International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 5, October 2018, pp. 3092~3102
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp3092-3102

Analysis of Blackhole Attack in AODV and DSR

Niranjan Panda, Binod Kumar Pattanayak
Department of Computer Science & Engineering, ITER, S'o'A University, India

Article Info

Article history:

Received Oct 23, 2017
Revised Mar 14, 2018
Accepted Aug 20, 2018

Keyword:

AODV,
Blackhole Attack,
DSR,
MANET.

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) are supreme ruler and demoralization wireless scheme. MANETs are infrastructure less i.e. their structure is not fixed, and the nodes be able to move about and can leave the network whenever they want. The nodes are to perform as more over router and host. In MANETs, the node can be in contact with every node as their configuration is not fixed and the nodes starts transmitting the packets to each other for the establishment of the connection. To hitch the link, the nodes make use of some routing protocols like Ad-Hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Destination-Sequenced Distance Vector (DSDV). Security in MANET is the key matter meant for the fundamental utility of network. There are many attacks caused in MANET. Blackhole attack is one that occurs in MANET. A Black hole attack is an attack where the node, which is malicious advertise itself as having the optimal route to the destination and drops all the packets instead of forwarding further to the destination. Here, we have shown the blackhole attack in AODV and DSR. Through simulation we evaluate the performance of the two above protocols under blackhole attack.

Corresponding Author:

Niranjan Panda,
Department of Computer Science & Engineering,
ITER, S'o'A University, Bhubaneswar, India.
Email: niranjanpanda@soauniversity.ac.in

1. INTRODUCTION

Mobile Ad-Hoc Networks (MANETs) are independent and deconcentrate systems or wireless systems. In the network system, MANETs always comprises of the mobile nodes which may be structures or subsystems, acting as a router as well as host. In the network, depending on each other's connection they can form different network configuration or topography by their self-arrangement power, without any fixed infrastructure. Routing protocols are the most fascinating, ambitious and challenging areas in MANET research. Many routing protocols that have been designed for MANETS such as AODV, DSR, DSDV, OLSR etc. The very intensive worry for the basic functionality in MANET is routing security. Due to the characteristics like open access medium, dynamically altering topology, deficiency of central management and monitoring systems, cooperative algorithms and deficiency of transparent defense mechanism of MANETs often ill used by attackers and endure security attacks. The network services accessibility, data integrity and confidentiality can be gained by safeguarding the security problems that have been detected within the network. Moreover, the wireless connection makes MANETs to be more susceptible to the attacks by providing access to on-going communications. Varieties of attacks are found out in the MANETs and classified as; wormhole attack, blackhole attack, sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), impersonation attack etc.

Antecedently, many more works are performed on issues of security. One of the attack is Black Hole Attack. Blackhole Attack deeply related to reactive routing protocols in MANET like AODV and DSR. In our work we condense or concentrate our study on the two routing protocols AODV and DSR. We have analyzed the effect of Blackhole attack on the AODV and DSR routing protocol through a simulation carried

out using NS-2. Its consequences are explained by expressing how this attack interrupt the execution of MANET routing protocols.

In chapter 2 we presented a study of routing protocols emphasizing on AODV protocol and DSR protocol in detail. In chapter 3 we discussed about the blackhole attack in MANETs in details. In chapter 4 we discussed how black hole attack makes the protocols to misbehave and also described how the new protocols supporting attacks are implemented in NS-2.35. Chapter 5 discusses the performance metrics, analysis and comparison of blackhole attack in AODV and DSR and Finally in Chapter 6 we discussed about future research directions and concluded our work.

2. DIFFERENT MANET ROUTING PROTOCOLS

According to MANETs operational functionalities, the routing protocols [1-2] are divided into three categories such as reactive routing protocols, proactive routing protocols and hybrid routing protocols. The power structure of the MANET routing protocols is represented using Figure 1.

