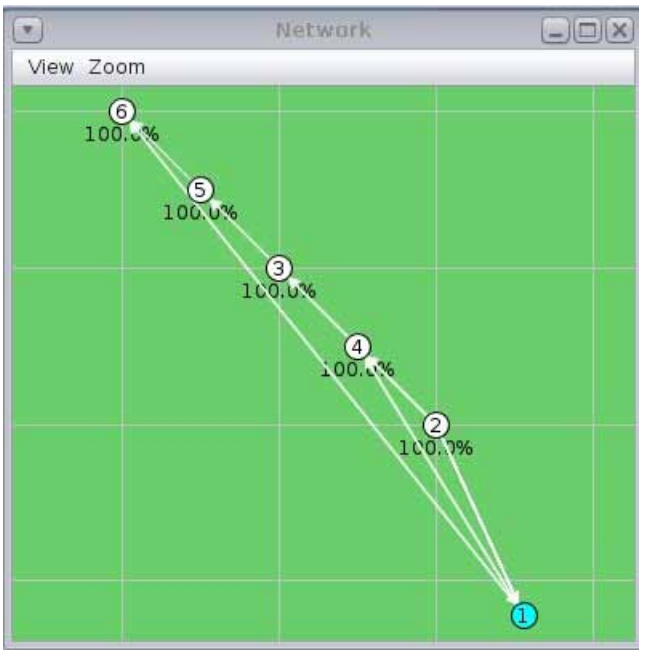
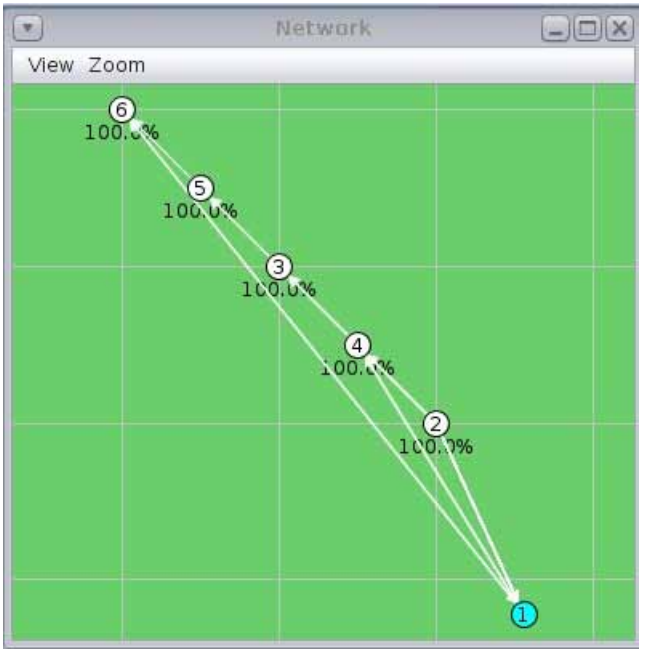


Figure 2. Screenshots for Identity Spoofing Attack in Cooja



Power Consumption: It is the amount of joules consumed to deliver the data from source to destination. Readings of the required amount of power for each scenario are noted down into the table 2 and 3. It clearly shows that when Location Spoofing and Identity Spoofing attacks take place in a network; power consumption will be high. Total Power Consumption can be calculated by using following formula:

$$E_T = E_{Tr} + E_{Rc} \quad (1)$$

where E_{Tr} is the amount of power required to disseminate the m bits of the data from source to destination mote and E_{Rc} is the amount of power required to receive the m bits of the data by the mote. Table 3 and Table 4 lists the readings recorded for the power consumption with in the network during simulation time. Recorded readings clearly signifies that Power consumption is less in the absence of Location Spoofing and Identity Spoofing attack. In the presence of these attacks, Power consumption is higher in the network because of malicious activities initiated by an Intruder. Table 3 represents effect of Location Spoofing attack on the Power Consumption attribute in IoT Network. Table 4 represents effect of Identity Spoofing attack on the Power Consumption attribute in IoT Network. Figure 3 represents Consumed Power Graph for 6 and 12 Motes for Location Spoofing Attack. Figure 4 represents Consumed Power Graph for 6 and 12 Motes for Identity Spoofing Attack.

