International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey of Reactive Routing Protocols for Detection & Prevention of Selective Black-hole Attack in MANET

Mithun S[1], A Thomas Paul Roy[2], Dr.K.Balasubadra[3]

[1]PG Scholar, PSNA College of Engineering & Technology, Dindigul, Tamilnadu-624622, India

[2]Assistant Professor, PSNA College of Engineering & Technology, Dindigul, Tamilnadu-624622, India

[3]Professor, RMD Engineering College, Kavaraipettai, Tamilnadu-601 206, India

Abstract: ***Black-hole attack in MANET refers to a Network layer attack. In networking, black holes refer to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. In fact wireless network doesn't have a fixed topology, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic; hence the name. We present a comparison between Conventional Reactive Routing Protocols (DSR, AODV) with a Modified Approach to Analyze the Performance in the Presence of selective black hole attack. Performance Analysis of these protocols can be verified using ns2 simulator.***

Keywords: MANET, security, intrusion-detection, black-hole

1. Introduction

In a wireless Mobile Ad hoc Network (MANET), there are no routers or access points; data transfer among nodes is achieved by means of multiple hops. Every mobile node acts both as a host and as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important is an important issue for MANETs.

In a reactive routing protocol such as AODV (Ad hoc On-Demand Distance Vector)or DSR (Dynamic Source Routing), a route is searched and established only when two nodes intend to transfer data. Because most of these routing protocols assume cooperation between nodes for packet forwarding, a malicious node can launch routing attacks that disrupts the normal routing operations or Denial-Of-Service (DOS) attacks such as black hole or gray-hole attack that denies the service to the legitimate nodes on MANET.

2. Protocol Description

2.1 DSR Protocol

Dynamic Source Routing Protocol (DSR) DSR is an on-demand, source routing protocol. It is an on-demand protocol because routes are discovered at the time a Source sends a packet to the destination for which it has no cached route. 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 flooding 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 drop. The source either tries an alternate favorable path available or initiates the route discovery process again.

2.2 AODV Protocol

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV allows both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the IP address of source node, current sequence number, and broadcast ID, the RREQ also contains

the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source, nodes set up forward to the destination. Once the source node gets the RREP, it start to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop-count, it may update its routing information for that destination and begin using the better route.

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can restart route discovery.

2.3 Modified Protocol Approach

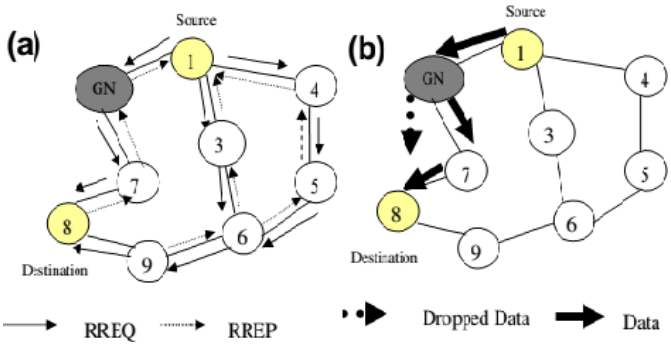

Figure 1: (a) Route Discovery (b) Data Transfer phase

According to DSR & AODV protocol, the source node has to broadcast the RREQ packet to find a path to reach the requested destination. The requested destination, or any intermediate node having the path, can send back the reply to the source node. As shown in Fig. 1a, the malicious nodes which perform gray-hole attack participate correctly in the route discovery process. They forward the RREQ packets as any other normal DSR nodes. When the route is selected through this malicious node to reach the destination, it selectively drops the data packets as shown in Fig. 1b. To mitigate gray-hole attack, when the destination nodes receive data packets from the source node, it starts the process of discovering the presence of any gray-hole nodes in the path. In our approach, when the source node has data packets to send to the destination, it divides the data to be transmitted into different blocks and sends one block of data at a time to the destination. It also intimates the number of data packets it sends in a block to the destination before the actual transmission of the data using a different route (2nd shortest path to reach destination).

We denote the number of packets forwarded by source node S to destination node D in a block be NS. Let nodes a_0, a_1, a_2, a_3,…a_n represent the source route or data forwarding route between source node S and destination node D. Any node a_i in the path has to keep count of the number of packets it forwards to its downstream node a_{i+1} as NFP a_i , a_{i+1}. When the destination node receives the data packets from the source, it starts a counter and keeps count of number of data packets it receives in a block. Let N_D denotes the packets received at the destination node, and then the probability of packets received at the destination node is calculated as follows.

$$P_D=N_D/N_S \quad (1)$$

If $P_D>T_{PL}$, then the destination node starts the process of detecting whether any malicious node is present in the route. If not, then the destination node sends the positive acknowledgement back to the source node. Here T_{PL} is threshold of the packet loss threshold value and takes values between 0 and 0.2. In our approach, the destination node starts the gray-hole detection process, when the data packet loss exceed 20% of the total packets sent by the source node. The source node starts transmitting the next block of data only after receiving the positive acknowledgement from the destination or receiving ALARM packet from the neighbor IDS node.

