Security Enhancement in AODV Protocol against Network Layer Attacks

Khushmeet Singh[1] and Amanpreet Kaur[2]
[1,2]*Centre for Computer Science and Technology, Central University of Punjab, Bathinda, India*
E-mail: [1]erkhushmeetsingh@gmail.com, [2]pandheraman@gmail.com

***Abstract*—A mobile Ad hoc network (MANET) is a wireless decentralized and self-configuring network in which nodes communicate with each other either directly or through intermediate nodes. Each node plays role of both transmitter and receiver. These unique features make MANET suitable for use in various emergency situations. Besides the various advantages, the open medium, rapidly changing topology and lack of centralized monitoring make MANET's vulnerable to different attacks. Hence it is vital to develop some security mechanism to protect MANET from attacks. In this paper performance of AODV Protocol is analyzed in presence of two network layer active attacks namely Blackhole and Malicious packet dropping. In active attack, an attacker disrupts the regular operation of the network, change the data or harm the system. Both these attacks are performed simultaneously on the network. Solution is proposed and simulated to prevent Blackhole attack. Malicious packet dropping attack is prevented by using watchdog intrusion detection system. Both solutions are combined and Performance of AODV and Modified AODV protocol is analysed under both attacks with respect to Packet Delivery Ratio, Average End-to-End Delay and Routing Overhead using NS2.**

Keywords: MANET, AODV, RREQ, RREP, CBR

I. INTRODUCTION

Today wireless networks are at its zenith. Every user wants wireless connectivity to communicate and transfer data with each other irrespective of their geographic position. Two main characteristics of wireless networks that propelled their widespread usage are mobility and ease of deployment. Laying cables in wired network is very time consuming and maintenance is also very high. Wireless communication today surrounds us in many colors and flavors, each with its unique frequency band, coverage, and range of applications. Among all the wireless networks, MANET is of its unique importance.

A mobile Ad hoc network (MANET) is a wireless decentralized self-configuring network in which nodes communicate with each other either directly or through intermediate nodes. Each node transmits and receives data through bidirectional links. All nodes are mobile and configure themselves in network without help of any infrastructure. Due to mobility, network topology changes over time because nodes join or leave the network at any time. These unique features (self-configuring, infrastructure-less, decentralized) make MANET suited for use in Emergency situations such as military operations, education, entertainment, sensor networks etc. Nodes may consist of broad range of devices like laptops, PCs, PDAs, smart phones as shown in Fig 1.

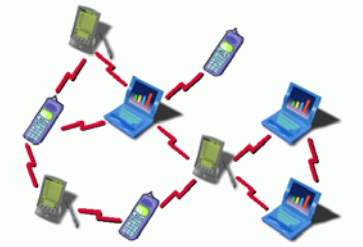

Fig. 1 Mobile Ad-hoc Network

Besides various advantages, the open medium, rapidly changing topology and lack of centralized monitoring make MANET vulnerable to various attacks that will be presented in later sections. In this case, it is vital to develop some security mechanism to protect MANET from attack. Security goals of MANET are same as compared to others networks i.e. Confidentiality, Integrity, Availability and Authenticity [10]. The rest of paper is organized as follows. Section 2 discusses various security goals in MANET. Section 3 discusses attacks in MANET. Section 4 describes the proposed solution to prevent Blackhole attack. Section 5 presents solution to prevent malicious packet dropping attack. Section 6 describes workflow of research. Section 7 presents the simulation set up and the metrics used to evaluate the performance. Results and discussion are shown in Section 8. Finally, paper is concluded in Section 9.

II. SECURITY GOALS IN MANET

Main aim of security services is to protect the data and the various resources from attacks. Various security goals in MANET are as follows [1]:

TABLE 1 SECURITY GOALS IN MANET

Security Goal	Purpose
Availability	Network services are always available whenever requested
Authenticity	Communication between nodes is legitimate
Data Confidentiality	Message exchange between two nodes cannot be understood by anyone else
Integrity	Message sent from sender node to receiver node was not modified by any malicious node during transmission
Non-Repudiation	Origin of the message is genuine. It guarantees that the sender and receiver of a message cannot deny later that it has not sent or receive the message

III. ATTACKS IN MANET

There are two basic types of network layer attacks in MANET namely active and passive attacks, which are further classified into various types. Difference between them is shown in Table 2 [1].

