A Light Weight Non-Cryptographic Solution for Defending Black Hole Attacks in Mobile Ad Hoc Networks

[1]Dr.M.Mohanapriya and [2]Dr.M.Mohanapriya
mohanapriya.m@cit.edu.in mohanapriya.m@cit.edu.in mohanapriyaasaithambi@gmail.com
[1,2]Assoicate Professor, Coimbatore Institute of Technology, india

Abstract
Mobile Ad hoc Network (MANET) is a self organizing network in which a group of wireless nodes communicate among themselves without requiring any centralized infrastructure. This important characteristic of mobile ad hoc networks allows the hassle free set up of the network for communications in different emergency situations such as battlefield and natural disaster zones. Multi hop communication in MANET is achieved only 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. In this paper we propose a light weight non cryptographic solution to defend the network from black hole attack and enables communication even in the presence of the attack. In this scheme, by analyzing only the control packets used for routing in the network, the nodes identify the presence of black hole attack. Based on 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 in the presence of attack.

Keywords:
Ad hoc Networks, MANET, DSR, Routing Protocols, Security Attacks, Black Hole Attack

1. Introduction

One kind of wireless network which operates without the support of any centralized infrastructure is Ad hoc wireless networks also known as infrastructure less networks. Ad hoc networks utilize multi-hop radio relaying for communicating among participating nodes in the network. 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, each node acts as both host and router. As the nodes are mobile the network topology is also dynamic in nature.

The features of Ad hoc networks including large level of user-mobility, quick and economically less demanding 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, emergency 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 Ad hoc networks is to find a secure and shortest path between source and destination nodes. It requires cooperation of all participating nodes in the network to find such routes between any source and destination. The routing protocols designed for 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 shortest path between source and destination on time. 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. As the nodes of the ad hoc network are resource constrained mobile nodes, any proposed solution for the security attacks should not be highly resource intensive which requires much processing by each node in the network.

Security attacks in MANET can be classified into passive and active attacks. In passive attacks, the attackers silently listen the traffic and learn valuable information such as originator and receiver of the message, duration of communication and so on. 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,

Manuscript received October 5, 2024
Manuscript revised October 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.10.15

Routing Table Overflow, Wormhole attacks, and so on [3], [4]. In setting up an ad hoc network, 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 compromised or malicious nodes that have been properly authorized by the target network. These compromised nodes are called inside attackers and the attack launched is called inside attacks. The inside attacks are very hard to detect as it is being launched by authorized but compromised nodes.

Black hole attack is an inside attack which can be easily launched on reactive routing protocols like AODV [5] and DSR [6]. In reactive routing protocols, during route discovery process, the source node broadcast RREQ packets in the network. Any node receiving the RREQ sends RREP back to the source node if it have a fresh or shortest route to the destination. Using the path in RREP, the source node sends data packets to the destination. In black hole attack, the malicious node exploits this feature to its advantage. In black hole attack, a malicious node can redirect all the data packets to itself by sending false RREP claiming a shortest or fresh route to the destination and then drops the data packets without forwarding it to the destination. Cooperative black hole attack is a kind of black hole attack where multiple attackers work in collusion to launch the attack. This is to avoid promiscuous monitoring or overhearing by other nodes when the attacker drops packet.

In this paper, we propose a non cryptographic and a light weight technique for detecting black hole attack in the network. In our approach, every node in the network when receiving a RREQ packet, records all the node ids present in the forwarding path of RREQ packet. Also when a node receives a RREP, to verify whether the replying node is a black hole node or not, it checks for the active participation of the replying node in RREQ forwarding process. Based on its judgment, it assigns a weight value for the replying node and forwards the RREP. Similarly every intermediate node in the RREP path, assigns a weight value for the replying node. The source node when receives the RREP packet, from the cumulative weight value assigned, decides whether to select that route for data transmission or not. DSR is one of the popular reactive routing protocols where the black hole attack can be easily launched; therefore, this study deploys and evaluates the proposed solution on DSR based MANET.

The significant merit of the proposed method when compared to other related works; it detects the presence of black hole attack without any computational complexity and also achieves better throughput or reduction in packet loss rate.