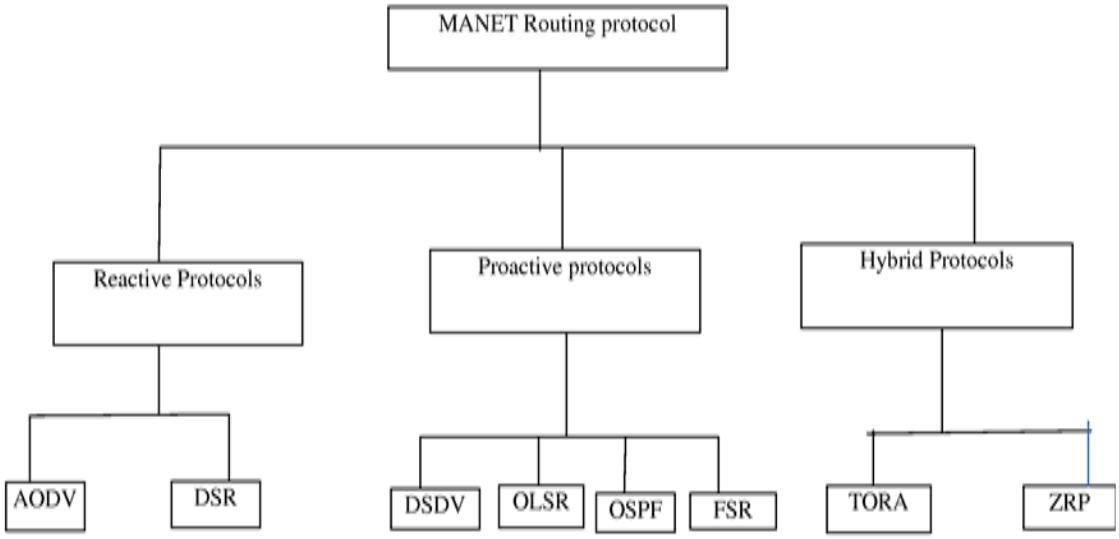

Figure 1. Manet routing protocol classification

2.1. Reactive protocols

Reactive protocols are well recognized as on demand protocols. They are known as such on-demand protocols because of the concept that they never begin route discovery process by themselves, until they are asked for it i.e these types of protocols are framed up the routes when demanded [3]. When a source node needs to start a conversation with another node within the network and having no route to that node, then it requests for a route to establish and a route discovery process is initiated by the protocol on demand. Reactive routing protocols use the flooding mechanism to spread the route request message during route discovery. No bandwidth is consumed for sending the routing information whereas bandwidth is consumed during the transfer of data by node.

2.1.1. AODV

2.1.1.1. Basics

AODV is explained in RFC 3561 [4]. As it is a reactive routing protocol, when it possesses no route information and a source node is desires to begin the communication to any other node within the mobile network then AODV uses the mechanism of flooding control messages for finding a route to the required node within the network. In AODV, the source routing option is not used. When the sender node wants to transmit the packet, it examines its routing table and looking forward for the next intermediate hop to the destination then sends the packet and so on. Control messages in AODV broadly classified into three types as explained below:

a. Route Request Message (RREQ): Initially when no path is available from a source node to destination node, then the source node floods the network with RREQs messages using expandable ring technique. Each RREQ message header maintains a time to live (TTL) field that implements the expandable ring by limiting on the number hops that the RREQ should be transferred. RREQ ID is a field in RREQ message which is used for unique identification of the RREQ packets in conjunction with source IP address. RREQ message also contains other fields like destination IP address, sequence numbers of source and destination along with the various control flags. The sequence number represents the freshness of the RREQ messages and the hop count represents the number of traversed nodes originating from source to the destination. Each intermediate node when receives a RREQ message, it increments the hop count field value by one and rebroadcasts the packet again for a fresher route to the destination.
b. Route Reply Message (RREP): On receiving a RREQ, any intermediate node that have a fresher route to the destination node or the destination node itself initiates a RREP and unicasts towards the source node or the originator of the RREQ. Each RREP packet contains different fields like IP address of source and destination, destination sequence number, route life time and the hop count along with the various control flags. When a RREP reaches an intermediate node, its hop count field value is incremented and re-forwarded towards the originating node following of the path established by the selected RREQ in reverse. This process is repeated until the RREP arrives the originating node and the route is established.
c. Route Error Message (RERR): During the active routes, link status is observed by every node in the network to its intermediate nodes. Whenever a broken link is found out in an active route by any node, then it initiates a RERR message and forwards to its neighbor nodes in order to make the notification to the other nodes that the link is being braked or down.

2.1.1.2. Route Discovery Mechanism in AODV

Considering a source node S which wants to communicate with the destination node D will generate a RREQ and broadcasts it to the neighbor nodes A and C. The nodes A and C on receiving the RREQS forward them to their neighbor nodes B and E respectively. This process is repeated until destination node D is reached. Locating any intermediate node that have a fresher route to the destination node or the destination node D a RREP is initiated and forwarded to the originating node S. RREPs arriving the source node following the reverse path traveled by the RREQs establishes a route between the source node “S" and destination node “D”. After the route establishment between “S” and “D”, communication can take place in between them. Figure 2 shows the interchange of RREQ and RREP messages during route discovery between source node and destination node.

