THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Improved Attack Detection Using Decision Tree Based Algorithm

Ritika
Department of Computer Science and Engineering
Guru Nanak Dev University, Amritsar, India

Abstract:
Security is an essential requirement in order to provide protected communication in wireless network and wired networks. Due to the dynamic topology and shared medium of MANETs, attackers can easily disrupt these networks. This paper focuses on detection of the multiple attacks. This paper introduces a new technique for the detection of wormhole and gray hole and other attacks in DSR protocol in order to make a wireless ad-hoc network secure. This technique detects the malicious nodes and avoids these nodes for participating in the network. The parameters used for evaluating the network performance are average end to end delay and throughput.

Keywords*: MANET, Security, Wormhole, Gray hole, DSR*

1. Introduction

The wireless network in which the number of nodes transfers data and services to each other without support of any centralized authority or fixed infrastructure is known as mobile ad-hoc network (MANET) [1]. A MANET is also called as an infrastructure less network because the mobile nodes in the network set up paths dynamically among themselves for communication purposes temporarily [2].The dynamic topology and infrastructure less characteristics of the MANET make it attractive for military purposes and business applications, personal area networks, sensors networks etc. Some examples of the uses of ad-hoc networks are: students using laptop in order to participate in an interactive lecture, business persons sharing information during a meeting, soldiers passing on some useful information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. The nodes in ad-hoc networks are allowed to move free within the network and can easily be removed from or added to the network at any time [3].The medium used in MANET for sharing the information is shared (wireless), so the attackers can easily access the useful information or can disturb the functionality of the network by introducing malicious nodes. Limited power supply, scalability, lack of secure boundaries etc [5], are responsible for making a MANET insecure. Due to these reasons the wireless networks are more exposed to threats or attacks than the wired networks.
So security is the most important need for these kinds of networks .MANET nodes includes laptops, PDA, cell phones etc. having limited computation, communication and energy resources [4]. Attack can modify the data transmitted within the network [6].

2. Overview of Worm Hole and Gray Hole Attacks

2.1. Wormhole Attack

A particularly complicated security attack is the wormhole attack. It is also known as tunneling attack. In this attack, a malicious node take over packets from one position in a network and tunnels them through an out-of-band channel to another malicious node located several hops away, which replays them to its neighboring nodes, as shown in Fig. 1.

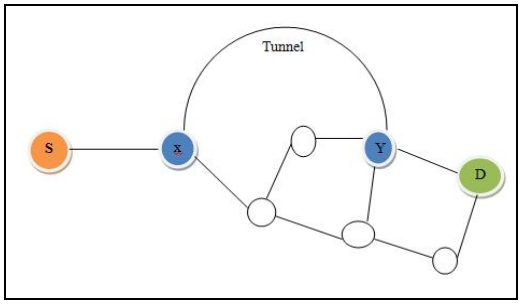

Figure 1: Worm hole attack

In the above figure X and Y are malicious nodes. S is source node and D is destination node. The tunnel between the malicious nodes is actually faster than links between non malicious nodes, so the tunneled packets delivered faster than packets through

other routes. Therefore, the malicious nodes are included in the route and take an advantage for future attack. Detection of wormhole attack is very tough and it requires the use of an unchangeable and independent physical metric, such as time delay [7].

2.2. Gray Hole Attacks

A Gray hole may demonstrate its malicious behavior in various techniques. In gray hole attack a malicious node drops the packets and does not forward them. In Another type of gray hole attack the malicious node starts dropping the packets for some time duration but also can switch to the normal behavior later on. A Gray hole may also act as a combination of above described 2 techniques, so making its detection very difficult. For example whenever the source node is willing to send data to destination node, first of all the source node broadcasts a Route request (RREQ) packets to its neighbors in order to discover a fresh path to the desired destination. Then the neighbor nodes try to find out whether it is the destination or it has the route to destination by seeing in its routing table. The route to the destination is indicated by the freshness of destination sequence number attached to it. The neighbor node then checks whether it has an appropriate route to the destination. When the malicious node know about this information, it indicates that it has the fresh route to the destination (i.e., highest sequence number). The malicious node sends a RREP (route reply) message back to the saved path to the source node. So the source node starts communicating through the path by trusting on the malicious node .But later on the gray hole node starts dropping the packets and does not forward to the other nodes. This attack is a refined form of black hole attack [8].

