***I.J. Wireless and Microwave Technologies*, 2016, 5, 54-60**
Published Online September 2016 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2016.05.06

***Available online at* http://www.mecs-press.net/ijwmt**

Securing DSR for Mobile Ad hoc Network with Message Digest Algorithm

Pooja Kundu[a], Neeti Kashyap[b]

[a]*M.Tech. Student, NCU,Gurgaon*
[b]*Assistant Professor, NCU,Gurgaon*

Abstract

Mobile ad hoc networks (MANETs) are very useful in various scenarios where there is need of fast deployment of the network and expensive set up is not required. With these benefits, there are some issues related to these networks. One of these issues is of secure communication. Malicious nodes can easily attack existing routing protocols for MANETs like DSR. In this paper we have proposed a modification of DSR by using message digest. The proposed work produces better results in terms of different metrics when compared with the results of DSR. When a route is set up between the two communicating mobile nodes, the data is sent through a secure key which is not impossible for the intruder nodes to intercept. This halts intrusion in the network. A message digest is created of the data packets.

Index Terms*:* MANET, ad hoc networks, intrusion detection, Black hole attack, Gray hole attack, Message Digest, Secure key.

1. Introduction

Mobile ad hoc networks (MANETs), because the name offers the impression it consists of mobile nodes. Nodes move freely within and outdoors such network. Nodes of these networks have to act as a router and contain a battery related to them, which is restricted in power or is anticipated to discharge when it is slow. There's no want of a base station for these networks as nodes are serving to one another to relay information packets. They're extensively helpful once we have to be compelled to deploy a network in a very disaster prone space, in defense work, just in case of associate degree emergency conference, classrooms, etc. They're low cost to handle as their created in a very specific space doesn't need a base station. Once nodes die out of battery or are near to die, they begin dropping packets resulting in decrease in packet delivery magnitude relation. This

*Corresponding Author: Contact number: 9996089448
E-mail address:poojakundu9999@yahoo.com

behavior of nodes is named stinginess. There are some malicious nodes within the network, that don't transfer packets to the destination and leads to denial of service. Existing routing protocols for MANETs don't take into account the problem of security. [10] They simply take into account the shortest path because the best path to transmit information. However, typically the trail will contain malicious or ungenerous nodes. [1] In our paper, we've got changed the DSR (dynamic supply routing) protocol with the assistance of message digest (MD5) to extend security and avoid selecting routes with malicious nodes. The projected formula secures the network from region attack and grey hole attack. The paper is split into many sections. Section a pair of consists of the introduction to DSR and a number of other security attacks within the impromptu networks, and section three consists of the analysis work wiped out detective work attacks and use of hash keys in impromptu networks to produce higher security. Projected work is delineating in section four together with the design of the modification done to the DSR. Simulation results which show comparison between the DSR and modified DSR are presented in the next section. Results deduced by simulating the network are concluded in the section 6.

2. Dsr and Attacks in Manet

2.1. Attacks in the MANET

MANETs are susceptible to various types of attacks such as Black hole attack, Sybil attack, and packet dropping attack. [2] Our proposed algorithm prevents Black hole attack and Gray hole attack. In black hole attack, a node claims that it has the route to the destination which is not true and starts dropping the packets. In figure 1, source node, S when broadcasts the route request (RREQ), nodes reply with route reply (RREP) if they have a route to the destination node. Some malicious nodes like M may falsely claim the route to the destination and sends RREP to the source nodes. When S sends data packets to M, it starts dropping the data packets and the packet delivery ratio decreases. Many techniques have been developed to combat with black hole attack. [3] Gray hole attack [4] are similar to black hole attack but unlike the Black hole attack they transfer the packet occasionally

