International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Mechanism to Counteract Attacks in MANETS

Susmitha A, Lipsa Dash
Sr. Asst. Professor, Department of ECE New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

Mobile adhoc networks has been experiencing tremendous growth in the last two decades as it possess a routable networking environment over a link layer adhoc network. Data is very important in today's communication scenario and protecting this data has always been challenging for researchers to think in the direction of data security. Transmission of data through a secured route in a network is very important in today's digital world. There are a number of protocols being proposed in context of MANETS among which OLSR is one of the frequently used for its efficiency in path calculation and bandwidth utilization. Protocols are usually vulnerable to various attacks while routing. This paper mainly focuses on mitigating denial of service attack as well as the black hole attack using fictitious node mechanism. The issues of denial of service attack and black hole attack is addressed by using the proposed algorithm which reduces the time of transaction and increases packet delivery ratio with less energy utilization. In this way proposed solution increases the performance of the network.

Keywords: MANET,OLSR,DOS,AODV

I. INTRODUCTION

Networks can be classified as wired and wireless. Mobile adhoc network is a collection of several autonomous mobile nodes which are able to connect on wireless medium forming a dynamic network. MANET systems contain network devices like sensor nodes, computers etc, channels and routing protocol. Construction of MANETs does not require any existing network infrastructure and this result in a low cost network which even provides freedom of mobility. Due to low cost and mobility, a MANET is suitable for applications such as disaster relief, vehicle networks, casual meetings, campus networks, robot networks, emergency operations, military service, maritime communications. When compared with conventional wired network it is somewhat difficult to perform routing in MANET because of its dynamic nature. Routing algorithms determine the choice of route for safer data transmission thereby increasing the communication efficiency. The routing protocols in MANET are developed to manage large number of nodes with resource constraint. The main threat in the process of routing is presence or absence of nodes at various places in the network. Reducing message overhead is of utmost importance despite of increasing number of nodes in the network. The second most important thought is to maintain small size of the routing table as larger size of routing protocol can affect the transmission of control packet in the network. The routing protocols are mainly classified into two categories: reactive routing protocols and proactive routing protocols.

Routing protocols are classified as follows

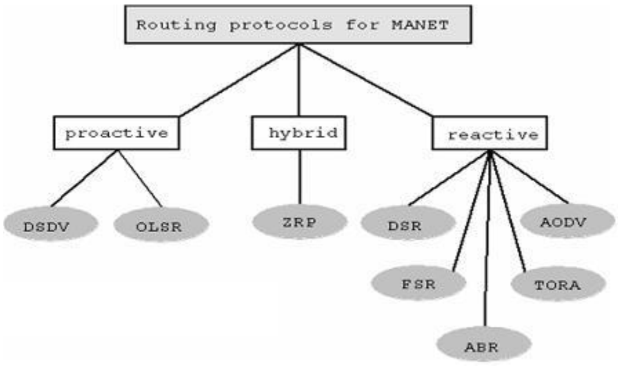


Figure 1. Classification of routing protocols in MANETS

Table-Driven (or Proactive)

The nodes maintain a table of routes to every destination in the network, for this reason they periodically exchange messages. At all times the routes to all destinations are ready to use and as a consequence initial delays before sending data are small. Keeping routes to all destinations up-to-date, even if they are not used, is a disadvantage with regard to usage of bandwidth and network resources.

DSDV (Destination-Sequence Distance Vector):DSDV has one routing table, each entry in the table contains: destination address, number of hops toward destination, next hop address. Routing table contains all the destinations that one node can communicate.

OLSR(Optimistic link state routing):optimistic link state routing protocol is optimization of classic link state routing protocol. LSR uses flooding technique where every node retransmits to all its neighbor ,whereas OLSR retransmits selectively based on certain set of rules which is called as multi point relaying(MPR) [2] i.e. forwarding agents for control messages. OLSR is widely used because it is efficient in bandwidth utilization and path calculation but is prone to many attacks since it relies on cooperation between nodes in network that is the presence of malicious nodes that will attack.OLSR uses two messages i.e. HELLO and TC.HELLO message is rebroadcasted to all nodes, every node that receives message and rebroadcasts to sender is first hop node all nodes will have topology information till 2 hop range with the help of which MPR selection will be done[1] MPR periodically the TC message that contain list of all nodes that have selected sender as MPR.