2.3.1 Algorithms

When the destination node discovers that the actual number of data packets it receives from its previous hop node is significantly less than the number of data packets the source node sends, it starts the gray-hole node discovery process. First it sends a QUERY REQUEST (QREQ) packet to the node in the source route (data forwarding path) at a 2-hop distance from it. If S, a_0,a_1,a_2,...,a_{n-3},a_{n-2},a_{n-1}, a_n, D represents the source route, then node D sends a QREQ packet to node a_{n-1}which is at 2-hop distance to node D.

(a) Grey-hole attack discovery process

If source node
    Intimate to the destination, the count of data packets in a block of data Send one block of data through the path selected through route discovery process
Else if destination node
    Compare the data packets received with the data count intimated by the source.
    Calculate the probability of packets received at the destination node as P_D.
If $P_D < T_{PL}$ (the value of T_{PL} is between 0 and 0.2)
    Send positive acknowledgement back to source node.
Else
    Initiate Gray Hole Attack Discovery Process
end if

(b) Grey-hole attack Prevention process

1) Send a QREQ packet to a node, say X, at 2-hop distance from it in the source route.
2) Receive the QREP packet from node X.
3) From the QREP packet, verify the count of data packets forwarded by all nodes from node X to itself.
4) If data packets forwarded count matches,
   - Repeat step 1 to a node, say Y, which is at 2-hop distance to node X in source route.
   - Repeat the step 2, 3 and 4.else if data packets forwarded count does not matches
   - Move both the node that sends QREP and its next node in the source route, to the suspected list.
   - Stop the process

Using the QREP packets a first level of verification of data forwarding behavior of the intermediate nodes in the source route will be carried out by the destination. If the difference in number of packets forwarded between any two intermediate nodes crosses the monitoring threshold value, the destination node marks both the intermediate nodes as suspected nodes. The Probability of malicious behavior, P_{mb} between any two nodes is calculated as follows:

$$Pmb = \frac{NFPan-2, an-1 - NFPan-1, an}{Ns} \quad (2)$$

In (2) $NFPa_{n-2}$, $a_{n-}1$ denotes the number of forwarded data packets by node a_{n-2} to node a_{n-1}. If $P_{mb} > T_m$,then either node a_{n-2} or node $a_{n-1}$is a malicious node. Here Tm is the monitoring threshold and can take values between 0 and 0.2.

3. Experimental Setup and Analysis

Property	Value
Coverage Area	1000m×1000m
Number of Nodes	20
Simulation Time	600s
Transmission Range	250m
Mobility	Random Way
Load	5Kb UDP
No of Grey Holes	2
Traffic	UDP-CBR
ID nodes	5

3.1 Packet DROP Ratio

Ratio of the total number of data packets dropped by the malicious nodes and also due to congestion to the total number of data packets sent.

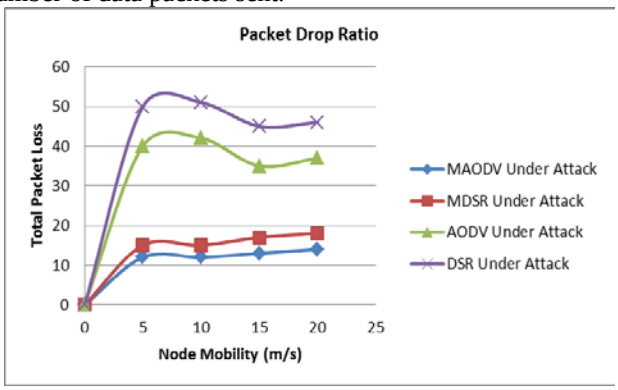

Figure 2: Packet Drop Ratio

3.2 Control Packet Overhead

AODV having high Packet Overhead because in addition to Route Discovery controls it using Sequence messages.

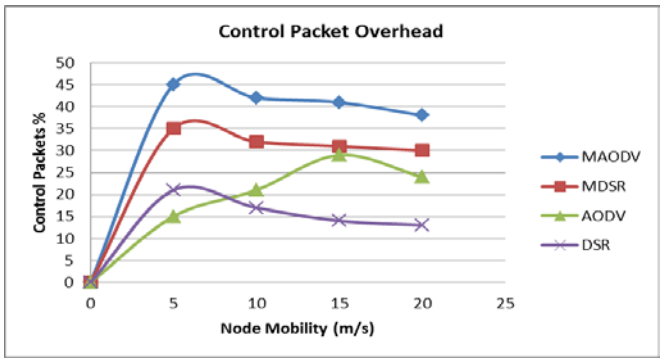

Figure 3: Control Packet Overhead

3.3 End to End Delay

If the source route is without any malicious nodes, then the end-to-end delay for transmitting data packets is less because, there is no additional overhead of checking for presence of attackers. Here we demonstrated all protocols with initial attack conditions.

