Indonesian Journal of Electrical Engineering and Computer Science
Vol. 21, No. 1, January 2021, pp. 582~590
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v21.i1. pp 582-590

Secure dynamic source routing protocol for defending black hole attacks in mobile Ad hoc networks

M. Mohanapriya[1], Nitish Joshi[2], Mohit Soni[3]
[1]Associate Professor, Coimbatore Institute of Technology, Coimbatore, India
[2,3]B.E. Scholars, M.B.M. Engineering College, Jai Narayan Vyas University, Jodhpur, Rajasthan, India

Article Info

Article history:

Received May 10, 2020
Revised Jul 13, 2020
Accepted Jul 27, 2020

Keywords:

Ad hoc networks
Network security
Routing protocols
Wireless networks
Wireless sensor networks

ABSTRACT

Wireless Ad Hoc Network is a dynamically organized network on emergency situations, in which a group of wireless devices send data among themselves without requiring any base stations for forwarding data. Here the nodes itself perform the functions of routing. This important characteristic of mobile ad hoc networks allows the hassle free set up of the network for communications in different crisis such as battlefield and natural disaster zones. Multi hop communication in MANET is achieved by the cooperation of nodes in forwarding data packets. This feature of MANET is largely exploited to launch a security attack called black hole attack. A light weight solution called SEC-DSR is proposed to defend the network from black hole attack and enables communication among nodes even in the presence of attackers. In this scheme, by analyzing only the control packets used for routing in the network, the compromised nodes launching the attack are identified. From the collective judgment by the participating nodes in the routing path, a secure route free of black hole nodes is selected for communication by the host. Simulation results validate and ensure the effectiveness of the proposed solution tested on an ad hoc network with compromised black hole nodes.

Corresponding Author:

M. Mohanapriya
Department of Computer Science Engineering
Coimbatore Institute of TEchnology
Avinashi Rd, Civil Aerodrome Post, Coimbatore, Tamil Nadu, India 641014
Email: mohanapriya.m@cit.edu.in

1. INTRODUCTION

Ad hoc wireless networks, also known as infrastructure less networks operates without the support of any centralized infrastructure. Ad hoc networks utilize multi-hop radio relaying for communication among the nodes. Unlike cellular networks, ad hoc networks lack base station and hence depend on cooperation of the participating nodes to enable communication among themselves. Hence, in this network, every node acts as both host and router. Due to the mobility of nodes the network topology is also dynamic in nature. The features of Ad hoc networks including user mobility and less overhead in deployment, makes itself suitable for deployment in several areas [1]. It includes military operations, collaborative and distributive computing, wireless mesh networks, wireless sensor networks, hybrid wireless networks, vehicular networks, critical operations such as search and rescue, crowd control, commando operations and also in natural calamities like tsunami, earthquakes etc., where infrastructure cannot be established. The main task in these networks is to find a secure and shortest path between the source and destination nodes. All participating nodes in the network should cooperate with each other to find such routes between any source and any destination. The

routing protocols of ad hoc networks are mainly categorized into proactive (Table-Driven protocol) and reactive routing protocol (On Demand routing protocol) [2]. The focus of these protocols such as DSDV (Destination Sequenced Distance Vector), AODV (Ad hoc On-Demand Distance Vector) and DSR (Dynamic Source Routing), OLSR (Open Source Link State Routing) is to find a path with less number of hops between source and destination. There is no security mechanisms incorporated in the protocols to check for secure routes. Also due to the lack of centralized infrastructure such as firewalls, it is difficult to employ existing security mechanisms of wired networks for verification of intruders or attacks in the network. One solution to protect ad hoc networks from security attacks is to make the participating nodes itself to verify the presence of intruders or to check for the possibility of attacks during communication. The ad hoc network usually consists of resource constrained mobile nodes. Hence any proposed solution for the security attacks should not be highly resource intensive which requires much processing by each node in the network.