3. DSR Protocol in MANET

The proposed solution is implemented by using DSR protocol i.e. Dynamic Source Routing protocol. Routing is an activity that connects a call from source to destination in the network. Routing activities are determining optimal routing paths and transferring the packets with in a network [10].DSR protocol comes under the category of on demand routing/reactive routing protocols. It is based on the source routing. In source routing the source node finds out the perfect sequence of nodes in order to send the packets to the destination node. The record of neighbor nodes which are going to be used in routing are stored in packet's header which has to propagate to the target node. It is necessary or every node to maintain a route cache where it caches source routes. When a source node is willing to send a packet to some other intermediate node, it first checks its route cache for a source route to the destination for successful delivery of data packets. If a route is found, the source node uses this route to transmit the packet otherwise it initiates the route discovery process. Route discovery and route maintenance are the two main features of the DSR protocol.

For example: Suppose there are 15 nodes in a network. Node 1 i.e. source node wants to send data to node 12 i.e. destination node. Then, first of all node 1 will find outs its route cache for a perfect roué for node 12.If node 1 is unsuccessful to find out a path to node 12,the route discovery process is initiated. For route discovery, the source node broadcasts a route request packet which can be received by all the neighbor nodes within transmission range of node 1. In this way the route from node 1 to node 12 is discovered .Because the mobile nodes are being used here, so the nodes can move in and out from the transmission range of other nodes. So there is need to maintain the routes which are stored in the route cache [9, 5].

4. Problem Definition

A MANET is inherently a self-organized network system without any fixed infrastructure. Typically, the nodes act as both host and router at the same time, i.e. each node in the network can be independent. The network functions like sending packets to another nodes and routing is performed by the nodes themselves participating in MANET due to the lack of centralized management. So due to these reasons securing a wireless network is a very tough task. To make a network secure is the essential requirement in MANET. There different kinds of attacks in wireless networks.

In Gray Hole Attack a malicious node drops the packet and does not forward them. Gray Hole attack can be act as a slow poison in the network side that is the probability of packet loss is undetermined. In these attacks a malicious node behaves as a non malicious node during route discovery process and starts dropping the packets silently as soon as the packets start arriving.

A worm hole attack is when two or more suspicious nodes may work together to exchange messages between them through accessible data path. A worm hole reflects the route that may seems fine to the destination but it always tunnels the packet to its misbehaving partner node. This attack is also known as tunneling attack.

The DSR protocol does not require any existing network infrastructure. It is completely self organizing and self-configuring. This protocol basically consists of two mechanisms: Route Discovery and Route Maintenance, where the route discovery mechanism handles the establishment of routes and the route maintenance mechanism keeps update the route information.

Objectives of Proposed Method Are:

- This main objective of this research work is to detecting the multiple attacks in DSR protocol using decision tree based algorithms.
- The main motivations to find the gray hole attack and wormhole attack in mobile ad-hoc networks by using the cluster head based approach.

4.1. Proposed Methodology

The followings steps are being executed in order to reach to the solution of the problem as given in Fig. 2:

Step1: Define network characteristics like nodes and malicious nodes (attackers) etc.

Step 2: When Simulation time is less than or equal to the maximum simulation time, Then execute the next step.

Step 3: Initiate the multiple non malicious nodes of the network.

Step 4: Initiate attacker nodes too.

Step 5: Data or packets should multicast.
Step 6: If process of multicasting of data is successful, then Increment the hit. Again step 2 should be executed for the all the nodes of the network.
Step 7: If it is unsuccessful, miss should be incremented.
Step 8: When Simulation time is not equal to the maximum simulation time, then attack should be detected on the basis of equation 1 as described below :

$$\text{Equation 1 : DT} = \left(\sum_{i=1}^{n} \text{miss}(i)/n\right.$$

Here equation 1 contains dynamic threshold values which is average of miss ratios of nodes,n.
Step 9: Finish

