MSBD:A MULTISHARED APPROACH FOR MANAGING MALICIOUS NETWORK WITH BLACKHOLE BASED ON BANDWIDTH

Vimalapriya M.D.[1], Santhosh Baboo S.[2]

[1]Research Scholar, Sathyabama University, Chennai, India
[2]Associate Professor, PG and Research, DG Vaishnav College, University of Madras, Chennai, India
Email: [1]prshvi@yahoo.co.in

Abstract

A Mobile Ad-hoc network is a self-organized network, without a central administration, and which frequently changes its topology. In this paper, we have analyzed the performance of Mobile Ad-hoc Networks (MANET) under blackhole attack. QoS parameters have been considered here such as End to End delay, Packet delivery ratio.

Key words: Manet, Blackhole, Bandwidth, Multishared, Packet Delivery Ratio, End to End Delay.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET)[1] is formed by some wireless nodes which communicates with each other without having any central administration to control their function. This type of network enables in establishing communication between nodes that may not be within the wireless transmission range of each other. Wireless networks have important applications in a wide range of areas. In MANET, as the nodes are utilizing open air medium to communicate, they encounter security problems compared to the wired medium. In ad hoc networks nodes act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack the network or the applications running on it [1][2].There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information,an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures. Routing algorithm is the part of network layer software which decides the output path through which an incoming packet should be transmitted on. Routing directs the passing of logically addressed packets from their source toward their ultimate destination through intermediary nodes. So routing protocol is the routing of packets based on the defined set of rules and regulations. Every routing protocol has its own algorithm on the basis of which it discovers and maintains the route. In all routing protocols, the information of route is stored in the data structure which also modifies the table as route maintenance is required. A routing metric is a value used by a routing algorithm to determine whether one route should perform better than another. Metrics can cover such information as packet loss rate,delivery ratio, bandwidth, delay, hop count, load, reliability. The routing table stores only the best possible routes while link-state or topological databases may store all other information as well. Mobile system is characterized by the movement of their constituents. The movement are frequently changing in speed, direction and rate that will be effect on the protocols and system designed to support mobility[1].

II. ROUTING PROTOCOLS

A. AODV

Ad Hoc On-Demand Vector Routing (AODV) protocol is a reactive routing protocol for ad hoc and mobile networks that maintain routes only between nodes which need to communicate. The AODV routing protocol builds on the DSDV algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information. That means, the routing messages do not contain information about

the whole route path, but only about the source and the destination.Therefore, routing messages do not have an increasing size. AODV has borrowed the concept of destination sequence number from DSDV [5], to maintain the most recent routing information between nodes. Whenever a source node needs to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. It uses destination sequence numbers to specify how fresh a route is (in relation to another), Whenever a node needs to send a packet to a destination for which it has no 'fresh enough' route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ (unless it has a 'fresher' one).When the intended destination (or an intermediate node that has a 'fresh enough' route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to note that the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonically increased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At each intermediate node, a route to the destination is set (again, unless the node has a 'fresher' route than the one specified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ had set this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route 'as fresh' as the received one, the shortest one will be updated. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP[3]. As the link is broken and node receives a notification, and Route Error (RERR) control packet is being sent to all the nodes that uses this broken link for further communication. And then, the source node restarts the discovery process. The AODV protocol is vulnerable to the well-known black hole attack[3][5].

III. BLACKHOLE ATTACK

MANETs are vulnerable to various attacks[. General

attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the and hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages such as sequence numbers and hop count A basic attack [4][6] that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In blackhole attack[4][6][7][8], the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects; data packets[4][6][7].

IV. SIMULATION ENVIRONMENT OF AODV UNDER BLACKHOLE

For simulation, we set the parameter as shown in Table 1. Random Waypoint Model (RWP) [1] is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and a node moves to this destination with a random velocity. The simulation is done using Network Simulator [9] [10] for 10, 20, 30, 40 nodes to analyze the performance of the network. The metrics used to evaluate the performance are given below.

Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at

intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds.

Table 1.