The security attacks launched in MANET are called as passive and active attacks. When the compromised nodes silently listen the traffic and learn valuable information such as originator and receiver of the message, duration of communication and so on, then it is a passive attack. The active attackers in addition to learning the traffic pattern also modify or drop the packets in the network. Some of the security attacks launched on MANET are black hole attacks, Cooperative Black Hole attacks, Gray hole attacks, Flooding Attacks, Routing Table Overflow attack, Wormhole attacks, and so on [3, 4]. When setting up the MANET, the participating nodes are properly authenticated and have proper credential requirements for being a part of the network. Hence these security attacks are mostly launched by malicious nodes that have proper credentials to participate in the target network. Hence the security attacks launched by these nodes are called inside attacks. Because the authorized nodes are the source of the inside attacks they are very hard to detect. Black hole attack is an inside attack and it can be easily deployed on on-demand routing protocols like AODV and DSR [5]. In reactive routing protocols, during the route set-up process, the source node broadcast a control packet called RouteREQuest (RREQ) packets in the network. A RouteREPly control packet (RREP) is sent back to the source host by any intermediate node only if it has a latest or shortest path to the destination. Using the path information in RREP packet, the source host sends data packets to the destination host. In black hole attack, the attacking node exploits this feature to its advantage. In black hole attack, the attacker can redirect all the data packets to itself by sending false RREP packet advertising a shortest or latest route to the destination host and then drops the data packets without forwarding it to the destination [6]. In cooperative black hole attack, multiple attackers work in collusion and launch the black hole attack. This is to avoid promiscuous monitoring or overhearing by other nodes when the attacker drops packet.

In this paper, a non cryptographic and a light weight technique called SEC-DSR is proposed for detecting black hole attack in the network. In this method, every node in the ad hoc network when receiving a RREQ packet, records the node ids contained in the route field of the RREQ packet. Also when an intermediate node receives a RREP checks for the active participation of the replying node in the RREQ forwarding process and decides whether the replying node is a black hole attacker or a normal node. Based on its judgment, it assigns a weight value for the replying node and forwards the RREP. Similarly all intermediate nodes in the RREP path, assigns a weight value for the replying node. When receiving the RREP packet, the source node decides whether to select that route for data transmission or not based on the cumulative weight value assigned. The black hole attack can be easily deployed on one of the commonly used reactive routing protocols called Dynamic Source Routing protocol; hence the proposed method is implemented and tested on DSR based ad hoc networks. The significant merit of the proposed method when compared to other related works; it detects the black hole attack without any computational overhead and also with minimum packet loss rate.

An accusation-based scheme was proposed in [7] where each node assign trust value for other nodes in the network by continuous monitoring of neighbors and forwarding accusations to other nodes when it detects an abnormal activity in its neighborhood. The malicious nodes certificates are revoked when the sum of accusations is greater than a assigned threshold. This method of detection increases control packets overhead in the network and also require promiscuous monitoring which results in fast depletion of energy in nodes. Similarly in [8], the authors proposed a neighbourhood watch mechanism, which sends accusation messages about suspected nodes to a predefined set of controller nodes. These controller nodes are responsible for deciding whether a node is an attacker or not based on the incoming accusation messages. A fuzzy based approach is proposed in [9] for trust prediction, by considering the previous data transmission history of every node for predicting the trustworthiness of a transmitter node. But this approach needs domain experts for tuning parameters and setting fuzzy rules. In [10], the authors proposed the concept of maintaining a trust bias for each node by taking into account the weights associated with direct trust based on observations and indirect trust based on recommendations by other nodes. Also the trust bias is adjusted and minimized based on these two weights. In [11], the authors proposed a trust model for securing the network. In this approach a decision for penalizing the malicious node is done using a voting scheme by other nodes in

