Review On Detection and Prevention of attack in IOT

Shilpa Dhiman[1], Dr. SandeepHarit[2]
[12] *Department of Computer Science and Engineering*
Punjab Engineering College, Chandigarh, Chandigarh, INDIA

Abstract- Internet of Things (IoT) is associate degree rising conception which can interconnect billions of devices (such as smartphones, sensors and alternative networking devices), to speak with one another. IoT may be a system wherever objects embedded with detector technology to act with one another over wireless communication medium to come up with, exchange and transfer knowledge without human interaction. This interconnection is relevant in many ways like timely coordination with many simple devices such as sensors, thermostats, fitbits, routers etc. Due to open and heterogeneous nature of these networks, they are highly prone to vulnerable attacks. So privacy and security is the biggest concern in this technology. This paper focuses on common IoT vulnerabilities like Distributed Denial of Service (DDoS), Data modification attacks in background section.

I. INTRODUCTION

This study based on the routing attacks in the internet of things in which we study about the attacks and its types. IOT is basically an advance technology based of different types of resources connected together to share the information and data. In IOT network resources like power, storage capability, and computational processors.In wireless network devices the attacks are mainly affecting the functionality of network layer which is responsible for the routing in IoT. There are mainly two types of attacks which are occurred in the network.

(a) Active Attack: In active attack, attacker modifies the content of data which is exchanged in the network. In this process attacker can inject the new packets, drop the packets and modify the existing data packets. This type of attacks is very harmful for the network and the senders. It is further divided into two parts the attack done by the node which present in network is called internal attack and node which attack from outside is called external attack.

(b) *Passive Attack:* In passive attack, the attacker captures the data without altering of modifying it. This attack does not affect the normal working of the network this is the main difficulty reason in detection. This attack is done mainly to gather the information about the communication between the sender and receiver.The IOT network is used in various fields for the effective communication process in which user sends their information from one node to another node. Sometimes a user sends the secret information, data on the wireless network, it is very important to send this information very safely. In this network sensor nodes used wireless communication and it is easy to eavesdrop. The attacker can easily inject malicious messages into the network.

1.1 Types of Attacks in IoT

Various types of attacks are discussed below:

(a) Grey Hole Attack: This attack is modification of black hole attack. In this attack attacker node behaves like a normal node for discovering route in the network. After it discovers the route then it drop the infected packets in network. This attack is difficult to detect because packet is dropped with certainty [4].

(b) Wormhole Attack: In wormhole attack, the attacker can record the data packets at one location in the network and retransmit the data from another route of the data. Wormhole attack is a serious issue that occurred into the wireless sensor network. In the figure [1.3] the tunnel may be a wired link or wireless link between two nodes, this creates an illusion that the end point are very close to each other [2]. A wormhole attack has two modes.

- Hidden mode
- Participation mode

(c) Sink Hole Attack: in this attack incorrect information of the routing is send to the nodes as it is low cost and it provides proper destination node. Due to incorrect routing information it leads to packet loss and manipulation in original data packets.

This attack disturbs all the network process because nodes are sometime dependent on each other for information [4].

II. RELATED WORK

ChoudharySarika et al. [1] worked on the detection and prevention of the attacks on internet of things. This work based on the selective forwarding and sinkhole attack on the nodes. In this work two algorithms that are key matching algorithm and cluster based algorithm proposed to the detection and prevention purpose. The proposed algorithm helps to detect the malicious node and prevent from the attack with effective accuracy rate.Vidhya, et al. [2] worked on the detection of sinkhole attack in AODV routing. This method uses energy power consumption in AODV and external energy by using battery. In this work MD5 algorithm is proposed for sink hole attack detection which prevent the network from the sever attack. This algorithm checks the energy transmitted by the node to the other nodes. This algorithm work effectively and enhance the packet delivery rate and throughput. It reduces the end to end delay in the network.Jahandoust, et al. [3] described the adaptive sinkhole aware algorithm in wireless sensor network. This work is

based on the finding probability of affected nodes by sinkhole attack. In this the routing of the nodes is based on AODV protocols to route packets over the most reliable nodes. The subjective model identifies the behavior of the nodes in data receiving and sending. The behavior of whole network is observed by using probabilistic automation and captures the behavior of the network which is generated at the base station. The result of the proposed approach
provides low packet loss rate and effective routing between the reliable nodes.Kalnoor, et al. [4] worked on the clustered network in wireless sensor network to detect the sinkhole attack. This method is based on the agent-based quality of service to detect the sinkhole attack. The agent-based approach detects the attack effectively and enhances the network performance. Agent based protocol is very helpful to provides the effective performance and throughput.Ronen et al. [5] worked on the extended functionality attacks on the IoT devices. Taxonomy of attacks was produced to classify the attacks in four categories. The study based on the attacks on the smart lights and the effects of attacks. In the 1st attack lights were used as covert in the li-fi communication system to transfer the data from high secure office building. In this experiment an attacks was done on the smart lights and easily able to read the data from the available equipment. The testing of the communication system at lower end and high end and find the loopholes in the system. On the basis of these loopholes feasible solutions are provided to solve the problem.Jan, Mian Ahmad, et al. [6] proposed a light weight mutual authentication scheme to check the validity of the participating devices before starting its communication. This experiment mainly produces to check the security level of the devices and related products to them. The proposed method provides the safety against key fabrication, denial of service attack, and eavesdropping. The limitation of this work is that it does not able to provide the solution against the Sybil attack.Zhang, Kuan, et al. [7] worked on Sybil attack and its defense methods using different approaches and techniques. In this study, Sybil attack is defined in three different types that are SA-1, 2, and 3 according to the capabilities of the attacker. This study opened some research issues in the internet of things against Sybil attackers.

