Novel method for Isolation of Wormhole Attack in MANET

Prabhat kiran Thakur
Research Scholar
nidhithakur64@gmaul.com
Doaba Group of Colleges, Kharar, Mohali

Moniderpal kaur
Assistant Professor
monugill22@gmail.com
Doaba Group of Colleges, Kharar, Mohali

Abstract - Wireless adaptor is also known as wireless clients. It has a central controller. Ad hoc mode is connecting wireless clients directly without the need of access point and wireless router. It has no central controller so it is called infrastructure less mode. Many kinds of attack can be done on this type of networks. In this we studied the wormhole attack and to secure the path of the packets from this attack using delay per hop method and isolate the node that is the cause of the wormhole attack in the network. This method neither used the synchronized clocks nor the special kind of hardware for detecting the wormhole. With the help of hop count method and using the AODV routing protocol we can detect the malicious node and a new path is formed to pass the packets to their destinations. This works will help to reduce the problem occurring for the cause of packet loss problem in the network and also helps to improve the performance of the network.

Keywords - MANET, AODV, Wormhole, Path establishment

I. INTRODUCTION

A network is a group of two or more computer systems which linked together. It is mode of exchange of information to communicate with one another. It is a connection of computer devices which are attached with the communication facilities. The physical connection between networked computing devices is established using either cable media or wireless media. Internet is the best-known computer network. When number of computer are joined together to exchange information they form networks and share resources. Networking is used to share information like data communication. Sharing resources can be software type or hardware types. It is a central administration system or can support these types of system. The ad hoc network is a decentralized type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. The ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it’s a network which is used in urgent situation causes. No fixed infrastructure in ad hoc network like base stations is required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. In routing each node participates by forwarding data for other nodes in ad hoc network the determination of which nodes forward data is made dynamically on the basis of network connectivity. The wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. All the nodes act as router in ad hoc network. MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. They have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topologies are used. An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. In the absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., they can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes.

As MANETs are illustrate by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes, topology changes and unreliable communication in the design. There are many types of protocol are available in MANET. Its efficiency of a routing protocol is determined by its battery power consumption of a participating node and routing of traffic into the network. Mobile Ad hoc Network is a mobile multi-hop which is wireless distributed network and self-organized in nature. The primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes. In MANET, constantly changing network topology causes link breakage and invalidation of end-to-end route. There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols. In MANETs, collection of mobile nodes may dynamically vary the topological structure. With respect to the more widely used mobile cellular networks. Mobile Ad Hoc Networks do not use any form of fixed infrastructure or centralized administration. These types of networks have the salient characteristics: dynamic topologies, bandwidth constraints, variable capacity links, limited physical security and energy –constrained operations.

II. LITERATURE SURVEY

A.vani, et.al (2011) presented in this paper [11] the infrastructure of a mobile ad hoc network (MANET) has no router for routing, and all nodes must share the routing protocol to assist each when transmitting messages. However, almost all common routing protocol at present consider performance as first priority, and have little defense against attack, he wormhole attack poses the greatest threat and is very difficult to prevent; therefore, this paper focuses on the wormhole attack poses the greatest threat and is very difficult to prevent; therefore this paper focuses on the wormhole attack, by combing three techniques. So that our purposed scheme has three techniques based on hop count, decision anomaly, neighbor list count method are combined to detect and isolate wormhole attacks in adhoc networks. That manages how the nodes are going to behave and which to route the packets in secured way.

Y. Xu, et.al (2007) proposed in this paper [14] a distributed wormhole detection algorithm for wireless sensor networks, a potential technology for infrastructure of many applications. Currently, most sensor networks assume they will be deployed in a benign environment; however, when a sensor network is deployed in some hostile environment, attack (especially those like wormhole attacks that don't need to capture the keys used in the network) sensor may affect current sensor network and may even disable their functions. This paper proposes a distributed wormhole detection algorithm called Wormhole Geographic Distributed Detection (WGDD) that is based on detecting disorder of the networks which is caused by the existence of a wormhole inside the network. Since wormhole attack are passive, this algorithm uses a hop-counting technique as a probe procedure to detect wormhole attacks, then reconstructs local maps in each node, and after that, uses a feature called "diameter" to detect abnormalities caused by wormholes. The main advantage of using a distributed wormhole detection algorithm is that such an algorithm can provide the approximate location of a wormhole, which may be useful information for further defense mechanisms. Simulation shows that the proposed detection method has both a low False Toleration Rate (FTR) and a low False Detection Rate (FDR) in detection wormhole attacks.

