Enhancing Security in DSR Protocol with Energy and Buffer Control Mechanism

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

Harwant Singh Arri
Department of Computer Science and Engineering,
Lovely Professional University, India

ABSTRACT

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. 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 it's really hard to decrypt the data. The packet loss will be less in the proposed technique and throughput will be increased.

Keywords- DSR, MANET, AODV, IN and RREP

1. INTRODUCTION

This paper contains the information about DSR protocol and how to prevent data from the attacker or from malicious nodes in DSR protocol using the energy and buffer control mechanism. As we know the DSR protocol works of selecting the shortest path between source and destination. While transferring the data from source to destination node the intermediates nodes are going to take part if the destination is not in the range of source. And these intermediates nodes can be malicious or attackers and may misuse the data. So, there should be some criteria for choosing the particular intermediate node for forwarding the data. DSR protocol only works for medium or small size of networks.

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 (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.

2. AD-HOC ROUTING PROTOCOLS

Ad-hoc routing protocols are divided in to two categories based upon which we can differentiate between the protocols.

Table 2.1 Comparison between proactive and reactive protocols

Comparison Factor	Proactive	Reactive
Availability of route	Always Available from routing tables.	Available only when needed after the Route Discovery
Control Overhead	High	Lower than Proactive routing protocols.
Periodic Updates	Yes, Periodic Advertisement	Not required, only when requested
Storage requirements	High	Lower than Proactive Routing protocols.
Bandwidth Requirements	High	Low
Power requirements	High	Low
Delay	Small as routes are pre-determined	Higher than proactive
Scalability	Up to 100 nodes	Up to few hundred nodes
Handling mobility	Occur at fixed interval	Use local route discovery
QOS	Mainly shortest path as the QOS metric	Few can support QOS, although most support shortest path.

3. PROPOSED WORK

As we know DSR protocol is on-demand and especially for the multi-hop transmission. During the route discovery process any of the route between 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 any path so the path through the attacker may be chosen. So, identifying the attacker's nodes is necessary for the secure transmission. And even if the attacker nodes capture the data then also the message should be in encrypted form, some encryption algorithm should be used. Because the attacker node 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. And even if it fails sometimes to identify the attacker node, the data that we are transferring should be in encrypted form.

3.1 Proposed Methodology

The proposed methodology is as follows-

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. 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.

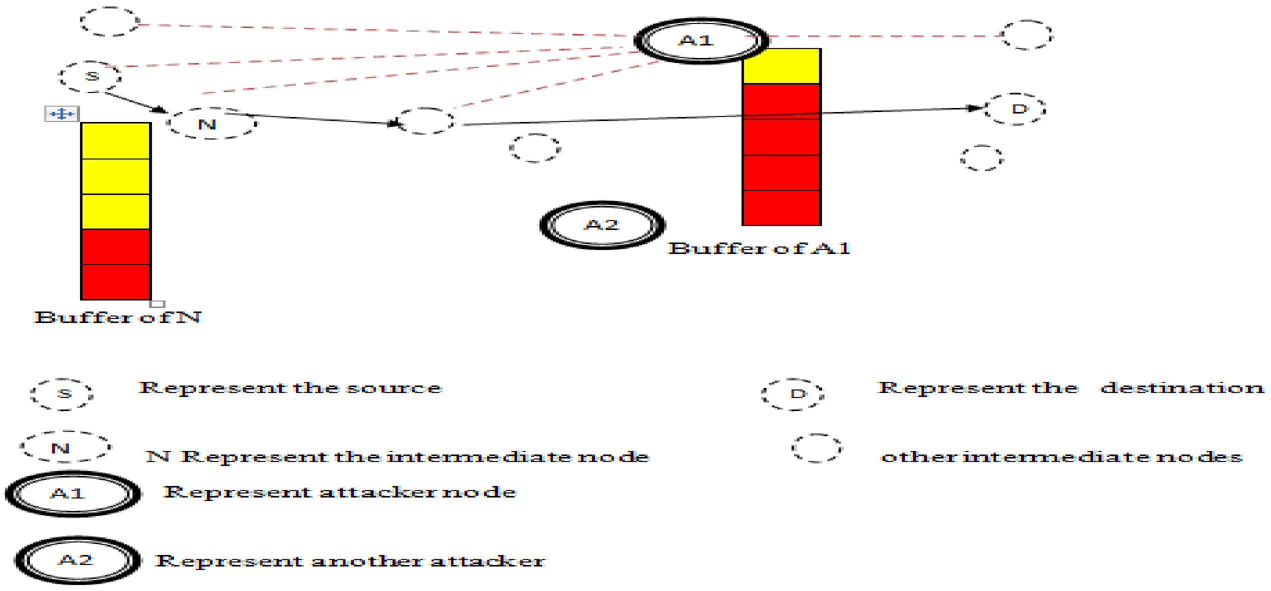
5. There may be some cases in which attacker have not lost energy and also have less buffer value. So, in those cases even if attacker captures data, the data should be in encrypted form and attacker will not able to understand it.