Table.1Existing Scheduling Model.

Author's Name	Year	Methodology Used	Proposed Work
ChoudharySarika et al.	2018	Key Matching Algorithm And Cluster Based Algorithm	Worked on the detection and prevention of the attacks on internet of things. This work based on the selective forwarding and sinkhole attack on the nodes.
Jahandoust, et al.	2017	Ad Hoc On-Demand Distance Vector (AODV) protocols	Described the adaptive sinkhole aware algorithm in wireless sensor network. This work is based on the finding probability of affected nodes by sinkhole attack.
Ronen et al.	2016	Smart Light Mechanism	Worked on the extended functionality attacks on the IoT devices. Taxonomy of attacks was produced to classify the attacks in four categories.
Zhang, Kuan, et al.	2014	Sybil Attack Mechanism	Worked on Sybil attack and its defense methods using different approaches and techniques.
Jan, Mian Ahmad, et al.	2014	eavesdropping	proposed a light weight mutual authentication scheme to check the validity of the participating devices before starting its communication. This experiment mainly produces to check the security level of the devices and related products to them. The proposed method provides the safety against key fabrication, denial of service attack, and eavesdropping. The limitation of this work is that it does not able to provide the solution against the Sybil attack.

Raza et al	2013	sinkhole and selective forwarding attack	worked on the intrusion detection in internet of things called SVELTE. The main focus in this work is to detect the sinkhole and selective forwarding attack. The proposed IDS worked like a mini firewall against the attacks on IOT nodes. The performance evaluation of the algorithm was based on the true positive rate, energy overhead, and memory consumption.
Salehi, S. Ahmad, et al.	2013	Sink Attack Mechanism	Proposed an algorithm to avoid the Sink-Hole attack.
Choi, Byung Goo, et al.	2009	sinkhole attacks	proposed an intrusion detection system and attach it of the wireless sensor network to detect the sinkhole attacks. In this work author studies and analyzed how sink hole attack is performed on the real network and uses MintRoute protocol. This protocol uses link quality metric to build the routing trees. By using tiny OS and proposed protocol sinkhole attack is detected effectively in random topologies also.

Salehi, S. Ahmad, et al. [8] in this paper, the author proposed an algorithm to avoid the Sink-Hole attack. In sinkhole attack, the intruder attracts the nearby nodes with unfaithful routing information, and presents change the data through these nodes. For detection of intruders in the sinkhole attack firstly finds the suspected nodes by analyzing the data. The proposed algorithm performance has been evaluated by the simulation process and it does provide the results with high accuracy. Raza, et al. [9] worked on the intrusion detection in internet of things called SVELTE. The main focus in this work is to detect the sinkhole and selective forwarding attack. The proposed IDS worked like a mini firewall against the attacks on IOT nodes. The performance evaluation of the algorithm was based on the true positive rate, energy overhead, and memory consumption.Choi, Byung Goo, et al. [10] proposed an intrusion detection system and attach it of the wireless sensor network to detect the sinkhole attacks. In this work author studies and analyzed how sink hole attack is performed on the real network and uses MintRoute protocol. This protocol uses link quality metric to build the routing trees. By using tiny OS and proposed protocol sinkhole attack is detected effectively in random topologies also.

III. CONCLUSION

IoT has created high expectations due to its capacity of transforming physical objects of different application domains into Internet hosts. However, attackers may also take advantage of the IoT great potential as a new way to threaten users' privacy and security. Therefore, security solutions for IoT should be developed. As in traditional networks, the IDS is one of the most important security tools for IoT.

IV. REFERENCES

[1]. Choudhary, Sarika, and NishthaKesswani. "Detection and Prevention of Routing Attacks in Internet of Things." *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018.

[2]. Saranya, P., Abin P. Varghese, and R. S. Balaji. "DETECTING AND PREVENTING THE WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORK." *traffic* 3.04 (2017).

[3]. Ma, Rui, et al. "Defenses Against Wormhole Attacks in Wireless Sensor Networks." *International Conference on Network and System Security*. Springer, Cham, 2017.

[4]. Saghar, Kashif, HunainaFarid, and Ahmed Bouridane. "Formally verified solution to resolve tunnel attacks in wireless sensor network." *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*. IEEE, 2017.

[5]. Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices: The case of smart lights." *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*. IEEE, 2016

[6]. Jan, Mian Ahmad, et al. "A robust authentication scheme for observing resources in the internet of things environment." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*. IEEE, 2014.

[7]. Zhang, Kuan, et al. "Sybil attacks and their defenses in the internet of things." *IEEE Internet of Things Journal* 1.5 (2014): 372-383.

[8]. Salehi, S. Ahmad, et al. "Detection of sinkhole attack in wireless sensor networks." *Space Science and* Communication *(IconSpace), 2013 IEEE International Conference on*. IEEE, 2013.

[9]. Raza, Shahid, Linus Wallgren, and Thiemo Voigt. "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad hoc networks* 11.8 (2013): 2661-2674.

[10]. Choi, Byung Goo, et al. "A sinkhole attack detection mechanism for LQI based mesh routing in WSN." *Information Networking, 2009. ICOIN 2009. International Conference on*. IEEE, 2009.