Reactive Protocols (On-demand Routing Protocols)

In on-demand trend, routing information is only created to requested destination. Link is also monitored by periodical Hello messages. If a link in the path is broken, the source needs to rediscovery the path. On-demand strategy causes less overhead and easier to scalability. However, there is more delay because the path is not always ready. The following part will present AODV, DSR, TORA and ABR as characteristic protocols of on-demand trend.

AODV Routing: Ad hoc on demand distance vector routing (AODV) is the combination of DSDV and DSR. In AODV, each node maintains one routing table.

Dynamic Source Routing Protocol: DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was specifically designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration.

Mobile ad-hoc networks are more vulnerable to be attacked than wired network due to their inherent characteristics. We can distinguish two main categories of attacks: Routing protocol dependent and routing protocol independent attacks [3]. Routing protocoldependent attacks are the attacks which are prone to occur onspecific routing protocols, such as DSR, AODV. Black hole attack (AODV) targets ad hoc on-demandrouting protocol, link withholding attack, link spoofing attack (OLSR) and colluding misrelay attack(OLSR) targets Optimized Link State Routing protocol.

Black hole Attack (AODV): AODV is a reactive protocol. In AODV, when a source node forwards a data packet to a destination node and does not have a direct route to D, it initiates route findingby broadcasting a route request Packet (RREQ) to neighbors and if the neighbor is intermediate node and does not have direct route to destination then intermediate node also rebroadcast the route request packet. This process is repeated until the RREQ reaches the destination node. When the first RREQ arrives, the destination node sends a route reply (RREP) to the source node through the same path from which the (RREQ) arrived. If the same RREQ arrives later then it will be ignored by the destination node.

Link Spoofing Attack (OLSR): OLSR is a proactive routing protocol, that is, it is based on periodic exchange of topology information. OLSR make use of multipoint relay (MPR) to implement an efficient flooding mechanism by efficiently decreasing the number of transmissions needed. In OLSR, each node selects its own MPR from its neighbors.

Colluding Attack: In this attack, multiple attackers work in collusion to drop or modify routing packets to disturb routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog.

Wormhole Attack: A wormhole attack is also known as tunneling attack and is one of the most severe and sophisticated attacks in MANETs. A wormhole attack is composed of colluding attackers and a wormhole tunnel. To establish a wormhole attack two or more colluding attackers records packets at one point in network and tunnels them to another point through wormhole tunnel which can be wired link, a high-quality wireless out-of-band link, or a logical link.

Flooding Attack: This is also known as resource consumption attack, it gives rise to DOS(denial of service) when used against on-demand ad hoc routing protocols. Its main aim is to unnecessarily consume bandwidth and nodes resources to disrupt the routing operation.

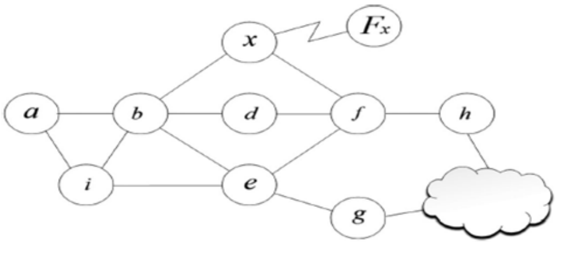
Denial of service attack: This is an attack in which any malicious nodes present in the network will falsely wins the trust of souse node for the transmission through it and then delays in transmission to the destination.

Proposed paper focuses on OLSR protocol that defends the both denial of service and the black hole attack using the same technique that was used by the attacker node in the network.

II. RELATED WORK

There are many solutions that are being proposed to mitigate the attacks that are being explained below

[1]This paper propose the DOS attack by fictitious node that does the isolation of node by winning the trust of source node and once the source node selects attacker as MPR the attacker node will isolate victim by not including the source node in its list, this makes the other nodes in the network feel that the victim has left the network



Example of a node isolation attack: node x claims to know every two-hop neighbor of b, as well as F_x, a non-existent node.

