Journal of Modern Technology and Engineering
Vol.3, No.3, 2018, pp.265-274

A NEW PROPOSED METHOD FOR DETECTION AND REMOVED BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK

Sh. Behzad*, **R. Fotohi**

Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran

Abstract. Security is an essential necessity in mobile Ad Hoc networks (MANET) to provider protected communication between mobile nodes. Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Due to security vulnerabilities of the routing protocols, wireless Ad Hoc networks may be unprotected against single black hole attack. In this paper a new proposed method by time and table for detection and removal black hole attack. We simulate the blackhole attack for Dynamic Source Routing (DSR) routing protocol which is one of the possible attacks on DSR routing. The simulation carried out on the proposed scheme. Simulation results show that the proposed method, the packet loss, throughput, and end-to-end delay with blackhole and without blackhole on DSR in mobile Ad Hoc network. We analyzed that the packet loss increases 75% and throughput and end-to-end delay decreases 80% in the network with a blackhole node.

Keywords: Mobile Ad Hoc networks, DSR, Black hole attack, routing protocol security.

Corresponding author: Shahram Behzad, Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran, e-mail: *sh.behzad173@gmail.com*

Received: 9 October 2018; Accepted: 13 October 2018; Published: 07 December 2018.

1 Introduction

Mobile Ad Hoc network is a set of wireless mobile nodes having no fixed infrastructure. In such networks, nodes route packets cooperatively in a multi-hop method (Behzad et al., 2018). Routing operation needs collaboration of all nodes to send packets from source node through intermediate nodes to the destination node. Therefore, selfish or black hole attack behavior of nodes can affect routing protocol DSR and network performance. The communication among these mobile nodes depends on the kind of routing mechanism used called multihop routing protocols such as DSR protocol. These routing protocols are having the functionality of forwarding the data packets from sender mobile number to the intended recipient (Behzad et al., 2017) manet topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. These feature nodes make mobile Ad-Hoc networks unpredictable in terms of scalability and topology. The Fig.1 shows that mobile Ad Hoc network.

Security in Mobile Ad-Hoc Network is the most significant connector for the basic capability of network. The availability of network services, secrecy and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security black hole attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the mobile Ad Hoc networks against the security threats. In DSR protocol, the black hole node reply will be received by the requesting node before the reception of reply from actual node; hence a black hole attack and forged route

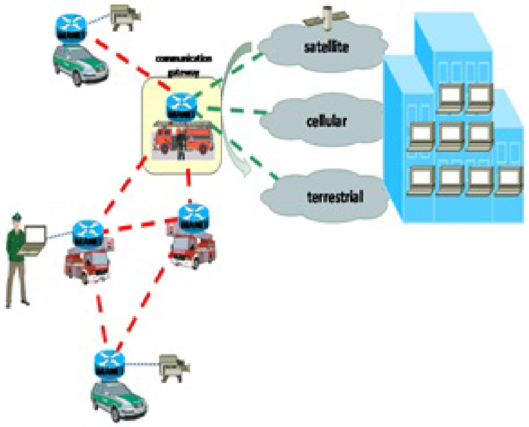


Figure 1: Mobile Ad Hoc network (MANET))

is created. When this route is establishment, it's up to the node whether to drop all the packets or forward it to the unknown address (Lu et al., 2009, December). The solution how black hole node Proportional in the data routes varies. Fig.2 shows how black hole Problems, here node ”E” want to send data packets to destination node ”D” and The initial process of route discovery. So if node ”F” is a black hole node then it will claim that it has active route to the specified destination as soon as it receives Route Request (RREQ) packets. It will then send the response to node ”E” before any other node. In this way node ”E” will think that this is the active route and thus active route discovery is complete. Node ”E” will ignore all other replies and will start sending data packets to node ”F”. In this way all the data packet will be lost consumed or lost.