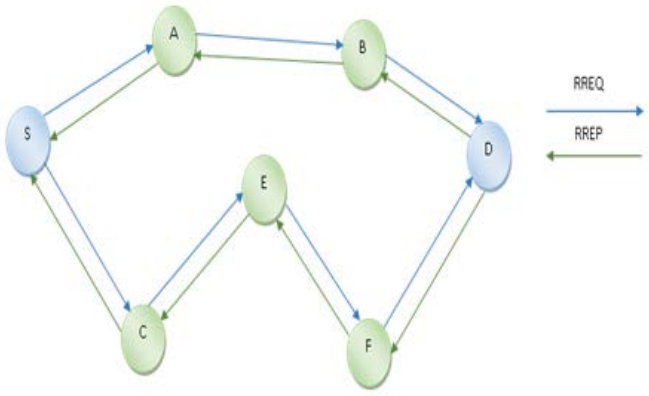

Figure 2. RREQ and RREP interchange during route discovery between source and destination node

2.1.1.3. Routing Maintenance

During a link failure in the path established between the source and destinations for communication, a RRER message is initiated and sent to the source informing about the down or broken link. From source broadcasting a RREQ message towards the destination node i.e. in Figure 3 from source “S” to destination “D”, at node “F” a broken link is encountered between “F" and “D”, so getting this link to be down a RERR message is initiated at node “F” and sent to the source node “S” making it aware about the link breakage.

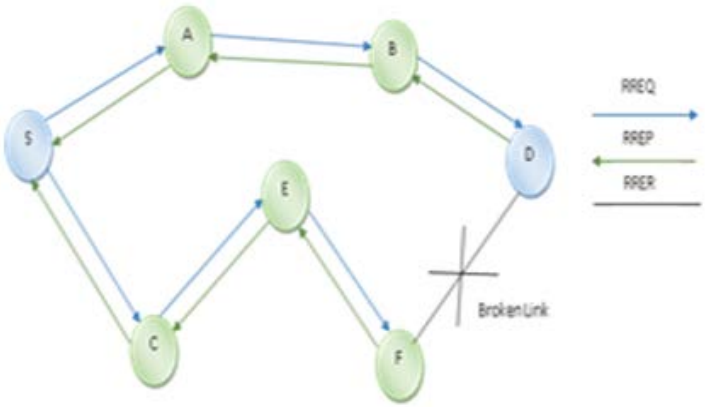

Figure 3. RREQ, RREP and RRER messages during route discovery between source and destination node

2.1.1.4. Advantage

The main advantage of this AODV protocol is that it is obtaining the routes that is being found on demand and that the current route towards the destination is determined using the destination sequence numbers which lowers the delay for the communication set-up.

2.1.1.5. Disadvantage

In AODV protocol discrepant routes may result at intermediate nodes due to the absence of fresh entries in the routing table, which means unavailability of current destination sequence number in presence of a very older source sequence number, may result in discrepant routes. If multiple RREPs are generated for a single RREQ packet, then this can residue to heavy control overhead.

2.1.2. DSR

a. Basics: DSR [5] is a reactive routing protocol in which route cache is updated with new routes obtained from the source to the destination node. For a node route is specified on-demand or when needed by a node for transmission of data. The processes during routing are Route Discovery Process and Route Maintenance Process which are discussed below.
b. Route Discovery Process: Routing cache is checked by a source node before transmission of data to another node and if no information is available about route to the destination or it is expired then a RREQ is broadcasted by the node and the process of broadcasting is repeated unless the RREQ reaches the destination node. Reaching the destination node, a RREP is generated and sent in reverse path to the source node [6] and receiving the RREP, its cache is updated with the new route information received. Further the entire traffic is routed through that newly created route.
c. Route Maintenance Process: During transmission if a node fails to find a next hop with the source data or route, then a RERR is initiated and sent to the source node making it aware about the route failure, and if it happens then the source node re-conducts the route discovery process.

2.2. Proactive protocols

Proactive routing protocols perform in a different way in comparison to reactive routing protocols. These protocols are table driven in nature [7] and each node maintains the routing information of the whole network. Any change in the network topology is reflected in the routing information table contained by each node and hence knows about the other nodes in progress. The routing information is constructed at nodes by exchange of connectivity information using HELLO messages and neighborhood information using TC messages. Optimized Link State Routing (OLSR) [8] is one of the example of proactive routing protocol.

2.3. Hybrid Protocols

In different Scenarios, reactive and proactive routing protocols work their best. A mix of both the protocols, named as hybrid routing protocol propose to make the use of proactive routing in some areas and reactive routing for the rest of network. The entire network is partitioned into small domains called zone and proactive routing is used within each zone decreasing the control overheads and delays using the information available in routing table. Reactive routing is used to route packets between different zones due to its efficiency with bandwidth in constantly changing network. Zone Routing Protocol (ZRP) [9] is one of the example of hybrid routing protocol.