the network. In [12] the authors used multipath forwarding technique to defend malicious packet dropping in the network. However there is no mechanism suggested to identify the compromised nodes in the network. In [13] a method proposed that involves only exchange of control packets to detect the black hole attack. In this approach the source node confirms the validity of the RREP path by extracting the next hop node information from RREP and confirms with the next hop node about its connectivity to the intermediate node that sends the route reply and also with the destination. The approach used by the authors of [14] employs explicit acknowledgements for fault detection. For every successfully received data packets the destination sends an acknowledgement back to the source. In [15] a guarding mechanism is proposed for detection of black hole nodes in the network. Here every node acts as a Guard node and maintains trust value for its neighbors and for the route selected. The trust value for a neighbor is calculated both by direct observation and also by the opinion of other nodes in the network. Promiscuous monitoring is employed by this approach which results in higher energy consumption. In [16] an approach for black hole attack detection using AODV protocol is proposed. Here the destinationsequence number value for a given RREP packet is verified by the source and if it exceeds the calculated threshold, the replying node is taken as suspicious node. Then the source sends a fake request packet with a non-existent destination address to the suspected node and checks whether it is receiving the reply for that fake request packet from the suspected node. In [17] a solution using control packets for malicious node detection is proposed. Before sending the data on the selected path, a data control packet is sent to the path, in order to check the path validity. The black hole node present in that path will drop the packet and in this way the malicious node is detected, else the path is chosen. Routing overhead is higher in this approach. In [18] watch dog method is proposed for monitoring the transmission of next hop neighbor. The approach increments the failure counts of the node if it does not forward the packet. The node is marked as attacker when the failure count exceeds some threshold value and the information is intimated to source node. In [19], an approach using timers and bait control packets is proposed for detecting black hole attack. The bait timer of each is set randomly and each time the timer expires the node broadcasts a request packet for a nonexistent node in the network. When the source node receives a RREP for the bait request it immediately marks the replying node as a black-hole and adds it to the black-hole list. In [20], a voting scheme for isolation of black hole nodes is proposed. The detection mechanism is divided into local and global context. Decisions about suspicious activity from the local context are passed to global context and based on the received information the global context punishes the suspicious node. In [21], The author proposed TEMAODV which is an extension of Multipath Ad hoc on Demand Routing protocol that uses local monitoring and control packets to establish two way trust on the route. In [22], the authors proposed a promiscuous monitoring of neighbor nodes to detect packet dropping by malicious nodes in AODV protocol. As it employs constant overhearing of neighborhood, the energy consumption of participating nodes in the network will be higher. In [23] an trust method called ESCT is proposed to prevent security attacks. In ESCT, each node makes the decision of suspected nodes by themselves and notify its direct neighbors. Then each node perform cooperative detection and finds additional trust information to distinguish normal and black hole nodes. Similar to our approach, ESCT employs self detection but then it notifies the trust information to all nodes in the network for cooperative detection of the attacker that results in high overhead. But in SEC-DSR, every node shares the trust information only with the source of the route to reduce control packet transmission overhead.

2. RESEARCH METHOD

The proposed method extends the existing DSR protocol and makes them less vulnerable to black hole attacks. The low processing speed, available processing capacity and power constraints of the ad hoc nodes are taken into account in the proposed solution. The normal protocol operation of DSR for route discovery is used in this method to identify the black hole attack. The assumption of the proposed solution is that all the nodes are legitimate nodes with proper credentials for participation in the network. The other assumptions are: If two nodes are in the coverage range of each other, then bidirectional communication is possible; the source host and the destination host of the generated traffic are always trusted nodes.

2.1. Dynamic source routing protocol

The two main functionalities of Dynamic Source Routing Protocol are route discovery and route maintenance. In the route discovery phase between any source and any destination, the Route Request (RREQ) packets are broadcasted in the network. The RREQ packets are generated by the source host in need of discovering a fresher route to a destination. When the destination receives the RREQ packet, it creates a Route Reply (RREP) packet for the first RREQ it receives (shortest path) and sends it back to the source by reversing the path information stored in the RREQ Packet. However, on receiving the RREQ, an intermediate node also can create and send the RREP back to the source node if it has a path to reach the destination. The

DSR protocol also has Route maintenance phase where the link breaks are handled. A link break occurs after establishing a route when a participating node in the route moves out of the transmission range of its upstream neighbor. Then the upstream neighbor sends a route error (RERR) message back to the source informing about the link break. The source node either forwards data using an alternate path available or if no path available then initiates again the route discovery phase.