Throughput: Throughput can be depicted as the measure of information going through a framework in a unit of time. In the IoT organization, the all-out number of sent information moderated in one moment to ascertain throughput. We ran for 15 minutes. Total 60 packets transmitted during this amount of time. Table 5 and Table 6 lists the readings recorded for the throughput calculation with in the network during simulation time. Recorded readings clearly signifies that throughput is higher in the absence of Location Spoofing and Identity Spoofing attack. In the presence of

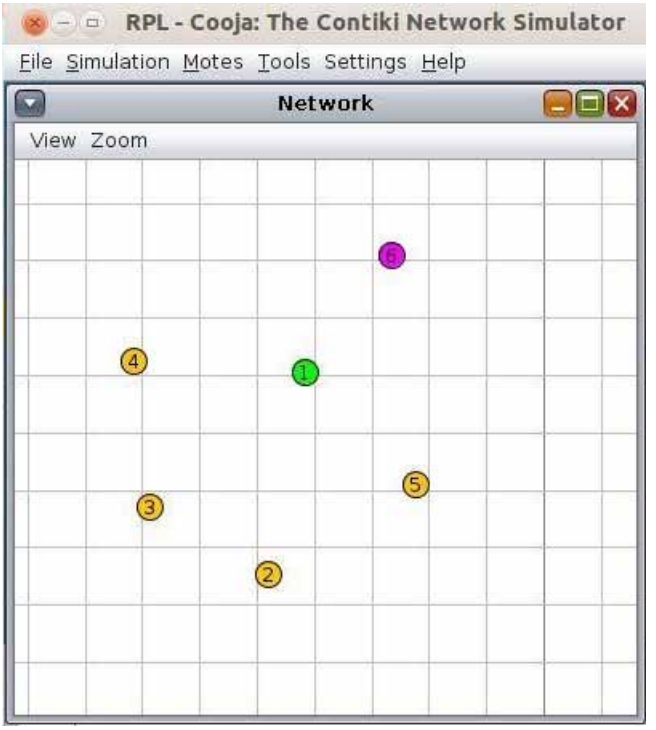
Table 3. Power consumption for 6 and 12 motes for Location Spoofing Attack

Power Consumption	Without Location Spoofing Attack (Power mW)	With Location Spoofing Attack (Power mW)
6 Mote	0.87	1
12 Mote	0.9	0.99

Table 4. Power consumption for 6 and 12 motes for Identity Spoofing Attack

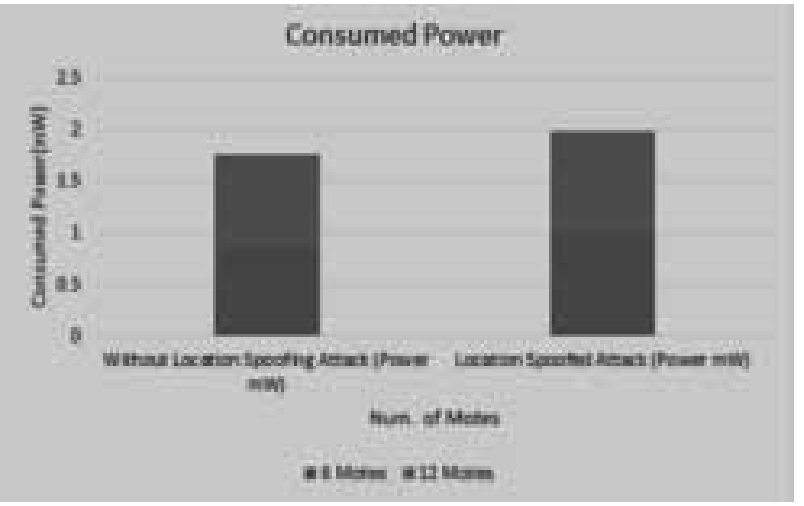
Power Consumption	Without Identity Spoofing Attack (Power mW)	With Identity Spoofing Attack (Power mW)
6 Mote	1.15	1.6
12 Mote	1.35	1.95

Figure 3. Consumed Power Graph for 6 and 12 Motes for Location Spoofing Attack



these attacks, throughput is lower in the network because of malicious activities initiated by an Intruder. Table 5 represents effect of Location Spoofing attack on the Throughput attribute in IoT Network. Table 6 represents effect of Identity Spoofing attack on the Throughput attribute in IoT Network. Figure 5 represents Throughput performance graph for 6 and 12 Motes for Location Spoofing Attack. Figure 6 represents Throughput performance graph for 6 and 12 Motes for Identity Spoofing Attack.

