ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Controlling Malicious Behavior of Nodes Using Energy and Buffer Mechanism in DSR

Priyanka

Department of Computer Science and Engineering, Lovely Professional University, India

Abstract: MANET's is the form of wireless network (WLAN). And Ad-hoc network is infrastructure less. They does not need any centralized system or any kind of infrastructure. Each node in the Ad-hoc network will act as router and will route the packet to the destination. DSR is an on-demand routing protocol. This means routes are not pre-established routes and routes are only active during the transmission. The main problem in the MANET is attack on data. As we know in MANET we cannot differentiate which node is the attacker node and which is benign node. So, the attacker node can easily capture the data. And these types of attacks are known as Black-hole, worm-hole and gray-hole attack. So, identifying which node is genuine node or for preventing the data from the attacker node is necessary in MANETs. This paper provides the good technique which helps in preventing from these types of routing attacks during data transmission. And this leads to the secure communication as we select the intermediate node on the basis of its energy and buffer state. This paper consider the two parameters for selecting the forwarding nodes, first one is their energy state and their buffer value. Only those nodes will participate in the transmission which have their energy state equal to some threshold value and have the less buffer value. Because the attacker nodes have less energy due to continuously sending the RREP message to the nodes and have high buffer value as it always attract the neighbor nodes for transmission. So, the implemented technique only selects the nodes which seem to be genuine on the basis of measuring two factors its thresh-hold energy and buffer value of the IN. And this result into the less packet loss as compared to the DSR. And even if the attacker captures the packets, the packets will be in encrypted form. Attackers have to decrypt the packet for reading it and its really hard to decrypt them. The packet loss will be less in the proposed technique and throughput will be increased.

Keywords: DSR, WLAN, MANET, IN, RREP and RREQ.

I. INTRODUCTION

In Dynamic routing protocol as the name suggest the routes are dynamic. The path can be different for the different packets even if they have the same source and destination. Dynamic routing protocol is good for the frequent changes of host. As we know in Ad-hoc network nodes frequently moves. But in DSR protocol all nodes are in promiscuous mode. This means whether the packet is for them or not it will send the packet to all nodes irrespective of the destination.

In Ad-hoc network there are some difficult problems for designing the routing protocol.

1) The main challenge for designing the routing protocol for the Ad-hoc network in wireless communication. Without any infrastructure and hardware making the communication is difficult.
2) Second main challenge is dynamic topology. As we know in Mobile Ad-hoc network the mobility of the host is always there. So, changing the network topology in the MANET is frequent. So, designing the routing protocol against the dynamic topology is really difficult.
3) Third one is broken link, links will be broken if any of the nodes moves to another location. During the data transmission through the particular link, if any of the node that comes in selected route moves to another network or another location. That link will said to be broken.

In DSR protocol when the source wants to send data to some destination, as we know DSR protocol is reactive so the route discovery process will start. Because the routes are not pre-established and for sending the data to the destination we must know the route.

This paper discuss about the DSR protocol which is efficient for the multi-hop communication. As the name suggests DSR (Dynamic Source Routing) is based on the source routing. And in DSR all information is maintained at the mobile nodes and periodically updated. And for the route establishment it has two phases.

1.1 Route discovery- When the source wants to send some data to the destination then the RREQ (Route Request) process will be start. The source node will broadcast the RREQ packets to all its neighbors. All the nodes maintain the list of INITIATOR ADDRESS and REQUEST ID. When the nodes receive the RREQ packet, it will check its list and if it already contains the INITIATOR ADDRESS and REQUEST ID in the list then it will discard the RREQ packet. If list doesn't contain the REQUEST ID then it will again broadcast the RREQ packet and this process will be continue until the RREQ packet will reach at the destination.

