MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs

Rutvij H. Jhaveri
Department of Computer Engineering
SVM Institute of Technology
Bharuch, India
rutusoft@yahoo.com

***Abstract*—Role of ad-hoc networks has become vital in ubiquitous computing. Ad-hoc On-demand Distance Vector (AODV) is such a routing protocol which is susceptible to a variety of security threats against ad-hoc networks. Blackhole and Grayhole attacks are such attacks that drop significant number of packets by performing packet forwarding misbehavior and breach the security to cause denial of service in Mobile Ad-hoc Networks (MANETs). In this paper, we discuss our previous work, R-AODV, to detect and isolate multiple Blackhole and Grayhole nodes during route discovery process and propose a modified version to improve the performance of MANET. We analyze the proposed solution and evaluate its performance using Network Simulator-2 (NS-2) under different network parameters.**

Keywords-MANET; Secure Routing; Blackhole Attack; Grayhole Attack; R-AODV; MR-AODV.

I. INTRODUCTION

Ad-hoc networks have become increasingly popular in recent years as they are rapidly deployable and provide connectivity irrespective of user's geographical position. They are adaptive wireless networks that do not have any fixed infrastructure [1]. Due to these characteristics they are used in many critical applications such as disaster relief, situational information in battlefield, vehicular computing, mobile offices and many more [2]. A MANET is an autonomous network with unclear boundaries which consists of self-configurable mobile nodes that connect with each other via wireless shared radio medium [3]. Nodes have limited resources and move arbitrarily with different speeds resulting in frequent topology changes [4]. Due to restricted communication range, nodes communicate via multi-hop wireless links and therefore, each node relays packets to peer node and performs two roles of host and router [5]. To communicate with other mobile node in the network, a node participates in ad-hoc routing and establishes a route using special routing protocols [6]. Security aspect has been overlooked during design of default routing protocols by assuming cooperative and trusted setting [7].

Fig. 2 and Fig. 3 Based on "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", by Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala which appeared in proceeding of 2012 Second International Conference on Advanced Computing & Communication Technologies published by CPS. © 2012 IEEE

AODV is one of such reactive routing protocols with weaker design, which is prone to numerous security threats including Denial-of-Service (DoS) attacks such as Blackhole and Grayhole attacks. Therefore, further research work focusing on introducing security into AODV protocol has been carried out by various researchers; though, most of them have different limitations as investigated and discussed in our publications viz. [2][4][6][7].

To eliminate drawbacks of existing approaches to thwart Blackhole and Grayhole attacks, we proposed a modification in AODV protocol viz. Reliable-AODV (R-AODV) that significantly improves performance of MANET as described in [2][6][7]. R-AODV greatly increases reliability of detection and isolation of multiple malicious nodes during route discovery process and discovers a short and secure route towards destination without introducing additional control packets [7]. In this paper, we investigate more existing mechanisms and propose a slight modification to R-AODV that attempt to reduce further rise in normalized routing overhead. We analyze the algorithm theoretically and evaluate it practically using NS-2.

Rest of the paper is organized as follows. Section II presents the related work. Section III describes our previous research work. Section IV discusses design and analysis of our algorithm to thwart Blackhole and Grayhole attacks. Simulation results and analysis is presented in Section V. Finally, conclusions are drawn in Section VI.

II. RELATED WORK

Ira *et al.* [8] proposed a cluster-based scheme BHAPSC to prevent Blackhole attack in MANET which detects existence of malicious nodes and discovers their exact position at specific time; it maintains a *Friendship Table* for checking relationship of cluster head with its neighbor node. If next hop node is not a friend then a *False* packet is sent to the stranger. A trust estimator is invoked to calculate a trust value and accordingly, the *Friendship Table* is updated. If trust value is out of tolerable range, stranger is broadcasted as a Blackhole. The scheme has limitations of increase in routing overhead due to generation of *False* packets; furthermore, maintenance of *Friendship Table* adds significant overhead. Moumita *et al.* [9] propose a two-step cooperative mechanism to detect multiple malicious nodes; it requires each node to keep track of its neighbor by maintain two tables namely *sequence table (SnT)*and *status table (ST)*;