Figure 4. Consumed Power Graph for 6 and 12 Motes for Identity Spoofing Attack



Delay: It signifies the normal amount of time required to convey the packet from source to desired end mote in the network. It can be calculated by using following formula:

$$\delta = \sum_{k=1}^{n} \left(\frac{T_i^r - T_i^s}{n} \right) \tag{2}$$

where δ represents end to end delay time to deliver the packets, i denotes the number of packets and n is total number of received packets. T_i^r denotes the received time stamp for ith packet and T_i^s denotes the sent time stamp for ith packet. Table 7 and Table 8 lists the readings recorded for the end

Table 5. Throughput for 6 and 12 motes for Location Spoofing Attack

Throughput	Without Location Spoofing Attack (KBPS)	With Location Spoofing Attack (KBPS)
6 Mote	48	26
12 Mote	52	23

Table 6. Throughput for 6 and 12 motes for Identity Spoofing Attack

Throughput	Without Identity Spoofing Attack (KBPS)	With IdentitySpoofing Attack (KBPS)
6 Mote	50	30
12 Mote	55	15

Figure 5. Throughput Graph for 6 and 12 Motes for Location Spoofing Attack

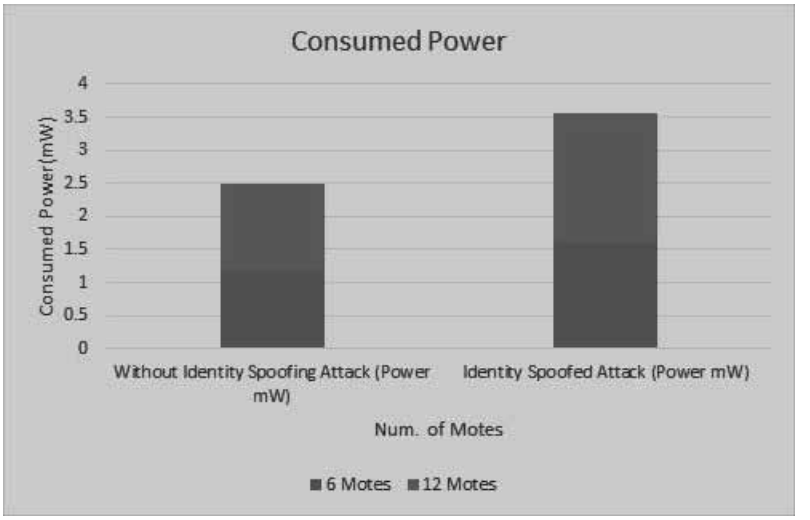
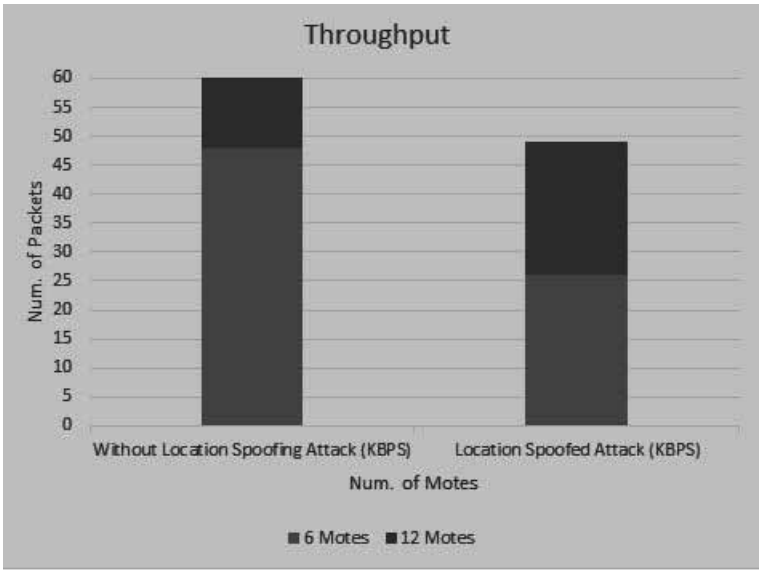


Figure 6. Throughput Graph for 6 and 12 Motes for Identity Spoofing Attack



to end delay calculation with in the network during simulation time. Recorded readings clearly signifies that end to end delay is less in the absence of Location Spoofing and Identity Spoofing attack. In the presence of these attacks, end to end delay is higher in the network because of malicious activities initiated by an Intruder. Table 7 represents effect of Location Spoofing attack on the delay attribute in IoT Network. Table 8 represents effect of Identity Spoofing attack on the delay attribute in IoT Network. Figure 7 represents delay attribute Graph for 6 and 12 Motes for Location Spoofing Attack. Figure 8 represents delay attribbute Graph for 6 and 12 Motes for Identity Spoofing Attack.