To solve this every node will create its own fictitious node and passes to the node next to them. Based on the reply messages it gets it checks for contradiction and verifies if the nodes are true nodes or the attacker.

[5]here node checks TC message of nodes MPR but has a drawback that it works only when there is single attacker .this means that if there are two attacker node there is a chance that the two nodes can defend each other to protect them from being identifies as attacker.

The other solution was to modify the HELLO message by including 2 hop neighbor therefore by finding contradiction between messages attacker can be found but this again increases the network overhead because the nodes keep moving[7].

[6] In this paper on receiving HELLO message node verified every node mentioned which requires two more control messages. On receiving message victim sends 2 hop verification request to preexisting channel all nodes will reply with 1 hop neighbor list ,if victim name is present in all list then it can elect as MPR . But this method has a problem in the initial network formation and also for the edge node verification.

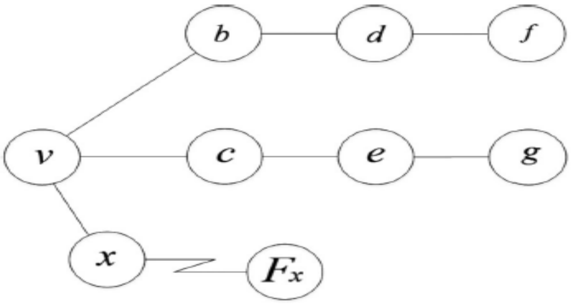
[4] In this paper black hole attack is being mitigated by using data routing information table that contains the details on how many transactions has happened from and through the node. There is one entry for every node in network if the table value is found to be 0 then the node will be black hole attacker and is isolated from network.

III. PROPOSED SOLUTION

This proposed method uses the fictitious node mechanism for identifying the attacker. The basic requirements is that

1. Node in the network should use only the information that is available with it
2. Instead of verifying the HELLO message node checks for the contradiction between message and known topology
3. Here we also assume that topology control message cannot be duplicated that is because no one can stop victim node from transmitting TC message that discloses the attacker.

For a node to defend itself it uses same technique as that of attacker that is by creating its own fictitious node. Details of that node will be included in the HELLO message and transmitted to all its neighbors. With the reply message that it receives by verifying the contradiction it finds if the node is real or attacker.



Identifying contradictions to prevent node isolation attack.

Consider the above here let v be victim and x is the attacker v send that it has a node vx in its HELLO message . now since x wants it to be selected as MPR it replies to v by telling that even x has the route to vx . by checking v gets to know that x is the attacker therefore x will be isolated during any transaction that causes the denial of service attack.

Using the same algorithm by imncluding DRI table in the routing table we can easyly defend black hole attack also . here we also use 2 more control messages ie further request (FREQ) and further reply (FREP).

Each node maintains the DRItable that keeps track of whether node has done transaction with its neighboring nodes. The table 3 column that is node id , from and through. During the transaction DRI table details will also be shared. Exanple of DRI table is given below

TABLE 1: SAMPLE DRI TABLE

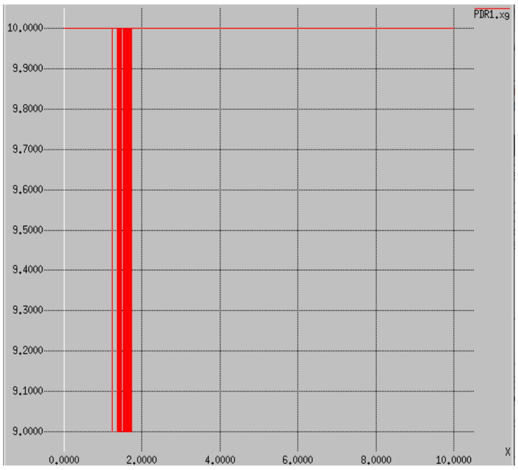
Node id	Data Routing Information	
	From	through
3	1	0
6	1	1
2	0	0

If at all souse node cant verify DRI table with its table then it sends FREQ messages to all the intermediate nodes IN.IN replies with FREP tat include DRI as well as next hop neighbore details.

