REVIEW ON DETECTION AND PREVENTION OF DDOS ATTACK IN MANET

Aaqib Rashid[1], Rubeena Sethi[2]
[1, 2]*ECE, ADESH INSTITUTE OF TECHNOLOGY GHARUAN MOHALI*

Abstract- Remote sensor systems (WSNs) are changing to genuine applications, where they confront assaults as of now experienced by the Internet and remote specially appointed systems. One such assault is that of forswearing of-benefit (DOS), which we accept will just turn out to be progressively predominant as sensor systems turn out to be increasingly unavoidable and available. With the innate asset confinements of WSN gadgets, they are especially vulnerable to the utilization and pulverization of these rare assets. We present a DOS assault scientific classification to distinguish the assailant, his capacities, the objective of the assault, vulnerabilities utilized, and the final product. We study vulnerabilities in WSNs and give conceivable guards. Ensuring WSNs against DOS assaults—while staying minimal effort and adaptable—is an essential research challenge that bears further investigation.

Keywords—*WSN, Detection, attack .preventation*

I. INTRODUCTION

Mobile adhoc network is a type of wireless network, which includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes [1] [2]. It is a network of devices that can communicate the information gathered by the wireless links. The data is forwarded through multiple nodes with a gateway and the data is connected to other networks like wireless Ethernet. These networks are used to control physical or environmental conditions like sound, pressure, temperature etc.

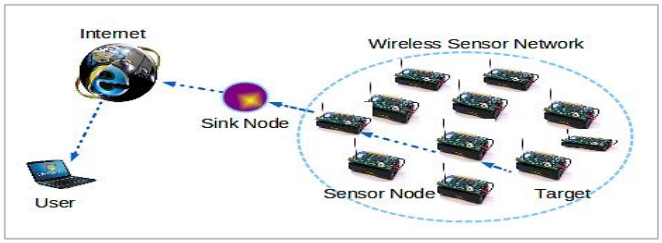

Figure 1:Mobile-adhoc-network

1.1 MANET Architecture

There are three main components in MANET: nodes, gateways and software. Spatially distributed measured node's interface with sensors to monitor assets. The collected data transmit to gateway wirelessly, and can operate independently. It is connected to a host system where we can collect data, process, analyze and present our measurement data by using software [3]. To extend MANET distance and reliability special type of measurement node is used such as router node. MANET is a widely used system because of its low costs and high efficiency. In a typical Mobile adhoc network (MANET), sensor nodes consist of sensing, communicating, and data processing components. Sensor nodes can be used in numerous industrial, military, and agricultural applications, such as transportation traffic monitoring, environmental monitoring, smart offices, and battlefield surveillance [4] [5]. In these applications, sensors are deployed in an ad-hoc manner and operate autonomously. In these unattended environments, these sensors cannot be easily replaced or recharged, and energy consumption is the most critical problem that must be considered. The sensor is a small device which is used to detect the amount of physical parameters, event occurring, measures the presence of an object and then it converts the electrical signal value according to need it actuates a process using electrical actuators [6].

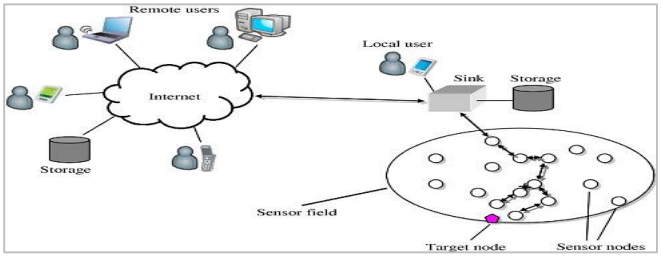

Figure 2: MANET Architecture

1.3 Attacks

In MANET, the attacks are mainly affecting the functionality of network layer which is responsible for the routing in MANET. There are mainly two types of attacks which are occurred in the mobile ad-hoc network.

1. 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 [7] [8]. 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.

2. 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.

3. 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 [9]. This attack is done mainly to gather the information about the communication between the sender and receiver.

1.3.1 Attacks on Mobile adhoc networks

Mobile adhoc 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.

Types of Attacks in MANET

1. 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 [9].

2. 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 Mobile adhoc network. In the figure 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 [10].

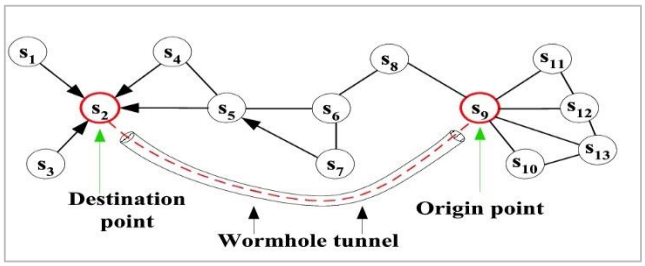

Figure 3: Wormhole Attack

A wormhole attack has two modes.