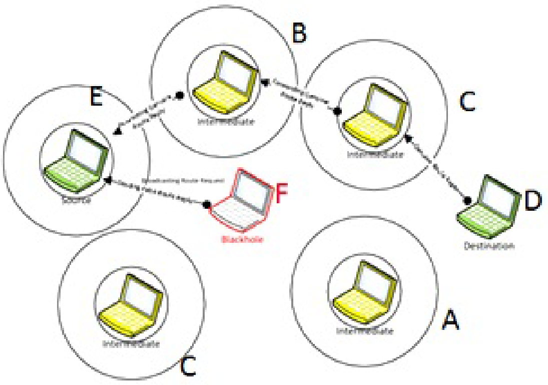


Figure 2: Black hole attacks in MANET

The selfish or black hole behavior of nodes can affect routing and network performance. This paper assumes that an efficient defense can be inspired by human immune system. In other words, we believe that the mechanism by which the human immune system detect and defense against various attacks can be borrowed to design an efficient defense scheme against black hole attack. We implement the proposed scheme over DSR routing protocol in ns-2 environment. The purpose of this paper is to evaluate and analyze network performance parameters under this attack, which is called Deep Black hole attack, for DSR protocol. In the second section of paper, related works are presented. Afterwards, section 3 consists of an overview of DSR protocol. Black hole and Deep Black hole attacks are both explained in section 4. Simulation, evaluation, and analysis of the effects of Deep Black hole attack in a DSR based MANET can be found in section 5. Finally, conclusion and future works are added in the 6th section.

2 Related works

Security and presentation of different safety obstacles and malicious node such as black hole node in mobile Ad Hoc networks as well as finding appropriate solutions against them is a challenging research area for researchers. Black hole attack is one of the famous related attacks (Biswas & Ali, 2007). The other solution in (Behzad & Dadgar, 2017) proposed that the node must maintain two tables for last packet that it sent to other nodes. One table maintains the last packet sequence number for last packet send to other nodes and the other maintains the last packet sequence number received from the nodes. In this solution the node will send RREQ packet. On the behalf of this RREQ packet all the nodes will reply with the packet of RREP to insure the node that they are not attacking node. As same as the above solution this proposed solution is good for single node attack but not suitable for attack because when number of nodes increased then it creates Congestion and can responsible for overhead on to the node. Black hole attack operates in (Behzad & Jamali, 2015) in two different phases. It works by both propagating fake RREQs, and generating RREQ based false RREPs. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to separate. This malicious node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. This solution assumes that there exists at most one malicious node and thus cannot cover the case with two or more malicious nodes, which is quite possible in real situations. An algorithm presented in (Behzad et al., 2017) claims to detect the black Hole attack in a MANET which is based on relationships of a trust level among the nodes. However, in the real network, it is very difficult to set an appropriate value for the trust level. In the method, every node has a function of learning the traffic flow in the network and evaluating the possibility criterion of black hole attack based on such learning results in order to detect the malicious node. If the value of the criterion is larger than a predetermined threshold, the node judges that there exists a black hole attacker. Bala proposes a trust based approach (Palanisamy et al., 2017) using AODV (Cai et al., 2009, September) protocol. But they do not consider the data packets. Instead they consider only control packets like RREQ, RRER and RREP and network layer acknowledgement. A black hole can even drop data packets by perfectly transmitting control packets. There the system fails by thinking that there is no black hole, as the control packets are transmitted without any delayer drop. Satoshi has proposed a method (Bala et al., 2009) based on the number of RREQ messages sent and RREP messages received. It calculated the average sequence number and try to find out the malicious node, as the malicious node will send RREP messages with extremely higher sequence number(Behzad et al., 2017). The method provides a data learning scheme to detect a black hole attacker. In this scheme, every node has knowledge of the current value of SN by the exchange of route messages such as RREQ and RREP. If a node receives a RREP message with a SN that is much larger than a threshold plus the current SN value, this node will believe that the RREP message is generated by a malicious node. Obviously, this method depends on the value of the threshold and may lead to a high rate of misjudgment. A Balaji Proposes a trust based approach (Biswas & Ali, 2007) using AODV (Pequeno & Rivera, 2007) protocol. But they do not consider the data packets. Instead they consider only control packets like RREQ, RRER and RREP and network layer acknowledgement. A black hole can even drop data packets by perfectly transmitting control packets. There the system fails by thinking there is no black hole as the control packets are transmitted without any delay or drop. Satoshi has proposed a method (Kurosawa et al., 2007) based on the number of RREQ messages sent and RREP messages received. It calculated the average sequence number and try to find out the malicious node, as the malicious node will send RREP messages with extremely higher sequence number. There are chances of getting RREP packet with highest sequence number from a genuine node too. On the values from this watchdog, trust value on the neighbor is being increased or decreased dynamically (Kurosawa et al., 2007). The method is implemented only on DSR protocol.