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.63

moreover, each node also maintains a *neighbor list (N_List)*; using the information, an intermediate node can detect suspicious node; in the second step source node broadcasts and notifies all the neighbors of the suspicious node to cooperatively participate in the decision process; source node uses a *Voter Table* for gathering votes of neighbors for the suspicious node; during voting process, *Test Packet* and *Acknowledgement Packet* are used to update the *Voter Table*. A *Warning* message is sent to notify other nodes in the network and update their *Status Tables*. The mechanism, though, has drawback of adding significant overhead on each node for maintain numerous tables; furthermore, additional packets such as *Test Packet*, *Acknowledgement Packet* and *Warning* message adds to routing overhead. A Watchdog mechanism proposed by Surana *et al.* [10] uses promiscuous mode to detect a malicious node during route determination phase and provides an alternate route; it maintains two extra tables *pending packet table* and *node rating table*. If packet is not forwarded by adjacent node, the *node rating table* is updated accordingly. If total number of packets dropped exceeds *threshold1*and ratio of the number of dropped packets to the number of forwarded packets exceeds *threshold2* then promiscuous mode tells other nodes about the malicious nodes. However, as the approach uses promiscuous mode, it consumes more energy, adds computational overhead to nodes and does not support directional antennas; adding to this, it adds overhead in terms of maintenance of two extra tables. Shalini *et al.* [11] present an advanced algorithm to detect and prevent cooperative Blackhole and Grayhole attacks using end-to-end checking with prelude and postlude messaging; source node divides data packets small equal parts; message flow is monitored independently by neighbor nodes of source and destination nodes; source node checks whether the data loss during transmission is out of tolerable range; if it exceeds the threshold then a backbone network of trusted nodes collects the outcome of monitoring nodes and malicious nodes are detected and removed; the algorithm has time complexity of O(n) to find a chain of malicious node. Although, the algorithm has limitation of increase in routing overhead due to introduction of prelude and postlude messages; moreover, each node looses a lot of energy for monitoring and there may be a significant data loss before a malicious node is detected.

III. PREVIOUS WORK

As a process of discovering an efficient solution to counter Blackhole and Grayhole attacks in MANEEs, we started with literature survey as presented in [4] which describes theoretical background of routing protocols, security threats at various layers of protocol stack, types of DoS attacks, overview of Blackhole and Grayhole attacks and investigation of present solutions to thwart these attacks. We proposed an approach to prevent both attacks as described in [2]; the article proposed a modification to AODV protocol to introduce security aspect into it. In [6], we presented a slight modification to the previously proposed algorithm to make a reliable protocol viz. R-AODV and monitored its performance in ideal scenarios with zero packet loss and attempted to eliminate drawbacks in the existing solutions. A detailed description of Blackhole and Grayhole behavior, further investigation of existing approaches and performance comparison of standard AODV and R-AODV under attack, in practical scenarios with various network parameters is presented in [7]. We provide a brief overview of R-AODV in the following subsection.

A. R-AODV

As described in [6] and [7], R-AODV improves route discovery process of AODV by bringing in security into AODV protocol and prevents Blackhole and Grayhole nodes from taking part in data transmission phase. It uses number of sent out RREQs, number of received RREPs and routing table sequence number to dynamically calculate a PEAK value after every received RREPs; the PEAK value is calculated by adding these three parameters to the previous PEAK value. Destination sequence number of received RREP is compared with this PEAK value to detect existence of a malicious node. R-AODV uses default routing packets viz. RREQ and RREP to notify other nodes in the network about existence of malicious nodes rather than using additional control packets that attempts to reduce rise in routing overhead. We modify the functionalities of node sending RREQ, node receiving RREQ and node receiving RREP. Source node sending RREQ propagates information about adversaries to other nodes in the network; nodes receiving RREQ isolate the malicious nodes; nodes receiving RREP detect the existence of malicious nodes. Thus, R-AODV detects and isolates multiple malicious nodes during route determination phase which helps setting up a short and secure route towards destination.