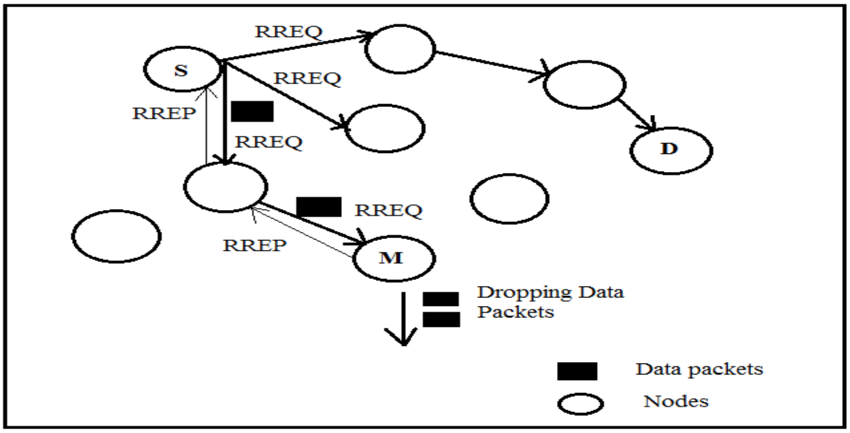


Fig.1. Black Hole Attack

2.2. DSR

Dynamic source routing protocol [5] is used by wireless ad hoc networks. This routing protocol is called an on- demand protocol which does routing whenever demanded. When a routing path has to be established only then the request is broadcasted in the network. To broadcast the request to other nodes in the network, a route request packet is used. In a route request packet, several fields are present like source id, destination id, packet length, flags. Neighboring nodes when receive a route request packet, they check their table for if they have the rout to the destination or route to the intermediate nodes. Each node maintains such table with it which specifies route information. Those nodes which can help to establish the rout reply with a route reply packet. Thus, DSR protocol works with the help of these packets.

3. Related Work

The technique used in [6] states that the reliability of nodes is measured with the help of information present in the fidelity table. If a node has 0 value for the fidelity level, then it is a black node which can cause black hole attack. An on-demand routing protocol, AODV is modified and alarm packets are being sent on detection of a black node so that other nodes get information about the malicious nodes which belong to the network.

There are other techniques as well for detection of black hole attack. Thachilet. al. in [7] proposed a trust based scheme in which nodes are responsible for maintaining trust values at their level and nodes which have trust value below a certain value called threshold then the node is called a black node. A DSR based scheme BDSR [8] uses a bait technique to allure malicious nodes. In [9] a game theoretic approach is implemented. Black hole attacks are one of denial of service attacks. The presented approach asks the nodes to help in mitigation against such attacks. Nodes listen to their neighboring nodes and try to find the suspicious node if any. They work together to filter out such nodes. Filtering of packets is done as there senders sign them. Those nodes which help to perform this are rewarded in the form of incentives.

4. Proposed Work

The proposed work is a modification to the existing routing protocol DSR. The modification is done to the existing route request format and route reply format used by DSR protocol. Each maintains a routing information table when DSR protocol is being used by the network. This table is also modified and new field is added to it.

4.1. Modified Routing Information Table

Routing information table is modified by adding a new field to it which is success and is called modified routing information table (MRIT). The value under the success field is initially set to 0. Information about one hop away neighbors can be gathered with the help of MRIT. When a node successfully transmits the data packet without dropping it, the value at success field in the MRIT is incremented by 1. If a node does not succeed to transmit the data packet, the success value is decremented by 1. When several options are present to send the packet to the destination then this table can be used to find out which nodes have a high success rate. MRIT is updated either when a connection is established or packets are successfully transmitted or when a node which is malicious transmits a data packet as a reply to the node requesting path. An example of MRIT is shown in the table 1.

Table 1. Modified routing information table

Node_id	Send_to	Receive_from	Success
1	4	1	0
2	2	4	3
3	3	2	2
4	1	3	2

4.2. Modified RREQ and Modified RREP

DSR protocol uses RREQ and RREP for communication’s link establishment. In our algorithm we use the modified RREQ (MRREQ) and modified RREP (MRREP). A message digest of destination node’s address is created at the source node and is added to the broadcasted MRREQ. A key which is secret, shared between nodes acting as source and destination. When the destination node sends reply with the help of MRREP, it also sends a message digest of its address encrypted with the shared key. A malicious node is not able intercept the secret key and is not able to convince the source node to transmit the data packet by using it as an intermediate node.