2.2. Proposed method

In the proposed work, any node receiving a RREP control packet will assign a weight to the intermediate node that creates and send the Route Reply on behalf of any destination host. The proposed method adapts the same approach followed by DSR for the route discovery process in the forward direction i.e., from the source to the destination. As in Figure 1, initially any host needs to send data to any other host, it broadcasts a RREQ packet to find route for that particular destination. The other nodes on receiving the RREQ packet will either broadcast the RREQ packet, or drops the packet and send RREP if they have the route to that particular destination. Also in the proposed method, all nodes maintain a table named as RREQ forwarding table. The node receiving RREQ packets enters the node ids of particular source and destination pair mentioned in the RREQ packet in the table along with the node ids of all the nodes involved so far in forwarding the request packet. When a RREP comes for the corresponding RREQ, every node receiving the RREP verifies if the replying node is an intermediate node or the destination node. If the reply is from an intermediate node, then the nodes check in their RREQ forwarding table, whether the intermediate node is involved in RREQ forwarding process for the same source and destination pair. If so, then it will be assigned with the weight 1. If not, then the nodes receiving the RREP check in their table, whether the intermediate node that generated the RREP is involved in RREQ forwarding process of any other source - destination pair. If so, then its node id is present in the table, and hence it will be assigned with the weight of 0.5. As the behavior of black hole node is to drop all RREQ packets it receives and to send a RREP immediately for every RREQ it receives, the node id of the black hole node will not present in the RREQ forwarding table of other nodes and the weight assigned for the black hole node by other nodes for forwarding the RREQ will be always 0. For ex, the RREQ forwarding table maintained by node X is given in Table 1. From the cumulative weight value assigned for the replying node, the source node calculates its trust value. If the trust value of the replying node is below 0.5 threshold value, the source node drops the RREP packet and selects the next RREP with assigned threshold value exceeds or equals 0.5. If the RREP comes from destination node, the intermediate nodes forwarding RREP does not verify the table and directly assigns weight value 1 for the replying node.

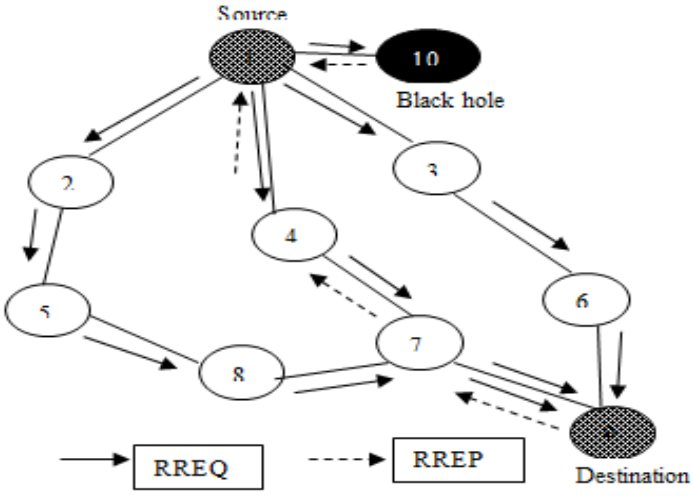


Figure 1. Route discovery phase

The routing tables maintained by each ad hoc node are periodically refreshed in reactive routing protocols since the ad hoc network made up of mobile nodes and the network topology will be constantly changing. Similarly the RREQ forwarding table maintained by the ad hoc nodes is also periodically refreshed in order to observe the behavior of nodes from time to time. In Figure 1, The host with node id 1 broadcasts a RREQ packet to discover route for another host with node id 9. The normal nodes receiving the RREQ

forwards the packet again until it reaches destination. But the black hole nodes 8 and 10 will immediately send RREP claiming they are having path to reach node 9. Node 9 also sends a RREP back to the source node 1. The route reply packet RREP from black hole node 10 reaches node 1 first. In the scenario given in Figure 1, the source node is the next hop node for Node 10, hence the source node when it receives the RREP, it checks its RREQ forwarding table and identifies that node 10 is not involved in any RREQ forwarding process and hence assigns a weight of 0 to the replying node. Then for the RREP from another black hole node 8, both the forwarding nodes 5 and 2 as well as the source node 1 adds the weight value as 0 in the RREP. The trust value calculated for the replying nodes 8 and 10 from the cumulative weight value is below 0.5 threshold value, so the source node 1 ignores the RREP coming from them and selects the next RREP coming from the destination node 9.

Table 1. RREQ forwarding table of Node X

Source Node in RREQ	Destination Node in RREQ	Nodes in RREQ Path
A	G	A,B,G,D
B	I	G, H, B,A,F

The cumulative weight value and trust value for the replying node is calculated as follows:

$$\text{Cumulative weight value} = \sum_{i=1}^{k} Wij \quad (1)$$

In (1) Wij is the weight assigned by node i for the replying node j. Assuming k nodes in the RREP path, k-1 intermediate nodes and the kth node as source node, i varies from 1 to k.

