Novel Approach for Isolation of Wormhole Attack in Mobil Ad hoc Networks

Abstract

The wireless nature of communication makes wireless networks unreliable as any attack with intent to steal the data can do so by deploying malicious nodes in the network. In MANET different mobiles are connected through wireless link. There are different types of attacks possible in MANET. Wormhole attack is one of the types. In this type of attack node transfer from other path rather than path assigned to source and destination. So lost of data is possible. In this research work, the novel scheme is proposed which detect and isolation malicious nodes from the network. The malicious nodes are responsible to trigger wormhole attack in the network. The proposed technique is implemented in NS2 and simulation results shows that proposed technique performs well as compared to other techniques.

KEYWORDS:

Wormhole, Threshold Technique, MANET, NS2

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. 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. It has an attractive topological architecture and promotes [1] the easy mobility. The node act as the router and they route r transmit the packet from one node to the other. Depending upon the type of application that is utilizing MANET it is possible to define the density and numbers of nodes. Several applications today are deploying MANETs within them for benefiting their advantages [2]. There is a need to resolve various issues and challenges within certain applications. Increasing the mobility of nodes to autonomous, mobile and wireless domains is the major objective of MANETs. Here, the routers and hosts are combined such that in an ad hoc fashion the network routing infrastructure is generated. A set of countermeasures were recognized along with several security vulnerabilities within the wireless environment. However, a guaranty that is orthogonal to the security based challenge is provided very less. 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. The information can be transmitted securely by ensuring security of communication in MANETs [3]. 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 MANET is classified by two types of attacks i.e. Data traffic attacks and Control traffic attacks. They are classified on the basis of the characteristics and goals of the attacks. For example in MANET there are two attacks Black-hole attack and the gray-hole attack. Both plays almost same functions i.e. both the attacks allows the user to drops the packets while transferring it from one node to another. But the only difference is that the Gray hole attack is based on two conditions; time or sender node and gray hole attack behaves as a black hole attack when it starts dropping packets [4]. Due to this fact they both are categorized under same attack. 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 [5] in which the vulnerabilities are inherited from the radio communication to routing, man-in-middle and other injected attacks. Mobile wireless networks are generally more prone to physical security threats than are fixed, hardwired networks. Existing link-level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level encryption, at the network layer, the most pressing issue is one of inter-router authentication prior to the exchange of network control information [6]. Several levels of authentication ranging from no security (always an option) and simple shared-key approaches, to full public key infrastructure-based authentication mechanisms will be explored by the group. As an adjunct to the working groups' efforts, several optional authentication modes may be standardized for use in MANETs. Wormhole 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 [7]. When this link becomes the cheapest cost path to the desired location the malicious nodes are selected and sends the packets to the desired location. 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.

Literature Review

Harsányi et al.[8] 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 of network is only utilized here. Majumder et al.[9] 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. Rmayti et al.[10] 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 kinds of malicious nodes existing in the network can be detected through this 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.. Thanuja et al.[11] 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. Ali et al.[12] 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. The shared key encryption is used to broadcast the messages with the node ID. There is a secure and efficient broadcasting of packets through the prevention of wormhole attack in WSNs by applying the proposed approach. Ananthi, et al.[13] presented that several types of attacks can be detected easily by applying the smart attack detection (SAD) mechanism. Various types of attacks possible in the network are detected through SAD. An analysis was performed with the help several parameters to evaluate the outcomes of proposed approach in these networks. There is a reduction in the performance level in terms of throughput and maximization of end to end delay in case of presence of attacks. The proposed work can be extended by recognizing denial of service attacks from VANETs.

Research Methodology

In the existing work, Delphi technique is proposed which can check per hop delay and node which is increasing delay is detected as the malicious node from the network. In the network due to some issues like multipath routing per hop delay can be increased which reduce the accuracy of malicious node detection. In this work, a novel technique is proposed which is based on the IDN (intrusion detection nodes) nodes. In the proposed technique delay of each node is calculated. The delay on each node is calculated by connectivity factor of each node. The node which is increased delay maximum than the defined delay is detected as the malicious node from the network

The proposed work is implemented as per the following procedure. Following are the various steps of the proposed flowchart