TABLE 2 ACTIVE VS. PASSIVE ATTACKS

Active Attacks	Passive Attacks
In this, attacker disturbs the operation of the Network.	In this, attacker does not disturb the operation of the Network.
Attacker's goal is to modify or harm the system.	Attacker's goal is just to obtain information not to modify or harm the system.
Active attacks are easy to identify because the network operation is irregular.	Passive attacks are very difficult to identify because the network operation is regular.
Examples: Black hole, Gray hole, Sybil, Sleep deprivation, Rushing, Malicious Packet Dropping.	Examples: Eavesdropping, Traffic Analysis, Location Disclosure.

This research work focuses on two active attacks namely Blackhole and Malicious Packet dropping.

A. Blackhole Attack

In this attack a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node. When path is selected by the routing protocol, it starts dropping the routing packets and does not forward packets to its neighbors [4]. The way the intruder node initiates the Blackhole attack may vary in different routing protocols. In case of AODV Protocol, the destination sequence number (DSN) and hop count is used to perform this attack. Destination sequence number is used to represent the freshness of the route. A high value of destination sequence number means a fresher route. To convince the target nodes, the attackers may reduce the hop count data or increase the destination sequence number (DSN).In addition, the attackers can also combine both techniques to increase severity of attacks.

As shown in the Fig. 2, an attacker node M, listens to communication channel of node S. Node M sends a forged RREP to node S immediately after node S broadcasts RREQ. Using the forged RREP, node M claims that it has both valid routing path and shortest distance to the destination node D. Because node S has no knowledge about node D in previous, node S will consider the message from the attacker as legitimate route message. Complete mechanism of this process is shown in Table 3 to Table 6. Route Request (RREQ) and Route Reply (RREP) messages exchange in route discovery process are shown in table 3 and table 4. Node S will update its routing table as indicated in table 5. Due to this attack, node S also rejects the legitimate RREP from node B [5].

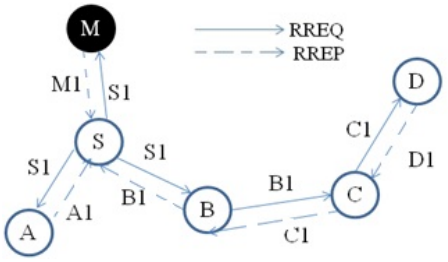

Fig. 2 BlackHole Attack

TABLE 3 ROUTE REQUEST MESSAGES

LastHop	S	S	S	A	B	C
Next Hop	M	A	B	S	C	D
RREQ	S1	S1	S1	--	B1	C1
HopCount	0	0	0	1	1	2
DSN	1	1	1	1	1	1
Origin	S	S	S	S	S	S
Dest	D	D	D	D	D	D

TABLE 4 ROUTE REPLY MESSAGES

LastHop	M	D	C	B
Next Hop	S	C	B	S
RREP	M1	D1	C1	B1
HopCount	1	0	1	2
DSN	1	1	1	1
Origin	S	S	S	S
Dest	D	D	D	D

TABLE 5 ROUTING TABLE UNDER BLACKHOLE ATTACK

S Routing Table Under Attack			
Destination	**NextHop**	**DSN**	**HopCount**
S	0	0	0
D	M	1	2

TABLE 6 ROUTING TABLE WITHOUT BLACKHOLE ATTACK

S Routing Table without Attack			
Destination	NextHop	DSN	HopCount
S	0	0	0
D	B	1	3

In Network simulator, any node is selected as Blackhole through TCL (Tool command Language) script. In AODV.cc file, the following changes is to be done in Receive_Route_Request function to perform Blackhole attack.

1. If (Node=Blackhole){
2. Generate Max_Sequence_Number
3. Send Route_Reply with Max_Sequence_Number and Hop_count=1
4. }

B. Malicious Packet Dropping

Once the path is established between source and destination nodes, the source node starts sending the data packets to next nodes in the path and so on. All routing protocols in MANETs are generally based on the assumption that all the participating nodes are fully cooperative. But some nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. Such nodes are called as selfish or misbehaving nodes. This is also known as a data packet dropping attack. Packet dropping attacks differ from blackhole attack because there is no attempt to capture the routes in the network. To perform this attack the following changes is to be done in Route_Resolve function of AODV.cc file:

1. If (Node=Selfish)
2. Drop Packet

Selfish node is selected through TCL script. While routing data packets, Route_Resolve function is used to select next hop node.

