Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs

RUTVIJ H. JHAVERI[1]
SANKITA J. PATEL[2]
DEVESH C. JINWALA[3]

[1]Shri Sád Vidya Mandal Institute of Technology, Bharuch, India
[2, 3]Sardar Vallabhbhai National Institute of Technology, Surat, India
[1]rutusoft@yahoo.com
[2]sjp@coed.svnit.ac.in
[3]dcj@svnit.ac.in

Abstract. Design of basic routing protocols along with inherent characteristics of Mobile Ad-hoc Networks (MANETs) makes them vulnerable to various types of DoS attacks at the network layer. For secure data transmission in wireless shared medium, communication route must be kept free from adversaries. In this paper, we provide a secure route discovery mechanism for MANETs using Ad-hoc On-demand Distance Vector (AODV) routing protocol against two of the most common Denial-of-Service (DoS) attacks, Blackhole attack and Grayhole attack that disrupt route discovery process by sending forged routing information. In our solution, a node detects unusual routing information when it receives route reply from misbehaving neighbor node launching attack and alerts other nodes about the adversary without using additional control packets; routing packets are used not only to pass routing information, but also to propagate information about malicious nodes. The solution isolates multiple malicious nodes during route discovery process and assures selection of short and secure route to destination. Simulation results in ns-2 prove the reliability and efficiency of our protocol.

Keywords: MANETs, Route Discovery, Blackhole/Grayhole Attack, R-AODV.

(Received January 10th, 2012 / Accepted March 4th, 2012)

1 Introduction

MANETs use radio frequencies to transmit and receive data packets in wireless medium. Multi-hop links are used for communication between two mobile nodes [3]. Unlike wired networks, each node acts as a host when it requests or provides information to other nodes and acts as a router to relay routing packets to neighbor nodes in the network to discover and to maintain routes [17]. As MANET lacks base station as well as preset infrastructure nodes assist each other to manage the network. Due to rapid deployment and self-configuration nature, mobile nodes establish ad-hoc network anytime and anywhere; this is the reason why MANETs are vital in applications such as automated battlefields, military, rescue systems, vehicular computing, electronic payments and many other vital applications [14]. Network size, network density and mobility of nodes may vary for different applications. Mobility and limited radio range often cause change in route and topology; therefore, routing is a key challenge. For mobile nodes to connect each other in physically insecure environment, security is an essential aspect. As an adversary can take part in data transmission only after becoming a part of route towards destination, secure route discovery process is imperative. Security issue has been overlooked in the design of most of the default routing protocols.

As discussed in [7], routing protocols are mainly devised into three categories: proactive protocols, reactive protocols and hybrid protocols. In proactive protocols, a route can be selected immediately as they construct route in advance; however, during reconstruction or failure of network they react slowly. Reactive protocols construct route on demand; they are energy efficient and effective in maintaining routes; however, they take high latency time in finding routes. Hybrid protocols combine the benefits of proactive and reactive protocols. AODV protocol has gained popularity over the years in the class of on demand protocols due to its loop-free routing; it requires less number of broadcasts compared to DSDV protocol . However, adversary can carry out many attacks on AODV as designers of AODV have not taken security aspect into account; moreover, many attacks can be carried out just by not following the protocol rules of AODV. MANETs are susceptible to various active and passive attacks on the network layer; one of the classes of active attacks is DoS attacks that badly disrupt fundamental functionalities of an ad-hoc network. Wormhole attack, Sinkhole attack, Blackhole attack and Grayhole attack are major DoS attacks in MANETs [12]. In this paper, we concentrate on Blackhole and Grayhole attacks that degrade performance of network by packet forwarding misbehavior during data transmission phase.

Blackhole attack takes place when an adversary takes part in route discovery process and endorses itself as destination node or an intermediate node to the destination with fresher route [7]; source node unknowingly puts trust in the adversary and as a result, a forged route is created through the adversary and all traffic is routed through it; thus, the adversary intercepts and drops all the received packets. Grayhole attack is another form of Blackhole attack that intercepts and drops packets for specific time duration and behaves as a genuine node for the remaining duration by forwarding packets. Detection of Grayhole attack during data transmission phase is extremely difficult due to this unpredictable behavior. It is important to bring trust among all mobile nodes taking part in data transmission by establishing a secured route and by isolating all the malicious nodes.

In this paper, we present a novel technique that improves route discovery process of AODV by introducing security aspect into the protocol. Our technique sets up a short and secured route with minimal overhead by giving additional responsibilities to each node involved in the route discovery process; an intermediate node receiving route reply from neighbor node starts detection process and marks that node as malicious node if it sent abnormal routing information. The intermediate node propagates the information about the malicious node in the network with default control packets. Moreover, source node initiating route discovery process appends a blacklist of malicious nodes in route request packet to inform other nodes in the network. Thus, route request and route reply packets are also used to isolate malicious nodes.

The rest of this paper is organized as follows. Section 2 describes theoretical background. Related work is described in Section 3. In Section 4, we discuss design of our protocol to prevent Blackhole and Grayhole attacks in MANETs. Evaluation of our mechanism with simulation results is presented in Section 5. Section 6 concludes the paper.

2 Theoretical Background

In this section, we discuss the working of Blackhole and Grayhole attacks along with the outline of AODV routing protocol.

2.1 Blackhole and Grayhole Attacks

Blackhole and Grayhole attacks are widespread DoS attacks on MANETs. In Blackhole attack, an adversary announces a valid shortest path to the destination by transmitting anomalous routing information [2]. Out of replies from different nodes during route discovery, the source node considers path from the malicious node considering it as a genuine node having fresher path to the destination. As a result, a bogus route will be created through that node. The adversary causes denial-of-service by absorbing traffic as it intercepts and drops the data packets forwarded through it [3]. Figure 1 shows the Blackhole behavior of the attacker Y that drops the packets sent by source S towards destination D.