IV. PROPOSED APPROACH: MODIFIED R-AODV

As an attempt to further improve performance of MANET, we further modify the functionality of node receiving RREP in R-AODV. Fig. 1 [7] compares the route discovery processes of R-AODV and Modified R-AODV (MR-AODV) in presence of a malicious node. As shown in Fig. 1(a) [7], when a malicious node is detected by an intermediate node after receiving RREP, R-AODV marks the RREP as DO_NOT_CONSIDER and marks the node sending RREP as MALICIOUS_NODE in the routing table; the RREP is then forwarded on the reverse path to the source which updates routing tables of all the nodes on the reverse path with malicious node entry; a route towards destination is chosen by selecting unmarked RREPs.

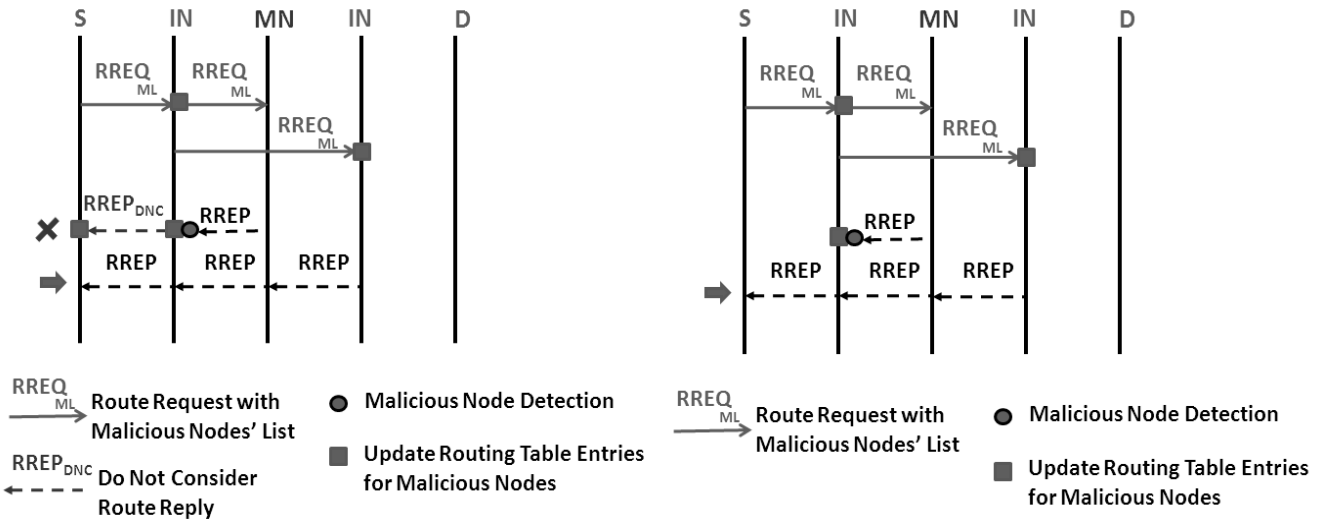


Fig. 1 Comparison of route discovery processes of R-AODV and MR-AODV under attack [7]

On the other hand, in MR-AODV, when a node detects a malicious node, it updates the routing table with malicious node entry and discards the RREP as shown in Fig. 1(b); it is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag; thus, all RREPs reaching to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node. Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior. In the following subsection we represent design of MR-AODV in form of flow-charts based on the designs discussed in [2], [6] and [7].

A. Design of Algorithm

We present the functionalities of node sending RREQ, node receiving RREQ and node receiving RREP in form of flow-charts as follows:

1) Node broadcasting RREQ: Fig. 2 [2] shows the functionaliy of node broadcasting RREQ.

2) Node receiving RREQ: Fig. 3 [2] represents the functionality of node receiving the broadcasted RREQ.

3) Node receiving RREP: Fig. 4 [2][6][7]depicts the functionality of node receiving RREP.