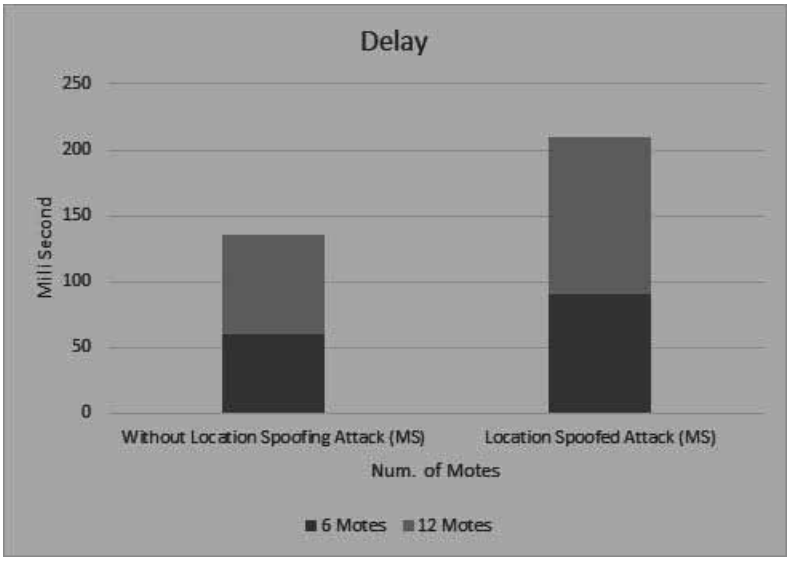
Table 7. Delay for 6 and 12 motes for Location Spoofing Attack

Delay	Without Location Spoofing Attack (ms)	With Location Spoofing Attack (ms)
6 Mote	60	90
12 Mote	75	120

Table 8. Delay for 6 and 12 motes for Identity Spoofing Attack

Delay	Without Identity Spoofing Attack (ms)	With Identity Spoofing Attack (ms)
6 Mote	70	100
12 Mote	90	125

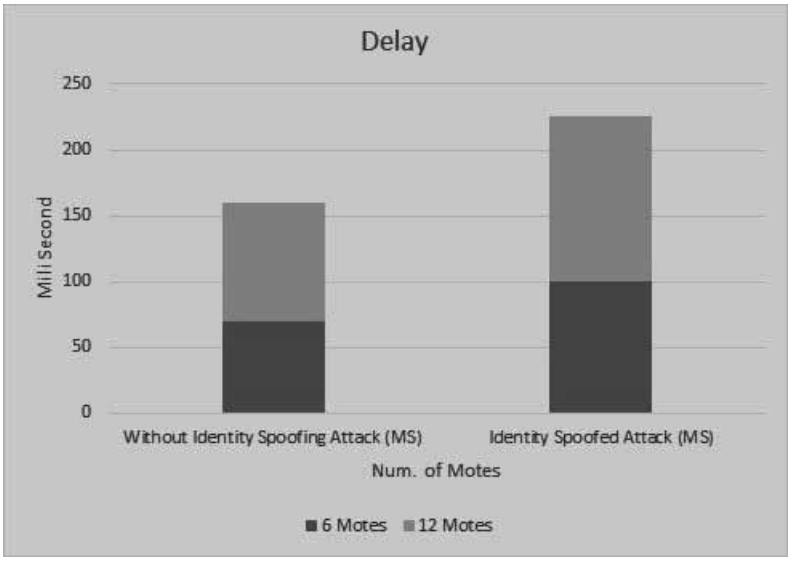
Figure 7. Delay Graph for 6 and 12 Motes for Location Spoofing Attack