Trust Value of the Replying node j is calculated as follows by the source node:

$$\text{Trust Value (Tj)} = \text{Cumulative Weight value / Total No. of nodes in RREP path} \quad (2)$$

If Tj>= 0.5, the route is selected for transmitting data packets; otherwise not selected. Procedure 1 depicts the function of intermediate nodes when receiving RREQ packets. Procedure 2 explains the function of nodes when receiving RREP packets.

Procedure 1: Action of nodes in forwarding RREQ packets

if source host

Generate a RREQ control packet and broadcast it to find route to reach a particular host.

else if an intermediate node

if a RREQ packet is received

1) For the source–destination pair in the RREQ packet, enters the node ids in the RREQ path into the RREQ forwarding table.
2) Check for the path to reach destination in its routing table.
   a) If found, drop RREQ and send back a RREP back to the source node using the same route.
   b) If not found, forward the RREQ to its neighbor nodes.

else if a black hole node

On receiving a RREQ, drops it send a RREP immediately to the source host in the same path from where it receives the RREQ.

else destination node

Drops RREQ, create and send a RREP back to the source host.

end if

Procedure 2: Action of nodes when receiving RREP Packets

if not the source host (any other nodes)

When RREP packet is received

1) Checks whether the RREP is from the intended destination host or from any intermediate node.
2) **if** RREP is sent by an intermediate node:
   a) Verify whether the replying node is involved in any RREQ forwarding process by checking its RREQ forwarding table
   b) Add to the existing weight value of the replying node a weight of 1, if the replying node is involved in the RREQ forwarding process of the same source-destination pair.

c) If not, add a weight of 0.5 to the weight value of the replying node, if the replying node is participated in RREQ forwarding process but for some other source-destination pairs.
d) If the replying node is not participated in any RREQ forwarding, add a weight of 0 and then forwards the RREP.

3) **else if** reply is from the destination node
a) Add a weight of 1 to the existing weight value in the Route REPly packet and forwards it.

else if source host

On receiving a RREP packet

A. **if** reply from destination, send the data packets in the same path.
B. **else if** reply from an intermediate node
a) Add weight of 1 or 0.5 to the existing weight value of the replying node based on its participation in the RREQ forwarding process.
b) Calculate Trust value (T_j) for the replying node (say node j) using formula (2).
c) If T_j>=0.5, the RREP packet is accepted and the data packets are transmitted in the same path.
d) If T_j<0.5, the RREP packet is not accepted and the source host accepts the next RREP with T_j>=0.5.
e) Initiates black hole node isolation process.

end if

2.3. Black hole node isolation

Once the source node concludes from the calculated trust value and suspects that the replying node may be a black hole attacker, then it broadcast the suspected node id information to the entire network by sending a BHN (Black Hole Node) packet. All nodes receiving the BHN packet, checks whether the node id mentioned in BHN packet is recorded in its RREQ forwarding table, if not, it confirms the node as black hole and remove its entry from its routing table and discards any packets coming from it. Subsequently, the isolation of black hole nodes is collectively done in the network.

3. RESULTS AND DISCUSSION

Ns2 is used as the network simulation tool to validate the efficiency of the proposed method in the presence black hole attack. 50 legitimate mobile nodes executing the proposed solution were randomly distributed, and a couple of black hole attackers, are randomly selected to launch the attack. For simulation the total coverage area used is 1500 X 1500 m2. Totally 50 mobile nodes are used as participating nodes in the ad hoc network each following Random Mobility model for mobility. The nodes move in the speed of 20m/s. For the performance analysis, out of 50 nodes, 0 to 20 nodes are randomly selected as black hole nodes for every simulation. 10 source and destination pairs are selected for generating data traffic. UDP-CBR (Constant Bit Rate) is the data traffic type selected for data communication. An average of 10 experiments results taken to represent the experimental data.