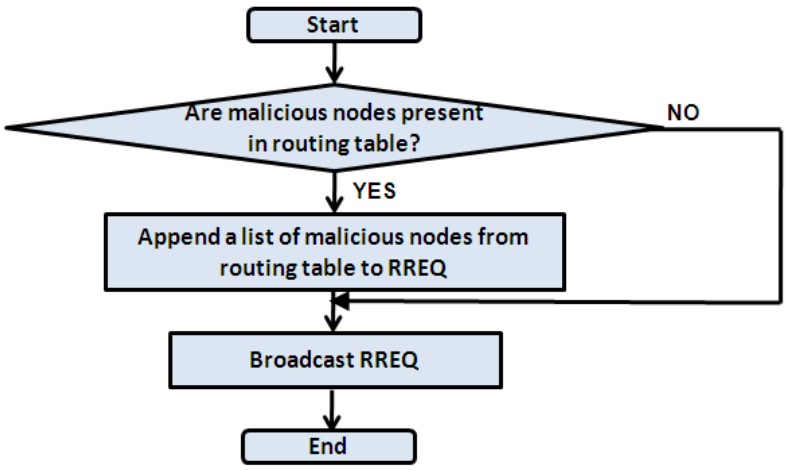


Fig. 2 Flow-chart for node broadcasting RREQ [2]

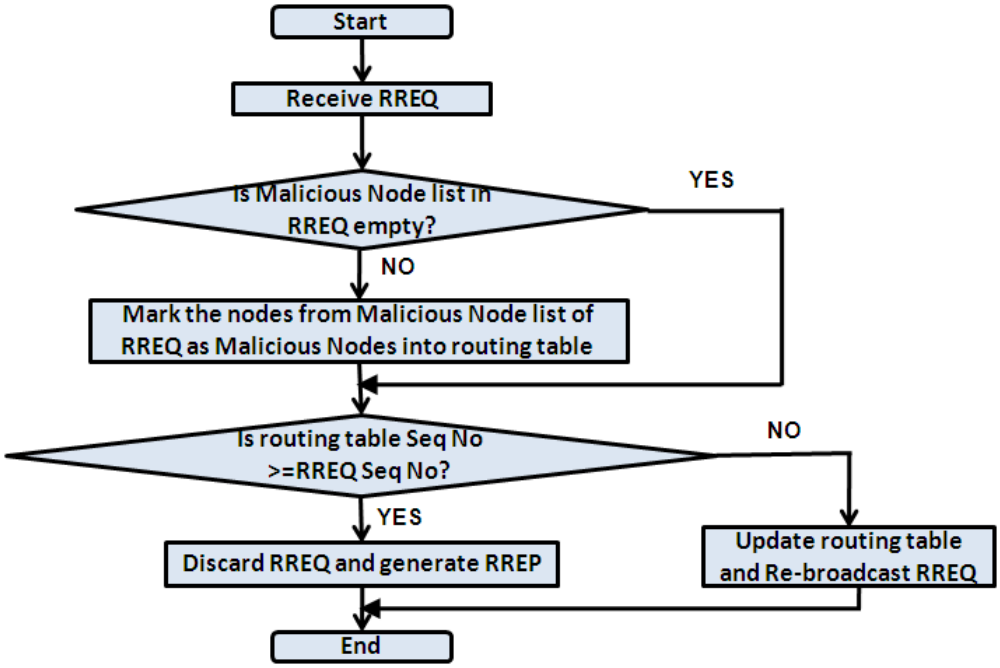


Fig. 3 Flow-chart for node receiving RREQ [2]

