The Novel Scheme for Isolation of Malicious Nodes from Mobile Ad-hoc Networks

Shivani , Munish Katoch

Research scholar, Assistant Professor

Deptt. Computer Science Sri Sai University Palampur

Abstract

In MANET different mobile nodes are connected through wireless link. MANET distinctive mobiles are linked through wireless link every mobile are loose to transport i.e. no crucial controller to be had. In MANETs, collection of cellular nodes may dynamically vary the topological shape. With recognize to the extra extensively used ad Hoc Networks do not use any shape of constant infrastructure or centralized administration those forms of networks have the salient characteristics: dynamic topologies, bandwidth constraints, variable capability hyperlinks, confined bodily safety and electricity –confined operations. There are different types of attacks in MANET. Sinkhole and Wormhole attacks is one of the sorts, in this type of attacks node transfer from other course in place of path assigned to supply and vacation spot. So misplaced of statistics is viable. . In this research work, the novel scheme is proposed which detect and isolation malicious nodes from the network. The proposed technique detect and isolate the attacker node using different techniques such as watchdog technique, which detect the malicious nodes by using ICMP. The malicious nodes are responsible to trigger wormhole and sinkhole attack in the network. The proposed technique is carried out in NS2 and simulation outcomes suggests that proposed technique performs properly in comparison to different techniques.

KEYWORDS:

MANET, Wormhole Attack, sinkhole Attack, AODV, Security, NS2.

1 Introduction

MANET is a type of ad hoc network and does not require any infrastructure for forwarding the data packets from one end to another. It is an ad hoc network and simply known as the mobile ad hoc network and self-ordered, continuous, less complicated infrastructure as compared to

wireless sensor network. Both mobile and ad hoc network consists of flat infrastructure network[1]. MANET contains a sharable medium which has high demand in radio communication. The architecture of the MANET is somewhat like a computer or nodes in which the devices act as the router and the end host. In MANET the connected devices and the nodes are independent from one another [2]. It has an attractive topological architecture and promotes the easy mobility. The node act as the router and they route r transmit the packet from one node to the other. The network that uses wireless links for connecting the mobile routers and has no access points in it is known as MANET. There are autonomous mobile devices deployed in this network. The mobility of these devices is free and they can arrange on their own in arbitrary manner [3]. A wireless medium is shared by the nodes and erratic and dynamic changes can be observed in the topology. Since the nodes are allowed to move to any location in these networks, it is very frequent to break the communication link. These are the set of rules used to navigate the path of the packet data from source to the destination in any wireless network [4]. Proactive Routing is also known as the table driven routing protocol. It maintains the routing table which contains information regarding network's architecture. It is quite useful for the datagram traffic and collects substantial signal traffic and power consumption. The reactive routing is also known as the demand routing protocol and it is used to discover protocol route whenever required. The route discovery is set up by the node on the basis of their demands. The features of hybrid routing are inherited from reactive as well as from the proactive routing protocols. It basically tries to ruin the reduced controlled traffic from proactive systems. The discovery of route is delayed by the maintenance of the routing table. It is very difficult to secure the wireless ad hoc networks. To develop good security solutions, initially it is important to understand the possible form of attacks [5]. The information can be transmitted securely by ensuring security of communication in MANETs. As compared to the wired networks, it is more likely for cyber attacks to enter the MANETs due to the unavailability of any central co-ordination approach and shared wireless medium. The main objective and purpose of the ad hoc network and MANET networks is spread the network globally and use it as commercial and domestic application purposes but it is most important issue in case of research. The researchers are still doing work on this in order to make it more secure and protective. MANET has so many applications from simple wireless home network and office networking to the sensor networks and tactical network environments. The security of networks plays very important role in the development of any network [6] in which the vulnerabilities are inherited from the radio communication to routing, man-in-middle and other injected attacks. Worm Hole Attack is cosmological term; it connects two different points in space through shortcut route. Similarly, like a WSN, MANET consists of one or more attacking node which distorts the routing by ruining the circuit of the network and therefore disturbing the normal flow of the delivery packets. When this link becomes the cheapest cost path to the desired location the malicious nodes are selected and send the packets to the desired location [7]. The attacking node either checks the traffic or disrupts the flow. Wormhole attack enters in the network with the single node but sometimes with two or more than two malicious nodes which are connected through a wormhole link. In case if a packet is to

be transmitted, the packet header is updated and the identity is encapsulated by the nodes [8]. Closed Wormhole Attack causes no affect on the packet header when the route discovery is performed. Therefore, the existence of this attack is not known by the legitimate nodes. In Half Open Wormhole Attack the legitimate nodes can see one malicious node since within the packet header, the entries are updated and there is no visibility of other node[9].