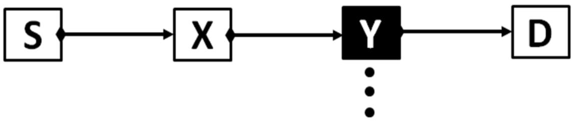


Figure 1: Blackhole behavior

Grayhole attack is an extended version of the Blackhole attack where adversary behaves as a genuine node for certain time and turns into malicious node later on. Figure 2 demonstrates malicious behavior of Grayhole attacker Y. Malicious node Y initially pretends to be a normal node as shown in Figure 2(a); it forwards all packets from source S to destination D and later on, as shown in Figure 2(b), node Y starts malicious activity to drop packets sent by S. After some time, Y starts behaving as a genuine node again. This unpredictable nature of Grayhole node makes it very hard to detect it during data transmission session.

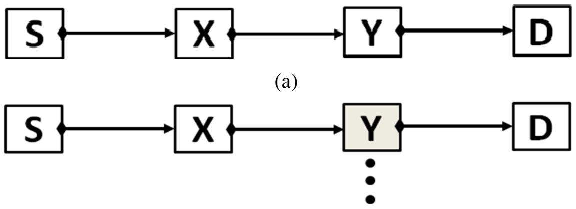


Figure 2: Grayhole Behavior

2.2 Overview of AODV

AODV is a reactive protocol in which route discovery process is started by the source node to set up path to the destination before beginning a communication session [7][12]. It does not get involved in periodic routing table exchanges like proactive protocols; due to on-demand nature, nodes do not have to maintain routes to other nodes until they wish to communicate with other nodes [15]. Each node periodically broadcasts a HELLO message to peer nodes to advertise its existence in the network. Instead of keeping track of nodes on entire route, a node keeps track of only its next hop node. AODV produces loop-free routes because of the concept of sequence numbers borrowed from DSDV [13]. AODV uses three control packets: RREQ (Route Request), RREP (Route Reply) and RERR (Route Error). When source node wants to communicate with destined node that is not its neighbor, it broadcasts an RREQ packet and starts route discovery process. This RREQ continues to be rebroadcasted by the intermediate nodes to their neighbors until it is received by the destination itself or by an intermediate node having fresh enough route to the destination. This node discards the RREQ, generates an RREP and forwards it on the reverse path to the source node. When a node notices a link break or when it receives a data packet that is to be sent to the destination for which it does not have an active route, it generates an RERR packet [7].

Thus, RREQ and RREP are used during route discovery phase, while RERR is used during route maintenance phase [12]. When a node receives a control packet related to a specific node, it compares the sequence number with that of the routing table; if it is greater, routing table gets updated otherwise the control packet is discarded [7]. Working of AODV in normal conditions is demonstrated in Figure 3; source node S broadcasts an RREQ to find route to destination node D. Two intermediate nodes INs send RREPs on the reverse path in response to the RREQ. S considers the fresher and shorter route represented by one of the RREPs to establish route to D; other RREPs are discarded.

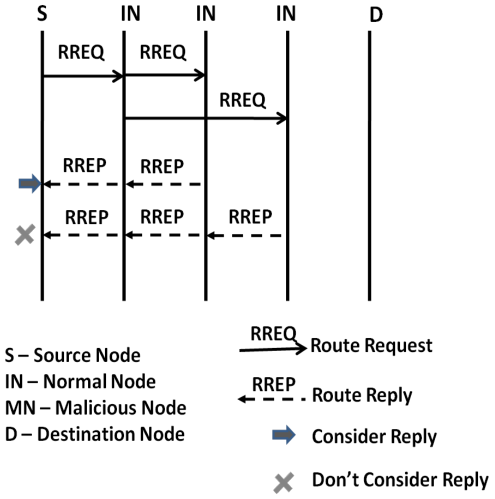


Figure 3: Route discovery in AODV

3 Related Work

Marti et. al [11] proposed a mechanism with Watchdog/Pathrater to detect malicious node. Promiscuous mode is used to listen to the next hop nodeś transmission where a node confirms next hop node has indeed forwarded the packet. If the node finds next hop node not forwarding packet within specific time, it is accused as a malicious node. Using results of Watchdog, Pathrater algorithm rates paths and highest rating path is chosen. The drawbacks of this mechanism are that the watchdog algorithm may accuse good nodes as malicious nodes and it does not consider partial dropping and ambiguous collisions; also, exchanging ratings in Pathrater algorithm lead to blackmail attack. Anti-Blackhole Mechanism discussed by Ming-Yang et. al [16] estimates the difference between number of RREQs and RREPs transmitted from a node; the node forwarding RREP, but not re-broadcasting RREQ for a definite route will have its suspicious value increased in the nearby nodeś suspicious node table. The node broadcasts a BLOCK message when the suspicious value of a node goes beyond threshold and the suspicious node is isolated cooperatively. However, introduction of BLOCK packet raises routing overhead and it also assumes that an authentication mechanism already exists in MANET. DPRAODV protocol suggested by Payal et. al [15] periodically calculates the difference of destination sequence number of RREP and that of routing table entry and compares it with threshold value; for greater difference than threshold the node sending RREP is marked as a malicious node. Node detecting the malicious node broadcasts an ALARM packet to inform neighbor nodes about existence of a malicious node. The protocol, though, adds overhead in generating the ALARM packet and broadcasting it leads to higher routing overhead. Nital et. al [12] provided a modification in AODV called MOSAODV that uses heuristic approach to calculate MOS_WAIT_TIME which is the amount of time source node waits after first RREP received for other RREPs; a table Cmg_RREP_Tab is used to store all RREPs. Out of all RREPs source node discards RREPs with higher sequence number considering those from malicious nodes. Limitation of this solution is that selecting the value of sequence number to detect malicious reply is presumed; also, the solution adds overhead in terms of MOS_WAIT_TIME and Cmg_RREP_Tab. Vishnu et. al [8] discussed a solution that establishes a backbone network containing trusted nodes; source node requests an unused IP address from a trusted node; route discovery process includes the unused IP for the search of the destination node; detection process is initiated by the source node if an RREP is sent by a malicious node for the unused IP. However, the mechanism assumes high battery power and high communication range of backbone nodes; assumption is also made that number of adversaries must be less than genuine nodes at any time which may not be likely in many scenarios.