3. BLACK HOLE ATTACK IN MANET

In black hole attack attacker nodes exploit the vulnerability in route discovery process of on-demand protocols and inject false route to the destination. On receiving a RRER message intermediate attacker node sends a RREP with a higher destination sequence number than the RREQ message received claiming to the destination. When an attacker chooses the concept of rushing along with high power transmission to make this attack. It is quite impossible to find out a route not passing through the attacker node. Once the node chosen as an intermediate node or becoming part of routes in the network starts misusing or discarding the traffic being routed through it creating a black hole. This attack can be severe when the attacker becomes the part of more number of routes.

3.1. Types of Blackhole Attack

Basically, black hole attack can be categorized into two types as:

a. Single Blackhole Attack
b. Cooperative Blackhole Attack

3.1.1. Single Blackhole Attack

In single black hole attack, a particular attacker node advertises itself for having fresh routes to destination node following the shortest path and it helps the attacker node to reply all the RREQs being the part of route, further during data transfer intercepts the data packets and retaining it [10]. In reactive routing protocols that uses flooding mechanism a mischievous and forged route is created as the attacker nodes RREP is received before the legitimate ones. Being the part of route, the attacker node behaves to drop all the packets received or to send it for an arbitrary address [11]. Overall, we can say that to make a black hole attack the attacker node becomes the part of the route but how it is not specified as it differs from protocol to protocol. In Figure 4 and 5source node “S” want send data to destination node “D” and hence, a route discovery process is initiated by the protocol from “S” to “D” and “A”, ”B”,”C”,”E” are the intermediate nodes. Considering “B” as an attacker node and claims to have active routes to the destination “D”, on receiving RREQ packets “B” sends a RREP to “S” before other legitimate nodes making “S” to believe that “B” is a legitimate node and can be a part of the active route. Hence all other RREPs from legitimate nodes are discarded by “S” and making the route discovery come to an end. Onwards “S” sends the data packets through node “B” which may be dropped or fabricated by “B” leading to a black hole attack.

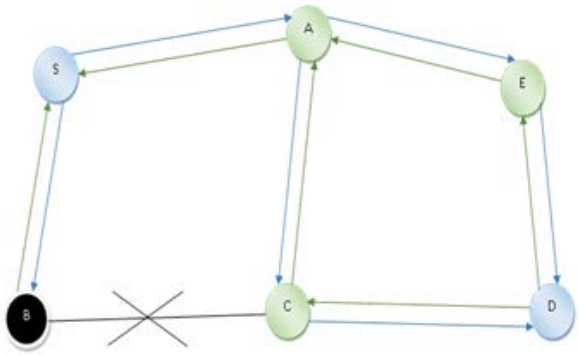

Figure 4. Single blackhole attack

3.1.2. Cooperative Blackhole Attack

Cooperative black hole attack signifies that the attackers acts in a group. In Figure 5, “S” is the source node and “D” is the destination node, nodes “A”, “B1”, “B2”, “C”, “E”, “F” are the intermediate nodes. Considering “B1” and “B2” be the cooperative Black hole nodes, when “S” want to send a data packet “D”, a route discovery is initiated by sending RREQ packets to the neighboring nodes. The attacker nodes being part of the network, also accept the RREQ and send the RREP to “S” immediately. The RREP from “B1” reaches first at “S” before any other nodes RREP. Hence source ode “S” starts sending packets to “B1” assuming it to be legitimate node. Attacker node “B1” instead of forwarding the data packets, drops them or transmitted to the other attacker node “B2”. Further “B2” drops all the packet instead of forwarding it to towards destination.

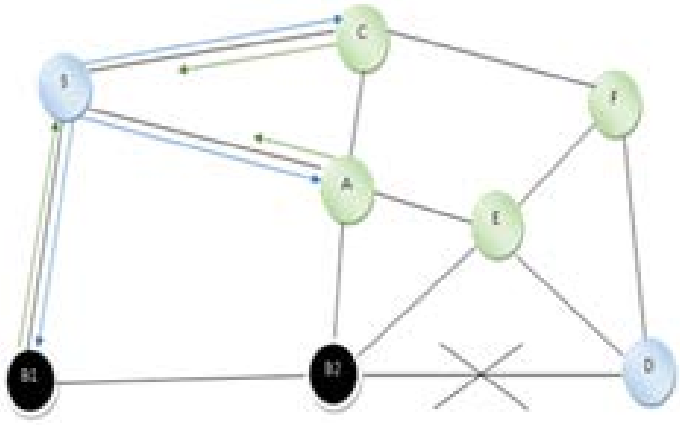

Figure 5. Cooperative blackhole attack

According to [12], in the Figure 6 when the “S” sends a ``Further Request (FRq)" to “B2” through a different routing path (S-A-B2) other than the routing path through “B1” and asks “B2” for having any routing path to “B1” and “D”. As “B2” is working in cooperation with “B1”, its “Further Reply (FRp)” will be “yes” to both the questions. Hence as suggested in [13], node S starts passing the data packets considering the route (S-B1-B2) is secure. However, in actuality, the packets are dropped by node “B1” or “B2” compromising the network security.