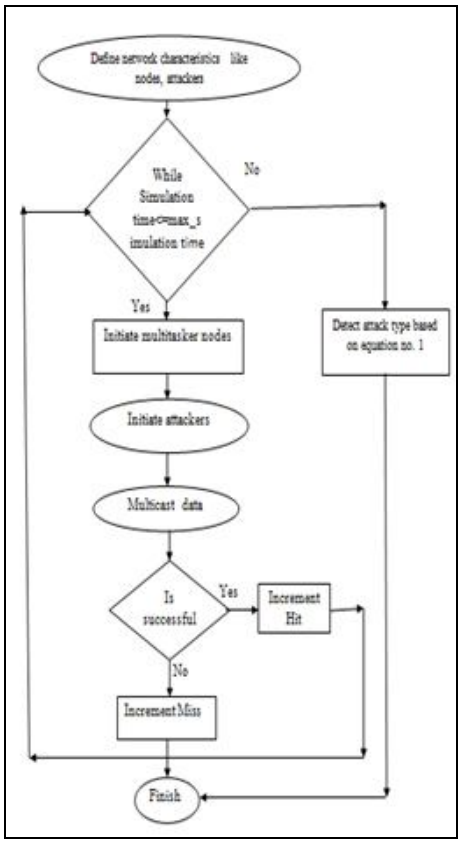

Figure 2: Flow Chart of Proposed Technique

4.2. Proposed Algorithm

Here: (miss/total) = miss_ratio
{
Step 1: (miss_ratio) ≥ 0.8, Then it is a black hole attack.

Step 2: (miss_ratio) ≥ 0.5, Then it is a gray hole attack.
Step3:(miss_ratio) ≥ 0.3 && (miss_ratio) < 0.5, It is a worm hole attack.

Step 4: (miss_ratio) < 0.3, It is a packet drop attack.

}

5. Simulation Results

The proposed approach has been implemented in MATLAB simulation tool. We have taken the simulation scenario of 15 nodes as shown in Fig. 3.Where nodes 2,10,13,11 are detected as the malicious nodes.

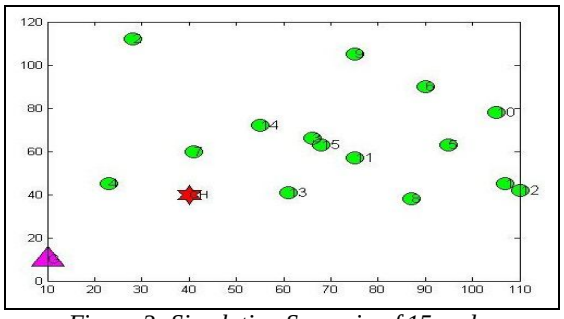

Figure 3: Simulation Scenario of 15 nodes

The figure 4 shows the hit /miss ratio for the malicious node 2. According to dynamic threshold values, it is an attacker node. It hits for 2 times. Number of misses for this node is 3.Total tries by this node are 8. So hit ratio is 0.2500 and miss ratio is 0.3750.As its miss ratio is greater than 0.3 and less than 0.5.So, it is a wormhole attack.

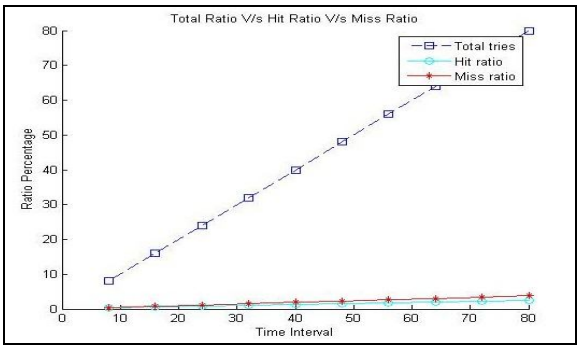

Figure 4: Hit /Miss/Total Ratio of Worm hole Attack

The figure 5 depicts that node 10 is an attacker node.It hits 3 times and misses for 2 times. The number of total tries are 5.Therefore,the hit ratio for this node is 0.60 and miss ratio is 0.40. So this is also a worm hole attack because its miss ratio is greater than 0.3 and less than 0.5.

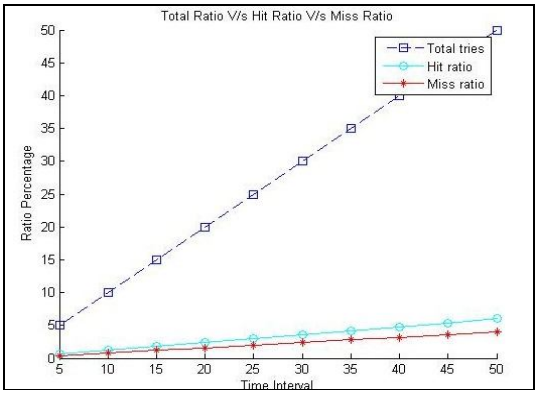

Figure 5: Hit /Miss/Total Ratio of Worm hole attack

The figure 6 shows node 13 is a kind of attacker node. The number of hits by node 13 are 2 and number of misses are 3. The numbers of total tries are 5.Therefore, the hit ratio for this node is 0.40 and miss ratio is 0.60. So this is a kind of gray hole attack.