A one-way hash code is embedded with data packets in the scheme proposed by Mamatha et. al [10] that uses simple acknowledgement and principle of flow conservation. For every correctly received packet verified by the hash code, ACK message is sent and for the incorrect one CONFIDENTIALITY LOST is sent. If total transmission time is more than predefined time, it increments a miss counter and counts the ratio of the total missed packets to the total sent packets. If it is out of tolerable range it detects misbehavior and chooses replacement node for future sessions. However, the scheme adds overhead to the sender due to calculation of total transmission time; also, introduction of ACK/CONFIDENTIALITY LOST control packets leads to increase in routing overhead. Sukla et. al [4] proposed a mechanism using Prelude and Postlude messaging to check the packet loss; a Prelude message is sent to inform the destination about starting data transmission; after completion of data transmission phase, the destination node sends Postlude message to the source node containing the number of packets received. If the difference of sent packets and received packets is out of acceptable range, the source node sends Query message to the neighbors that detect packet forwarding misbehavior and reply to the source; positive reply from neighbor about suspicious node increments a voteCount value of that node in a separate table. If voteCount passes threshold value, that node is isolated by sending a Broadcast message to other nodes. The mechanism has shortcomings of increasing routing overhead due to introduction of new control packets: Prelude, Postlude, Query and Broadcast; also, it adds to overhead in terms of maintaining three new tables as well as computing the difference and the threshold value. A solution proposed by Oscar et. al [6] detects packet forwarding misbehavior in promiscuous mode by principle of flow conservation and accuses nodes that are consistently misbehaving; a node maintains a table to monitor its neighbors for successful/unsuccessful packet transmission through them or packet reception from them by using MREQ, MREP and MACK packets; a misbehavior threshold value is used to distinguish genuine nodes from misbehaving nodes. However, this mechanism increases routing overhead due to introduction of new control packets; also, malicious nodes can drop packets before being isolated as collecting response from neighbors and identifying and accusing misbehaving nodes require some time. Piyush et.al [1] discussed a solution that creates a backbone network of strong nodes for monitoring overall traffic using promiscuous mode and carrying out end-to-end checking with destination for every sent data block using Prelude and Postlude messages. In the case of failure in receiving a data block, the backbone network initiates detection process to remove a chain of malicious nodes. However, the mechanism increases routing overhead as it uses many additional control packets; also, assumption about strong nodes having powerful battery and high radio range is made; also, requirement that a node has more strong nodes as neighbors than malicious nodes may not be always satisfied when nodes frequently change their positions. A scheme proposed by Chen et. al [18] uses Creating Proof Algorithm, Checkup Algorithm and Diagnosis Algorithm; each node has to create an evidence of receiving message with aggregate signature using Creating Proof Algorithm; when unusual packet dropping occurs, Checkup Algorithm uses CREQ and CREP messages to check intermediate nodes; Diagnosis algorithm accuses a suspicious node as malicious node when suspicious value for packet forwarding misbehavior crosses the threshold. The mechanism has shortcomings of higher routing overhead due to addition in control packets and higher computational cost due to the basic limitations of aggregate signatures.

It is imperative to design a protocol that removes limitations of above solutions and finds a secured route to the destination during route discovery phase without introducing new control packets.

4 R-AODV: The Proposed Solution

Figure 4 shows the route discovery process of default AODV in the presence of an attacker. Source node S wishes to send data to destination D broadcasts RREQ; a malicious node MN replies back with RREP containing unusually high destination sequence number misleading S as if it has a fresher route to D; another normal intermediate node IN sends RREP having legitimately higher sequence number. As RREP of the attacker holds higher destination sequence number of all received RREPs, source node unknowingly selects path through MN to transfer data packets and therefore, MN intercepts and drops some or all of the received packets that causes denial-of-service in the network. This issue states the requirement of a variation of AODV protocol that efficiently discovers a secure route to the destination.

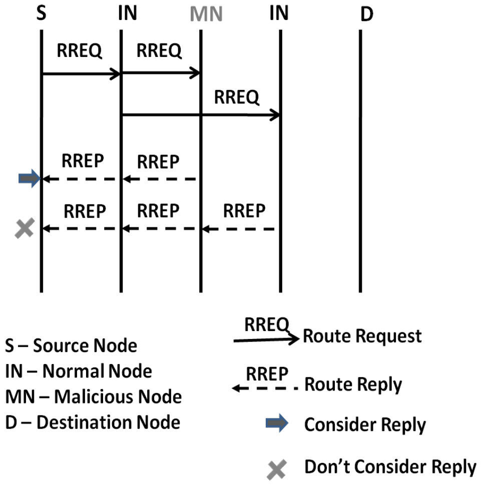


Figure 4: Route discovery in AODV in presence of attacker

Our solution, Reliable-AODV (R-AODV), does not introduce extra control packets to propagate malicious nodeś information to other nodes in MANETs. Also, we do not assume promiscuous mode as it doesnt́ support directional antennas; moreover, promiscuous mode consumes more energy and adds computational overhead to mobile nodes. We modify the structures of RREQ and RREP and add a field in the routing table. In AODV, structure of RREQ packet contains hop count, broadcast ID, destination IP address, destination sequence number, source IP address, source sequence number and timestamp; in R-AODV, a MALICIOUS_NODE_LIST is appended to RREQ packet to notify other nodes about malicious nodes in the MANET. In AODV, structure of RREP packet contains destination IP address, destination sequence number, hop count, source IP address, life time and timestamp; we add a flag called DO_NOT_CONSIDER to RREP to mark/identify reply from a malicious node. In AODV, routing table contains destination IP address, sequence number, hop count, next hop IP address, precursor list, time when entry expires; we add another field to this called MALICIOUS_NODE for marking a node as malicious node. Traffic conditions in a MANET determine the value of a nodeś sequence number [9] and state of a node can be expressed by number of sent out RREQs, number of received RREPs and routing table sequence number; we use these three parameters to calculate a PEAK value; to detect the existence of a malicious node, destination sequence number of the received RREP is compared with this PEAK value. We modify functionalities of nodes sending RREQ, nodes receiving RREQ and nodes receiving RREP and put in more responsibilities as shown in the following algorithm while functionality for nodes sending RREP remains as it is. RREQ and RREP routing packets are used to propagate information about malicious nodes to other nodes in the network.