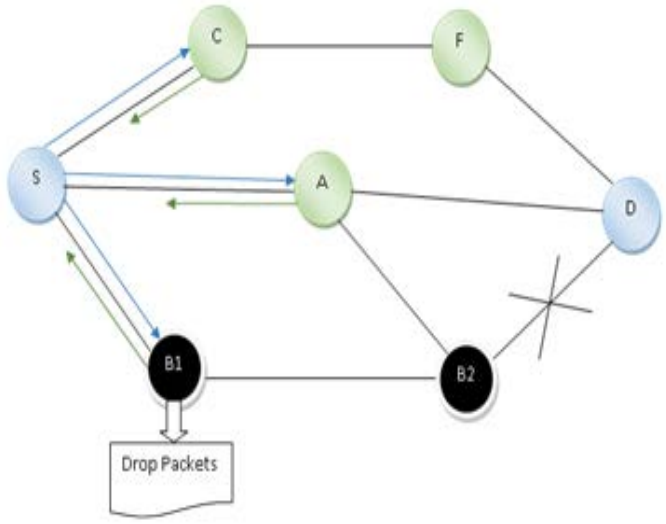

Figure 6. Cooperative blackhole attack

3.2. Blackhole Attack in AODV and DSR

Considering AODV and DSR, black hole attacks can be classified into two categories according to the presence of attacker nodes. They are:

a. Internal Blackhole Attack
b. External Blackhole Attack

3.2.1. Internal Black Hole Attack

In this type of black hole attack an internal compromised node exists between the source and destination nodes. It becomes the part of an active route and conducts the attack. Internal black hole attacks are named so as the attacker node by self belongs to the data route. This type of attacks is more endangered to guard against as it is so difficult to detect the internal compromised nodes.

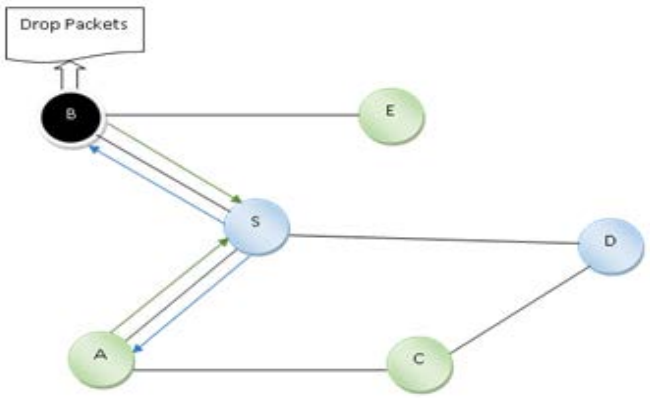

Figure 7. External blackhole attack

3.2.2. External Black Hole Attack

In external blackhole attacks attackers stay outside of the current network and deny access to network traffic or disrupting the network or creating congestions as shown in Figure 7. Further the external blackhole attacks may lead to internal blackhole attack by compromising some of the internal legitimate nodes involving them in attacking other nodes in MANET.

4. IMPLEMENTATION OF THE BLACK HOLE ATTACK IN AODV AND DSR USING NS-2.35

In our case, we use ns-2.35 for the simulation of the blackhole attack in AODV and DSR, and also to compare the performance metrics of both routing protocols AODV and DSR in presence of blackhole attack.

4.1. Blackhole Attack in AODV

The attacker node should be able to participate in the AODV messaging for this the new protocol which exhibits blackhole attack. AODV protocol is modified by adding the lines in Figure 8 to aodv.cc and the lines in Figure 9 to aodv.h to exhibit blackhole behavior. After adding the lines, the new routing protocol of AODV is configured to show the blackhole attack in Figure 10.

```
#endif // DEBUG

   // Just to be safe, I use the max. Somebody may have
   // incremented the dst seqno.
   seqno = max(seqno, rq->rq_dst_seqno)+1;
   if (seqno%2) seqno++;

   sendReply(rq->rq_src,           // IP Destination
             1,                    // Hop Count
             index,                // Dest IP Address
             seqno,                // Dest Sequence Num
             MY_ROUTE_TIMEOUT,     // Lifetime
             rq->rq_timestamp);    // timestamp

   Packet::free(p);
 }
//blackhole attackers
//Malicious nodes  generates fake route replies using following codes

else if(malicious==true)
 {
 seqno = max(seqno, rq->rq_dst_seqno)+1;
```