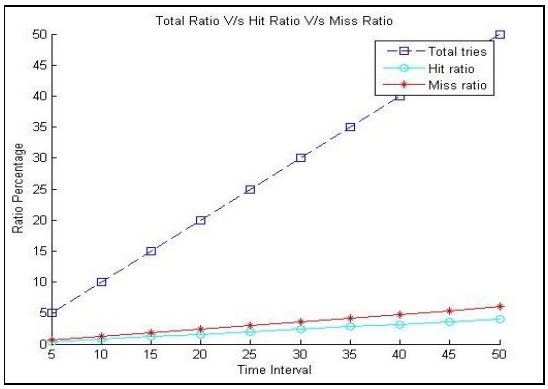

Figure 6: Hit /Miss/Total Ratio of gray hole attack

In figure 7 shows node 11 is an attacker node. The node 11 does not hit successfully, so its number of hits are 0 and number of misses are 5.The number of total tries by this node are 5.Therefore, the hit ratio for this node is 0 and miss ratio is 1. So this is a kind of black hole attack because its miss ratio is greater than 0.8.

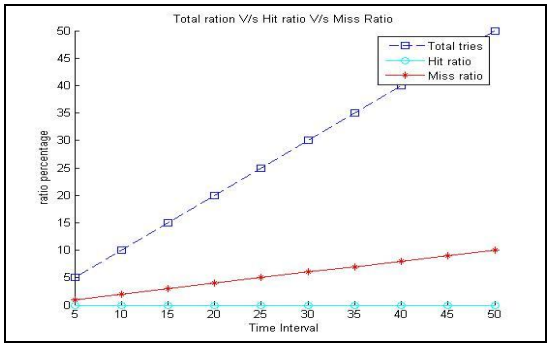

Figure 7: Hit /Miss/Total Ratio of black hole attack

The table 1 is showing the values of total number of tries, number of hits and number of misses of node 10.

Total number of tries	Number of hits	Number of misses
5	3	2

Table 1: Hits/misses of node 10

The Fig. 8 shows the hit/miss analysis for nodes 10.As it is clearly visible from this figure total number of hits are more than number of misses.

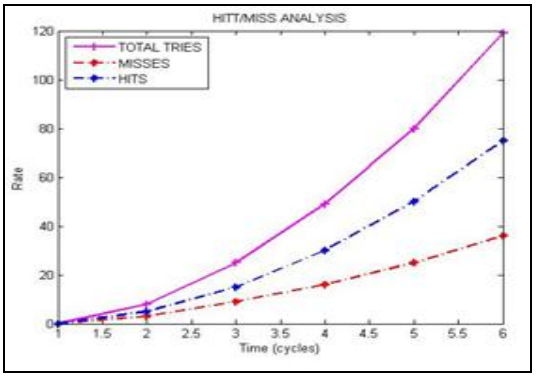

Figure 8: Hit miss analysis of node 10

6. Comparison of Proposed Technique and Existing Technique

Table 2 is demonstrating the comparative analysis between the proposed and the existing technique for the parameter average end to end delay. When a packet is transmitted from source to destination it takes time to reach and calculates the difference between send times and received times. Route discovery, congestion, queuing and propagation etc. are included in the delay metric.

Table 2 has shown that the new technique is better than the existing as the value of delay is less in the proposed approach. The proposed technique provides more accurate results for end to end delay than the existing technique.

Rounds	Old Technique	New Technique
1	0.8	0.5
2	2.4	1.5
3	4.6	3
4	7.5	5
5	11	7.5

Table 2: End to end delay

So, average end to end delay for old technique = 5.3 sec.

Average end to end delay for new technique = 3.5 sec.

Fig. 9 is showing the comparative analysis between the proposed and the existing technique with respect to average end to end delay metric. Magenta color represents the old technique whereas blue color represents the new technique. Y axis has shown the delay. X axis has shown the time (cycles).

This figure has shown that the new technique is better than the existing as the value of end to end delay is less in the proposed technique as compared to existing technique. Thus proposed has shown quite effective results. In an ad-hoc network delay should be as less as possible.

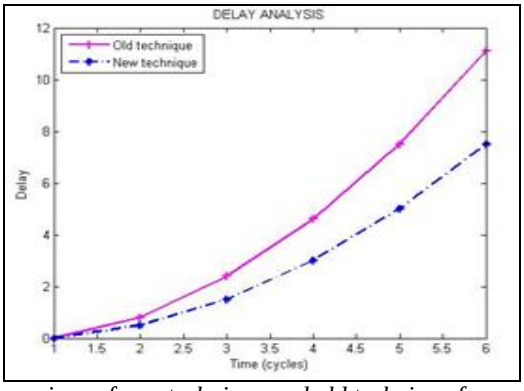

Figure 9: Comparison of new technique and old technique for parameter Delay

Table 3 is showing the comparative analysis between the proposed and the existing technique for parameter throughput. Throughput is the average rate of successful data packets received at destination.