3 Over view of DSR routing protocol

DSR protocol is a reactive routing algorithm designed for mobile Ad Hoc network. The process of routing in DSR is composed of two main phases known as route discovery and route maintenance. Routing in DSR is completely carried out in an on-demand method (Behzad et al., 2018). Route discovery phase is a process under which source node, in order to send data packets, obtains a valid route to the destination node. For this, source node creates a RREQ packet and relays it in the network. Such a packet will be received by all of the sources neighbor nodes. Each RREQ packet contains an identifier and a list of addresses of intermediate nodes which this packet has passed from them. Such a list is initially empty at the time of creating RREQ by the source node. When a node receives a RREQ packet, creates a RREP regarding information included in the list of addresses inside the packet and sends it back to the source node if only it be the destination node itself or have had a route to the destination. Once source node receives such a RREP packet, it first adds this route to its route cache and then starts to send data packets using the route included in the packet. If the receiver of RREQ has not had a route the destination and has not previously received this RREQ packet, appends its address to the list of nodes inside the packet and rebroadcasts that. When the destination node receives a RREQ, it can create and send back the RREP to the source node using the route which can be computed by inverting the list of addresses inside the RREQ packet. Route maintenance is a mechanism by which, as source node is using a route to send its data packets, can discover changes of topology and send remainder of its packets through an alternative route if it be convinced that the current route has been broken and not usable anymore (Behzad et al., 2017).

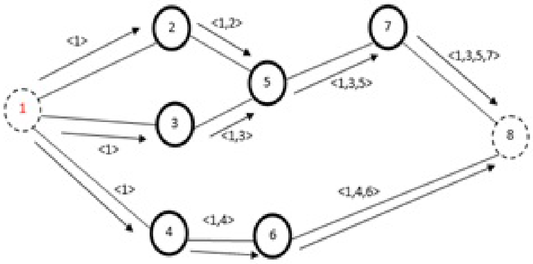


Figure 3: Depicts a discovery route in DSR protocol (All-over distribution)

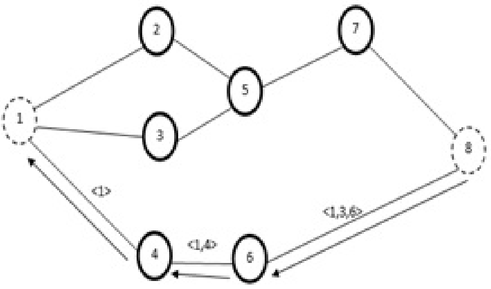


Figure 4: A sample of route discovery in DSR protocol

4 Black hole attack in mobile Ad Hoc network

In this section, ordinary Black hole attack and single Black hole attacks are introduced. In this attack, a black hole node tries to send fake RREPs to route requests in order to advertise itself as having the shortest path to the destination. These false RREPs deceive the source to divert the traffic of the network toward the black hole node for either eavesdropping or absorbing traffic, to drop the data packets. Cooperative black hole attack occurs when several malicious nodes cooperate to each other in order to absorb data packets. During Black hole attack, a malicious node uses its routing protocol in order to with the release of false news, to get the shortest path to the destination node or to the packet that wants to avoid. This black hole node advertises its availability of fresh routes irrespective of checking its routing table. The attacker node will always have the possibility in replying to the route request and thus intercept the data packet and retain it (Behzad & Dadgar, 2017). In protocol based on flooding, the black hole node reply will be received by the requesting node before the reception of reply from actual node; hence a black hole and forged route is creation. When this route is created, it's up to the node whether to drop all the packets or forward it to the unknown address. Fig. 4 shows the black hole Problems. Here node "E"' wants to send data packets to destination node "D" and the initial process of route discovery. So, if node "F" is a black hole node, then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "E" before any other node. In this way node "E" will think that this is the active route and thus active route discovery is complete. Node "E" will ignore all other replies and will start seeding data packets to node "F". In this way all the data packet will be lost consumed or lost Behzad et al. (2017).