IV. Proposed Solution to Prevent Blackhole Attack

In case of AODV Protocol, when a node receives a packet of type REPLY, it calls AODV: recvReply (Packet *p) function. Node updates its route table entry if sequence number of incoming packet is greater than previously stored number in routing table or Hop count is less than previously stored value in routing table. Proposed Algorithm to prevent Blackhole Attack is as follows:

1. If(SSN < DSN) or
2. (SSN = DSN) and
3. (SHC>CHC){
4. if (SSN < DSN) and (CHC!=1){
5. Call procedure Update Route Table entry}
6. if (SSN < DSN) and (CHC==1){
7. if (Source=Destination){
8. Call procedure Update Route Table entry}}}

Where

SSN=Stored Sequence Number

DSN=Destination Sequence Number

SHC=Stored Hop Count

CHC=Current Hop Count

Now if Blackhole Node send Route Reply with Hop count=1, Packet is rejected and no updation is done in routing table. But in case, if genuine nodes send reply with hop count = 1, Routing table is updated. If(source=destination) in line 7 of algorithm means if destination IP address send by source in Route Request Packet is equal to Destination IP address send by destination node in Route Reply Packet. It means that there is no intermediate node between source and destination. So Route Reply by any node with hop count equal to one is always rejected except if destination IP address by source in RREQ is equal to destination IP address by destination node in RREP [10]. Flowchart for this process is shown in Fig 3.

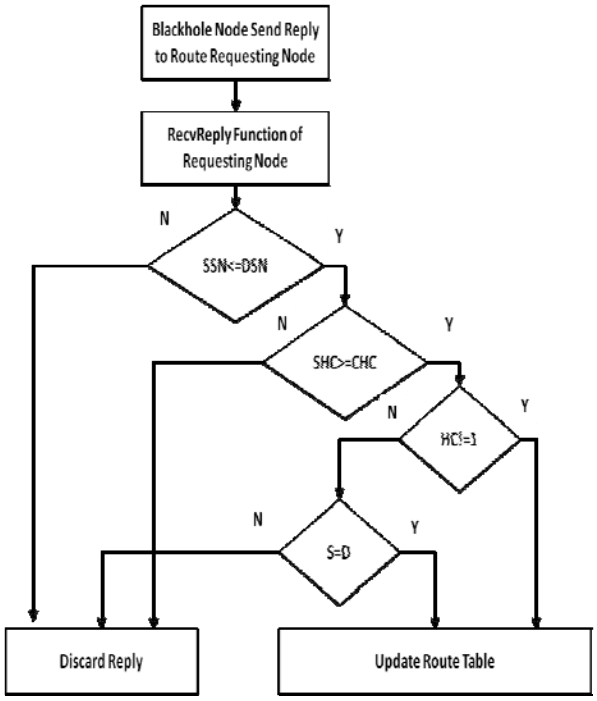

Fig. 3 Flowchart for Proposed Algorithm to Prevent Blackhole Attack

V. Preventing Malicious Packet Dropping Attack

The watchdog method maintains a buffer that contains recently sent packets. This helps in detecting misbehaving nodes. When any node forwards a packet, it is ensured by node's watchdog that the next node in the path also forwards the packet. If the next node does not forward the packet then it is termed as misbehaving. This is done by node's watchdog by listening to all nodes promiscuously. In this scheme, every packet overheard by the watchdog is compared with the packet in the buffer. A match confirms successful delivery of the packet and it is removed from the buffer. Beyond the timeout period, if a packet remained in the buffer then a failure counter for the node responsible for forwarding the packet is incremented. Node is termed as malicious if this counter exceeds a predetermined threshold. Network is informed by the node that detects the problem sending a message. Flowchart for this process is shown in Fig. 4 [7].