4.1 Algorithm

Actions by Intermediate Node Receiving RREP

Step-1 If the node sending RREP is already marked as MALICIOUS_NODE in the routing table, mark the RREP as DO_NOT_CONSIDER and forward it on the reverse path. Go to Step 6.

Step-2 If the received RREP is already marked as DO_NOT_CONSIDER, mark the node sending RREP as MALICIOUS_NODE in the routing table and forward it on the reverse path. Go to Step 6.

Step-3 Calculate the PEAK value.

Step-4 If RREP has destination sequence number less than or equal to the PEAK value, consider the node sending RREP as an honest node; update the routing table if it has destination sequence number less than that of RREP and forward RREP on the reverse path. Go to Step 6.

Step-5 If RREP has destination sequence number greater than the PEAK value, mark the node sending RREP as MALICIOUS_NODE in the routing table and mark RREP as DO_NOT_CONSIDER; forward it on the reverse path.

Step-6 Terminate the action.

Actions by Source Node Receiving RREP

Step-1 If the node sending RREP is already marked as MALICIOUS_NODE in the routing table, mark RREP as DO_NOT_CONSIDER. Go to Step 6.

Step-2 If the received RREP is already marked as DO_NOT_CONSIDER, mark the node sending RREP as MALICIOUS_NODE in the routing table. Go to Step 6.

Step-3 Calculate the PEAK value.

Step-4 If RREP has destination sequence number less than or equal to the PEAK value, consider the node sending RREP as an honest node; update the routing table if it has destination sequence number less than that of RREP. Go to Step 6.

Step-5 If RREP has destination sequence number greater than the PEAK value, mark the node sending RREP as MALICIOUS_NODE in the routing table and mark RREP as DO_NOT_CONSIDER.

Step-6 Consider the RREP having fresher shortest path to the destination out of all the received unmarked RREPs.

Step-7 Terminate the action.

Actions by Source Node Sending RREQ

Step-1 If one or more MALICIOUS_NODE entries exist in the routing table, construct and append a MALICIOUS_NODE_LIST to RREQ.

Step-2 Broadcast RREQ.

Step-3 Terminate the action.

Actions by Intermediate Node Receiving RREQ

Step-1 If the received RREQ has non-empty MALICIOUS_NODE_LIST, mark the specified nodes as MALICIOUS_NODEs in the routing table.

Step-2 If the destination sequence number in the routing table is greater than or equal to that of RREQ, discard RREQ and send RREP to the source node on the reverse path. Go to Step 4.

Step-3 Update the routing table if its destination sequence number is less than that of RREQ; rebroadcast RREQ.

Step-4 Terminate the action.

Actions by Destination Node Receiving RREQ

Step-1 If the received RREQ has non-empty MALICIOUS_NODE_LIST, mark the specified nodes as MALICIOUS_NODEs in the routing table.

Step-2 Update the routing table by incrementing the destination sequence number in RREQ; discard RREQ and send RREP with the updated sequence number to the source node on the reverse path.

Step-3 Terminate the action.

Figure 5 shows the route discovery process of R-AODV in the presence of an attacker. During route discovery phase, S appends a MALICIOUS_NODE_LIST to RREQ if it has one or more MALICIOUS_NODE entries in the routing table. Every intermediate node IN receiving the RREQ updates its routing table with MALICIOUS_NODE entries. An IN receiving RREP from malicious node MN with sequence number higher than the calculated PEAK value marks that RREP as DO_NOT_CONSIDER and the node sending RREP as MALICIOUS_NODE node in the routing table; RREP updates routing tables of INs and S with MALICIOUS_NODE entry of MN on the reverse path to S. When S broadcasts RREQ in future, it appends a MALICIOUS_NODE_LIST in RREQ to inform other nodes about the existence of MN along with other recorded malicious nodes. As a result, replies from MN and other malicious nodes remain unconsidered and they remain isolated from genuine nodes.

5 Evaluation of R-AODV

This section shows the performance evaluation of our solution R-AODV under different metrics with various network parameters with simulation environment described as follows.

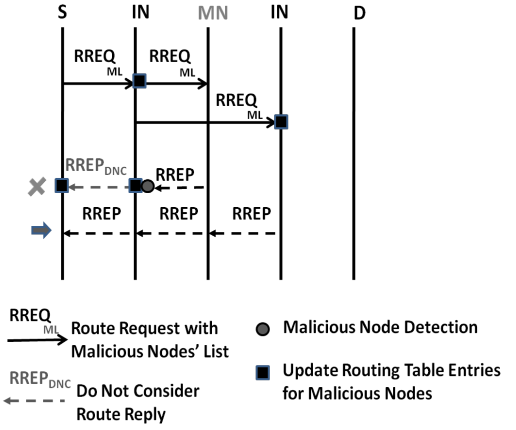

S
IN
MN
IN
D
RREQ ML
RREQ ML
RREQ ML
RREP DNC
RREP
RREP
RREP
RREP
RREQ ML Route Request with Malicious Nodes' List
RREP DNC Do Not Consider Route Reply
● Malicious Node Detection
■ Update Routing Table Entries for Malicious Nodes

Figure 5: Route discovery in R-AODV in presence of attacker

5.1 Simulation Environment

Our simulations are performed using ns-2 network simulator (Ver.-2.34) [5] which is one of the most popular network simulation tools that provides implementations of a variety of routing protocols. We use random waypoint model for generating various network scenarios; cbrgen and setdest utilities are used to generate connection patterns and mobility models respectively. Two new routing agents are included in ns-2 containing Blackhole and Grayhole attacks. In order to implement Blackhole/Grayhole attack, malicious node puts higher sequence number in RREP than in received RREQ; in order to implement Grayhole behavior, initially the malicious node forwards data packets, later on starts dropping data packets for a certain time period and then forwards data packets again to the destination. We randomly move 10 to 50 nodes in the area of 800m x 800m for the simulation time of 50 seconds. Transmission range of each node is 250m. We use UDP at the transport layer. We vary following network parameters in our simulations:

- Network Size: Number of mobile nodes
- Mobility: Maximum speed of mobile nodes
- Pause Time: Time period to target another random destination
- Traffic Load: Number of sources
- Number of Attackers: Number of Grayhole/Blackhole nodes

Table 1 shows the input parameters to generate scenarios.