The performance of the proposed method is also compared with another approach, given in [23], where every node detects the trust value on other nodes by itself. Similar to our approach, DSR is selected as the routing protocol in [23]. The performance of the proposed work is evaluated using the metrics like Packet Delivery Ratio, Routing overhead, End to End communication delay and Energy consumption. The energy consumption by nodes is estimated using a wireless radio model as given in [23-25]. Let et and er be the energy consumption measure of sender and receiver respectively. The value is measured in J/bit. The formula for calculating the energy consumption in a node when transmitting a one bit data is given below:

$$= et + c. d2 \quad (3)$$

In the (3), 'c' is the constant measured in J/bit/m2.

The distance d is set to 250m (transmission range of a node). The values of et and er are set to 50nJ/bit. Also the value of c is set to 10pJ/bit/m2 as recommended in [25]. The energy consumption for receiving one bit data by a node is calculated as follows:

$$Erx = er \quad (4)$$

Figure 2 shows the percentage of packets received by destination nodes in DSR, ESCT and in the proposed approaches Secure DSR (Sec-DSR) under the same environmental setup. The packet delivery ratio

for DSR drops alarmingly with only 5 black hole nodes in the network. The black hole node attracts all the data traffic towards itself and drops the data packets. So the packet delivery ratio of Dynamic Source Routing Protocol is approximately 40% under attack. Both in ESCT and in Sec-DSR the packet delivery ratio is approximately 90% even with 40 percent attackers inside the network. In our approach, the route will not be strictly selected if the replying node not participated in any RREQ forwarding process. Hence PDR in our approach is better than in traditional DSR and slightly improved over ESCT.

Routing overhead gives the percentage of control packets generated and forwarded for the total number of data packets transmitted in the network. Under the attack the routing overhead in Sec-DSR is around 20% which is an increase of 5% approximately when compared to DSR as shown in Figure 3. In Sec-DSR there was no additional control packets transmitted during route discovery. Once the source evaluate that the route reply packet is coming from a black hole attacker, then it will generate an additional BHN packet and send to the network. Hence there is a slight increase in routing overhead when compared to DSR. However, Routing overhead in ESCT is considerably higher. In ESCT, nodes periodically broadcast Hello messages to discover the current topology and neighbors and share the self-detection results in the network. Also it introduces the investigation request/reply control packets for self-detection. These additional control packets results in increased routing overhead.

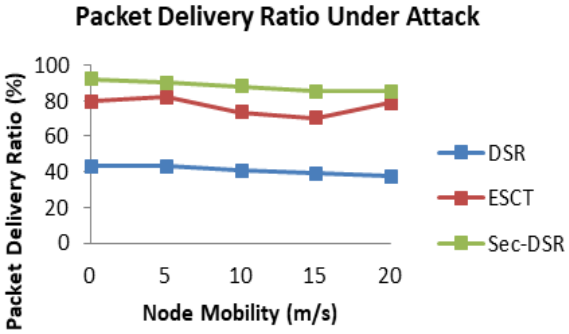


Figure 2. Packet delivery ratio in the presence of black hole nodes

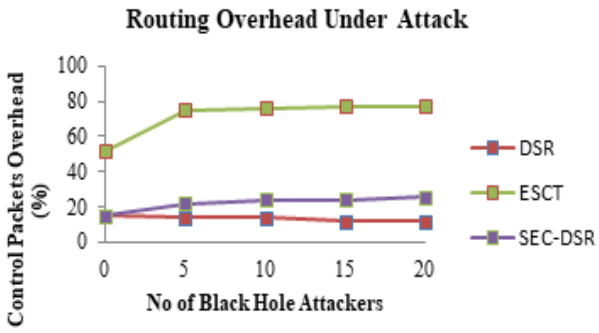


Figure 3. Control packets overhead in the presence of black hole nodes

Figure 4 shows the end -to-end delay in data communication between a source and destination in the presence of black hole nodes in the network. In ESCT and in Sec-DSR the nodes try to avoid routes with black hole nodes even if it sometimes results in using longer paths than using the shortest path. Hence the presence of more attackers inside the network increases the end-to-end delay both in Sec-DSR and in ESCT as shown in Figure 4. But in DSR protocol in the presence of more attackers, most data packets cannot be received by the destinations and they are dropped by the black hole nodes. The dropped or lost data packets are not considered for measuring packet delay. Hence end-to-end delay of DSR is better than SEC-DSR and ESCT.