Figure 8. Lines added to aodv.cce

```
/*
 * Packet RX Routines
 */
void            recvAODV(Packet *p);
void            recvHello(Packet *p);
void            recvRequest(Packet *p);
void            recvReply(Packet *p);
void            recvError(Packet *p);

/*
 * History management
 */

double          PerHopTime(aodv_rt_entry *rt);


nsaddr_t        malicious; // To define the malicious
```

Figure 9. Lines added to aodv.h

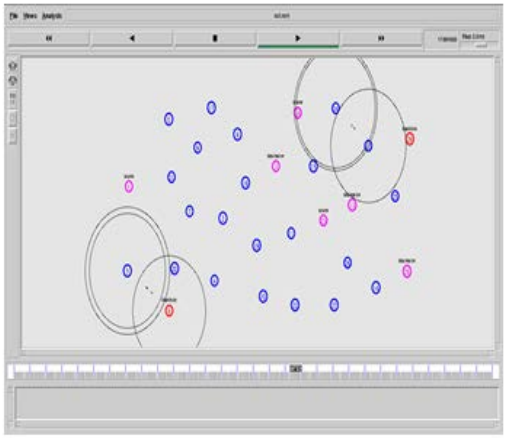

Figure 10. Implemented blackhole attack scenario in aodv

4.2. Blackhole Attack in DSR

The attacker node should be able to participate in the DSR messaging for this the new constructed protocol which exhibits blackhole attack. DSR protocol is modified by adding the lines in Figure 12 to the dsragent.cc and lines in Figure 13 to dsragent.h for the blackhole behavior. Then the new routing protocol of DSR is configured to show the blackhole attack in Figure 11.

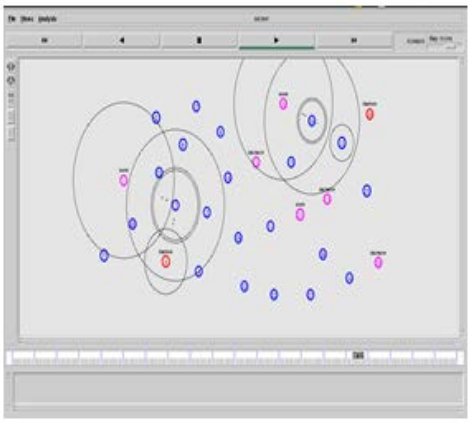

Figure 11. Implemented blackhole attack scenario in DSR

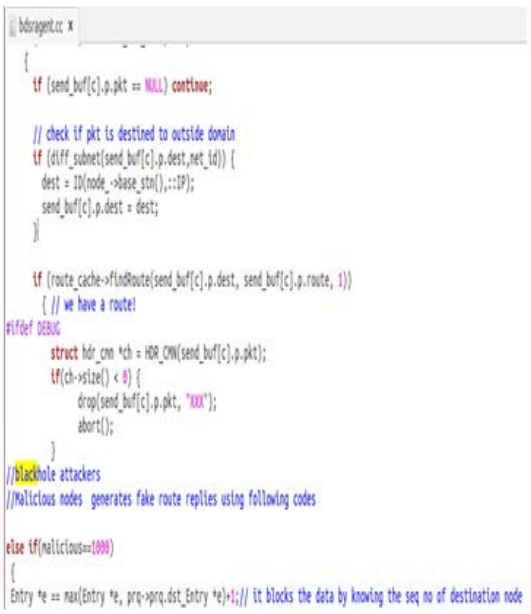

Figure 12. Lines added to dsr.cc

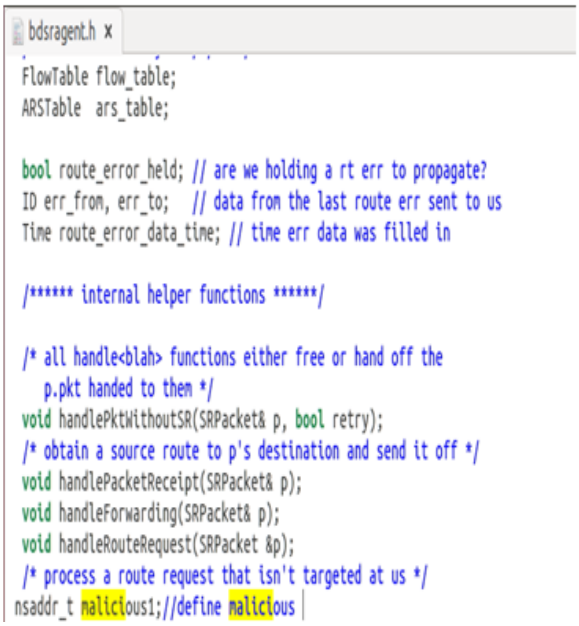

Figure 13. Lines added to dsr.h

5. PERFORMANCE METRICES OF BLACKHOLE ATTACK

Here, in this section performance metric of the blackhole attack in AODV and DSR is compared and analyzed, which of the routing protocol is better in presence blackhole attack. This is being shown in the Figures 14 to 16

5.1. End-to-end Delay

End-to-end delay is the time taken by a packet to get transmitted from the source node to destination node successfully including the hop delays, transmission delays and queue delays. Performance of a network increases with the decrease in end to end delay values.