Table 1: Simulation parameters

Parameter	Value
Simulator	NS-2 (ver.-2.34)
Terrain Area	800m x 800m
Simulation Time	50 sec
MAC	802.11
Traffic Type	CBR (UDP)
Maximum Bandwidth	2 Mbps
Routing Protocols	AODV and R-AODV
Transmission Range	250 m
Data Payload	512 Bytes/Packet
Pause Time	1 to 5 sec
Maximum Speed	10 to 50 m/sec
Number of Nodes	10 to 50
Number of Sources	1 to 5
Number of Malicious Nodes	1 to 5

5.2 Performance Metrics

To evaluate the performance of our solution, we use the following metrics:

Packet Delivery Ratio (PDR): The ratio of the number of data packets received by the application layer of destination nodes to the number of data packets transmitted by the application layer of source nodes.

Average End-to-End Delay: Average time taken by the transmitted data packets to reach to the corresponding destinations.

Normalized Routing Overhead: The ratio of the number of routing control packets to the number of data packets.

5.3 Simulation Results and Analysis

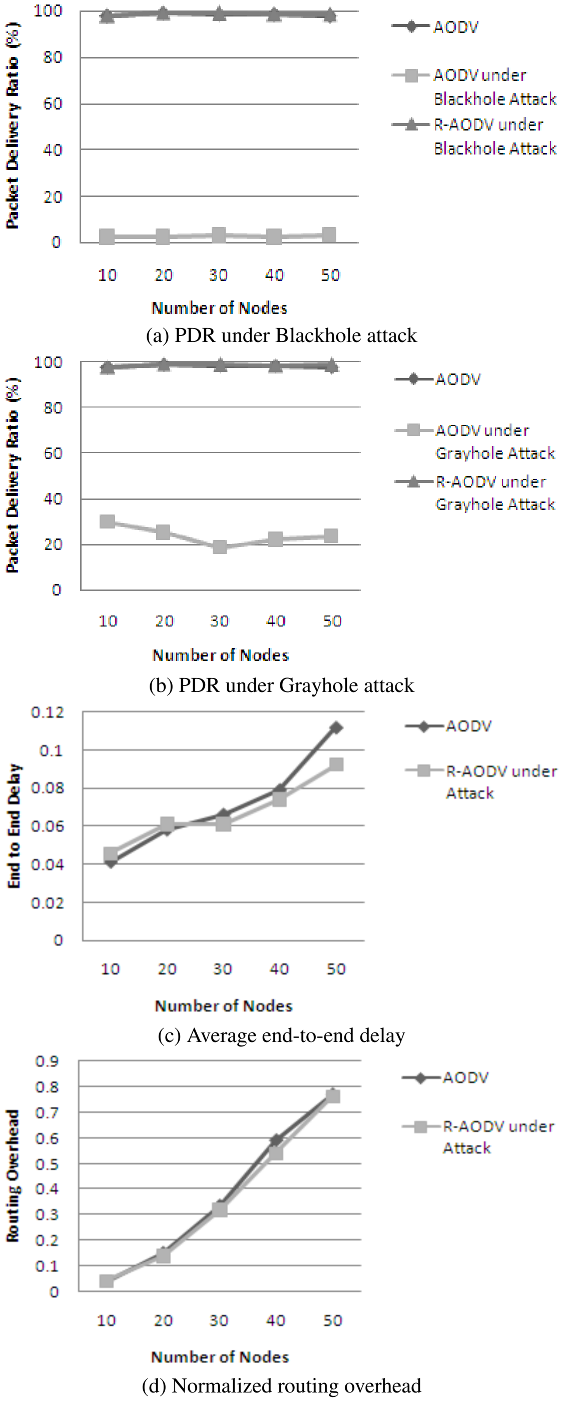
We evaluate the performance of our protocol R-AODV under Blackhole and Grayhole attacks and compare it with AODV by varying different network parameters. As R-AODV isolates both Blackhole and Grayhole nodes, PDR, average end-to-end delay and normalized routing overhead of R-AODV under both attacks remain same. As AODV under attack gives less end-to-end delay and very high routing overhead, we compare only default AODV and R-AODV for both the metrics.

Figure 6 shows the performance comparison of AODV and R-AODV under attack by varying network size between 10 to 50 and keeping pause time as 2.0 sec and maximum speed as 50 m/sec. As Blackhole node intercepts and drops all packets, PDR of AODV drops significantly which is below 4% as shown in Figure 6(a); PDR of AODV under Grayhole attack varies between 18% to 30% as the malicious node does not drop all packets as shown in Figure 6(b); under both attacks, R-AODV isolates misbehaving nodes and gives nearly

97% to 100% PDR which is nearly same as default AODV. For AODV, as the number of mobile nodes increases, average delay increases and normalized routing overhead also increases as more routing control packets are required to establish path. In comparison with AODV, delay for R-AODV starts staying below that of AODV with increase in network size; as shown in Figure 6(c) average end-to-end delay for AODV varies between 0.041 sec to 0.112 sec while that for R-AODV varies between 0.046 sec to 0.092 sec; with varying network size, normalized routing overhead of R-AODV stays between 0.042 to 0.762 which is equivalent or less than that of AODV as shown in Figure 6(d).