The structure of this paper is organized as follows: Section 2 discusses the related works for defending black hole attacks in MANET; DSR protocol explained in Section3; The implementation of our approach is discussed in section 4; Section 5 explains the experimental data and analysis; Conclusion is given in section 6.

2. Related Works

An accusation-based scheme was proposed by Arboit et al.[7] in which nodes monitor their neighbors to send accusations whenever they detect misbehavior from the vicinity. Nodes use the received accusations to assign a trustworthiness value to all other nodes in the network, and revoke their certificate when the sum of accusations is greater than a configurable threshold. The nodes in this mechanism, however, maintain data and receive accusations from all other nodes to assign the trustworthiness value which increases control packets overhead in the network and also requires promiscuous monitoring which results in fast depletion of energy in nodes. Fernandes et al. proposed a controller-node-based access control mechanism for Ad hoc networks, called ACACIA [8]. The system uses a neighbourhood watch mechanism, which constantly generates accusation messages to the random controller sets. Then, these controller sets appraise a reputation to the nodes depending on the incoming rate of accusation messages, and exclude the nodes with low reputation. Therefore, the system drawback is the high control-message overhead, and the low reputation accuracy on different network conditions, such as number of neighbours that generate different reputation values. Xia et al. [9] applied fuzzy inference rules for trust prediction, considering past and current service experiences for predicting the service capability of a transmitter node. One drawback of fuzzy logic-based trust prediction is that it requires domain experts to do parameter tuning and set the fuzzy rules incorporating the knowledge of the causal relationship between the input and output parameters. Chen et al. [10] proposed the concept of trust bias minimization by dynamically adjusting the weights associated with direct trust (derived from direct evidence such as local observations) and indirect trust (derived from indirect evidence such as recommendations) so as to minimize trust bias. Ferraz et al. [11] proposed a robust and distributed access control mechanism depending on a trust

model for securing the network and encouraging good cooperation by isolating misbehaving nodes in the network. The access control responsibility is viewed in two different contexts namely the local and global. In the local context responsibility, the neighbour nodes are intimated to notify about the suspicious behaviour of the global context. While the global context examines the gathered information, a decision would be made to penalize the malicious node using a voting scheme. Karlof and Wagner [12] used multipath forwarding technique to identify packet dropping attacks in a wireless sensor network. However the attackers were not detected and isolated from the network in this approach. Deng [13] proposed a routing security protocol to detect the black hole attack.

The authors introduce a Further request (FREQ) and a Further reply (FREP) to avoid the black hole attack. If an intermediate node wants to send RREP, it has to send its next hop node back to the source. After receiving a route reply, the source extracts the next hop information and then sends a FREP packet to the next hop to verify whether it has a link to intermediate node which sent the route reply and whether the next hop has a route to the destination. Upon receiving the FREP having the check result from the next hop, the source node can confirm the validity of the path. If the check result value is yes, the source node concludes the route is valid. One drawback of this approach is that it cannot avoid the black hole attack in which two black hole nodes work in collusion, i.e., if the next hop node is a colluding attacker, it sends the FREP confirming the validity of the route. The fault detection mechanism proposed in [14] is based on explicit acknowledgements. The destination sends back ACKs to the source for each successfully received packet. The source can initiate a fault detection process on a suspicious path that has recently dropped more packets than an acceptable threshold. This technique employs encryption and decryption which results in more computational complexity at each node. Raza et al. [15] proposes a guard node based technique for identification of black hole nodes in the network. Here every node acts as a Guard node and calculates trust level of its neighbors and the trust level of the route to be selected. The trust value for a neighbor say B is calculated based on two factors; i) by direct observing of its behavior based on the successful transmission of RREQ, RREP and RERR packets; ii) based on the opinion of other nodes about node B. In this approach each node has to promiscuously listen and monitor the traffic pattern of the neighbor nodes which results in loss of energy in each node whereas our approach does not require it. Jhaveri et al. [16] proposed an approach which is based on the fabricated highest sequence number by a malicious node in order to detect the attacker node. Whenever the destination sequence number value in the RREP packet of a particular node exceeds the calculated threshold, the node is then declared as suspicious. A bait request packet with non-existent destination address is sent to the suspicious node. If the node replies the bait request packet, it is isolated as malicious node. But the malicious nodes by analyzing traffic patterns easily identify fabricated sequence numbers and not reply to those baits. Dorri et al.[17] proposed a solution called detecting and eliminating black holes (DEBH) for isolating the black hole nodes.