1.2 Route Maintenance- Links can be broken betweens the nodes due to the mobility or may be because of other reasons. And in DSR if the link broke between the nodes which comes in the route, then the RERR

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

(Route Error) packet will be sent to the source. The main purpose of RERR packet is informing the source node about the broken link. All the nodes that hear the RERR packet will update their route cache to remove the broken route. So, in DSR the route cache reduce some of the cost of the route discovery if the route is already available in the cache.

II. PROBLEM FORMULATION

DSR is an on-demand routing protocol. This means routes are not pre-established routes and routes are only active during the transmission. The main problem in the MANET is attack on data. As we know in MANET we cannot differentiate which node is the attacker node and which is benign node. So, the attacker node can easily capture the data. And these types of attacks are known as Black-hole, worm-hole and gray-hole attack. So, identifying which node is genuine node or for preventing the data from the attacker node is necessary in MANETs. This paper provides the good technique which helps in preventing from these types of routing attacks during data transmission. And this leads to the secure communication as we select the intermediate node on the basis of its energy and buffer state. This paper consider the two parameters for selecting the forwarding nodes, first one is their energy state and second is buffer value. Only those nodes will participate in the transmission which have their energy state equal to some threshold value and have the less buffer value. Because the attacker nodes have less energy due to continuously sending the RREP message to the nodes and have high buffer value as it always attract the neighbor nodes for transmission. And even if the attacker captures the packets, the packets will be in encrypted form. Attackers have to decrypt the packet for reading it and it's really hard to decrypt the data. The packet loss will be less in the proposed technique and throughput will be increased.

III. PROPOSED TECHNIQUE

As we know DSR protocol is on-demand and especially for the multi-hop transmission. During the route discovery process the shortest route between the source and destination will be chosen. And it is really hard to identify the attacker node among the other nodes in the mobile Ad-hoc network. So, identifying the Attacker node is necessary for the reliable transmission. When the sender is sending the data towards the destination then attacker may capture the data because the attacker or malicious node always sending the RREP packets to its neighbors informing that I have the shortest path towards the destination. As we know DSR protocol chooses the shortest path so the path through the attacker have will be chosen. So, identifying the attacker's nodes is necessary for the secure transmission. And if the attacker nodes capture the data then it may misuse, drop or broadcast that data in to other networks. So, some mechanism should be there for identifying the genuine nodes while transmission based on some parameters while sending the data to the particular node.

Methodology in steps-

1) In DSR protocol packets can choose any of the paths even if they have same source and destination. So, during the data transmission there should be some mechanism for selecting the particular path for sending the data to any of the intermediate node.
2) It is really hard to identify the attacker node in mobile ad-hoc network. But for the data transfer we have to send it through the intermediate nodes if destination is not in the direct range of the sender.
3) The attacker node is always sending the RREP to all its neighbors' node informing that it has the path to the destination.