Figure 7 shows the effect of mobility on the performance of AODV and R-AODV under attack for a MANET containing 30 nodes with pause time of 2.0 sec with maximum speed of nodes varying from 10 m/sec to 50 m/sec. Even though under both attacks, AODV gives significantly less PDR, R-AODV performs its basic functionality to deliver data packets to the destination and gives equivalent PDR as normal AODV which is between 98% to 100% as shown in Figure 7(a) and Figure 7(b). Average end-to-end delay for R-AODV stays within acceptable range of 0.057 sec to 0.073 sec compared to range of 0.063 sec to 0.071 sec for AODV as shown in Figure 7(c). Due to increase in mobility more link breakages occur and route discovery process occurs frequently which induces higher routing overhead for AODV. Figure 7(d) shows that R-AODV under attack gives normalized routing overhead between 0.109 to 0.319 compared to 0.099 to 0.336 for AODV with the increase in mobility.

A mobile node changes its location after the specified pause time. Figure 8 depicts the performance comparison of AODV and R-AODV under attack by varying pause time between 1.0 sec to 5.0 sec for a MANET of 30 nodes by keeping maximum speed of nodes as 50 m/sec. R-AODV securely transmits data packets and gives tremendous improvement by giving PDR nearly 99% under both attacks which is equivalent to AODV as shown in Figure 8(a) and Figure 8(b). Graph of average end-to-end delay for R-AODV swirls around that of normal AODV ranging between 0.060 sec to 0.073 sec as shown in Figure 8(c). R-AODV shows remarkable improvement in normalized routing overhead and its graph always stays below to the graph of default AODV; normalized routing overhead for R-AODV varies in the range of 0.272 and 0.337 compared to the range of 0.304 to 0.345 for AODV as shown in Figure 8(d).



(a) PDR under Blackhole attack

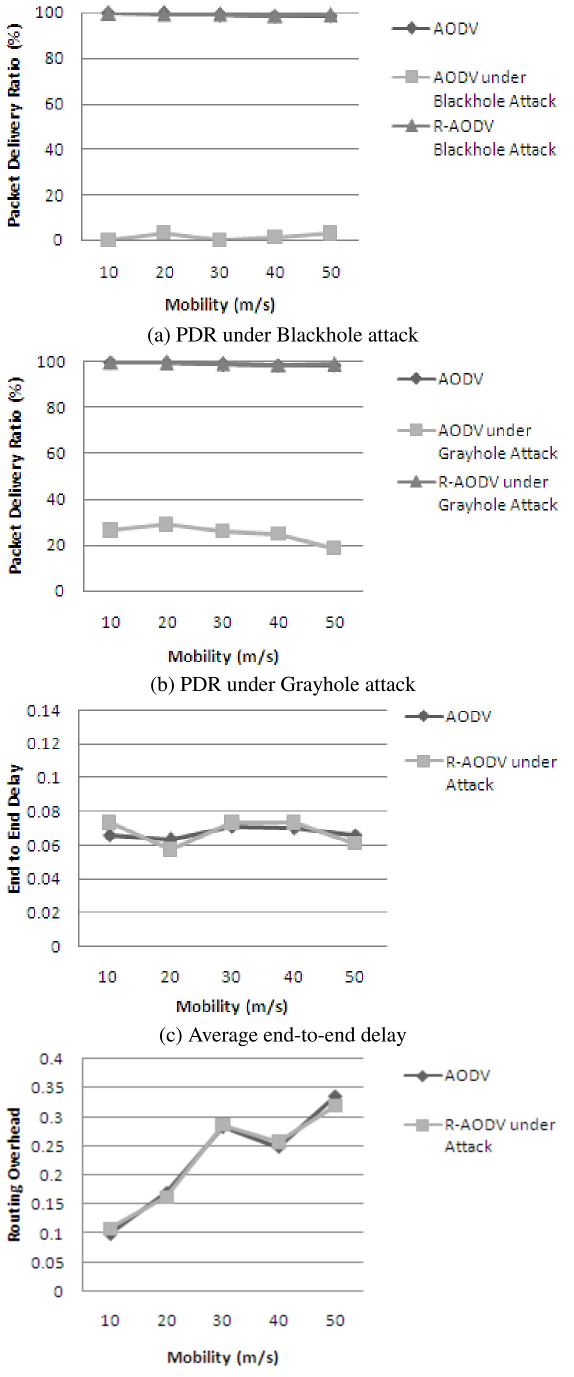
(b) PDR under Grayhole attack

(c) Average end-to-end delay

(d) Normalized routing overhead

Figure 6: Effect of network size

It is imperative that a routing protocol doesnt́ break out and performs equally well as traffic load increases. Figure 9 depicts the effect of traffic load on AODV and R-AODV under attack with network size of 20, maximum speed of 50 m/sec and pause time of 2.0 sec by varying number of sources from 1 to 5. As the num-