The main aim of this research paper is to isolate and detect the malicious node from the mobile ad-hoc network and prevent it from the network, and detect the sinkhole and wormhole attack in the network. And to improve the using routing protocol.

The organization of this research paper is the literature reviews for isolations of sinkhole and wormhole are introduce in section 2. The methodology which are used in the proposed work are introduce in section 3. The experimental result of proposed work and comparison between existing work in section 4. And the last section 5 is conclusion and future scope.

Literature Review

Harsányi et al. [10] proposed a new approach through which the wormhole attacks can be identified from the networks. Also, any kinds of nodes that are affected through this attack are also needed to be identified here. Utilizing any special measurement is not to be included within this approach. The connectivity information is to be applied here. For detecting wormhole attack in WSNs, a novel approach is proposed in this paper. Before the occurrence of attack there is no need of special hardware, guard nodes or any statistical information of network in case of proposed approach. Further, this approach does not need any costly calculations. With the help of performing several tests along with several communication models and methods, the effectiveness of proposed algorithm can be achieved.

Majumder et al. [11] proposed a novel approach based on the AD of statistical approach such that the wormhole attack can be avoided as well as prevented to enter the network. Within this proposed algorithm, there is no need to include any extra resources such as GPS. It is thus assumed here that the closeness of nodes to destination is more when the fake path is chosen to transmit packets from source to destination. For preventing the wormhole attack from entering the network, the calculation of time consumed is important to be calculated. As per the simulations performed it is seen that absolute deviation technique provides better results than AODV. The wormhole attack can be detected within very less time by the absolute deviation covariance and correlation. This approach also helps in measuring the packet drop pattern.

Rmayti et al. [12] proposed a novel mechanism which can be applied to check whether a wormhole attack is present in the assumed shortest path or not. The fact that the length of path is minimized when a wormhole tunnel passes through it is considered as a base to propose novel approach. Any kind of specific hardware or clock synchronization is not required here. Only the information that is being exchanged amongst various nodes is required. Thus, it is seen that when the length of wormhole tunnel is known and there is a well selection of the value of detection

threshold, the detection rate of malicious nodes is high as per the simulation results achieved. Further, when the length is greater than 4 hops, all the wormhole links can be detected easily by the proposed model.

Thanuja et al. [13] proposed a novel approach for improving the security of existing methods which will result in enhancing the overall performance of network. For the detection and prevention of vulnerabilities of MANETs in correct manner, a Black Hole detection behavior and wormhole detection behavior approaches are combined within the proposed algorithm. In close wormhole attack, the source and the destination node are made to believe that they are one step away from one another. Wormhole attack is happened due to the modification of the contents so that the nodes lies between them are unaware about this wormhole attack. Each node has to forward to it to another node in the tunnel, thus ending up in the packet drop.

Ali et al. [14] proposed a novel approach by combining RSA and symmetric key which is known to be a cryptographic approach. It is possible to broadcast the packets from one node to rest of the nodes in a secure and efficient way by applying this proposed mechanism. The shared key and identifier (ID) of the nodes is distributed through this RSA technique. In this two or more than two malicious nodes makes the tunnel and forwards the data packets from one malicious node to another from one end of the tunnel to the other and finally these packets are broadcasted to the network. These malicious nodes will ruins the working of the network due to the dynamic and mobility nature. This attack creates a secret tunnel inside the network; from here all the data can be extracted.