CONCLUSION

IoT is the collection of various connected devices and things. It is widely used nowadays in various fields of society for the automation and decision making process. The usage of this advanced technology will not be beneficial to society without proper security safeguards. In this paper, we have experimented the impact of Location Spoofing and Identity Spoofing attacks on the performance of the network. We have simulated these attacks in the Cooja simulator and observed that in the presence of these both attacks; network performance degrades in terms of Power consumption, Throughput and Delay. Because of that, the lifespan of the IoT network also gets to decrease. It also leads to ambiguous device identification when we do not focus on Location Spoofing attack. So, it is very much necessary to identify and eliminate these types of threats from the network as early as possible during communication. In future research direction, researcher can propose a solution to address Location Spoofing attack and Identity Spoofing attack by designing a context aware multi

Figure 8. Delay Graph for 6 and 12 Motes for Identity Spoofing Attack



attribute authentication methodology. Researcher also can enhance features provided by RPL protocol to identify susceptive IP-MAC address binding entries and to eliminate those records from Neighbor cache (NC) to provide protection against Identity Spoofing threat.

REFERENCES

Alizai, Z. A., Tareen, N. F., & Jadoon, I. (2018). Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*. doi:10.1109/ICAEM.2018.8536261

Alotaibi, M. (2018). An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 70072–70087. doi:10.1109/ACCESS.2018.2880225

Aman, M. N., Basheer, M. H., & Sikdar, B. (2019). Two-Factor Authentication for IoT With Location Information. *IEEE Internet of Things Journal*, *6*(2), 3335–3351. doi:10.1109/JIOT.2018.2882610

Babaei, A., & Schiele, G. (2019). Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. *Sensors (Basel)*, *19*(14), 3208. doi:10.3390/s19143208 PMID:31330874

Bhattarai, S., & Wang, Y. (2018). End-to-End Trust and Security for Internet of Things Applications. *Computer*, *51*(4), 20–27. doi:10.1109/MC.2018.2141038

Chatterjee, B., Das, D., Maity, S., & Sen, S. (2019). RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning. *IEEE Internet of Things Journal*, *6*(1), 388–398. doi:10.1109/JIOT.2018.2849324

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).* doi:10.1109/I-SMAC.2017.8058363

Gope, P., & Sikdar, B. (2019). Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. *IEEE Internet of Things Journal*, *6*(1), 580–589. doi:10.1109/JIOT.2018.2846299

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 82721–82743. doi:10.1109/ACCESS.2019.2924045

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. *IT Professional*, *19*(5), 27–33. doi:10.1109/MITP.2017.3680960

Krishna, B. V. S., & Gnanasekaran, T. (2017). A systematic study of security issues in Internet-of-Things (IoT). *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC).* doi:10.1109/I-SMAC.2017.8058318

Loske, M., Rothe, L., & Gertler, D. G. (2019). Context-Aware Authentication: State-of-the-Art Evaluation and Adaption to the IIoT. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT).* doi:10.1109/WF-IoT.2019.8767327

Mohamad Noor, M. B., & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283–294. doi:10.1016/j.comnet.2018.11.025

Nandy, T., Idris, M. Y. I. B., Md Noor, R., Mat Kiah, L., Lun, L. S., Annuar Juma'at, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S. (2019). Review on Security of Internet of Things Authentication Mechanism. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 151054–151089. doi:10.1109/ACCESS.2019.2947723

Naveed Aman, M., Taneja, S., Sikdar, B., Chua, K. C., & Alioto, M. (2019). Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff. *IEEE Internet of Things Journal*, *6*(2), 2843–2859. doi:10.1109/JIOT.2018.2875472

Voas, J., Agresti, B., & Laplante, P. A. (2018). A Closer Look at IoT 's Things. *IT Professional*, *20*(3), 11–14. doi:10.1109/MITP.2018.032501741

Wang, N., Jiang, T., Lv, S., & Xiao, L. (2017). Physical-Layer Authentication Based on Extreme Learning Machine. *IEEE Communications Letters*, *21*(7), 1557–1560. doi:10.1109/LCOMM.2017.2690437

Wazid, M., Das, A. K., Odelu, V., Kumar, N., Conti, M., & Jo, M. (2018). Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet of Things Journal*, *5*(1), 269–282. doi:10.1109/JIOT.2017.2780232

Zhao, Y., Li, S., & Jiang, L. (2018). Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment. *Security and Communication Networks*, *2018*, 1–13. doi:10.1155/2018/9178941

Zhong, C. L., Zhu, Z., & Huang, R. G. (2017). Study on the IOT Architecture and Access Technology. *2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES).* doi:10.1109/DCABES.2017.32