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

Algorithm

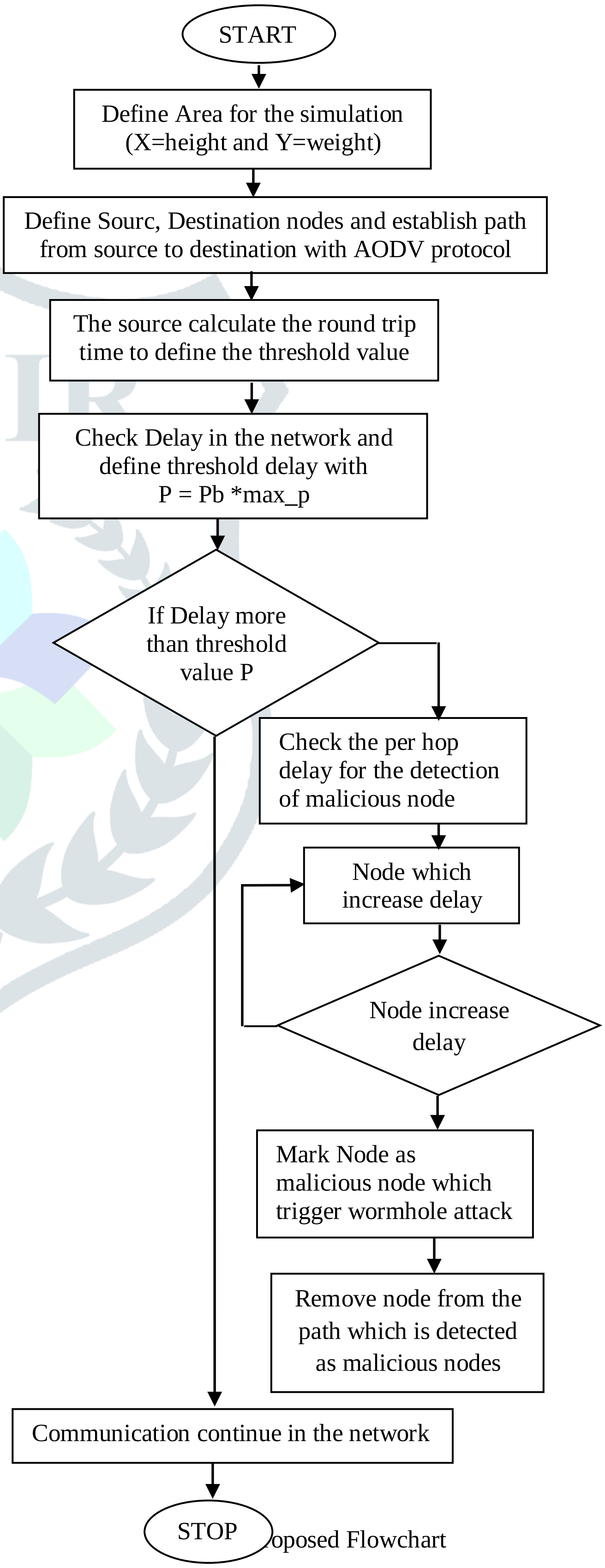
The proposed technique detects and isolates malicious nodes from the network. The proposed algorithm is described below:-

Input : Number of Mobile nodes
Output : Detection of Malicious node

1. Deploy network with finite number of mobiles nodes

2. Path Establishment ()

```
2.1. Source send route request packets in the network

        2.2. The nodes which are adjacent to destination
reply with route reply packets
        2.3. The source selects best path on the basis of
hop count and sequence number

3. Calculate Threshold value ()

        3.1. Repeat for all nodes
                P = Pb *max_p
                Until reach to max_p

4. Detect malicious node ()

        4.1. Repeat loop for all nodes
                If node (i) data rate < P
                Malicious node =node(i)
                Return malicious node

5. Apply multipath routing for the selection of new path

6. if source receive route reply from malicious nodes

        Discard the route reply

        If the route trip time is high

        Discard the route reply

Else

Process the request

7. Select the path from source to destination on the basis of
hop count and sequence number

        If malicious node exists in the path

        Discard path

        Else

        Process the path for data transmission
```


START
Define Area for the simulation (X=height and Y=weight)
Define Sourc, Destination nodes and establish path from source to destination with AODV protocol
The source calculate the round trip time to define the threshold value
Check Delay in the network and define threshold delay with P = Pb *max_p
If Delay more than threshold value P
Check the per hop delay for the detection of malicious node
Node which increase delay
Node increase delay
Mark Node as malicious node which trigger wormhole attack
Remove node from the path which is detected as malicious nodes
Communication continue in the network
STOP

oposed Flowchart

Experimental Results

The proposed work is implemented in NS2 and the results are evaluated by making comparisons against proposed and existing work in terms of throughput, packet loss and energy consumption.