1. Hidden mode
2. Participation mode

3. DDOS 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 [10].

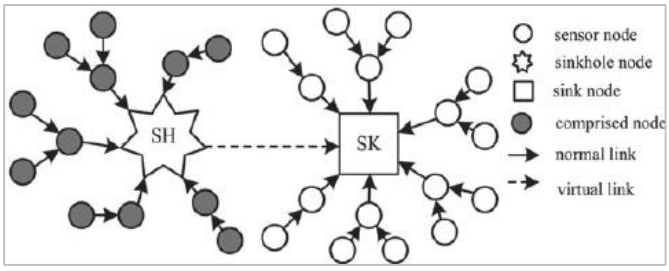

Figure 4: Sinkhole Attack

II. LITERATURE REVIEW

Zhang, Zhaohui, et al. [1] explained an energy efficient sinkhole detection approach which detects the malicious node effectively than the existing nodes. In this approach frequency of all nodes is established by m routes with optimal hops from per node to sink node. This method is based on the dynamic programming. This approach enhanced the detection rate and false positive rate.Devibala, K., et al. [2] proposed neighbor constraint traffic centric approach which is used to detect sinkhole attack and improve the quality of the MANET.It identifies the malicious node by the data send by neighbor node. It verifies the location of the node from where data is send to the node. This method provides sinkhole detection with high throughput and packet delivery ratio.Yasin, N. this work Acceptance Acknowledgement approach is used to Mohammaed, et al. [3] described the anomaly detection approach which detects the sinkhole attack in Mobile adhoc networks. This type of attack is not easy to detect due virtual path of the node. In activate the digital signature system. This approach does not make any impact on the network and provides high detection rate of the malicious node.Saghar et al. [4] proposed the RAEED protocol which is used to detect the simple and intelligent tunnel attacks. This protocol helps to reduce the problem of DOS attack which disturbs the data routing and forward the data comes from the sink node. In future this work will be enhanced by applying formal methods to verify the communication issues.Vidhya, et al. [5] 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 DDOS 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. [6] described the adaptive sinkhole aware algorithm in Mobile adhoc 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. [7] worked on the clustered network in Mobile adhoc 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.Tan, Shuaishuai et al. [8] in this paper, the author proposed optimized link state routing mechanism to solve the issues of attacks in the Mobile adhoc network. In this protocol trust based mechanism is used with fuzzy rules to evaluate the trust values of the mobile nodes. This algorithm selects the route on the basis of maximum path trust value between the nodes. To evaluate the trust of nodes trust factor collection method is used. It generates only relevant information and do not generate extra control messages. In results it enhances the packet delivery ratio and latency and reduced the network overhead. Choi, Byung Goo, et al. [9] proposed an intrusion detection system and attach it of the Mobile adhoc network to detect the sinkhole attacks. In this work author studies and analyzed how DDOS 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. Krontiris, Ioannis, et al. [10] proposed sinkhole detection on the basis of LQI in meshed routing network. Sinkhole attack can also modify in various type of attack. The attack can be detected by using few detector nodes.

Table.1 Literature Inferences

Author's Name	Year	Methodology Used	Proposed Work
Zhang, Zhaohui, et al.	2018	Dynamic Programming	Explained an energy efficient sinkhole detection approach which detects the malicious node effectively than the existing nodes.
Mohammaed, et al.	2017	Acknowledgement Approach	Described the anomaly detection approach which detects the sinkhole attack in Mobile adhoc networks.
Vidhya, et al.	2017	MD5 Algorithm	Worked on the detection of sinkhole attack in AODV routing.
Jahandoust, et al.	2017	Probabilistic Automation	Described the adaptive sinkhole aware algorithm in Mobile adhoc network.
Tan, Shuaishuai et al.	2015	Trust Based Mechanism	Proposed optimized link state routing mechanism to solve the issues of attacks in the Mobile adhoc networks.
Choi, Byung Goo, et al.	2009	MintRoute protocol	Proposed an intrusion detection system and attach it of the Mobile adhoc network to detect the sinkhole attacks.

IV. REFERENCES

[1]. Zhang, Zhaohui, et al. "M optimal routes hops strategy: detecting sinkhole attacks in Mobile adhoc networks." *Cluster Computing* (2018): 1-9.

[2]. Devibala, K., et al. "Neighbor constraint traffic centric distributed sinkhole detection and mitigation approach for quality of service improvement in Mobile adhoc networks." *Industry Interactive Innovations in Science, Engineering and Technology*. Springer, Singapore, 2018. 357-366.

[3]. Yasin, N. Mohammaed, et al. "ADSMS: Anomaly Detection Scheme for Mitigating DDOS attack in Mobile adhoc network." *Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference on*. IEEE, 2017.

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

[5]. Vidhya, S., and T. Sasilatha. "Sinkhole Attack Detection in MANET using Pure MD5 Algorithm." *Indian Journal of Science and Technology* 10.24 (2017).

[6]. Jahandoust, Ghazaleh, and FatemehGhassemi. "An adaptive sinkhole aware algorithm in Mobile adhoc networks." *Ad Hoc Networks* 59 (2017): 24-34.

[7]. Kalnoor, Gauri, JayashreeAgarkhed, and Siddarama R. Patil. "Agent-Based QoS Routing for Intrusion Detection of Sinkhole Attack in Clustered Mobile adhoc networks." *Proceedings of the First International Conference on Computational Intelligence and Informatics*. Springer, Singapore, 2017.

[8]. Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "Trust based routing mechanism for securing OSLR-based MANET." *Ad Hoc Networks* 30 (2015): 84-98.

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

[10]. Krontiris, Ioannis, et al. "Intrusion detection of sinkhole attacks in Mobile adhoc networks." *International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics*. Springer, Berlin, Heidelberg, 2007.