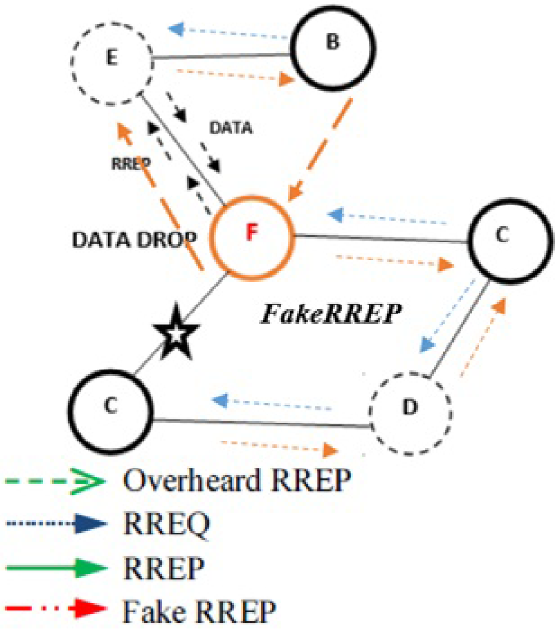


Figure 5: Problems of black hole attacks (Biswas & Ali, 2007)

A. Proposed Method

In this paper we present the new method by time and table for identify and removing black hole attacks, which are described in detail in the proposed method.

Step 1. If the message's time is greater than 5, it detects this as a malicious node and does not accept this message to select the route, and if more than several times the message is returned within this time frame, this path is set to 10 seconds as a malicious node. Detects and blocks malicious nodes in the table. And if this continues, this node will identify the node as a malicious node or black hole and will remove this route. Black hole attacks are one of the most influential attacks on wireless networks that have devastating effects on routing.and the number of dropped packets would increase and have a significant effect on other criteria in the network, such as operational potency, packet delivery rate, end to end delay and packet loss.

The proposed method is as follows.

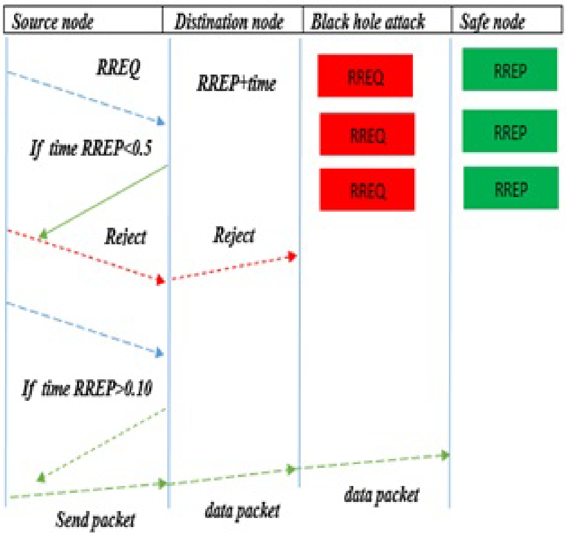
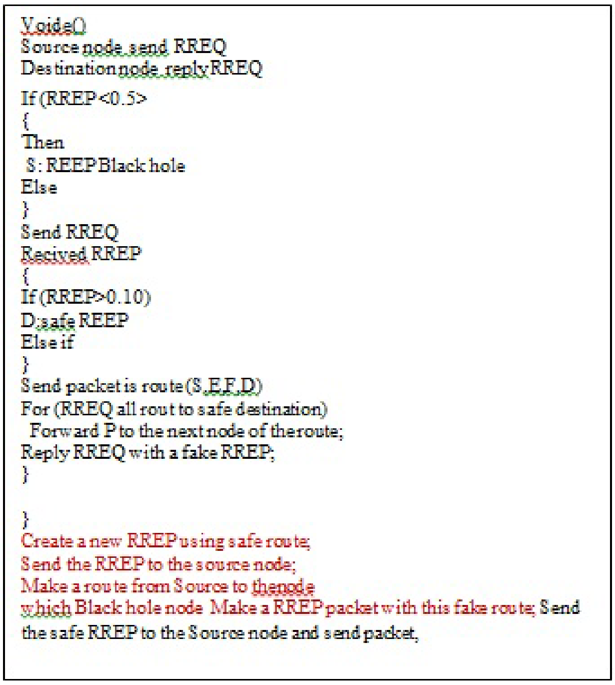