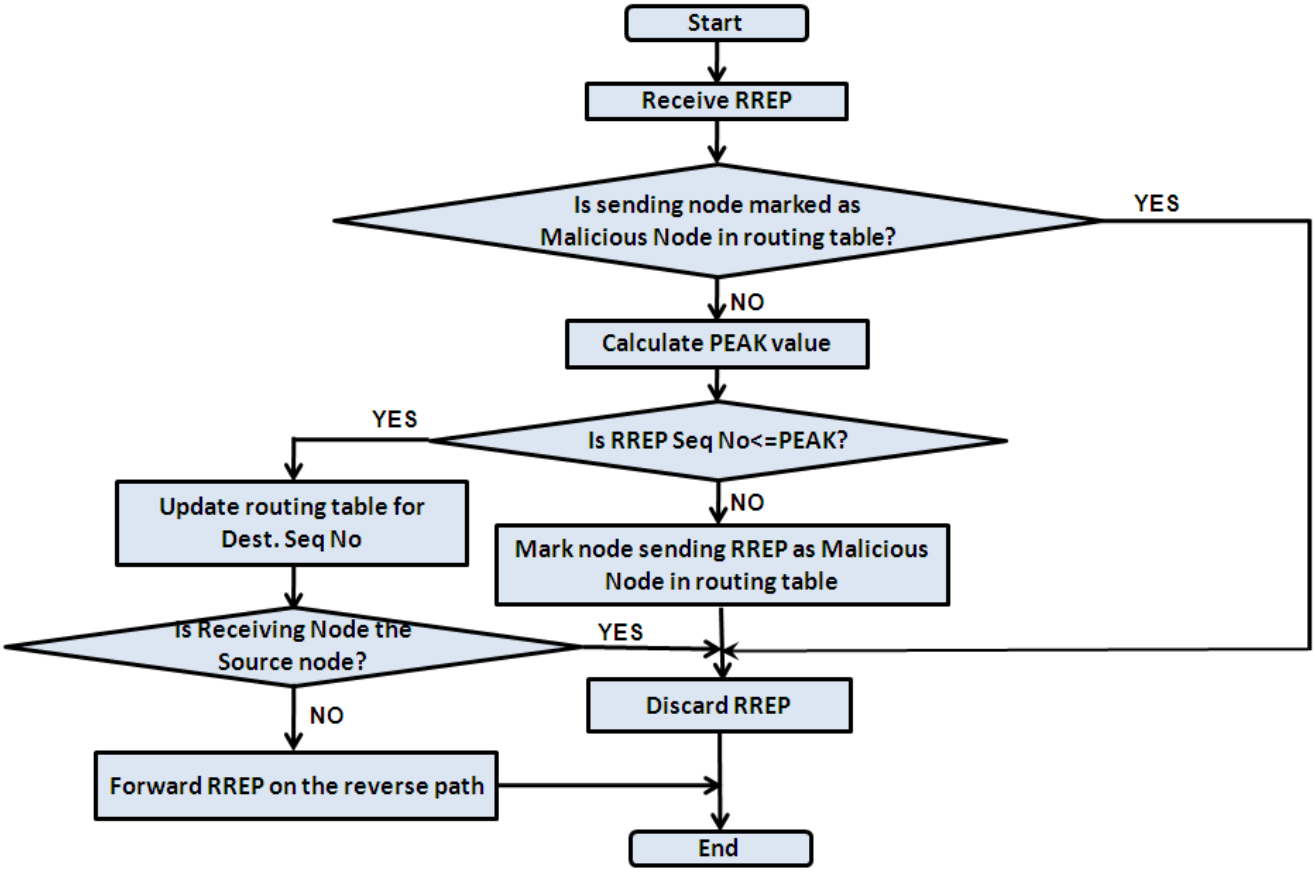


Fig. 4 Flow-chart for node receiving RREP [2][6][7]

B. Algorithm Analysis

MR-AODV has following similarities with R-AODV:

- It adds computing overhead in the form computation of PEAK value.
- 4 Bytes of PEAK value are allocated in memory.
- Two variables used for calculation of PEAK value viz. NO_OF_SENT_RREQ and NO_OF_RECEIVED_RREP allocate 2 Bytes each.
- MALICIOUS_NODE_LIST in RREQ contains 2 Bytes for each entry of blacklisted node. The overhead in time is in terms of generation of MALICIOUS_NODE_LIST.
- Routing table is modified by addition of a MALICIOUS_NODE field which requires 2 Bytes for each node entry.
- It does not require any extra table to maintain.
- It decreases normalized routing overhead as it does not introduce any extra control packets.
- If attacker generates destination sequence number which is less than or equal to PEAK value, the node is not detected as a malicious node.