Proposed Methodology

In MANET the security issues are always causes the data delay problem and packet loss. but the principal problem occurs for the duration of 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 some other nodes also available than malicious nodes which detect the packet dropping and redirect them to the source node. So here low performance of the system can be improved by prevent them from internal attacks i.e. by detecting packet dropping. Only the simple mobile nodes are not sufficient to isolate the malicious node and to detect the sinkhole and wormhole attack in the mobile ad-hoc network. Hence to isolate and prevent the wormhole and sinkhole in the network by watchdog technique, the delay of each node is calculated by connectivity factor of each node. The node which is increased delay maximum the defined delay is detected as the malicious node. The proposed methodology are modify the existing routing protocol in which the whole nodes are alert in network. The proposed

technique take less time to detect the malicious node from the network, To detect the malicious node the technique is based on per hop delay, and the per hop delay is calculated on the basis of round trip time. This is designed to find out the malicious node. This work will helps to reduce the problem arise in hyperlink failure and packet misplaced trouble. Now the performance degradation problem will also improve.

Overview of Proposed System

The proposed advanced routing protocol has able to isolate the bath attacks- sinkhole and wormhole attack. Sinkhole attack, the intruder node/malicious node sends fake routing information claiming that its associated an optimum route to the target that causes different nodes within the Ad Hoc Network to route data packets through it. A wormhole attack can easily be launched by attacker without having knowledge of the network or compromising any legitimate nodes or cryptographic mechanism. Wormhole attack the tunnel is either the wired link or a high frequency links. This creates the illusion that the two end points of the tunnel and very close to each other. . The rounds trip time is calculated on the basis of time when the source send the route request packets and when the source receives reply message. The source node selects the best path on the basis of hop count and sequence number. The source starts sending the data on the selected path. The source analyzes the network parameters for the detection of malicious node.

$$\text{Threshold delay} = \frac{Round\ trip\ time}{2P} = \frac{ti - ts}{2P} \quad \text{--- (1)}$$

The round trip time is calculated with the ti and ts which are time of sending route request packets and time of receive route reply packets

The delay at each hop is calculated with the equation number 2

$$\text{Delay} = \sum_{i=0}^{i=n} Packet\ arrive\ time - Packet\ send\ time \,/ \sum_{i=o}^{i=n} number\ of\ connection \quad \text{--- (2)}$$

When the delay is higher than the threshold delay, then sensor node is considered as the malicious node.

When the malicious node is detected from the network then the source node will send alert message to each node in the network. When the node receives the alert message, it will remove the malicious node from the path. The technique which is proposed in this research work, is efficient in terms of complexity and also various congestion values are included for the detection of malicious nodes.

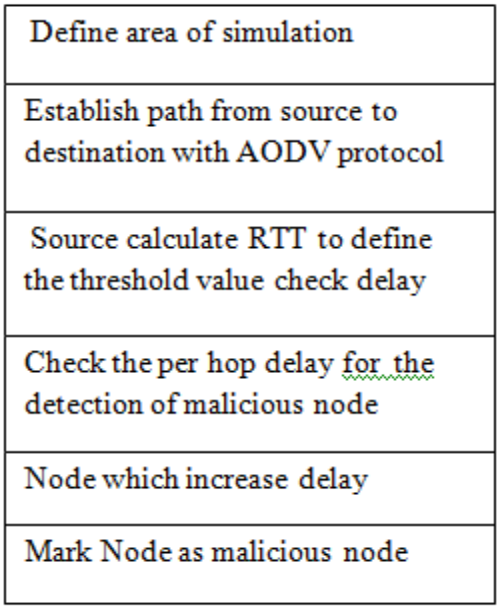

Figure:1. Process Flow of Detection of Malicious node

Step 1: In the first step, the network is deployed with the finite number of mobile nodes. The mobile nodes have predefined configurations

Step2: In the second step, the path is established from the source to destination with the reactive routing protocol. The per hop delay will be checked on the selected path for the detection of malicious nodes

Step 3: In the third step, per hop delay will be checked and if any node is increasing per hop delay, then that will be detected as the malicious node.

Step 4: In the last phase, the, malicious node will be isolated from the network. The technique of multipath routing will be applied for the isolation of malicious node

Experimental Results

The Proposed technique is implemented in AODV routing protocol. The experimental result of proposed technique is detect and mitigation of wormhole and sinkhole attack. The performance of existing and proposed technique are compared. The NS2 simulator are used to carry out the experimentation.