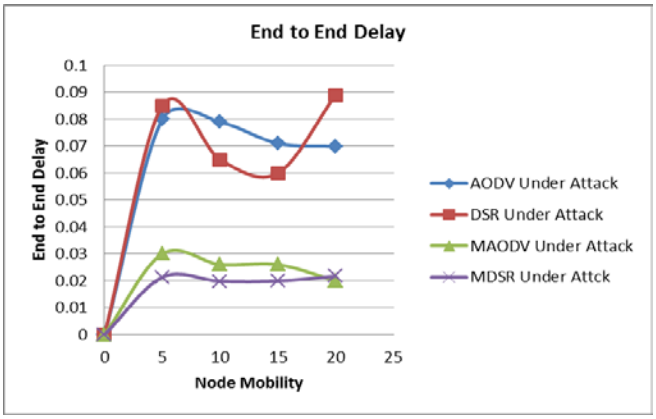

Figure 4: End to End Delay

4. Conclusion

This paper we have analyzed performance of two conventional Reactive routing protocols with a Modified approach that Detect & Prevent selective Black hole attack in MANET. According to scientific analysis Modified AODV protocol behaves better in Packet Drop Ratio, but MDSR is better in Controlling More number of Packets, because AODV using Sequence messages in addition to Route Discovery controls. Overall Modified Approach is Highly favourable.

References

[1] M. Mohanapriya , Ilango Krishnamurthi, Modified DSR protocol for detection and removal of selective black hole attack in MANET June 2013
[2] Abolhasan Mehran, Wysocki Tadeuz. A review of routing protocols for mobile ad hoc networks. Int J Ad hoc Networks 2004; 2(1):1–22.

[3] Johnson DB, Maltz DA, Hu Y-C. The dynamic source routing protocol for mobile ad-hoc network (DSR). IETF Internet Draft 2004.
[4] Zapata Manel G, Asokan N. Securing ad-hoc routing protocols. In: Proc. of the ACM workshop on wireless security (WiSe), 2002.
[5] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, Elizabeth Belding-Royer. A secure routing protocol for ad hoc networks. In: Proc. of the IEEE International Conference on Network Protocols (ICNP'02), November 2002.
[6] Hu Yih-Chun, Perrig Adrian, Johnson David B. Ariadne: a secure on-demand routing protocol for ad hoc networks. In: Proc. of the ACM conference on Mobile computing and networking (MobiCom), 2002. p. 12–23.
[7] Papadimitratos Panagiotis, Hass Zygmunt J. 'Secure routing for mobile ad hoc networks. In: Proc. of the SCS communication networks and distributed systems modeling and simulation conference (CNDS), January 2002.
[8] Deng H, Agarwal P. Routing security in wireless ad hoc networks. IEEE Commun Mag 2002;40(10):70–5.
[9] Semih Dokurer, Erten YM, Can Erkin Acar. Performance analysis of ad-hoc networks under black hole attacks. In: Proc. of the IEEE SoutheastCon, 2007. p. 148–53.
[10] Tamilselvan Latha, Sankaranarayanan V. Prevention of black hole attack in MANET. In: Proc. of the international conference on wireless broadband and ultra wideband, communication, 2007.
[11] Tamilselvan Latha, Sankaranarayanan V. Prevention of co-operative black hole attack in MANET. J Networks 2008;3(5):13–20.

Author Profile

Mithun S received his B.Tech Degree in Computer Science from College of Engineering Kottarakkara Under Cochin University, Kerala in 2012 and pursuing M.E. in Computer Science from PSNA College of Engineering Tamilnadu under Anna University Chennai. His current Research areas include Network Security, Data mining & Cloud Computing.

A Thomas Paul Roy, Assistant Professor in the department of CSE., PSNACET, since from 02-04-2005, received B.E. in Electrical and Electronics Engineering from MK University, Madurai, India in 2000. Received M.E. in Computer science and Engineering from Anna University, Chennai, India in 2005. Pursuing Ph.D. in the field of Network security at AUC under Computer science and Engineering department. His current research interest include Network security, networks and Wireless sensor networks.

Dr. K.Balasubadra, received her B.E. Degree in Electronics and Communication Engineering in 1988 through PSNA College of Engineering and Technology, Dindigul Madurai Kamaraj University and M.E Degree in Applied Electronics through the Government College of Technology, Coimbatore under Bharathiar University in 1997. She did her Doctorate Degree in Information and Communication Engineering from Anna University, Chennai, in 2009. She has 23 years of teaching experience to UG and PG classes and has guided many B.E. and M.E projects. Presently she is guiding ten PhD scholars and she is a research paper reviewer in conferences in National and International levels. Her research interests are Analog VLSI, Optical Communication and Wireless networks. She has published 5 papers in International Journals and 15 papers in conferences in National and International levels. She is a Life member of Indian Society for Technical Education and was a member in IEEE for more than 10 years. She is a recognized research supervisor of Anna University of Technology