Table 3 has shown that the new technique is better than the old technique as the value of throughput is more in the case of proposed technique. Therefore proposed algorithm has shown fairly effective outcomes.

Rounds	Old Technique	New Technique	Expected
1	2	5	8
2	6	15	25
3	14	30	49
4	25	50	80
5	39	75	119

Table 3: Throughput

Figure 10 is showing the comparative analysis between the proposed and the existing technique with respect to throughput. It needs to be maximized. Figure 10 has shown that the new technique is better than the existing as the value of throughput is more in the proposed technique. Expected throughput is the ideal throughput, which can never be achieved in an ad-hoc network .Therefore proposed algorithm has shown fairly effective results.

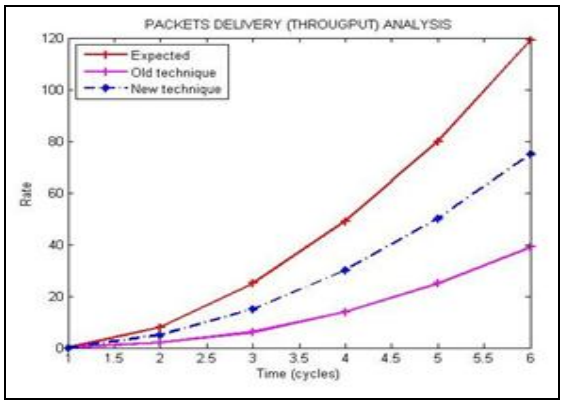

Figure 10: Comparison of new technique and old technique for parameter Throughput

7. Conclusion and Future Work

In MANET security the most important requirement. For a secure communication a MANET should be free from the security attacks (like wormhole, gray hole etc.).But due to dynamic topology and infrastructure less characteristics a MANET becomes an easy target to the intruders as compared to the wired networks. The gray hole and wormhole attacks easily interrupt the network functions. So it is very hard to detect such kind of attacks and make a network secure. The proposed technique detects the wormhole, gray hole and other attacks and make the network secure by dropping these malicious nodes in the routing of the network. The proposed technique has been implemented in MATLAB. To justify the algorithm 15 nodes are taken for experimental purpose. The simulation results of the proposed technique are better than the existing technique. Moreover this proposed technique does not disturb the overall network performance of the network. The comparison has shown that the proposed algorithm has shown quite effective results.

In future this research work will be extended by using genetic decision tree based algorithm for detecting types of attacks in improved and more efficient way. However, only DSR routing protocol is used in this research work, so in order to enhance the results further we will use various routing protocols like ad-hoc on-demand distance vector (AODV), signal stability routing (SSR) etc.

8. References

1. Jyoti Thalor,Ms. Monika "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.
2. Pradip M. Jawandhiya, Mangesh M. Ghonge, DR. M.S.Ali, Prof. J.S. Deshpande "A Survey of Mobile Ad Hoc Network Attacks",International Journal of Engineering Science and Technology Vol. 2(9), 2010.
3. Rahul Sharma, Naveen Dahiya, Divya Upadhyay,"An Analysis for Black Hole Attack in AODV Protocol and Its Solution", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue.4, April 2013, pg.391 – 395.
4. Humaira Ehsan, Farrukh Aslam Khan "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs",11th International Conference on Trust, Security and Privacy in Computing and Communications,IEEE,2012.
5. Yudhvir Singh,Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak **"**Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", Third International Conference on Advanced Computing & Communication Technologies,IEEE,2013.
6. Aarti,Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013.
7. Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", 2013 UKSim 15th International Conference on Computer Modelling and Simulation, IEEE.
8. Usha, G., and S. Bose. "Impact of Gray hole attack on adhoc networks" International conference on Information Communication and Embedded Systems (ICICES), IEEE, 2013.
9. Rahul Kulkarni Asha S. Nitin Kulkarni,"A Comparative Analysis Of AODV, DSR Routing Protocols In Mobile Ad-Hoc Networks", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 2 Issue 7, July – 2013.
10. Ashok M.Kanthe, Dina Simunic and Ramjee Prasad"Effects of Malicious Attacks in Mobile Ad–hoc Networks",International Conference on Computational Intelligence and Computing Research,IEEE, 2012