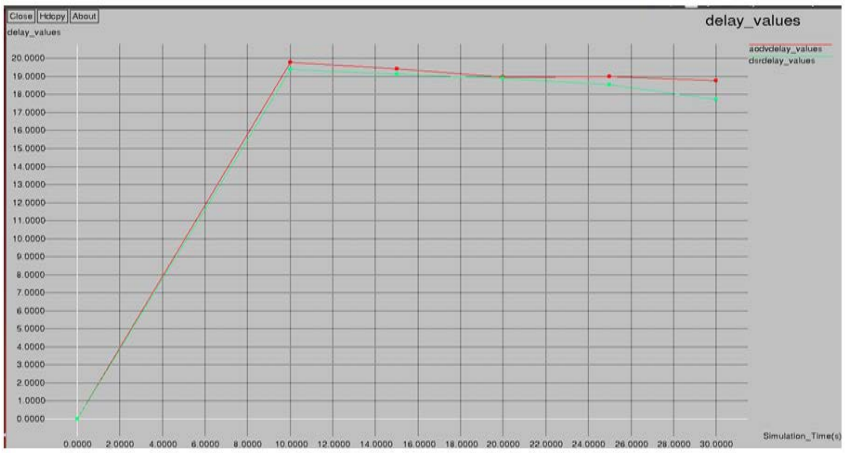

Figure 14. Comparison of End-to-end delay in blackhole attack of AODV and DSR

5.2. Packet Delivery Ratio

Packet Delivery Ratio is the ratio of the total number of data packets received at the destination with respect to the total number of packets sent by the source. Performance of a network increases with the increase in packet delivery ratio values.

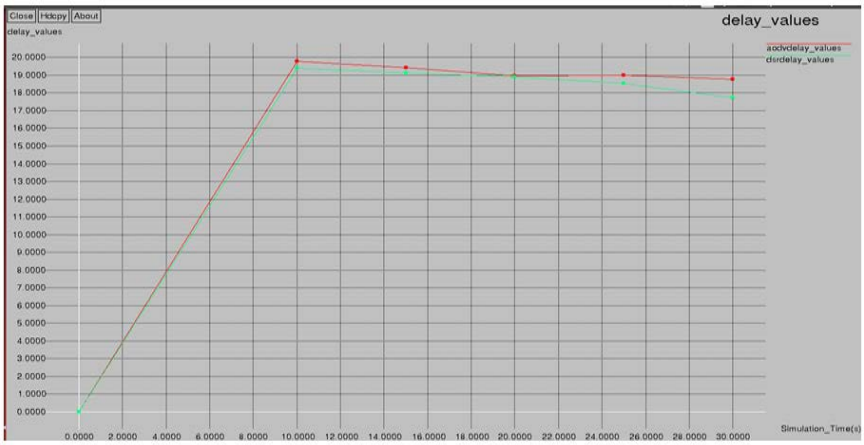

Figure 15. Comparison of packet delivery ratio in blackhole attack of AODV and DSR

5.3. Throughput

Throughput is the number of packets moved successfully from source to destination in a given time period and represented in bps. Performance of a network increases with the increase in throughput values.