Figure 6: Schema proposed method



```
VoideQ
Source node send RREQ
Destination node reply RREQ
If (RREP<0.5>
{
Then
 S: REEP Black hole
Else
}
Send RREQ
Recived RREP
{
If (RREP>0.10)
D:safe REEP
Else if
}
Send packet is route (S,E,F,D)
For (RREQ all rout to safe destination)
  Forward P to the next node of theroute;
Reply RREQ with a fake RREP;
}

}
Create a new RREP using safe route;
Send the RREP to the source node;
Make a route from Source to thenode
which Black hole node  Make a RREP packet with this fake route; Send
the safe RREP to the Source node and send packet,
```

Figure 7: Identifier algorithm for detection balck hole attack

Step 2. Save to complete the detector

At this stage those amounts of RREPs which could be collated with imposed conditions are collected and sent to next stage which is the Match stage, i.e. they have the two specified characteristics.

Step 3. Storing as the best identifier in the memory

Storing in the memory safe RREP Only those sets of RREPs are selected and registered in the immune memory as the best time and safest RREPs which passed the imposed conditions in the beginning stages.

5 Simulation results and analysis

In this section we present a set of simulation experiments to evaluate the effect of blackhole attack on DSR protocol in Mobile Ad Hoc network. We compared the performance of DSR and DSR under black hole attack against the performance of the routing protocols without Black hole attacks. First I have explained blackhole attack in detail with the help of the simulation in NS-2.we run two simulation, one DSR under black hole attack node and other including the Defense Against Black hole Attacks ,we have repeated the experiments by changing the Several times. To, 100,120,140,160,180, and 200 to see the simulation parameter are show in Table 1 the metrics used to evaluate the performance are given below.

Table 1. Simulation Parameters

Simulator	NS2.34
Area	100 X100
Number of Mobile Node	50
Routing Protocol	(DSR)
Transmission Range	250m
Antenna	Omni Antenna
Time Simulation	200s
MAC Layer	802_11
Traffic Type	CBR (UDP)
Buffer Size	50 Packet
Node placement	Random
Black hole Node	10node
Queue Type	Drop tail
Publication Type	Two ray ground

A: Packet delivery ratio (%)

PDR is the number of packages that are delivered to the destination from the source, divided by the total number of packages in the network. This parameter is also called as success rate of the protocols:

PDR = (Number of seed Packet / Number of received Packet)* 100

Where PDR is the package delivery rate, SendPacketNo is the number of sent packages, and RecievePacketNo denotes the number of received packages.