However, unlike R-AODV, MR-AODV:

- Does not allocate 2 Bytes for DO_NOT_CONSIDER flag.
- Only RREQ is used to notify other nodes in the network about existence of malicious nodes; RREP is not used for this purpose. As RREP is unicasted while RREQ is broadcasted, this proves to be a better choice which helps to reduce routing overhead.

Both R-AODV and MR-AODV are equally capable of isolating multiple malicious nodes and giving equal rise in PDR, but MR-AODV has an edge over R-AODV as it discards RREP sent by malicious nodes instead of forwarding it on the reverse path

V. SIMULATION RESULTS AND ANALYSIS

In this section we discuss experimental setup, performance metrics, simulation results and analysis.

A. Experimental Setup

The simulations are carried out on NS-2 (Ver. 2.34) simulator [12] installed in Fedora environment. We implement three new protocols as described in [13]. We implement BlackholeAODV and GrayholeAODV to add Blackhole and Grayhole behaviors respectively; furthermore, MR-AODV protocol is implemented as a solution to thwart both attacks; all three protocols can take part in AODV messaging. We use random waypoint model as the mobility model and set the traffic source to Continuous Bit Rate (CBR); nodes move within an area of 800 m x 800 m; we have used packet size of 512 Bytes. Simulation parameters are presented in Table I.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC	802.11
Application Traffic	CBR (UDP)
Maximum Bandwidth	2 Mbps
Routing Protocols	AODV and MR-AODV
Transmission Range	250 m
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	10 to 80
Maximum Speed	10 m/s to 50 m/s
Number of Sources	1 to 5
Number of Adversaries	1 to 5

B. Performance Metrics

We use following metrics [7] to compare performance between AODV and MR-AODV:

1) Packet Delivery Ratio (PDR): The ratio between the total number of packets received by destination nodes and the total number of packets generated by source nodes.

2) Average End-to-End Delay: Average time consumed by data packets to reach to respective destinations.

3) Normalized Routing Overhead: The ratio of total number of control packets to the total number of data packets.

C. Results

We evaluate performance of MR-AODV under attack by varying network size, mobility, traffic load and number of adversaries as shown in the following subsections.

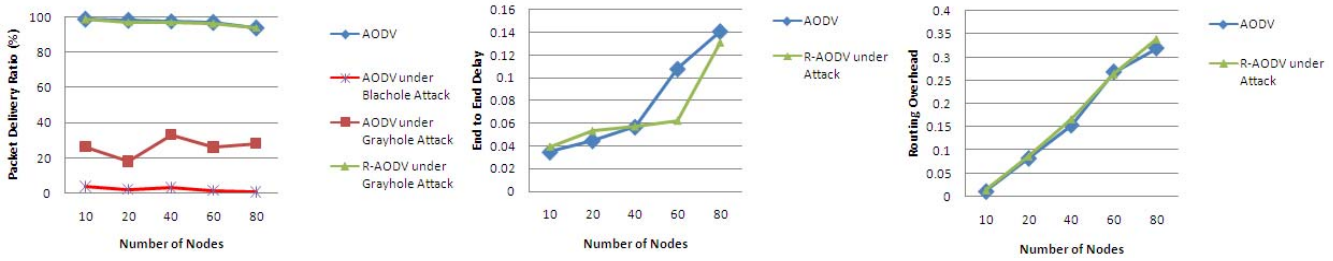
1) Effect of Network Size: Performance comparison of standard AODV and MR-AODV by varying network size from 10 to 80 by keeping number of sources as 1 and maximum speed as 50 m/s is shown in Fig. 5. We can conclude from Fig. 5(a) that AODV under both attacks gives significantly less PDR, while MR-AODV gives almost equivalent PDR as that of standard AODV; Fig. 5(b) shows that average end-to-end delay of MR-AODV stays within acceptable range; graph of normalized routing overhead for MR-AODV is remarkable as it almost replicates the behavior of AODV as shown in Fig. 5(c).