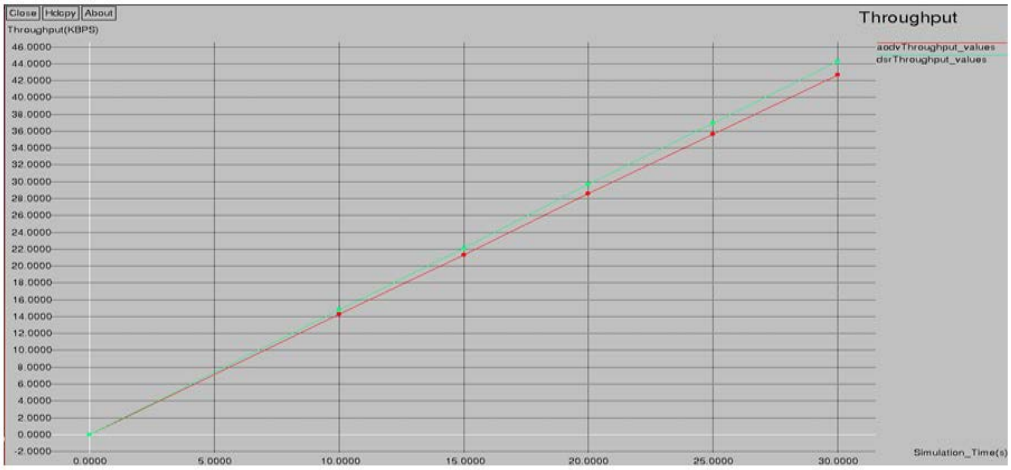

Figure 16. Comparison of throughput in blackhole attack of AODV and DSR

6. CONCLUSION

MANETs require no fixed infrastructure and can be easily deployed in hostile situations where the implementation of a traditional network is not so easy. Hence MANETs are broadly used nowadays in the field of communications. Due to MANETs properties and importance, there are many more challenges to overcome. Routing and security are the most challenging features to deal with considering the aspects of MANET's deployment. In our paper, we have made a brief study about behavior of MANETs, its routing protocols and analyzed a specific attack called blackhole attack on protocols AODV and DSR. Both the protocols are analyzed in presence of blackhole attack with three different scenarios, in reference to the different types of performance parameters such as end-to-end delay, packet delivery ratio and throughput. In case of end-to-end delay, DSR is better protocol than AODV under blackhole attack. In case of packet delivery ratio, AODV is shown as better protocol than DSR under blackhole attack. Finally, in case of throughput, DSR is shown as better protocol than AODV under blackhole attack. We can conclude as a result of our research and analysis done through the simulation of AODV and DSR under blackhole attack that protocol AODV is more vulnerable to black hole attack in comparison to protocol DSR.

REFERENCES

[1]. Larsson, Tony, and Nicklas Hedman. "Routing Protocols in Wireless Ad-hoc Networks-A Simulation Study (Master's thesis)." *Dept. Com. & Eng., Luleå Univ., Stockholm* (1998).

[2]. Panda Pankajini, Gadnayak Khitish Ku., Panda Niranjan, "MANET Attacks and their Countermeasures: A Survey", *International Journal of Computer Science and Mobile Computing*, Vol. 2, Issue. 11, pp. 319 – 330, Nov 2013.

[3]. Mbarushimana, Consolee, and Alireza Shahrabi. "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks." *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*. Vol. 2. IEEE, 2007.

[4]. Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[5]. Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." *Ad hoc networking* 5 (2001): 139-172.

[6]. Zhu, Chunhui, Myung J. Lee, and Tarek Saadawi. "Rtt-based optimal waiting time for best route selection in ad hoc routing protocols." *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*. Vol. 2. IEEE, 2003.

[7]. Abolhasan, Mehran, Tadeusz Wysocki, and Eryk Dutkiewicz. "A review of routing protocols for mobile ad hoc networks." *Ad hoc networks* 2.1 (2004): 1-22.

[8]. Clausen, Thomas, and Philippe Jacquet. *Optimized link state routing protocol (OLSR)*. No. RFC 3626. 2003.

[9]. Haas, Zygmunt J., Marc R. Pearlman, and Prince Samar. "The zone routing protocol (ZRP) for ad hoc networks." (2002).

[10]. Biswas, Kamanashis, and Md Ali. "Security threats in mobile ad hoc network." (2007).

[11]. Pequeño, Guillermo Alonso, and Javier Rocha Rivera. "Extension to MAC 802.11 for performance Improvement in MANET." (2007).

[12]. Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." *ACM SIGCOMM computer communication review*. Vol. 24. No. 4. ACM, 1994.

[13]. Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." *IEEE Communications magazine* 40.10 (2002): 70-75.

BIOGRAPHIES OF AUTHORS

Niranjan Panda is an Assistant Professor in the Computers Science and Engineering Department, Siksha 'O' Anusandhan University, Bhubaneswar, India since 2011. He is presently continuing as a Ph.D. scholar at Siksha 'O' Anusandhan University. He got his M.Tech. degree from KIIT University, Bhubaneswar, India and B.Tech. Degree from Utkal University, Bhubaneswar, India in 2010, 2005 respectively. His research interests include Ad hoc networks, Computer Security, Intelligent Systems and Image Processing.

Binod Kumar Pattanayak is a Professor in the Computer Science and Engineering Department, Siksha 'O' Anusandhan University, Bhubaneswar, India since 1999. He got his Ph.D. from Siksha 'O' Anusandhan University, M.S. in Computer Engineering from National Technical University, kharkov, Ukraine and B.Sc. from Revenshaw University, Cuttack, india. His research interests include Ad hoc networks, Compiler Design, Software Engineering, Computer Architecture, Intelligent Systems.