B: Packet loos (%)

Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. The lower value of the packet loss means the better performance of the protocol. The PLR is calculated in Equation (1) follows: (Behzad et al., 2018)

$$PLR = \left(\frac{\sum_{j=1}^{n} Number\ of\ sent\ packets}{\sum_{j=1}^{n} Number\ of\ recevied\ packets} \right) \times 100 \quad (1)$$

F: Packet Drop (%)

Dropping packets, where malicious nodes drop packets and end up never forwarding them to a valid next hop. Thus, we can define DPR as shown in Equation (2)

$$DPR = \left(\frac{\sum_{j=1}^{n} Number\ of\ droped\ packets}{\sum_{j=1}^{n} Number\ of\ droped\ packets + sent\ packets} \right) \times 100 \quad (2)$$

G: Throughput (%)

Throughput is the number of the data packets delivered from source to destination per unit of time. Throughput is calculated as received throughput in bit per second at the traffic destination. The throughput is calculated in Equation (3) as follows:

$$\left(\frac{\sum_{j=1}^{n} Packets\ recieved}{\sum_{j=1}^{n} Packets\ originated}\right) \times 100. \tag{3}$$

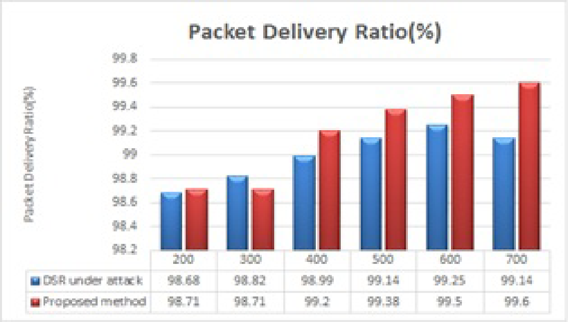


Figure 8: Packet delivery ratio vs pause time

Compares the performance of proposed method with that of DSR under black hole attacks for detection of the black hole attacks. As shown in the Fig. 8, proposed method increases the packet delivery actio by more than 40% over than DSR under attacks, respectively.

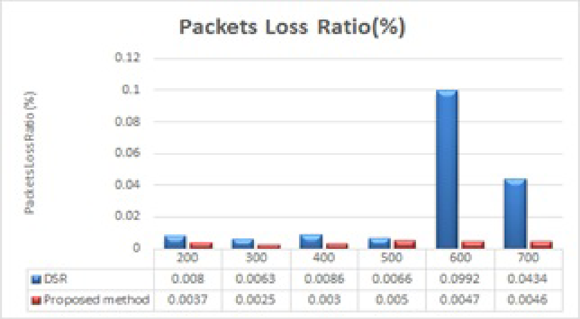


Figure 9: Lost packets vs. pause time

DSR protocol has lost more packets than a proposed method approach and it shows the success of destructive nodes in operating the attack of black hole on this protocol. Fig. 9 shows the packet loss ratio of Proposed method at the different time Than the DSR under attack is better

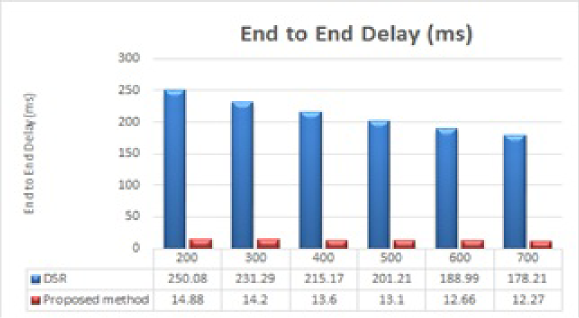


Figure 10: End to End Delay vs. Time

As shown in the Fig. 10, when there are destructive nodes in the network, the proposed algorithm by low end-to-end delay can identify the destructive nodes and aware another nodes, but DSR protocols are disable because it has more end-to-end delay. This result reflects that our detection method is valid for defence against black hole attack at different times.

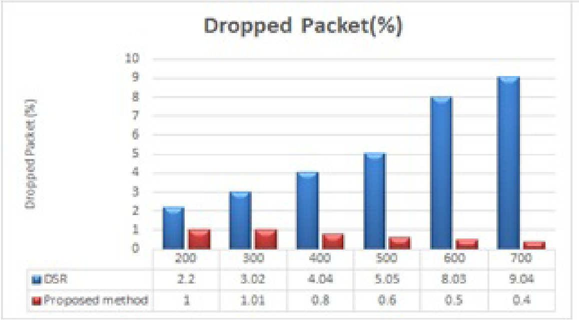


Figure 11: Dropped Packet vs Time

Show that Black hole has dramatically the drop packet, ratio compared to proposed method, displays the dropped packets in the network. The proposed method technique drops a minimal number of packets compared to the other technique.