This approach uses a data control packet and an additional black hole check (BCh) table for malicious node detection. Whenever an intermediate node sends the RREP packet back towards source node, it should also append its BCh table with it. After getting all the replies from intermediate nodes, a secure route is selected based on the BCh table of each node. Before sending the data on the selected path, a data control packet is sent to the path, in order to check the path validity. If a black hole node manages to enter the path, it will surely drop the data control packet and in this way the malicious node is detected, else the path is chosen. Control packets overhead is more in this approach. Each node maintains BCh table for every other nodes which can increase the delay during the routing process. Tarun Varshney et al[18] applies watch dog mechanism to detect misbehavior nodes by monitoring the transmission of next hop neighbor. In watchdog, the copies of the packets that are forwarded by a node are kept in a buffer and it eavesdrops on the transmission of next link to confirm that it forwards packet properly. The overheard packet is then compared with the packet that is kept in buffer. The packet in the buffer is removed if there is a match. Otherwise, the watchdog increments the failure counts of the node which is responsible for forwarding packets. The node is detected as misbehaving node when the failure count exceeds some threshold value and a notification message is sent to source node. In [19], an approach to resist smart black-hole attacks by employing timers and baiting messages is proposed. Here each node has a bait-timer,

the value of the timer is set randomly and each time the timer expires it broadcasts a bait request with a randomly generated fake id. When the black-hole receives the baited request it sends a reply to the source node claiming that it has a route; when the source node receives the reply it immediately considers the node which responded as a black-hole and adds it to the black-hole list. Lyno Henrique et al[20] propose a distributed access control mechanism based on a trust model to secure the network and stimulate cooperation by excluding misbehaving nodes from the network. The mechanism divides the access control responsibility into two contexts: local and global. The local context responsibility is the neighborhood watch to notify the global context about suspicious behavior. In its turn, the global context analyzes the received information and decides whether it punishes the suspicious node using a voting scheme. In [21] an evolutionary self-cooperative trust (ESCT) scheme is proposed that relies on trust-level information to prevent various routing disruption attacks. In ESCT, each node runs self-detection independently, and then broadcasts detection results that indicate benign and malicious peers to its direct neighbors. After that, based on self-detection and information received from neighbors, each node can perform cooperative detection to derive further trust information to distinguish malicious and benign nodes. Similar to our approach, it employs self detection but shares the trust information to all nodes in the network for cooperative detection resulting in high overhead. But in our approach, every node shares the trust information only with the source of the route to reduce control packet transmission overhead.

3. Dynamic Source Routing Protocol

DSR has two main functionalities: route discovery and route maintenance. The basic approach of this protocol during the route discovery phase is to establish a route by broadcasting Route Request (RREQ) packets in the network. The destination node on receiving a RREQ packet, responds by sending a Route Reply (RREP) packet back to the source by reversing the route information stored in the RREQ Packet. On receiving the RREQ, any intermediate node can send the RREP back to the source node if it has the route to reach the destination. During the Route maintenance phase, the link breaks are handled. A link break occurs when any intermediate node which involves in the packet forwarding process moves out of the transmission range of its upstream neighbor. If an upstream node detects a link break when forwarding a packet to the next node in the route path, it sends back a route error (RERR) message to the source informing it of that link break. The source either tries an alternate path available or initiates the route discovery process again.

4. Proposed Methodology

In this section, we propose a light weight technique that can be extended to the existing DSR protocol and make 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 in route discovery process is used to identify the black hole attack. Our solution assumes that all the nodes are authenticated and can participate in communication i.e., all nodes are authorized nodes. The other assumptions are: If node A and node B is in the transmission range of each other, then bidirectional communication is possible; Source node & destination node are taken as trusted nodes by default.