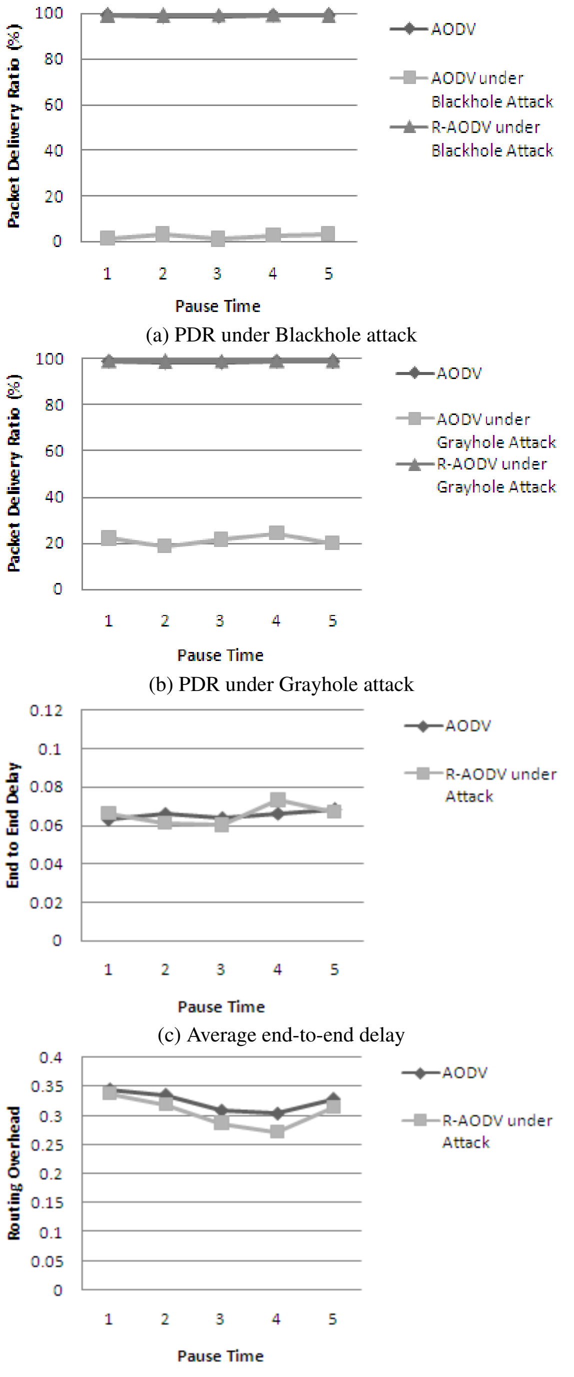
(a) PDR under Blackhole attack

(b) PDR under Grayhole attack

(c) Average end-to-end delay

(d) Normalized routing overhead

Figure 7: Effect of mobility



(a) PDR under Blackhole attack

(b) PDR under Grayhole attack

(c) Average end-to-end delay

(d) Normalized routing overhead

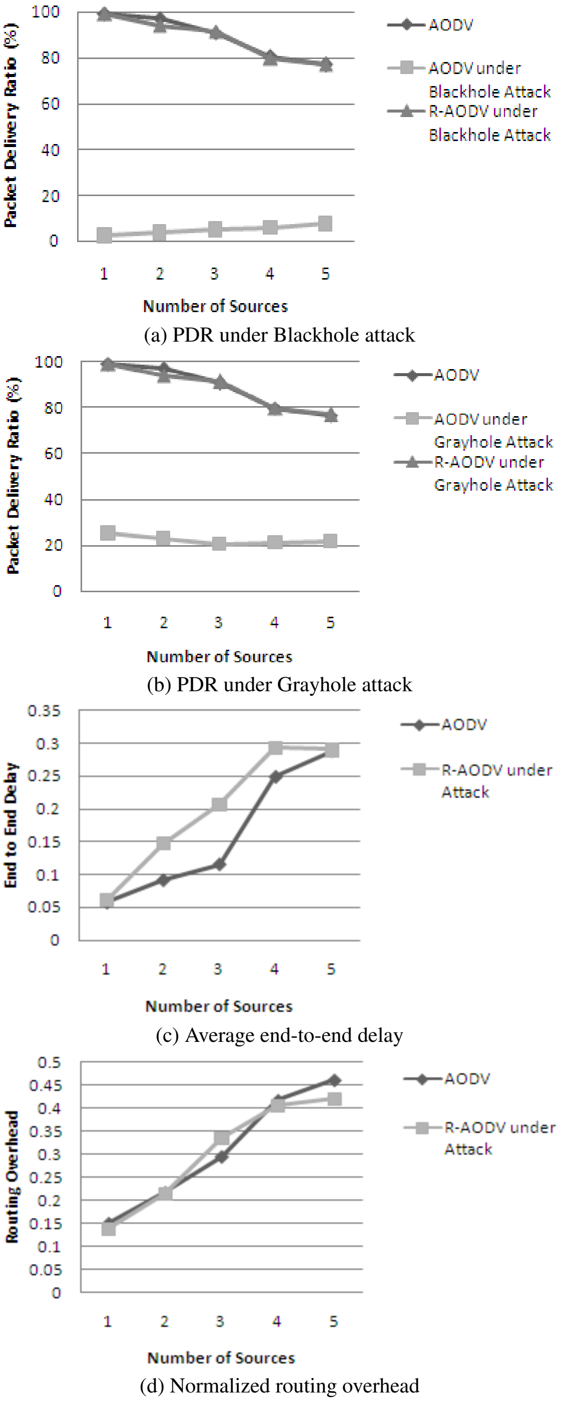
Figure 8: Effect of pause time

ber of sources increases PDR of normal AODV decreases from nearly 99% to around 77% due to increase in packet loss because of congestion. PDR of AODV under Blackhole attack moves between nearly 2% and 8% while under Grayhole attack it moves between 20% and 25%. Even when traffic load increases, R-AODV proves its reliability by giving noticably high PDR under attacks which is nearly equivalent to that of AODV as shown in Figure 9(a) and Figure 9(b). For normal AODV, as traffic load increases average end-to-end delay and normalized routing overhead increase due to relative increase in number of control packets and decrease in number of data packets; R-AODV under attack gives higher average end-to-end delay varying between 0.061 sec to 0.293 sec compared to the range of 0.058 sec to 0.288 sec for AODV as shown in Figure 9(c); the graph of normalized routing overhead for R-AODV moves between noticable range of 0.139 to 0.421 as compared to the range of 0.151 to 0.462 for AODV as shown in Figure 9(d).

Many solutions exist that may not perform well when multiple malicious nodes are present or when a node has more number of malicious nodes as neighbors than number of genuine nodes. On the other hand, R-AODV performs equally well even if number of malicious nodes is more than legitimate nodes in MANET. Moreover, R-AODV proves its reliability when any node in the network has more malicious nodes as neighbors than genuine nodes; the node detects all its neighbor nodes behaving maliciously and propagates their information to other genuine nodes. The performance of R-AODV under multiple malicious nodes with network size of 20 nodes, mobility of 50 m/sec and pause time of 2.0 sec is evaluated in Figure 10. PDR of AODV under Blackhole attack drops from nearly 2% to 0% as the number of malicious nodes increases from 1 to 5 as shown in Figure 10(a). Under Grayhole attack PDR decreases from neraly 25% to around 13% with increase in number of malicious nodes as shown in Figure 10(b). On the other hand, R-AODV isolates multiple malicious nodes and gives more than 95% PDR for all five cases.