Mohan Seth, (2013) presented in this paper [7] the Wormhole attacks can destabilize or disable wireless sensor networks. In a typical wormhole attack, the attacker receives packets at one point in the network, forwards them through a wired or wireless link with less latency than the network links, and relays them to another point in the network. This paper describes a wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. The two characteristics to keep tracks of all its neighboring nodes and checks are done when a node is received from its neighbor or not. The main advantage of the algorithm is that it can provide the approximate location of wormholes, which is useful in implementing countermeasures.

K. Nirmaladevi, et.al (2023) projected [23] a Trustable Energy-based Clustering and Optimized Routing (TECROP). It was a Selfish Node-aware Trustable and Optimized Clustering-based Routing (SN-TOCRP) algorithm in which hierarchical clustering was adopted for creating node clusters. The Fuzzy based Crow Search Algorithm (FCSA) was generated for choosing cluster Heads (CH). The authentication technique was utilized to detect the selfish node so that CHs were authenticated. The Bandwidth-aware Trust-based Routing Protocol (BTRP) method was implemented for detecting and isolating mischievous and faulty nodes. The Modified Glow swarm optimization (MGSO) was effective for estimating the trust. The projected approach secured the network concerning packet delivery ratio (PDR) up to 96%, loss ratio around 0.045%, average delay of 0.325 ms with throughput up to 76 Kbps, end to end delay (EED) around 0.425 ms and energy usage of 88 mJ.

S. Shafi, et.al (2023) investigated a [24] Machine Learning and Trust Based AODV Routing (ML-AODV) which alleviated the flooding and blackhole attacks in Mobile Ad hoc Network (MANET). The primary task was to estimate the trust for selecting the supportive intermediate nodes in the network at every node to avoid the flooding assault. This model aimed to select nodes of highest trust value for exploring the Blackhole intrusion. The energy disparity and delay were eliminated after finding the finest optimal path for transmitting the packet. For this, machine learning (ML) based Artificial Neural Network (ANN) with Support Vector Machine (SVM) algorithm was employed. The investigated model was capable of maximizing the throughput up to 4% and reliability by 44%, and alleviating delay by 12%, overhead by 15%, packet loss ratio (PLR) by 10%.

R. Prasad P, et.al (2021) developed an [25] Enhanced Energy Efficient-Secure Routing (EEE-SR) method to access the secure data in antagonistic climate. The data was broadcasted securely in the network by associating the nodes with security policy. The nodes selected for transmitting data were helped in revealing their validation and the accessible energy threshold was considered at the nodes to select routing path in the set-ready which sent packets in the network. The shortest path was adopted in network for determining the reliability of nodes while managing the trust. This method was proved applicable to prolong the life span of network and diminish the energy usage, packet loss and end-to-end delay (EED).

III. RESEARCH METHODOLOGY

The advantage of Delphi is that it does not require clock synchronization and position information and it does not require the mobile nodes to be equipped with some special hardware, which in turn provide higher power efficient.

The Disadvantage of Delphi method is it cannot pinpoint the wormhole location. This disadvantage of Delphi method can be overcome by using Wormhole Geographic Distributed Detection which is an another method to detect the wormhole attack dependent on the existence of disorder in the network.