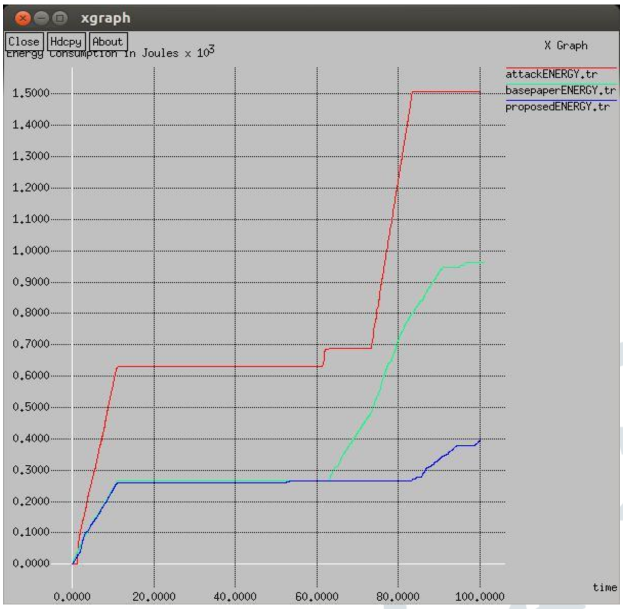


Figure 2: Energy consumption

As shown in figure 2, the energy consumption of the attack scenario, base paper scenario and proposed technique scenario is compared for the performance analysis. It is analyzed that proposed scenario has least energy consumption than other scenarios.

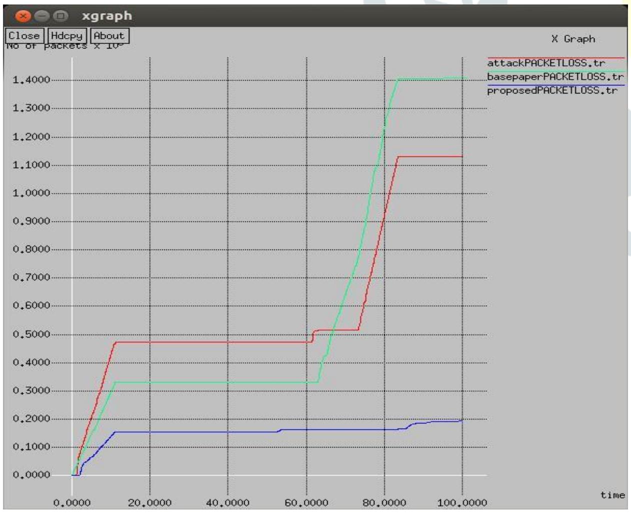


Figure 3: Packet loss Comparison

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

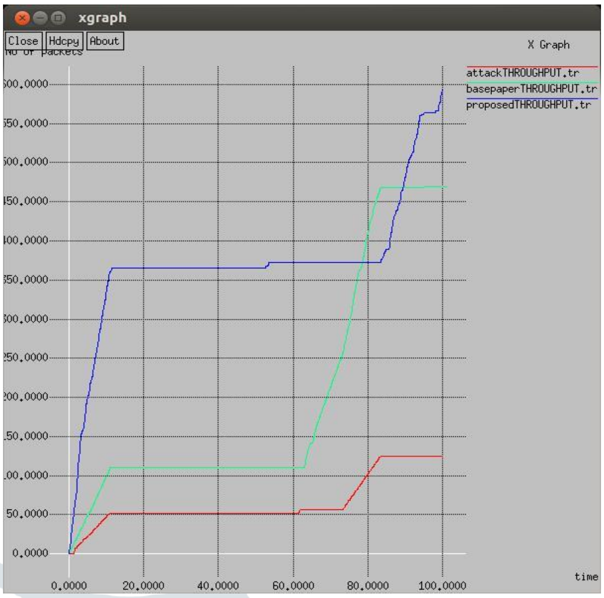


Figure 4: Throughput Comparison

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

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 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 energy consumption, throughput and packet loss.

References

[1]. V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," IEEE MILCOM, 2002.

[2] P. Kyasanur, and N. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," DCC, 2003

[3]KimayaSanzgiri, 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.

[4] 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

[5] 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.

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

[7] 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

[8] KarolyHars ´ anyi, Attila Kiss and TamasSzir ´ anyi, “Wormhole Detection in Wireless Sensor Networks Using Spanning Trees,” 2018, IEEE

[9] VasiliyKrundyshev, Maxim Kalinin and Peter Zegzhda, “Artificial swarm algorithm for VANET protection against routing attacks,” 2018, IEEE

[9] SayanMajumder and Prof. Dr. Debika Bhattacharyya, “Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach,” 2018, IEEE

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

[11] 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

[12] Shahjahan Ali, Prof. Parma Nand and Prof. ShaileshTiwari, “Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique,” 2017, IEEE

[13] J. Vijitha Ananthi, 2 S. Vengatesa, “DETECTION OF VARIOUS ATTACKS IN WIRELESS ADHOC NETWORKS AND ITS PERFORMANCE ANALYSIS,” 2017, IEEE