4.1 Protocol Description

In our proposed work, every node receiving a RREP packet will assign a weight to the intermediate node that generated the Route Reply on behalf of any destination. In our proposed method, the route discovery process in the forward direction i.e., from the source to the destination is similar to that of the DSR routing protocol. Initially the source node broadcasts a RREQ packet to find route to a particular destination. The nodes on receiving the RREQ packet will either broadcast the RREQ packet again, or drops the packet and send RREP if they have the route to the destination. Also in our method, all nodes maintain a table named as RREQ forwarding table. The node receiving RREQ creates an entry in the table for a particular source and destination pair mentioned in the RREQ, and stores the node ids of the nodes involved so far in forwarding the request packet in the table. When a RREP comes for the 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 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, then it will be assigned with the weight of 0.5. As the nature of black hole node is to drop any RREQ packet it receives and to send a RREP immediately to the source, the node id of the black hole nod will not present in the table and the weight assigned for the black hole node by other nodes forwarding the RREP will be always 0. For ex, the RREQ forwarding table for some node X is shown 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. The routing tables maintained by each ad hoc node are periodically refreshed in reactive routing protocols since the ad hoc nodes are 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 Fig.1, The Source node 1 broadcasts RREQ packet to find route to reach the Destination node 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 the destination. The destination node will also send a RREP back to the source node. The RREP from black hole node 10 reaches node 1 first. As the source node is the next hop node for Node 10, 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 node 8, the forwarding nodes 5 and 2 and source node 1 adds the weight value 0 for the black hole node 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 drops the RREP packet and selects the next RREP coming from the destination node 9 itself.

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

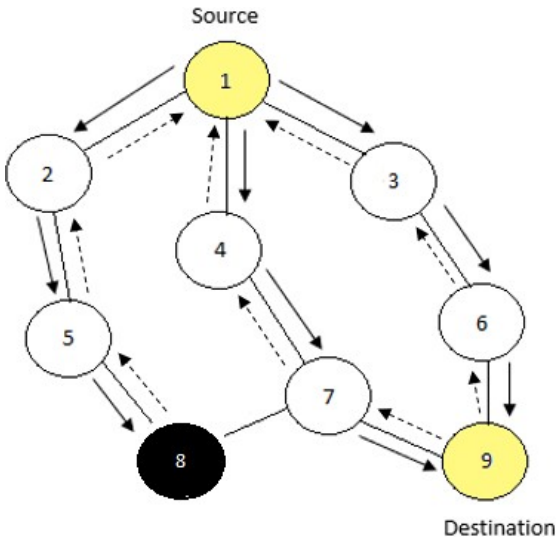

Figure 1: Route discovery phase

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

In (1) W_{ij} 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 source node, i varies from 1 to k where k^{th} node is the source node.

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

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

If $T_j >= 0.5$, the route is selected for transmitting data packets; otherwise not selected. Procedure 1 shows the action of intermediate nodes when receiving RREQ packets. Procedure 2 shows the action of nodes when receiving RREP packets.

Procedure 1: Action of nodes in forwarding RREQ packets

if source node

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

else if an intermediate node

On receiving a RREQ packet

a. For the source–destination pair in the RREQ packet, enters the node ids in the RREQ path into the RREQ forwarding table.
b. Check for the path to reach destination in its routing table.
   i. If found, drop RREQ and send back a RREP in the same path to the source node.
   ii. 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 back to the source node in the same path from where it receives the RREQ.

else destination node

Drops RREQ and send a RREP back to the source node.

end if

Procedure 2: Action of nodes when receiving RREP Packets

if an intermediate node

On receiving a RREP packet

a. Checks whether the RREP is from original destination node or from an intermediate node.
b. **if** reply is from an intermediate node:
   i. Verify whether the replying node is involved in any RREQ forwarding process by checking its RREQ forwarding table
   ii. 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.
   iii. 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.
   iv. If the replying node is not participated in any RREQ forwarding, add a weight of 0 and then forwards the RREP.
c. **else if** reply is from the destination node
   i. Add a weight of 1 to the existing weight value in the RREP packet and forwards it.

else if source node

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 node accepts the next RREP with $T_j >= 0.5$.
   e. Initiates black hole node isolation process.

end if

4.2 Black hole node isolation

Once the source node verifies from the trust value of the replying node, that the replying node may be a black hole node, then it broadcast the suspected node id information to the entire network by sending a BHN (Black Hole Node) Packet. Every node receiving the BHN packet, checks whether the node id 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 black hole node is isolated from the network.