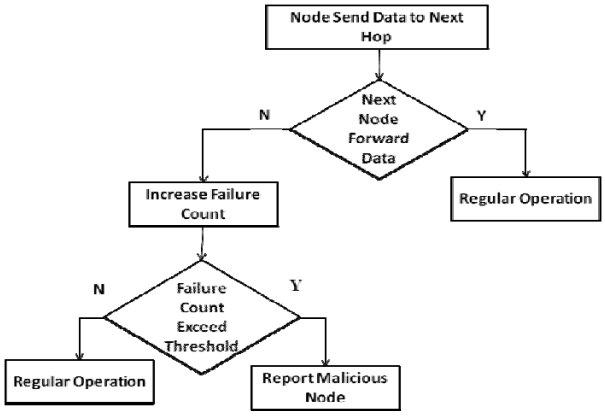

Fig. 4 Flowchart for Watchdog Intrusion Detection System

VI. Work Flow

In this Research Work, Blackhole and Malicious Packet Dropping attack is simultaneously performed on AODV protocol. Proposed solution to prevent Blackhole attack is combined with Watchdog IDS. Main aim of this simulation is

- To analyse performance of AODV protocol in presence of dual attack (i.e. Blackhole and Malicious Packet Dropping) without any prevention scheme.
- To analyse performance of AODV protocol in presence of dual attack with prevention scheme.

Performance metrics calculated under these scenarios are discussed in section VII.

VII. Simulation Environment and Performance Metrics

The simulation is conducted within the Network Simulator (NS) 2.35 environment on a Ubuntu 12.10 operating system. The system is running on a laptop with Core i3 CPU and 4-GB RAM. Each network scenario is run five times and Average is calculated.

The various parameters analyzed and measured are as follows:

A. Average end-to-end delay (AED)

It is calculated for each data packet by subtracting the sending time from the received time of the packet at final destination.

$$AED = \frac{\sum_{I}^{N} (T_R - T_S)}{N}$$

Where

N = Number of successfully received packets
T_R = Packet Received Time
T_S = Packet Sent Time

TABLE 7 Simulation Parameters

Channel type	Wireless channel
Number of nodes	100
Traffic type	CBR
Data Payload	512 bytes/packet
MAC Types	802_11
Node Placement	Random
Mobility	Random way point
Node Speed	10 m/s
Area of simulation	1000m X 1000m
Number of Malicious Nodes (Selfish+Blackhole)	2–10
Time of simulation	150 sec
Protocol	AODV

B. Packet Delivery Ratio (PDR)

It is the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

$$PDR = \frac{\sum \text{Received packets at}}{\sum \text{Sent packets by sources}}$$

C. Routing Overhead (RO)

It defines the ratio of the amount of routing-related transmissions (i.e. Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR)) to total transmissions (i.e. data transmission and routing transmission).

$$RO = \frac{\sum \text{Routing transmissions}}{\sum \text{Data transmissions} + \sum \text{Routing transmissions}}$$

VIII. Result Analysis

A. Packet Delivery Ratio

Packet delivery ratio generally decreases in presence of Selfish and Blackhole nodes. As shown in Fig. 5, PDR decreases with increase in number of malicious nodes in case of standard AODV protocol. But decrease is less in case of Modified AODV protocol.

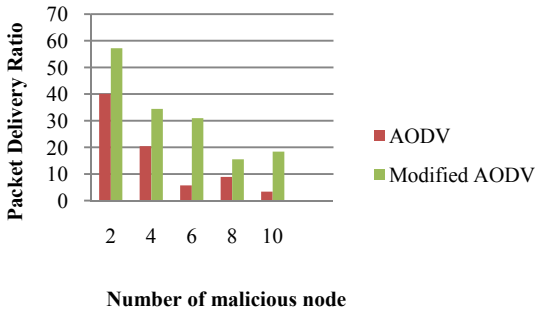

Fig. 5 Packet Delivery Ratio in Presence of Malicious Node

B. *Routing Overhead*

Routing overhead generally increases in presence of selfish and Blackhole nodes. As shown in fig.6, RO increase with increase in number of malicious nodes in case of standard AODV protocol. But increase is very less in modified AODV as compared to standard AODV protocol.

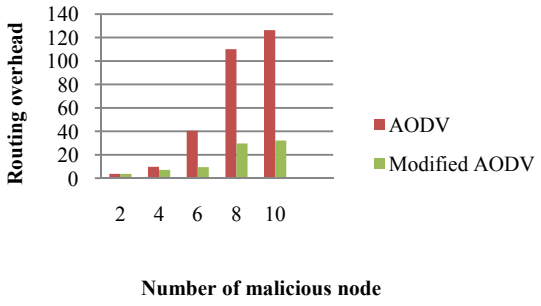

Fig. 6 Routing Overhead in Presence of Malicious Node

C. *Average End-to-End Delay*

Average End-to-End delay shows fluctuating behavior in both cases as shown in fig.7. Reason behind this behavior is that, nodes are randomly moving in 1000 m*1000m area. Sometimes sender and receiver nodes are close to each other and sometimes they are far apart from each other. Besides this reason, malicious nodes are also randomly selected; therefore number of malicious nodes in path increases or decreases.