4.3. Working of Algorithm

When a packet of data has to be transferred by the source node, it tries to take help from intermediate nodes present in between the node acting as a source and the node acting as a destination. Firstly, a MRREQ is broadcasted in the network. A key is shared between the nodes acting as source and destination, which is not known to other nodes and thus a secret key. Nodes which can act as intermediate nodes reply with a MRREP. When MRREP reaches to the source node, it does the following:

- Checks the message digest of the destination node address in MRREP.
- Declares a path validated or invalid.
- Chose the validated path with maximum values for success field in the MRIT.
- Decrements or increments the success value of nodes in MRIT.

With the concept of secrecy of the key, it is used by the source node to compare the message digest in MRREQ and MRREP. If they match then the route is a valid route. Several valid routes can be available. Out of those paths, a path having the maximum number of success value of intermediate nodes is chosen as the best path to transmit the data packet. After the path is validated, MRIT table is updated and the values of success field are incremented for the nodes present in the validated route.

A malicious node is detected when it sends the false reply that it has a route to the destination because it fails to create a message digest same as that of the original destination address. When any node acts as a malicious node and other nodes help to do so, in that case the path is declared invalid by the source node. Also, each node which is present in the network updates its MRIT by decrementing the value of success of all the nodes present in the invalid path. Figure 2 explains the working of the proposed work.

The success value helps further while choosing the path to send the data packets. This is why it is updated every time; a path is validated and even when the path is declared invalid. When a node reaches a negative value of success field in MRIT, it is declared a black node. Such node is not used in future for communication in the network. Following is the pseudo code of the above mentioned algorithm:

```
1. Source node generates message digest.
2. Source node broadcasts MRREQ.
3. Intermediate nodes send MRREP.
4. At source node, validation test is done.
5. If a path passes the validation test route is validated

increment the success value
else
route is invalid
decrement the success value
```