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.

Figure 3.1


A1
S
N
D
A2
Buffer of A1
Buffer of N
S Represent the source
D Represent the destination
N N Represent the intermediate node
other intermediate nodes
A1 Represent attacker node
A2 Represent another attacker

This technique has the two parameters on which we can decide the forwarding nodes. As we know in worm-hole attack attacker always send the RREQ packets to all its neighbor nodes informing that I have the path to the destination. So it becomes easier for the attacker. The attacker node continually sends the packet to its neighbor nodes so the energy of the attacker node keeps on decreasing. And the second parameter is its buffer value, as the attacker nodes attract its neighbors for the transmission its buffer will be nearly full. As the attacker node always attract its neighbors that's why the attacker node will always involved in the communication. The node which is not attacker node will have less buffer value and more energy. And even if the attacker node captures the packet then the attacker node will not able to decrypt the data because the data which is going to transfer has been encrypted.

3.2 Algorithm

Data: n_i (any given node), S (sender), $D^k_{1\text{-hop}}$ for all k€N_1^l, B€Br_1^i (Buffer of nodes from 1 to i), E€E_{k1}(Energy of node), energy threshold.

Result: F_i , the forwarder list

Begin

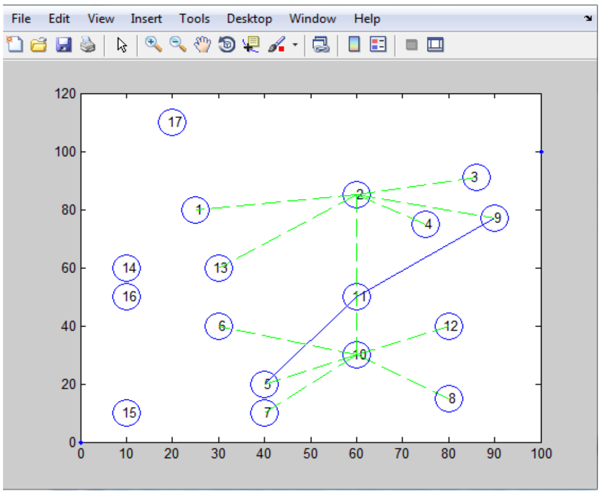
```
C ← $N_1^i – N_1^S$
    /* Select neighbours with one-hop dominating nodes other than one hop neighbours and node itself
For $n_k$ € C do
$\mu[k] \leftarrow Ø$
For $n_l$€ $D_{1\text{-hop}}^k$ do
If $n_{l\ 1}$€ $(N_1^i+n_i)$&& ($B_l$!= full) && $E_e$ > threshold
$\mu[k] \leftarrow \mu[k] +\{n_l\}$
For $n_k$€ C do,
For $n_m$ € $\mu[k]$ do
If ($n_l$ != $n_k$) € C ,$n_m$€ N
$\mu[k] \leftarrow \mu[k]- n_m$
If $\mu[k]$ ==0 then
If ($B_k$ != Full && energy > threshold)
C ← C- $n_k$
$F_i \leftarrow$ C
Return $F_1$
End
```