5. Experimental Setup and Analysis

This paper applied ns2 to validate the efficiency of the proposed method against black hole attack. 50 normal nodes executing the proposed solution were randomly distributed, and a couple of malicious nodes, are randomly selected to perform black hole attack. Ten pairs were randomly chosen for data communication, each sending 5 kb UDP–CBR (Constant Bit Rate) per second. All normal nodes were moved in a Random-way point model, with random speeds ranging between 0 and 20 m/s. In addition, four types of pause times of the normal nodes, 0 s, 5 s, 10 s, and 15 s were separately considered. Pause time affects the frequency of network topology changes. Table 2 lists the parameters used for simulation. An average of 10 experiments results taken to represent the experimental data.

Also our approach is compared with an existing approach proposed in [21]. Similar to our approach, in [21], every node detects the trust value on other nodes by itself. Also it does not employ cryptographic approach for detection. Similar to our approach, DSR is selected as the routing protocol. To evaluate the performance of our approach, the following metrics are measured:

- Packet Delivery Ratio: Ratio of the total number of data packets received to the total number of data packets sent.
- Overhead (bit/s): denotes the amount of traffic added by our approach in order to detect black hole nodes.
- End to end delay (s): denotes the time elapsed between the moment of sending of a bit by the source node, and the moment of its reception by the destination node.
- Energy Consumption (J/bit): The energy consumption by nodes is estimated using a typical free space wireless radio model [21], [22], [23]. Let e^t be the energy consumed by a transmitter and e^r be the energy consumed by a receiver when a node is sending (receiving) 1 bit information (measured in J/bit). Let c be the free space constant measured in J/bit/m^2. The energy consumption when a node transmits 1 bit information to its neighbors is calculated as follows:

$$E^{tx} = e^t + c.\ d^2 \quad (3)$$

The distance d is set to 250m (transmission range of a node). The values of e^t and e^r are set to 50nJ/bit. Also the value of c is set to 10pJ/bit/m^2 as recommended in [22]. The energy consumed by a node for receiving 1 bit information from a neighbor is calculated as follows:

$$E^{rx} = e^r$$

Table 2: Simulation Parameters

Property	Value
Coverage Area	1000 x1000 m
No. of Nodes	50
Simulation time	200s
Transmission Range	250m
Mobility Model	Random
Load	5 kb UDP packets, every
Mobility Speed	1s
No. of Black Hole nodes	20 m/s
Connections	0 - 20
Traffic Type	10
Pause Time	UDP-CBR
	0,5,10 and 15s

5.1 Packet Delivery Ratio (PDR)

Fig. 2 shows the percentage of packets received by destination nodes in DSR, ESCT and in our approach under the same environmental setup. The packet delivery ratio for DSR drops drastically with the presence of only 5 black hole attackers. Since black hole nodes always claim that they have the shortest route to a destination, they can attract and drop more data packets. So the packet delivery ratio of DSR is approximately 40% under attack. Both in ESCT and in our approach 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.