IV. PERFORMANCE METRICS AND RESULTS

In this section we show the results of the simulations. Each simulation was tested with and without attack. When no attack was carried out, the results are substantially better than the same simulation under attack with the protection of the proposed algorithm.According to the third simulation settings, attacking nodes are fixed without any movement. The number of fictitious nodes was estimated using the fictitious setting mechanism. In the simulation three parameters are being tested with and without applying the algorithm in the network environment.

First when we look at the packet delivery ratio the following results were obtained



Figuer 1. depicts packet delivery ratio without using the algorithm

Here x axis shows time in milli- seconds and y axis shows the number of packets transmitted. Transmission of data starts 1.0 as we can see lot of packets have been dropped, therefore causing loss in the system. Graph above represents the packet delivery ratio during one transaction.

Same scenario was tested by invoking the proposed algorithm on the same network, following results was analyzed

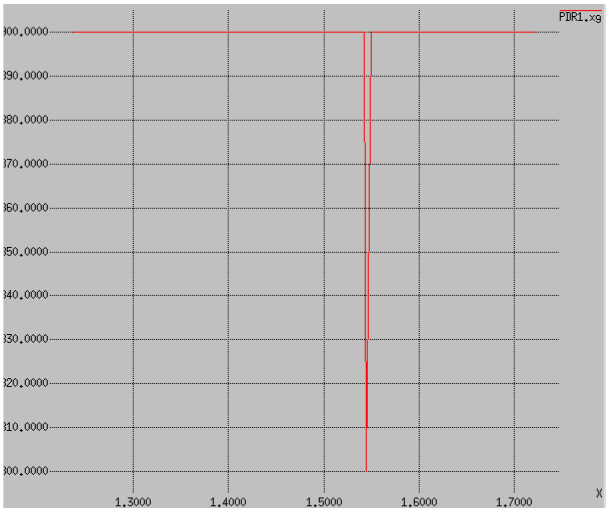


Figure 2. Packet delivery ratio with proposed algorithm

As depicted only at certain point of time i.e. during identification of the attacker node packet drop occurs otherwise PDR will always be one. Compared to fig 1 we can notice that the packet drop is extremely reduced when we use the proposed defending technique.

Next parameter being tested is the energy remaing in the nodes after the transaction of data packets is carried out. Initially in the implemented networkevery node is given 100 joules of energy. The left out energy in the network is calculated using the following formula:

Energy remaining in network =
total energy – average deplited energy

$$\text{Avg deplited energy} = \frac{\text{total energy deplited}}{\text{total nodes}}$$

Total energy = 100*no of nodes

Figure 3 shows the reamining energy graph. X axis represents the energy in a node and y axis represents time in milli seconds. Red line in the graph shows the energy in node when defending technique is used and the green line shows the energy level when algorithm is not used .

When both are compared we can see clearly that energy consumtion is less with the use of defending technique in the network.