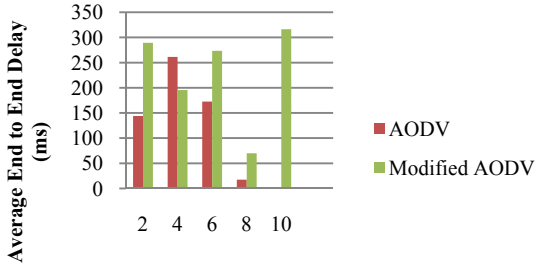

Fig. 7 Average End-to End Delay in Presence of Malicious Nodes

IX. Conclusion

The work presented here is primary concerned with security issues in Mobile Adhoc Network (MANET).The performance of AODV protocol is analyzed in presence of Blackhole and Malicious Packet dropping attack. Both these attacks are performed simultaneously on the network. Some nodes are programmed as Blackhole nodes and some as selfish. Packet delivery ratio decreases and routing overhead increases in presence of these attacks. Solution is proposed to prevent Blackhole attack. Malicious packet dropping attack is prevented by using Watchdog Intrusion detection System. Proposed solution to prevent Blackhole attack is combined with watchdog intrusion detection system in order to prevent both attacks. Modified AODV protocol shows better results i.e. increases packet delivery ratio and decreases routing overhead as compared to standard AODV Protocol.

References

[1] D. Djenouri, L. Khelladi, N. Badache " A survey of security issues in mobile ad hoc networks". IEEE communications surveys, Vol 3. No7, 2005.Retrived from: http://www.lsi-usthb.dz/Rapports_pdf /2004/ LSIIR-TR0504.pdf.

[2] M.Schutte, "Detecting Selfish and Malicious Nodes in manets". seminar: sicherheit in selbstorganisierenden netzen, hpi/ universität potsdam, sommersemester, 2006.Retrieved from: http://mschuette.name /files/uni /soN-text.pdf

[3] A.Nadeem, M.P Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks". IEEE communications surveys & tutorials.Vol 15 No 4 PP. 2027-2045.2013. doi:10.1109/surv.2013.030713.00201

[4] F.H Tseng, L.D Chou, H.C Chao." A survey of black hole attacks in wireless mobile ad hoc networks "Human-centric Computing and Information Sciences VOL 1. NO 1, PP 1-16. Retrivedfrom:http://link.springer.com/article/10.1186/2192-1962-1-4.

[5] S.Mandala, A.H Abdullah, A.H. A.S Ismail, H.Haron, A.H Ngadi, Y.Coulibaly, ." A Review of Blackhole Attack in Mobile Adhoc Network". 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME) Bandung, November 7-8.339-344. doi:10.1109/ICICI-BME.2013.6698520.

[6] P.Sahu, S.K Bisoy, S.Sahoo, "Detecting and Isolating Malicious Node in AODV Routing Algorithm". International Journal of Computer Applications, vol.66 No.16, PP 8-12, 2013.

[7] J.Hortelano, "SafeWireless", Avaiable at http://sourceforge.net/ projects/ safewireless/files/.

[8] A.Al-Roubaie, T.Sheltami, A.Mahmoud, E.Shakshuki, H. Mouftah, ".AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection. Paper presented at 24th IEEE International Conference on Advanced Information Networking and Applications.2010. DOI 10.1109/AINA.2010.136

[9] A.M Kanthe, D. Simunic, R. Prasad. "Effects of malicious attacks in mobile ad-hoc networks." Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference Pp. 1-5, 2012.

[10] K.Singh, A.Kaur, " Security Enhancement in AODV Protocol against Blackhole Attack" Paper Presented at *NCISC (National Conference on Information Security Challenges)* held in march 2014 at Babasaheb Bhimrao Ambedkar University(A central university) Lucknow, Vol 1 No 1, Pp. 59-64, 2014 .