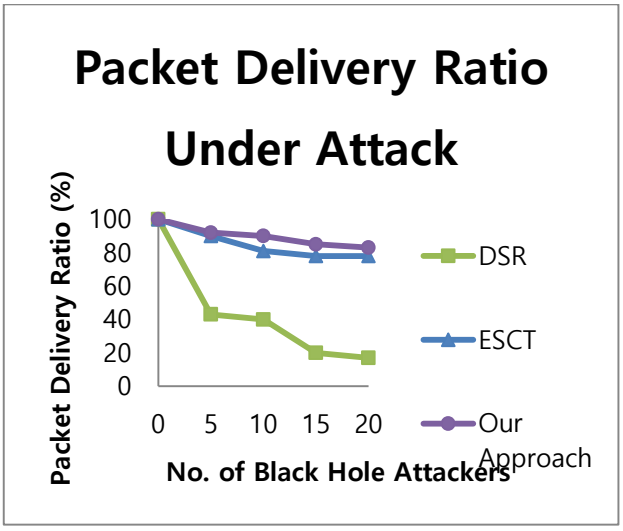

Fig.2 Packet Delivery Ratio in the presence of Black Hole Nodes

5.2 Routing Overhead

Routing overhead is the ratio of total number of generated control packets to the total number of data packets transmitted in the network. Under the attack the routing overhead in our approach is around 20% which is an increase of 5% approximately when compared to DSR as shown in Fig.3. In our approach there was no additional control packets transmitted during rout discovery process. Once the source node evaluate that the route reply packet is coming from black hole node, then it will generate an additional BHN packet and send to the network. Hence there is an slight increase in routing overhead when compared to DSR. However, ESCT achieves high PDR at the expense of increased routing. In ESCT, it requires nodes to periodically broadcast Hello messages to discover their current neighbor nodes and share self-detection results. In addition, it introduces the investigation request/reply control packets for self-detection. These additional control packets lead to increased routing overhead.

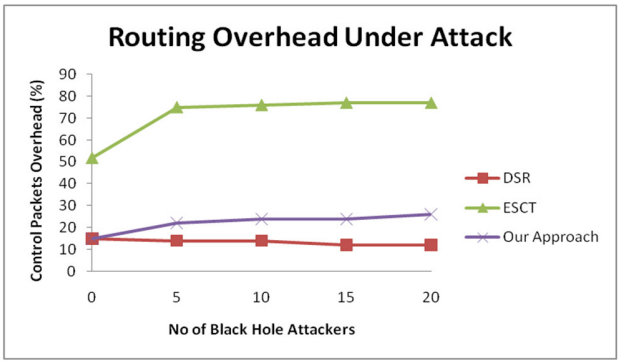

Fig.3 Control Packets Overhead in the presence of Black Hole Nodes

5.3 End-to-End Delay

In ESCT and in our approach the nodes try to avoid routes with black hole nodes even if it leads to use longer paths, instead of using the shortest path. Therefore, when there are more attackers inside the network, the end-to-end delay increases both in our approach and also in ESCT as shown in Fig. 4. But the end-to-end delay in DSR decreases because in the presence of increased number of attackers, most data packets cannot be received by the destinations but being dropped by the black hole nodes. All those lost data packets are not considered for packet delay measurement.

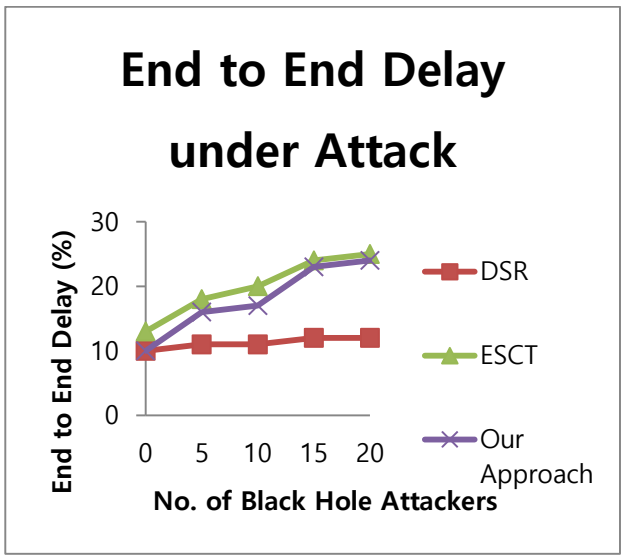

Fig.4 End to End Delay under Black Hole Attack

5.4 Energy Consumption

As compared to ESCT, our approach can greatly reduce the total energy consumed by 62.7 percent in an average. Since our approach does not rely on continuous overhearing or promiscuous monitoring to monitor neighbor nodes, a lot of energy can actually be saved. 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 Fig. 5. However, ESCT periodically broadcast Hello messages, IREQ messages and IREP messages which introduce more energy consumption in each node.