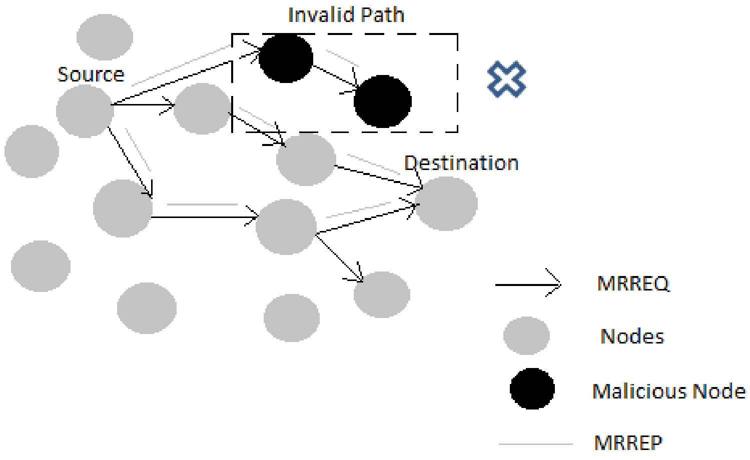


Fig.2. Secure packet transmission with modified DSR

5. Simulation Results

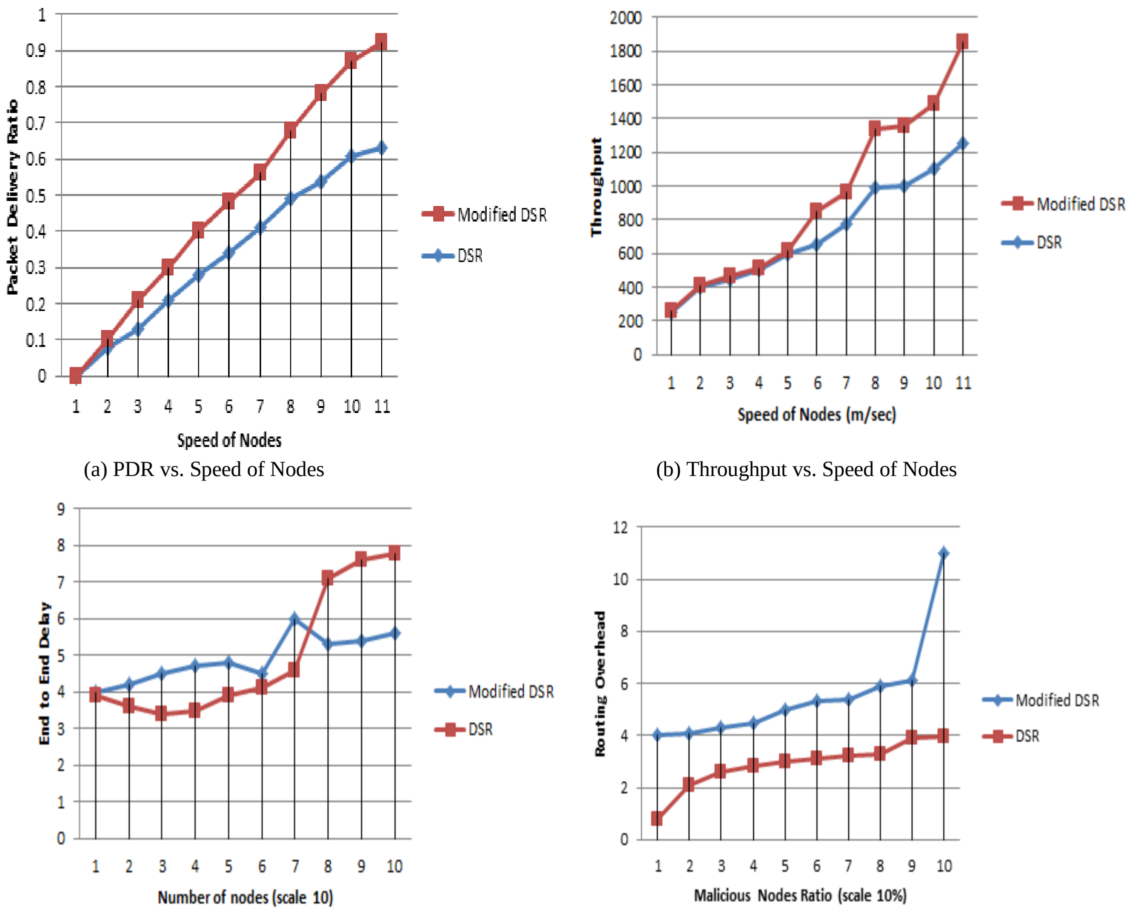
Network simulations are used in this section to demonstrate the improved performance by the modified DSR. For simulation the parameters used are listed in table 2. DSR shows a deficient delivery of packets in the presence of mobile nodes and malicious nodes. Since DSR protocol cannot detect and respond to attacks, packet delivery ratio is poor. PDR ratio tells how many packets are actually delivered to the destination out of the packets sent to the destination. On the other hand, when modified DSR protocol is used in a network, it delivered packet with 83% higher than the existing DSR protocol. Existing DSR protocol is not able to handle high speed of nodes but with the modifications suggested in the proposed work, PDR increases even when the mobility of nodes is increased. Mobility of nodes is measured in meters/ second. Figure 3(a) presents the comparison of DSR and Modified DSR on the basis of PDR vs. Speed of Node. Efficiency of modified DSR can be easily perceived with the help of figure 3(b). There is a significant improvement in throughput shown by the proposed algorithm when it is compared with the throughput of the existing DSR. There is no negative effect of increase in speed of nodes on the throughput.