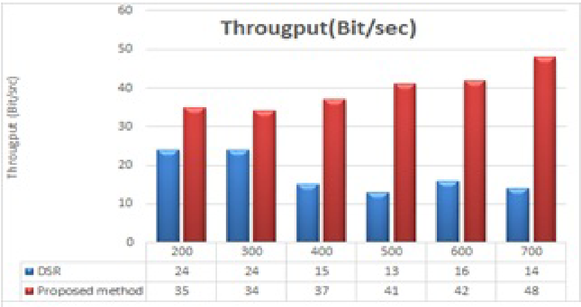


Figure 12: Throughput vsTime

Throughput for Propose method is high compared to that of DSR under attack. As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. The overall low throughput of DSR under attack is due to route reply. The black hole node immediately sends its RREP and the data is sent to the black hole node which cast off all the data. The network throughput is much lower. This result reflects that propose our detection is valid for Defense against black hole attack.

6 Conclusion

In this paper, we proposed an approach for detecting black hole nodes in mobile Ad Hoc network based on the new proposed method. The aim of the proposed algorithm by time and table in this paper is that we can identify the isolated node and delete them from routing in accordance to the behavior of nodes in the system. In the proposed method for the first step the origin loop analyzes the step numbers and the arrived RREPs from each loop and with its strong learning modifies and separating the path using the timed response. the route immediately and separates black hole loops from other existing time and table in occasional networks and then chooses the best route for send packet. We compared the efficiency of our defensive scheme i.e. new proposed method with DSR under black hole attack. Simulation results showed that, in average, the overall performance of proposed method is around 40% better than DSR under attack routing protocol in terms of throughput, end to end delay, packet drop ratio and lost packets. we can say that the proposed algorithm has better operation against black hole attack than the DSR protocol.

References

Bala, A., Bansal, M. & Singh, J. (2009, December). Performance analysis of MANET under blackhole attack. In *First International Conference on Networks & Communications*, IEEE, 141-145.

Behzad, Sh. & Jamali, Sh. (2015). A survey over black hole attack detection in mobile Ad Hoc network. *International Journal of Computer Science and Network Security (IJCSNS)*, *15*(3), 44.

Behzad, Sh., Fotohi, R. & Guliyev, A.M. (2017). Defence against black hole attacks in mobile Ad Hoc networks using artificial immune systems. *Journal of Modern Technology & Engineering, 2*(3), 231-248.

Behzad, Sh. & Dadgar, F. (2017). A hybrid method for detection and removal black hole attacks in mobile Ad-Hoc networks, *Journal of Modern Technology & Engineering* , *2*(1), 66-75.

Behzad, S., Fotohi, R., Balov, J.H. & Rabipour, M.J. (2018). An Artificial Immune Based Approach for Detection and Isolation Misbehavior Attacks in Wireless Networks. *Journal of Computers*, *13*(6),705-721.

Biswas, K. & Ali, M. (2007). Security threats in mobile Ad Hoc network. Master thesis.

Cai, J., Yi, P., Tian, Y., Zhou, Y. & Liu, N. (2009, September). The simulation and comparison of routing attacks on DSR protocol. In *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*, IEEE, 1-4.

Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A. & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile Ad Hoc networks by dynamic learning method. *IJ Network Security*, *5*(2),338-346.

Lu, S., Li, L., Lam, K.Y. & Jia, L. (2009, December). SAODV: a MANET routing protocol that can withstand black hole attack. In *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, 2, IEEE, 421-425.

Palanisamy, V., Annadurai, P. & Vijayalakshmi, S. (2010, December). Impact of black hole attack on multicast in Ad hoc network (IBAMA). In *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*, IEEE, 1-4.

Pequeno, G.A. & Rivera, J.R. (2007). Extension to MAC 802.11 for performance Improvement in MANET.