4. SIMULATION AND ANALYSIS

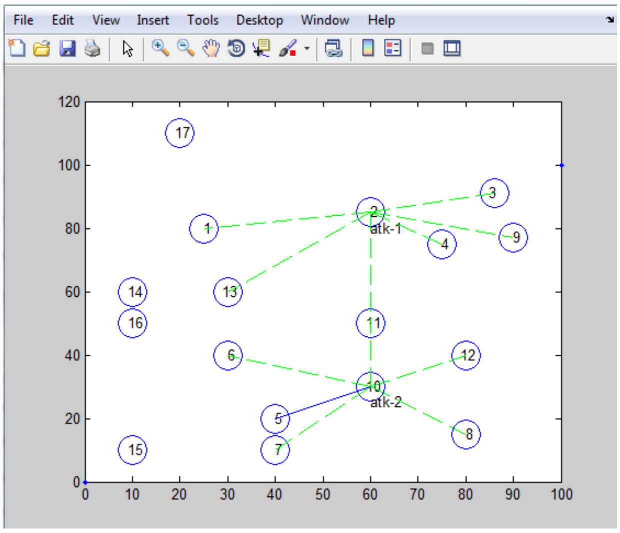
We have done simulation for the 17 nodes. And there are two attacker nodes present in the network node 2 (attacker) and node 10 (attacker). Initially the energy and the buffer of all nodes is equal. As we try to send the packets to the destination the attackers nodes keeps on sending the RREP packets, so there energy will decrease. And the buffer value of attacker nodes keeps on increasing as the communication start.

4.1 Simulation

The following simulation shows the buffer and energy mechanism. Attacker node 2 and 10 will always send the RREP to all its neighbours. And here the path will be selected on buffer and energy value.



Method 1



Method 2

4.2 Results

In method 2 the simulation without energy and buffer mechanism is there when the route will only selected on the basis of distance and in this case the attacker node 10 is capturing the packet because attacker node 10 sending RREP informing that it have path through to the destination.

Now the result graphs for the method 1 and method 2. The following graphs show how results are different. When the route is selected on the basis of energy and buffer value then the packet loss will be less. When the packet loss is less then automatically throughput will be increased.