Table 2. Simulation Parameters

Parameter	Value
Length of Packet	1000
Area	100*100
Number of Nodes	100
Malicious Nodes Ratio	10-40%
Traffic	CBR
Pause Time	2 sec

Another metric used to compare the proposed and existing protocol is with the help of End to End Delay. This metric tells the delay in time occurred while the packets are accepted or found by the node which is acting as destination. Initially, proposed algorithm lacked according to this metric in comparison to the DSR. But DSR is not able to handle a network with large number of mobile nodes. So, when there is an increase in nodes' number in the network, there is increase in delay in DSR protocol. Modified DSR protocol is able to handle the increment in the density of nodes in the network. Figure 3(c) proves that DSR cannot handle nodes' number when it's large and End to End Delay is increased.

Routing overhead is calculated by the ratio of packets transferred to the control packets required. DSR protocol uses lesser number of control packets in comparison to the proposed work. So when both of these protocols are compared on the basis of Routing Overhead vs. Malicious nodes ratio in the network, DSR performed better than the proposed algorithm. As shown in figure 3(d), the routing overhead needs to be tackled in future for the proposed work.



(a) PDR vs. Speed of Nodes

(b) Throughput vs. Speed of Nodes

(c) End to End Delay vs. Number of Nodes

(d) Routing Overhead vs. Malicious Nodes Ratio

Fig.3. Simulation Results

6. Conclusions

DSR protocol belongs to the group of the routing protocols which is used in a mobile ad hoc network but it does not provide an efficient and a reliable communication. Networks with mobile nodes are not safe and extra measures for security have to be taken. Path chosen for sending the data packets must be efficient as well as secure. None of the nodes must drop packets. Our proposed algorithm modified DSR in such a way that the black hole attack and gray hole attack are detected, throughput of the network is incremented, ratio of packets delivered has shown an incredible increment and end to end delay is lesser than the DSR protocol. In future, the proposed algorithm can be modified to provide security from other packet dropping attack and fabrication of messages with lesser routing overhead.

References

[1] Elizabeth M. Royer, and Chai-KeongToh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, pp. 46-55, April 1999.

[2] Kundu Pooja, NeetiKashyap, and NehaYadav."Literature Survey on Intrusion Detection Systems in MANETs." Information Systems Design and Intelligent Applications. Springer India, 2016.357-366.

[3] Al-Shurman, M., Yoo, S. and Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[4] S. Banerjee, “Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks,” in 2008 WCECS.

[5] David B. Johnson, and David A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[6] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of co-operative black hole attack in MANET." Journal of networks 3.5 (2008): 13-20.

[7] Thachil, Fidel, and K. C. Shet. "A trust based approach for AODV protocol to mitigate black hole attack in MANET." Computing Sciences (ICCS), 2012 International Conference on.IEEE, 2012.

[8] Tsou, Po-Chun, et al. "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs." Advanced Communication Technology (ICACT), 2011 13th International Conference on.IEEE, 2011.

[9] Wu, Xiaoxin, and David KY Yau. "Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach." Security and Privacy in Communications Networks and the Workshops, 2007.SecureComm 2007.Third International Conference on.IEEE, 2007.

[10] L. Zhou and Z. J. Haas - Securing ad hoc networks. EEE Network, Vol. 13, Nov.-Dec. 1999, pp. 24 -30, 1999

Authors’ Profiles

Pooja Kundu, Computer Science M.Tech. Student, NorthCap University, Gurgaon (Haryana).

Neeti Kashyap, Assistant Professor, Computer Science and IT Department, NorthCap University, Gurgaon(Haryana).

How to cite this paper: Pooja Kundu, Neeti Kashyap,"Securing DSR for Mobile Ad hoc Network with Message Digest Algorithm",International Journal of Wireless and Microwave Technologies(IJWMT), Vol.6, No.5, pp.54-60, 2016.DOI: 10.5815/ijwmt.2016.05.06