Table:1.Simulation Parameters

Parameters	Value
Topography	800X800
Mobility Model	Random Way point model
Connections	50 pairs(100 nodes)
Traffic Type	TCP-CBR
Transmission range	250m
Speed	150m/sec

This table1 define the simulation of parameters are used.

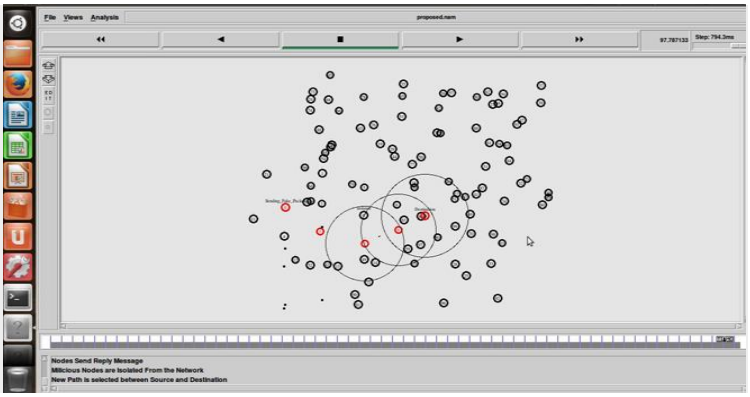

Figure 2. Establishment of Secure Path

The technique of multipath routing is applied for the selection of new path. In the approach of multipath routing, when the malicious node exists in the selected path then new path will be selected in which no malicious node exists.

Performance of proposed technique to analyze sinkhole and wormhole node of certain parameters.

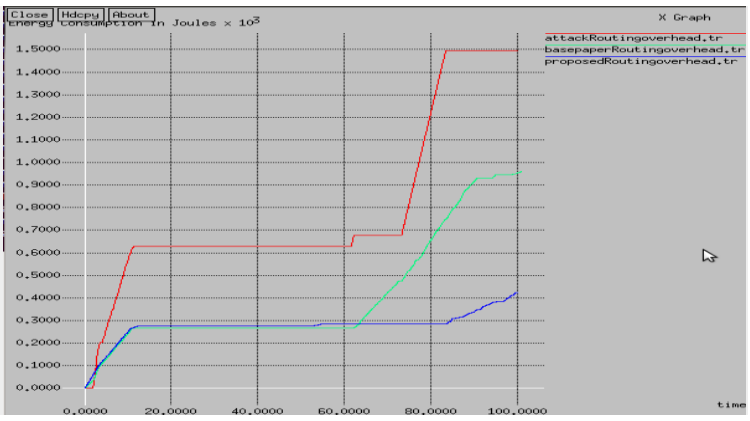

Fig 2: Routing Overhead

As shown in figure 2, the routing overhead of the attack scenario, basepaper scenario and proposed technique scenario is compared for the performance analysis. It is analyzed that proposed scenario has least routing overhead than other scenarios.

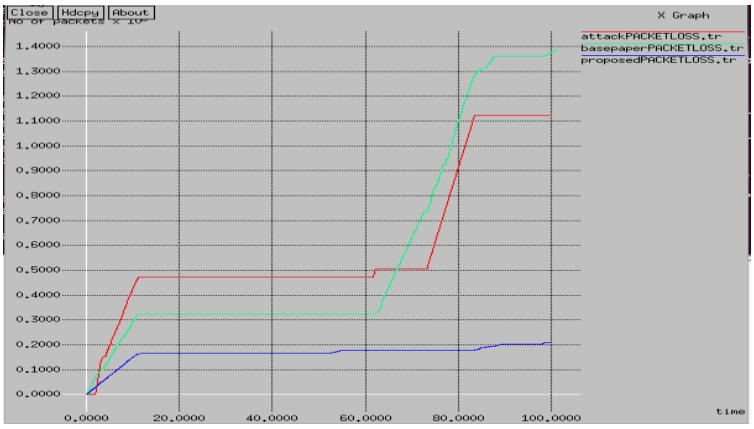

Fig 3: Packet loss Comparison

As shown in figure 3, the packet loss of attack scenario, basepaper scenario and proposed scenario is compared for the performance analysis. It is analyzed that packetloss of proposed technique is less as compared to other techniques.