- We deployed the wireless ad hoc network in a fixed area and with the fixed number of nodes, the network deployed in decentralized in nature and each node is capable of moving freely from one to the other location.
- After deploying the wireless ad hoc network we established the path from the source to the destination with the help of the AODV routing protocol.
- The source node floods the route request packets in the network for the path establishment to the destination and the adjacent nodes of the destination will reply back to the source node with the route reply packets
- After the sending of the route request packets and the route reply packets, we select the best path from the paths for sending the packets from the source to the destination.
- The malicious node existing in the path which will trigger wormhole attack and is responsible to increase the delay between the source and destination.
- By calculating the delay per hop for each node existing in the path the malicious node is detected.
- We trace the neighbor of each node in the network and its distance from the source node. This helps to find out the location of the node responsible for the wormhole attack.
- Then the malicious node is removed from the network and new path is formed from the source to the destination to send the data packets.

After this we further plotted the three graphs of throughput, energy loss and packet loss for both the scenarios that are with and without the wormhole attack in the network. The results showed the great differences.

IV. RESULT AND DISCUSSION

Network Simulation is an event based simulator. The network simulator is discrete event packet level simulator. It covers a very large number of different kinds of protocols application of different types of applications and packets. In it scripting language is used. It contains "NAM" files through which animation is run.

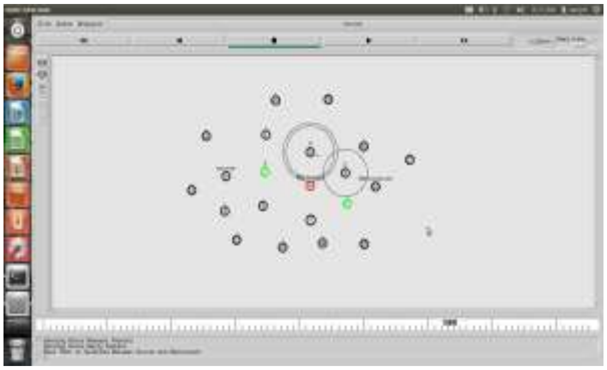


Figure 1: Isolation of attack

As shown in figure 1, the wireless adhoc network is deployed in the fixed area and with fixed number of nodes. The network is the decentralized type and nodes can move freely from one location to other location. The AODV routing protocol is used to establish path from source to destination. The source node flood route request packets in the network for path establishment to destination. The adjacent nodes of destination will reply back to source node with the route reply packets. The best path will be selected between source and destination. The malicious node exits in the path which will trigger wormhole attack and increase delay between source and destination. The delay in the established path will be increased and using the position used detection technique malicious node detected and isolated from the network

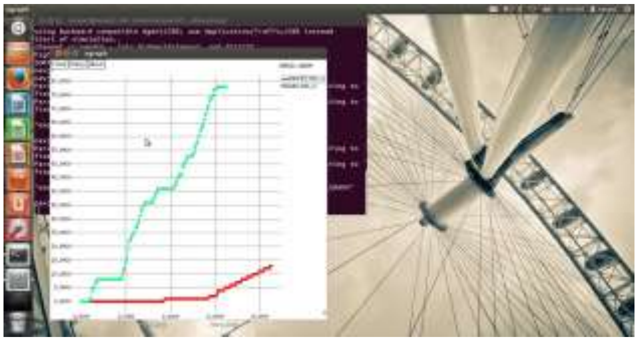
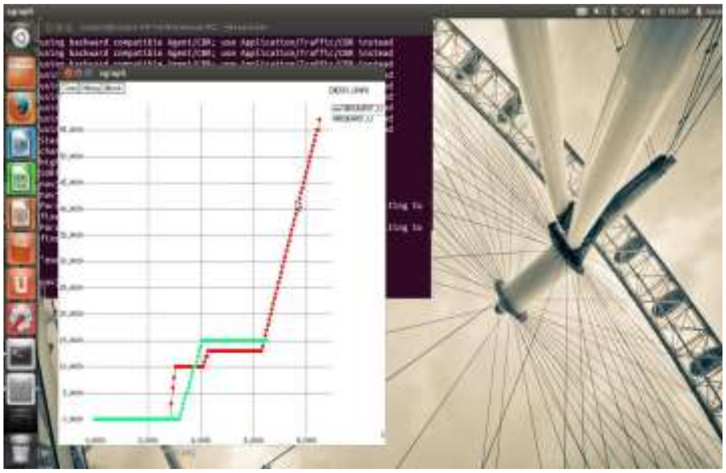