2) Effect of Mobility: Fig. 6 presents the performance evaluation of MR-AODV by varying maximum speed from 10 m/s to 50 m/s by keeping network size as 30 and number of sources as 1. AODV drops a large number of packets

under both attacks and network performance is compromised; on the other hand MR-AODV fulfills its design objectives and gives more than 97% in all five cases as shown in Fig. 6(a); average end-to-end delay of MR-AODV stays within noticable range as shown in Fig. 6(b); graph of normalized routing overhead for MR-AODV swirls around that of standard AODV as shown in Fig. 6(c) and stays within acceptable limits.

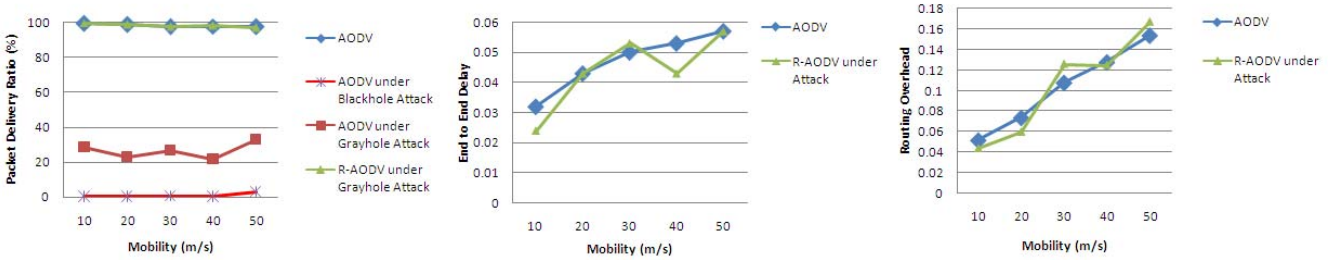
3) Effect of Traffic Load: Fig. 7 depicts performance of MR-AODV by varying number of sources from 1 to 5 by keeping network size as 20 and maximum speed as 50 m/s. As number of sources increases packet dropping increases due to congestion; therefore, graph of PDR for standard AODV starts declining as number of sources increases as shown in Fig. 7(a); MR-AODV proves its reliability to transfer data packets to corresponding destinations under both attacks and gives almost equivalent PDR as that of standard AODV; graph of average end-to-end delay for MR-AODV almost moves parallely with that of standard AODV and stays within acceptable range as shown in Fig. 7(b); graph of normalized routing overhead for MR-AODV stays within acceptable range as shown in Fig. 7(c)

4) Effect of Multiple Adversaries: Evauation of MR-AODV by increasing number of adversaries from 1 to 5 by keeping network size as 20, maximum speed as 50 m/s and number of sources as 1 is shown in Fig. 8. As the number of malicious nodes increases PDR of standard AODV under both attacks starts declining; on the other hand, MR-AODV does not break out under attack and isolates all malicious nodes; it gives more than 89% PDR in all five cases.



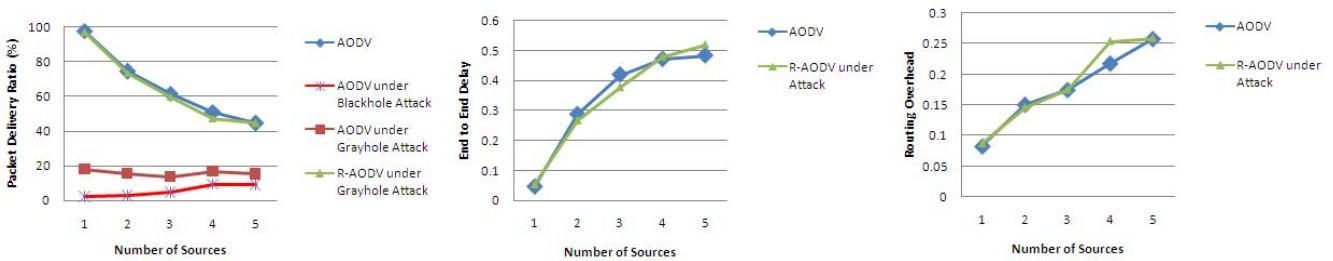
(a) (b) (c)