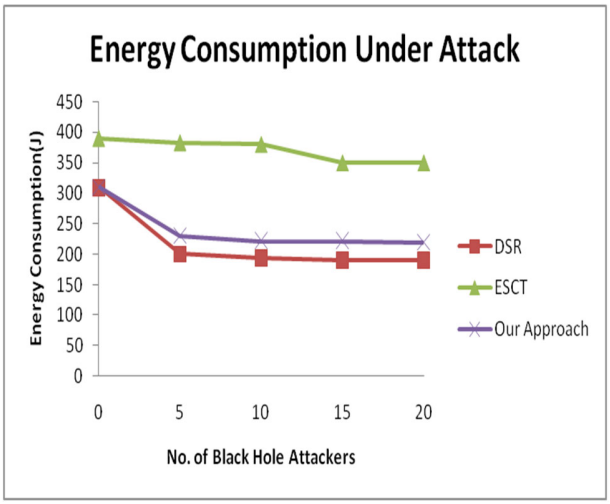

Fig.5 Energy Consumption under Attack

6. Conclusion

We proposed a light weight solution methodology to detect black hole nodes in MANET. It can be incorporated with any existing on demand ad hoc routing protocols. By the proposed algorithm, the source node detects the presence of malicious nodes in the source route and with the help of intermediate nodes the malicious nodes are isolated from the network. Also our approach uses only analysis of REQ and RREP packets to detect the presence of black hole nodes which makes our method suitable for the resource constrained characteristics of MANET. The simulation results show that the percentage of data packet delivery ratio in our proposed work is better than DSR in presence of multiple black hole nodes. Compared to other related works, the proposed protocol has more merits; the most important merit is that it achieves degradation in packet loss rate and higher PDR without any computational complexity or promiscuous listening. Moreover, cooperative black hole attack also cannot be launched, because our technique doesn't employ neighbor node monitoring.

References

[1] Lakhtaria KI, "Technological advancements and applications in mobile ad-hoc networks: research trends", IGI Global, 2012.

[2] A. Mehran, W. Tadeusz, D, "A review of routing protocols for mobile ad hoc networks", Ad Hoc Networks, p.1–22, 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, p.1249–1259, 2012.

[4] Garcia Teodoro P, Sanchez Casado L, Macia Fernandez G, "Taxonomy and holistic detection of security attacks in MANETs", CRC Press, p. 1–12, 2014.

[5] C. Perkins, E. Royer, "Ad hoc on demand distance vector (AODV) routing", Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99), p. 90–100, 1999.

[6] D.B. Johnson, A.D. Maltz, J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks", Ad Hoc Networking, Addison-Wesley, p. 139–172, 2001.

[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, p.17–31, 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", IEEE INFOCOM'10, 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, p. 248–266, 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, p. 59–74, 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, p. 142-155, 2014.

[12] Karlof C, Wagner D, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad hoc Networks, Vol. 1, p. 293–315, 2003 [Special Issue on Sensor Network Applications and Protocols].

[13] H.Deng, P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, Vol.40, p. 70-75, 2002.

[14] B.Awerbuch, D. Holmer, C. Nita Rotaru, H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", ACM Workshop on Wireless Security, p. 21-30, 2002.

[15] Imran Raza, S.A. Hussain, "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes", Computer Communications, p. 1796-1802, 2008.

[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, p. 2781-2798, 2015.

[17] Dorri, Ali, Soroush Vaseghi, and Omid Gharib, "DEBH: detecting and eliminating black holes in mobile ad hoc network", Wireless Networks, Vol. 24, p. 2943-2955, 2018.

[18] Tarun Varshney, Tushar Sharma, Pankaj Sharma, (2014), Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network.

[19] Adwan Yasin, Mahmoud Abu Zant, "Detecting and Isolating Black-Hole Attacks in MANET using Timer Based Baited Technique", Wireless Communications and Mobile Computing, Vol. 1, 2018.

[20] Lyno Henrique G. Ferraz, Pedro B. Velloso, Otto Carlos M.B. Duarte, “An accurate and precise malicious node exclusion mechanism for ad hoc networks”, Adhoc Networks, Vol.19, p.142-155,2014

[21] Ruo Jun Cai, Xue Jun Li , Peter Han Joo Chong, “An Evolutionary Self-Cooperative Trust Scheme

Against Routing Disruptions in MANETs”, IEEE Transactions On Mobile Computing, Vol. 18, P.42-55, 2019

[22] 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, p. 613–625, 2015.

[23] 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, p. 660–670, 2002.