Figure 2: Packets loss graph

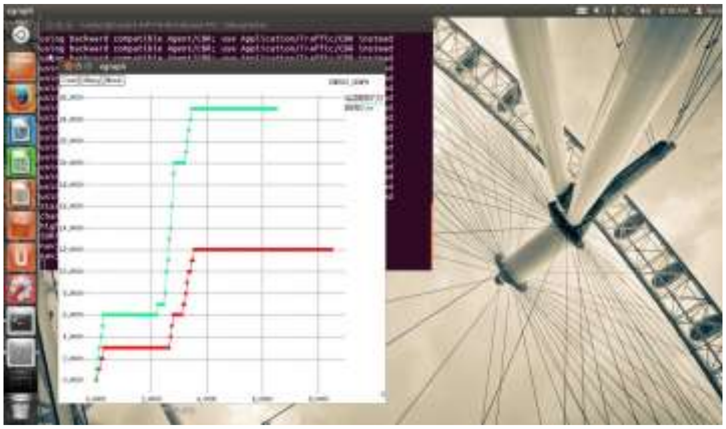
As illustrated in figure 2, the packetloss graph is shown in packetloss of attack scenario and packetloss in isolation scenario is shown. When the attack will be isolated from the network packetloss will be reduced



```
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
```

Figure 3: Throughput graph

As shown in figure 3, the throughput of attack scenario and isolated scenario is shown. When the attack will be isolated from the network throughput will be increased.



```
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
```

Figure 4: Delay graph

As illustrated in figure 4, the delay of the attack scenario and isolated scenario is show. The delay in the attacked scenario will be increased and attack in the new scenario will be reduced.

V. CONCLUSION

When the mobile nodes are mutually true, it leads to the reliable data transmission between the mobile nodes. But the main problem occurs during the drop of the packet. Drop of the packet is due to wormhole attack. Throughput sensitive wormhole attack is due to the drop of the packet. In this malicious node drop the packet so that it cannot be reach destination. By using ICMP packets nodes goes to the monitor mode. Here other nodes also available than malicious nodes which detect the packet dropping and redirect them to the source node. So here low performance of system can be improved by prevent them from internal attacks i.e. by detecting packet dropping. Due to packet drop, path is lost easily. In proposed work, monitoring node concept is important in throughput sensitive wormhole attack. This is designed to find out the packet drop nodes and those nodes are then isolated from the path forming a new path for the sending the packets to its destination. This work will help to reduce the problem occur in link failure and packet lost problem. Now the performance degradation problem will also improve.

VI. REFERENCES

[1]. A.vani, D.Sreenivasa Rao, “Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing in Ad Hoc Wireless Network”, 2011, International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 6, pp- 561-578.

[2]. Yurong Xu, Guanling Chan, James Ford, Fillia Makedon. F, “Distributed wormhole attack detection in wireless sensor networks”, 2007, Research Gate, volume 9, issue 3, pp- 145-159

[3]. Mohan Seth, “Detection of WormHole Attacks in Wireless Sensor Networks”, 2013, IEEE, volume 9, issue 3, pp- 193-205

[4]. K. Nirmaladevi and K. Prabha, “ A selfish node trust aware with Optimized Clustering for reliable routing protocol in Manet”, Measurement: Sensors, vol. 84, no. 6, pp. 751-756, 16 January 2023

[5]. S. Shafi, S. Mounika and S. Velliangiri, “Machine Learning and Trust Based AODV Routing Protocol to Mitigate Flooding and Blackhole Attacks in MANET”, Procedia Computer Science, vol. 218, no. 1, 2309-2318, 31 January 2023

[6]. R. Prasad P and Shivashankar, “Enhanced Energy Efficient Secure Routing Protocol for Mobile Ad-Hoc Network”, Global Transitions Proceedings, vol. 10, no. 2, pp. 126580-126592, 14 October 2021