Fig. 5 Effect of network size



(a) (b) (c)

Fig. 6 Effect of mobility



(a) (b) (c)

Fig. 7 Effect of traffic load

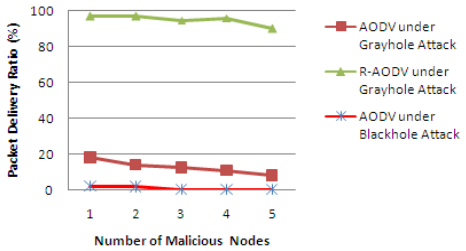


Fig. 8 Effect of multiple adversaries

VI. CONCLUSION

Default ad-hoc routing protocols are prone to various DoS attacks due to ignorance of security aspect during their designs. Blackhole and Grayhole attacks disrupt normal network functionality by sending bogus routing information during route discovery and construction phase. In this paper, we investigated further existing approaches to tackle Blackhole and Grayhole attacks and discussed our previous research work. We propose a modified protocol viz. MR-AODV based on our previous finding viz. R-AODV that eliminates limitations of existing mechanisms. MR-AODV isolates Blackhole and Grayhole nodes during route discovery phase as R-AODV and sets up a secure route for data transmission. It attempts to further reduce normalized routing overhead by decreasing number of forwarded reply packets sent by adversaries. Simulation results presented in form of graphs prove that MR-AODV is a reliable solution which gives significant improvement in PDR with acceptable average end-to-end delay and normalized routing overhead under various network parameters and traffic conditions.

ACKNOWLEDGEMENT

I would like to express my sincere feelings of gratitude to Prof. (Dr.) D.C. Jinwala and Mrs. S.J. Patel for their continuous motivation and valuable suggestions during my research work. I would also like to thank the reviewers for their helpful comments in improving the contents of this paper.

REFERENCES

[1] Jia Uddin and Md. Rabiul Zasad, "Study and Performance Comparison of MANET Routing Procols: TORA, LDR and ZRP", A Master's Article in Electrical Engineering, School of Engineering, Blekinge Institute of Technology, Sweden, May 2010.

[2] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.556-560.

[3] Akanksha Saini and Harish Kumar, "Comparison between Various Black Hole Detection Techniques in MANET", In Proc. of National Conference on Computational Instrumentation, March 2010, pp. 157-161.

[4] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad- hoc Networks: A Survey", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.535-541.

[5] Bala A., Bansal M. and Singh J., "Performance Analysis of MANET under Blackhole Attack", In Proc. of First International Conference on Networks &Communications, December 2009, pp. 141–145.

[6] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Solution for Grayhole Attack in AODV Based MANETs", In Proc. of Third International Conference on Advances in Communication, Network and Computing: Springer, February 2012. pp. 60-67.

[7] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP Journal of Computer Science. March 2012, Vol. 11 No. 1, pp. 1-12.

[8] Ira Nath and Dr. Rituparna Chaki, "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2 Issue 8, August 2012, pp. 113-121.

[9] Moumita Deb, "A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks", In Proc. of the World Congress on Engineering and Computer Science 2008, October 2008.

[10] Surana K.A., Rathi S.B. Thosar T.P. and Snehal Mehatre, "Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms", World Research Journal of Computer Architecture, Vol. 1 Issue 1, 2012, pp. 19-23.

[11] Jain, S., Jain, M., and Kandwal H., "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray hole Attacks in Mobile Ad hoc Networks", International Journal of Computer Applications, Vol. 1 No. 7, pp. 37-42.

[12] Kevin Fall, Kannan Varadhan: The ns Manual, http://www.isi.edu/nsnam/ns/doc/

[13] F. J. Ros and P. M. Ruiz, "Implementing a New MANET Unicast Routing Protocol in NS2", http://masimum.dif.um.es/nsrt-howto/pdf/nsrt-howto.pdf, December 2004.