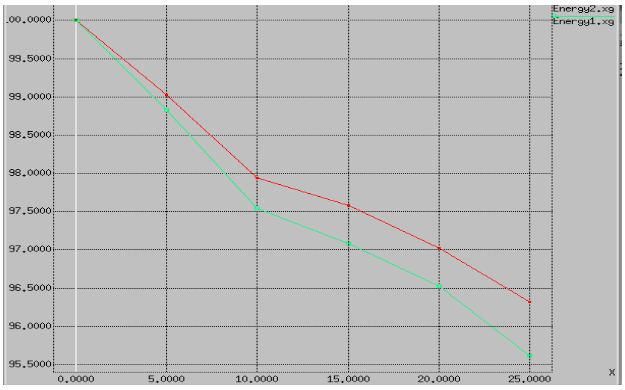


Figure 3. Remaining energy level in node

Figure 4 depicts the packet drop without the use of proposed algorithm

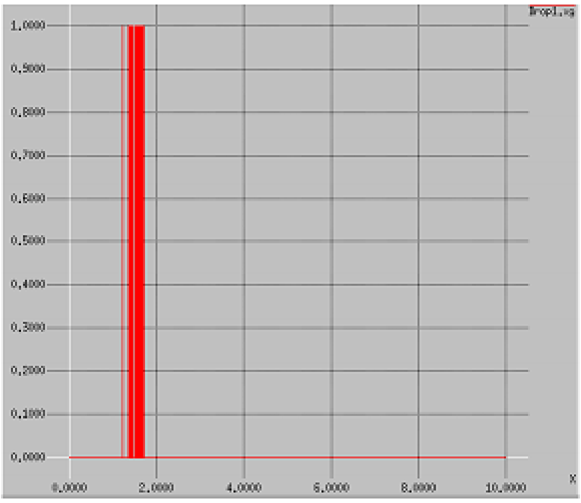


Figure 4. Packet drop without algorithm

Figure 5 shows the packet drop with the use of proposed algorithm.

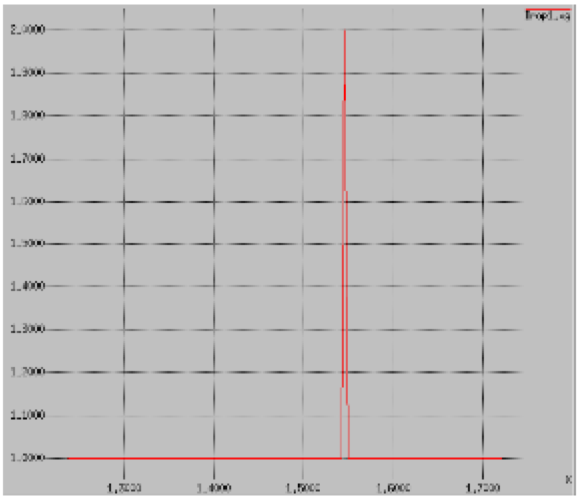


Figure 5. Packet drop when algorithm is applied

V. CONCLUSION AND FUTURE WORK

In this paper, we have presented a solution whose function is to prevent node isolation due to denial of service and black hole attack in which the attacker manipulates the victim into appointing the attacker as a sole MPR, giving the attacker control over the communication channel. We further strengthened the attack by giving the attacker the ability to follow the victim around.

Simulation shows that solution successfully prevents the attack, specifically in the realistic scenario in which all nodes in the network are mobile. Transmission time also is reduced with increase in packet delivery ratio. Energy is also managed so that the nodes in the network have longer life time. We expect that with little adjustments, proposed solution can protect OLSR from the family of attacks that centers around the falsification of HELLO messages with the intention of being appointed as sole MPR.

VI. REFERENCES

[1]. Nadav Schweitzer, Ariel Stulman, Member, IEEE, AsafShabtai, and Roy David Margalit " Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes"

[2]. P.Jacquet, P. Mijhlethaler, T.Clausen, A.LaouitiHipercom project, INRIA Rocquencourt, BP 105, 78153 Le chesnaycedex, france "optimistic link state routing protocol for ad hoc networks"

[3]. IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.4, August 2014 103 "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORK"

[4]. HesiriWeerasinghe, IEEE Student Member, Huirong Fu, IEEE Member" Preventing Cooperative Black Hole Attacks in Mobile Ad HocNetworks: Simulation Implementation and Evaluation"

[5]. S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network." (Aug. 10 2006) uS Patent App. 11/351,777.Online].Available: http://www.google.com/patents/US20060176829

[6]. M. Marimuthu and I. Krishnamurthi, "Enhanced olsr for defense against dos attack in ad hoc networks," Commun.Netw., J., vol. 15, no. 1, pp. 31–37, Feb. 2013.

[7]. C. E. Perkins and P. Bhagwat, "Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers," in Proc. Conf. Commun. Archit., Protocols Appl., 1994, pp. 234–244.

[8]. C. Perkins and E. Royer "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., Feb. 1999, pp. 90–100.

[9]. E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in Proc. 32nd IEEE Conf. Local Comput. Netw., Oct. 2007, pp. 1043–1052.

[10]. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proc. Med-Hoc-Net, 2003, pp. 25–27.