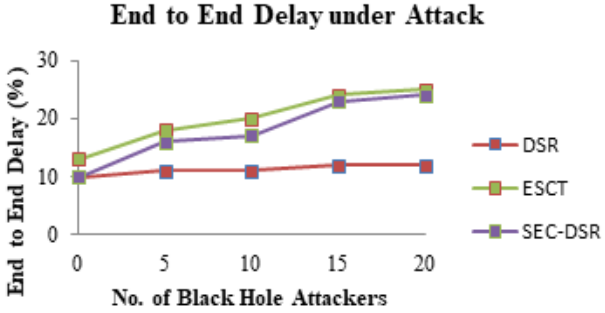


Figure 4. End to end delay under black hole attack

The total energy consumption by SEC-DSR is reduced by 62.7 percent in an average when compared to ESCT as shown in Figure 5. Since SEC-DSR does not employ continuous overhearing or promiscuous monitoring to monitor the neighborhood, energy consumption by individual nodes is reduced. And also in our approach only BHN packet is the extra control packet introduced hence energy consumption is only increased by 2% approximately when compared to DSR as shown in Figure 5. However, ESCT generates and forwards more control packets which results in more energy consumption in each node.

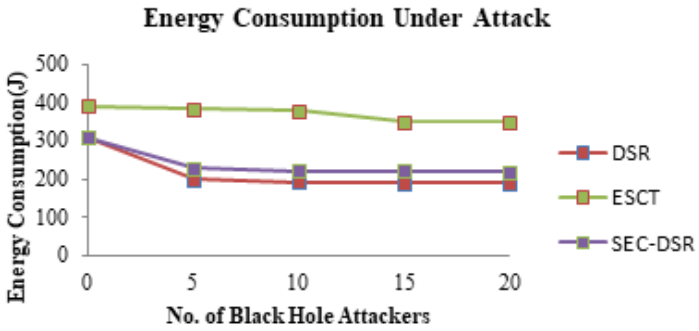


Figure 5. Energy consumption under attack

4. CONCLUSION

In this paper, a light weight solution methodology called SEC-DSR is proposed to detect and isolate black hole nodes in MANET. The method can be adopted with any on demand ad hoc routing protocols. SEC-DSR uses only analysis of RREQ and RREP packets for detecting the black hole attackers which make it suitable to deploy it in the resource constrained environment of MANET. The performance analysis of SEC-DSR shows better packet delivery ratio and better end to end delay in the presence of attackers. The method does not require any computational complexity or promiscuous listening.

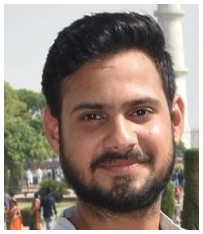
REFERENCES

[1] Obidike, G. C., Nwabueze, C. A. and Onuzulike, V. C., "Concept And Characteristics Of Mobile Ad-Hoc Network", *International Journal Of Innovative Engineering, Technology And Science*, vol. 2, pp. 133-142, Mar 2018.
[2] A. Mehran, W. Tadeusz, D, "A review of routing protocols for mobile ad hoc networks", *Ad Hoc Networks*, vol. 2, pp. 1-22, Feb 2004.
[3] Von Mulert J, Welch I, Seah WK, "Security threats and solutions in MANETs: a case study using AODV and SAODV", *Journal of Networks and Computer Applications*, vol. 35, pp. 1249-1259, Feb 2012.
[4] Garcia Teodoro P, Sanchez Casado L, Macia Fernandez G, "Taxonomy and holistic detection of security attacks in MANETs", *CRC Press*, pp. 1-12, Apr 2014.
[5] D.B. Johnson, A.D. Maltz, J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks", In: *Perkins, C.E. (ed.) In Ad Hoc Networking*, ch. 5, Addison-Wesley, pp. 139-172, 2001.
[6] C. Perkins, E. Royer, "Ad hoc on demand distance vector (AODV) routing", *Second IEEE Workshop on Mobile Computing Systems and Applications*. WMCSA '99, pp. 90-100, Feb 1999.
[7] G. Arboit, C. Crepeau, C.R. Davis, M. Maheswaran, "A localized certificate revocation scheme for mobile ad hoc networks", *Ad Hoc Networks*, vol. 6, pp. 17-31, Jan 2008.
[8] N.C. Fernandes, M.D.D. Moreira, O.C.M.B. Duarte, "A self-organized mechanism for thwarting malicious access in ad hoc networks", *29th Conference on Computer Communications. IEEE INFOCOM'10*, pp. 266-270, Mar 2010.
[9] H. Xia, Z. Jia, L. Ju, and Y. Zhu, "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory," *IET Wireless Sensor System*, vol. 1, pp. 248-266, Dec 2011.
[10] I. R. Chen, J. Guo, F. Bao, and J. Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", *Ad Hoc Networks*., vol. 19, pp. 59-74, Aug 2014.
[11] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks", *Ad hoc Networks*, vol. 19, pp. 142-155, Mar 2014.
[12] Karlof C, Wagner D, "Secure routing in wireless sensor networks: attacks and countermeasures", *Adhoc Networks*, vol. 1, pp. 293-315, Feb 2003.
[13] H.Deng, P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", *IEEE Communications Magazine*, vol. 40, pp. 70-75, Oct 2002.
[14] B.Awerbuch, D. Holmer, C. Nita Rotaru, H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", *1st ACM Workshop on Wireless Security*, Wise'02, pp. 21-30, Sep 2002.