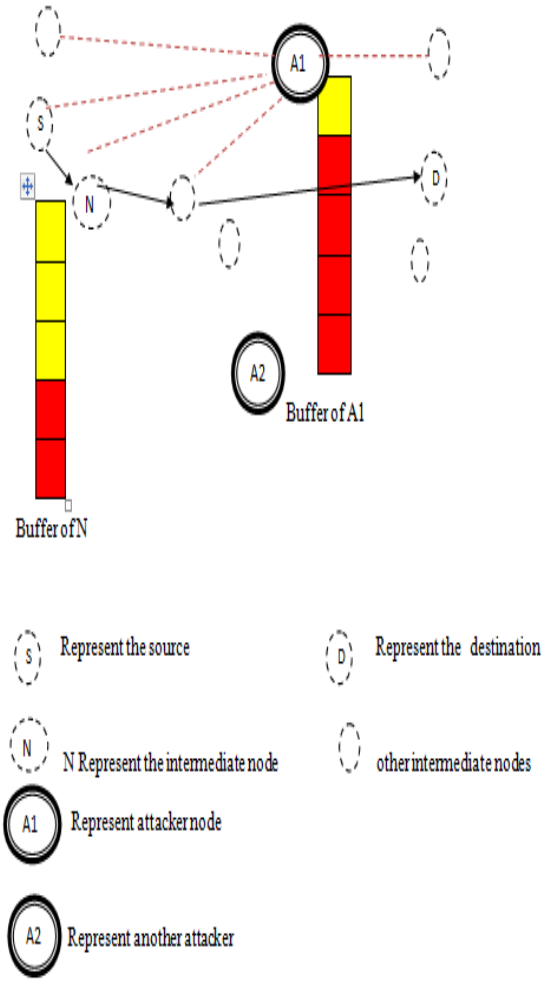

Figure 2.1 Nodes with Buffer

And this will result in to the energy consumption of the attacker node. Attacker node continuously sending the RREP to the node it will lead into decreasing in the energy of the attacker node. Attacker node has low energy.

4. As the attacker node always try to attract the neighbor node for the data transmission, attacker will always get involved in the communication. Each node have buffer associated with it in which all the request comes and served accordingly. Attacker node will mostly get involved in the transmission as it attracts more neighbors for transmission.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

5) There may be some cases in which attacker have not lost energy and also have less buffer value. So, in those cases even if attacker captures data, the data should be in encrypted form and attacker will not able to understand it.
6) The proposed technique is considering the two parameters for selecting the route the first one is energy and second is buffer value. While sending data to some intermediate node we firstly check the energy and buffer value of that intermediate node.
7) If that intermediate node is having more energy and less buffer value then we select that intermediate node for transferring the data. And if the energy value is low and buffer value is high then we will not send the data to that node and check for other intermediate node.
8) And even if the attacker node captures the data, data will be in encrypted form. So, it enhances security when the attacker captures data.

IV. CONCLUSION

It is really hard to identify the attacker node in the mobile Ad-hoc network. DSR protocol is for multi-hop transmission and it select the route on the basis of shortest distance. Only those nodes will participate in the transmission which have their energy state equal to some threshold value and have the less buffer value. Because the attacker nodes have less energy due to continuously sending the RREP message to the nodes and have high buffer value as it always attract the neighbor nodes for transmission. So, the implemented technique only selects the nodes which seem to be genuine on the basis of measuring two factors its thresh-hold energy and buffer value of the IN. And this result into the less packet loss as compared to the DSR. Attacking on the DSR protocol is easy as the protocol works on the shortest distance. Choosing the path on the basis on energy and buffer value in DSR protocol will result into increased throughput because of less packet loss and provide the extra security by encrypting the data. So, even if the attacker captures the data, the data will be in encrypted form. For future work we can implement this technique for the multicast routing protocols using some security models like PGP. So, that we can provide the security in multicasting and adding the security model will result in to more security.

REFERENCES

[1]. Hatware, Isha V., Atul B. Kathole, and Mahesh D. Bompilwar. "Detection of Misbehaving Nodes in Ad Hoc Routing." International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 2 (2012).
[2]. Sukumran, Sangheetaa, Venkatesh Jaganathan, and Arun Korath. "Reputation based dynamic source routing protocol for MANET." Int. J. Comput. Appl 47.4 (2012): 42-46.
[3]. Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Applications", International Journal of Computational Engineering & Management, Vol. 11, January 2011, 32-37
[4]. Hollick, Matthias, et al. "On the effect of node misbehavior in ad hoc networks." Communications, 2004 IEEE International Conference on. Vol. 6. IEEE, 2004.
[5]. Parashar, Gargi, and Manisha Sharma. "Congestion Control in Manets Using Hybrid Routing Protocol." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834.
[6]. Rohal, Pankaj, Ruchika Dahiya, and Prashant Dahiya. "Study and analysis of throughput, delay and packet delivery ratio in manet for topology based routing protocols (aodv, dsr and dsdv)." international journal for advance research in engineering and technology 1 (2013).