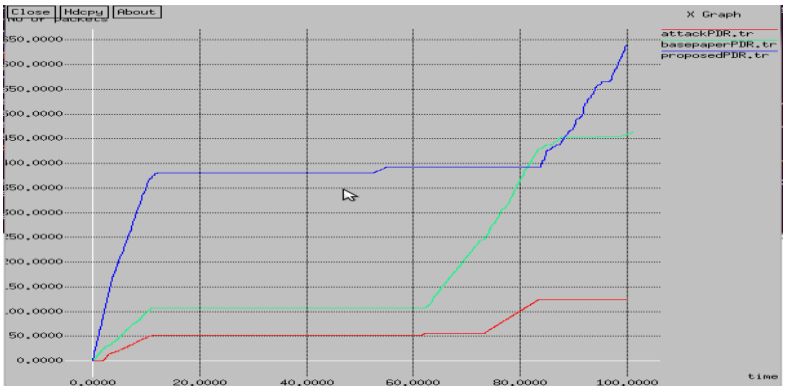

Fig 4: PDR Comparison

As shown in figure 4, the PDR of the attack scenario, base paper scenario and proposed scenario is compared for the performance analysis. It is analyzed that PDR of proposed scenario is maximum as compared to other scenarios.

Conclusion

The wireless mobile network is the decentralized type of network in which mobile nodes can join or leave the network when they want. The wireless mobile network is the network in which no central controller is present. Due to self configuring nature of the network security, routing and quality of service are the major issues of this network. The wormhole and sinkhole attack is the

active type of attack in which malicious nodes can enter the network and increase delay. The technique is the Delphi technique which is used in the existing work. The Delphi technique has less accuracy and high execution time for the detection of malicious nodes. In this research work, threshold based technique is proposed for the detection of malicious nodes from the network. The proposed and existing techniques are implemented in Ns2 and simulation result shows improvement in routing overhead, PDR and packet loss.

References

[1] Dr. Sasirekha, Dr. N. Radha "Secure And Attack Aware Routing In Mobile Ad Hoc Networks Against Wormhole And Sinkhole Attacks", 5090-5013 2017 IEEE.

[2] Shivani, Er. Munish Katoch "Security Aspects of Mobile Ad-Hoc Network: A Review" JETIR, October 2018 vol. 5, issue 10.

[3] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M "An Overview of Security Problem in MANET",International Journal of Advanced Research in Computer Science and mobile computing.

[4] Aarti and Dr. S.S Tyagi "Study of MANETS: "Characterstics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering.

[5] Kimaya Sanzgiri, Bridget Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, November 2002, pp. 78-90.

[6] Yi-an Huang and Wenke Lee, "Attack analysis and Detection for Ad-hoc Routing protocols", Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France, September 2004

[7] Y. Hu, A. Perrig, D. Johnson. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks". Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), March 2003.

[8] M. Alicherry and A.D. Keromytis, " Securing MANET Multicast Using DIPLOMA", in Proc. IWSEC, 2010, pp.232-250.

[9] Panagiotis, Papadimitratos; Zygmunt, J. Haas;,"Secure Routing for Mobile Ad hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002 63

[10] Karoly Hars ´ anyi, Attila Kiss and Tamas Szir ´ anyi, "Wormhole Detection in Wireless Sensor Networks Using Spanning Trees," 2018, IEEE

[11] Sayan Majumder and Prof. Dr. Debika Bhattacharyya, "Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach," 2018, IEEE

[12] M. Rmayti∗, Y. Begriche†, R. Khatoun†, L. Khoukhi∗ A. Mammeri, "Graph-Based Wormhole Attack Detection in Mobile Ad hoc Networks (MANETs)," 2018, IEEE

[13] Thanuja. R Sri Ram. E Dr.A.Umamakeswari, "A LINEAR TIME APPROACH TO DETECT WORMHOLE TUNNELS IN MOBILE ADHOC NETWORKS USING 3PAT AND TRANSMISSION RADIUS (3PATw)," 2018, IEEE

[14] Shahjahan Ali, Prof. Parma Nand and Prof. Shailesh Tiwari, "Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique," 2017, IEEE