[15] Imran Raza, S.A. Hussain, "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes", *Computer Communications*, vol. 31, pp. 1796-1802, Dec 2007.
[16] Jhaveri, Rutvij H., and Narendra M. Patel, "A sequence number based bait detection scheme to thwart gray hole attack in mobile ad hoc networks", *Wireless Networks*, vol. 21, pp. 2781-2798, Apr 2015.
[17] Dorri, Ali, Soroush Vaseghi, and Omid Gharib, "DEBH: detecting and eliminating black holes in mobile ad hoc network", *Wireless Networks*, vol. 24, pp. 2943-2955, Apr 2017.
[18] Tarun Varshney, Tushar Sharma and Pankaj Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad HocNetwork", *4th International conference on communication systems and Network Technologies*, CSNT-2014, pp. 217-221, Apr 2014.
[19] Adwan Yasin, Mahmoud Abu Zant, "Detecting andIsolating Black-Hole Attacks in MANET using Timer Based Baited Technique", *Wireless Communications and Mobile Computing*, vol. 1, pp. 1-11, Sep 2018.
[20] Lyno Henrique G. Ferraz, Pedro B. Velloso and Otto Carlos M.B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks", *Adhoc Networks*, vol. 19, pp. 142-155, Mar 2014.
[21] H. Xia, J. Yu, C. L. Tian, Z. K. Pan, and E. Sha, "Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks," *Journal of Networks and Computer Applications*, vol. 62, pp. 112-127, Feb 2016.
[22] G. Vaseer, G. Ghai, D. Ghai, and P. S. Patheja, "A Neighbor Trust-Based Mechanism to Protect Mobile Networks," *IEEE Potentials*, vol. 38, pp. 20-25, Feb 2019.
[23] Ruo Jun Cai, Xue Jun Li and Peter Han Joo Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs", *IEEE Transactions On Mobile Computing*, vol. 18, pp. 42-55, Jan 2019.
[24] W.B. Heinzelman, A.P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", *IEEE Transaction on Wireless Communication*, vol. 1, pp. 660-670, Oct 2002.
[25] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for WSNs," *IEEE Transaction on Information Forensics Security*, vol. 10, pp. 613-625, Mar 2015.

BIOGRAPHIES OF AUTHORS

Dr M.Mohanapriya is working as Associate professor in the department of Computer Science in Coimbatore institute of Technology. She completed her Ph.D in the area of Ad hoc Network Routing Protocols Security in the year 2014. Her research interests are Network Security, Internet of Things and Vehicular Networks.



Nitish Joshi is an energetic and great communicator with Networking, Web Development and Database enthusiast, and Eager-to-learn personality, persuing his Bachelor's degree in Engineering with IT stream at M.B.M Engineering College, Jodhpur, Rajasthan.

Mohit Soni is a data science and web development enthusiast and is a student of MBM engineering college pursuing Bachelor of engineering focussed on Information technology.