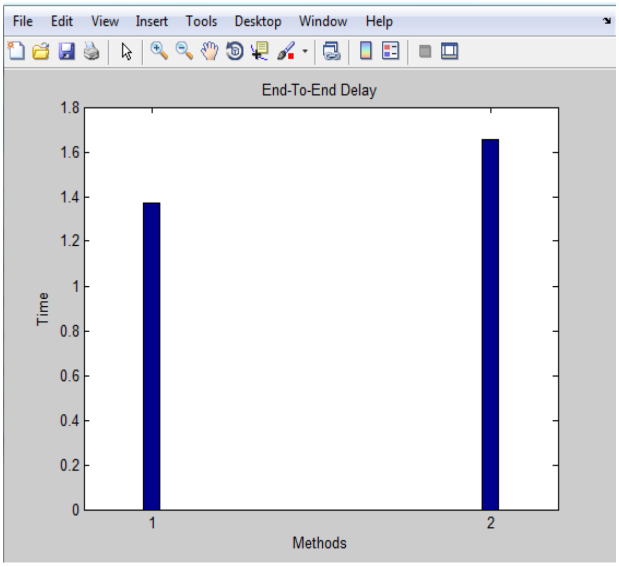


Figure 5.2.1 Graph for End-to-End delay

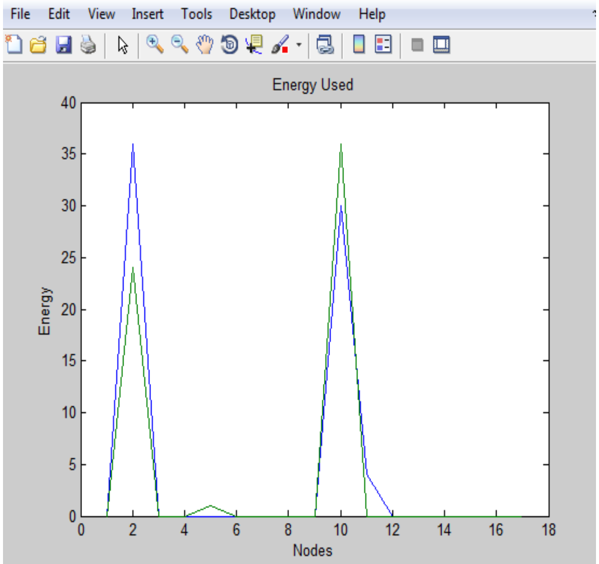


Figure 5.2.2 Energy Graph for nodes

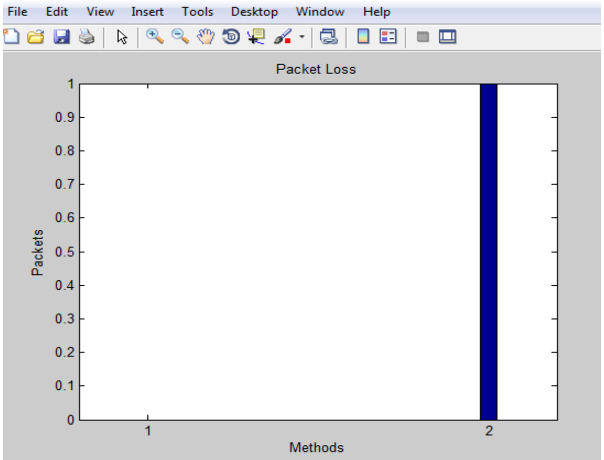


Figure 5.2.3 Packet loss for both methods

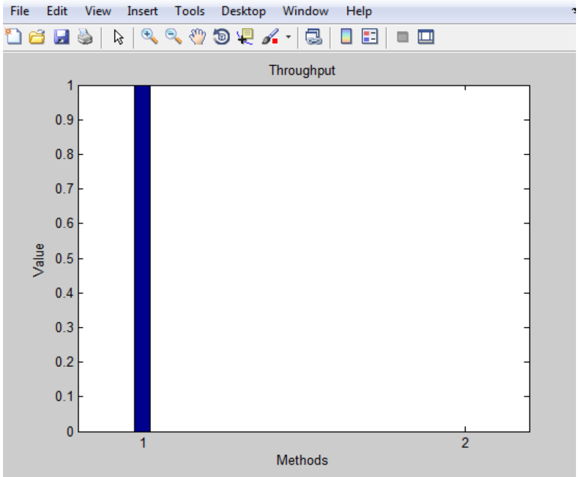


Figure 5.2.4 Throughput for both methods

We can clearly differentiate between the methods. Packet loss in case of DSR with buffer and energy control mechanism is less as compared to the DSR and if the packet loss is less then automatically the throughput will be increased in our case. And also the End-to-End delay in our case is less as compared to previous one. We can see the energy graph which also shows that energy consumption by the nodes. So, the results we got are better than the previous DSR protocols.

5. CONCLUSION AND FUTURE SCOPE

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. 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.

6. REFERENCES

[1] Tuteja, Asma, Rajneesh Gujral, and Sunil Thalia. "Comparative performance analysis of DSDV, AODV and DSR routing protocols in MANET using NS2."*Advances in Computer Engineering (ACE), 2010 International Conference on*. IEEE, 2010.

[2] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Wormhole attacks in wireless networks." *Selected Areas in Communications, IEEE Journal on* 24.2 (2006): 370-380.

[3] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi."Manet: Vulnerabilities, challenges, attacks application."*IJCEM International Journal of Computational Engineering & Management* 11 .2011 (2011): 32-37.

[4] Bouhorma, Mohammed, H. Bentaouit, and A. Boudhir. "Performance comparison of ad-hoc routing protocols AODV and DSR." *Multimedia Computing and Systems, 2009. ICMCS'09. International Conference on*. IEEE, 2009.

[5] Sanzgiri, Kimaya, et al. "A secure routing protocol for ad hoc networks."*Network Protocols, -2002. Proceedings. 10th IEEE International Conference on*. IEEE, 2002.

[6] Cai, Jiwen, et al. "The simulation and comparison of routing attacks on DSR protocol. "*Wir -eless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th Internatio -nal Conference on*. IEEE, 2009.

[7] Parashar, Gargi, and Manisha Sharma. "Congestion Control in Manets Using Hybrid Routi ng Protocol." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834.