6 Conclusion

Cooperative trusted environment among mobile nodes in MANET is absolutely vital. In this paper, we provided improvement in route discovery process of AODV protocol to isolate multiple Blackhole and Grayhole nodes. AODV fails to remove malicious nodes during route discovery process and therefore doesnt́ succeed to transfer all data packets to the destination under attack. On the other hand, R-AODV provides a simple and efficient way to detect and isolate multiple malicious nodes without introduction of any new control packet; default routing packets propagate information of adversaries to other nodes in the network. The mechanism provides high packet delivery rate with noticeable normalized routing overhead and acceptable average end-to-end delay under attack. The mechanism can be adopted by other reactive protocols.



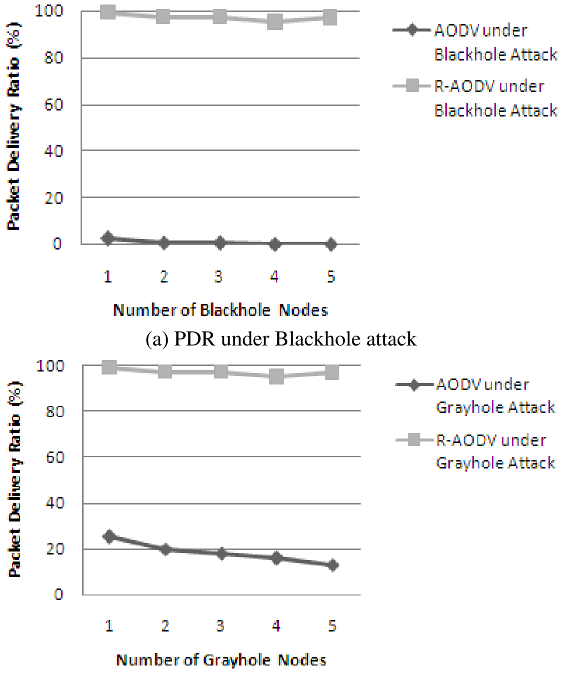
(a) PDR under Blackhole attack

(b) PDR under Grayhole attack

(c) Average end-to-end delay

(d) Normalized routing overhead

Figure 9: Effect of traffic load



(a) PDR under Blackhole attack

(b) PDR under Grayhole attack

Figure 10: Effect of number of malicious nodes

References

[1] Agrawal, P., Ghosh, R. K., and Das, S. K. Cooperative black and gray hole attacks in mobile ad hoc networks. In *Proceeding of 2nd International Conference on Ubiquitous Information Management and Communication*, pages 310–314, 2008.

[2] Al-Shurman, M., Yoo, S.-M., and Park, S. Black hole attack in mobile ad hoc networks. In *Proceeding of ACMSE 2004*, pages 96–97, April 2004.

[3] Bala, A., Bansal, M., and Singh, J. Performance analysis of manet under blackhole attack. In *Proceeding of 1st International Conference on Networks & Communications*, pages 141–145, December 2009.

[4] Banerjee, S. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In *Proceeding of World Congress on Engineering and Computer Science*, pages 337–342, October 2008.

[5] Fall, K. and Varadhan, K. The ns manual. *http://www.isi.edu/nsnam/ns/doc/*, 2010.

[6] Gonzalez, O. F., Ansa, G., Howarth, M., and Pavlou, G. Detection and accusation of packet forwarding misbehavior in mobile ad-hoc networks. *Journal of Internet Engineering*, 2(1):181–192, June 2008.

[7] Jhaveri, R. H., Patel, A. D., Parmar, J. D., , and Shah, B. I. Manet routing protocols and wormhole attack against aodv. *International Journal of Computer Science and Network Security*, 10(4):12–18, 2010.

[8] K, V. and Paul, A. J. Detection and removal of cooperative black/gray hole attack in mobile adhoc networks. *International Journal of Computer Applications*, 1(22):38–42, 2010.

[9] Kurosawa, S., Nakayama, H., Kat, N., Jamalipour, A., and Nemoto, Y. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. *International Journal of Network Security*, 5(3):338–346, November 2007.

[10] Mamatha, G. and Sharma, S. A robust approach to detect and prevent network layer attacks in manets. *International Journal of Computer Science and Security*, 4(3):275–284, August 2010.

[11] Marti, S., Giuli, T. J., Lai, K., and Baker, M. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceeding of 6th Annual International Conference on Mobile Computing and Networking*, pages 255–265, 2000.

[12] Mistry, N., Jinwala, D. C., and Zaveri, M. Improving aodv protocol against blackhole attacks. In *Proceeding of International Multiconference of Engineers and Computer Scientists*, volume 2, pages 1034–1039, March 2010.

[13] Perkins, C. and Bhagwat, P. Routing over multihop wireless network for mobile computers. In *Proceeding of SIGCOMM 1994*, pages 234–244, October 1994.

[14] Qasim, N., Said, F., and Aghvami, H. *Performance Evaluation of Mobile Ad Hoc Networking Protocols*, volume 39 of *Lecture Notes in Electrical Engineering*. Springer, 2009.

[15] Raj, P. N. and Swadas, P. B. Dpraodv: A dynamic learning system against black hole attack in aodv based manet. *International Journal of Computer Science Issues*, 2(3):54–59, 2010.

[16] Su, M.-Y. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, 34(1):107–117, January 2011.

[17] Tamilselvan, L. and Sankaranarayanan, V. Prevention of blackhole attack in manet. In *Proceeding of 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, pages 21–26, August 2007.

[18] Wei, C., Xiang, L., Yuebin, B., and Xiaopeng, G. A new solution for resisting gray hole attack in mobile ad-hoc networks. In *Proceeding of 2nd International Conference on Communications and Networking in China*, pages 366–370, August 2007.