Simulation	Parameters
Simulator	Ns-2(version 2.32)
Simulation Time	500 (s)
Number of Mobile Nodes	10,20,30,40
Topology	900*900 (m)
Routing Protocol	AODV
Traffic Constant Bit Rate	(CBR)
Pause Time	5 (m/s)
Max Speed	20 (m/s)

V. THE MSBD SOLUTION

The solution that we propose here is designed to prevent any alterations in the default operation of either the intermediate nodes or that of the destination nodes. Here we have incorporated the watchdog to detect misbehaviour or abnormal activity, once there is an abnormal activity our approach is initiated to improve the performance in this malicious network. The MSBD solution we follow, converts the data into 16 bit and splits the 16 bit data into Multishares. When multishared data is received by a node it checks the bandwidth of neighbouring nodes.Then it checks to find which of its neighbouring nodes have the highest Bandwidth and sends the data through these selected paths.

Pseudocode of our MSBD Solution

```
If Start of Simulation then
{
Initialize Bandwidth
Initialize all required fields
}
If RREQ then
{
RREQ broadcasted to neighbour nodes
IF node contains route to source
{
Send RREP
}
Elseif ( Node = Destination ) then
{
Send RREP
}
Else
{
Forward RREQ
}
End
If PACKET is data then
{
Conversion of it to 16 bit data Splitting of data into multishares
Checking the bandwidth of neighbour nodes
{
For (i=0;i<Count(0)-1;i++)
{
For(m=0;m<count(0)-1 m++)
{
If (BW(neighbour1(m)) < BW(neighbour1(m+1))
{
Temp=neighbour1(i+1)
Neighbour1(i+1)=neighbour(i)
Neighbour1(i)=temp
}
}
Transmit the multishared data through the selected paths With
Highest Bandwidth.
}
```

VI. SIMULATION RESULTS AND ANALYSIS

Simulation is done with 10,20,30,40 nodes to evaluate the packet delivery ratio and end to end delay. From the Fig1 and Fig 2 it is evident that on the average the PDR of AODV drops by 71.5% in the presence of blackhole attack and a rise in delay of about 13%,whereas according to Fig 3 and Fig4 when our solution is used the PDR is increased by 70% in the same malicious network and rise in delay is only of about 4.9%.

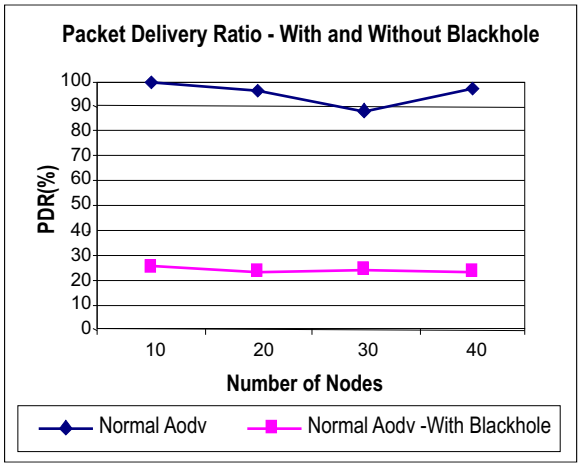

Fig. 1. Packet Delivery Ratio vz Number of nodes

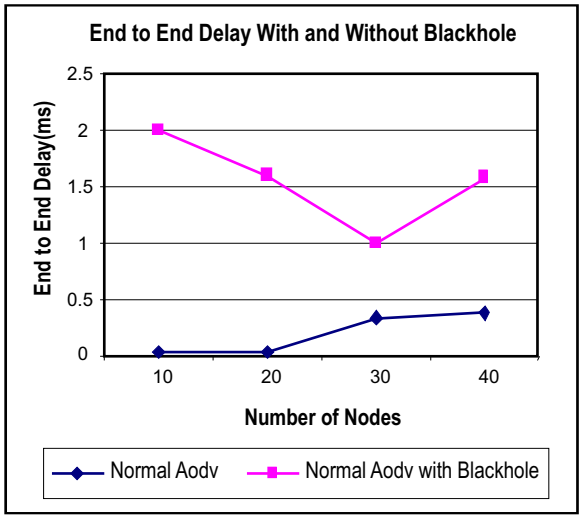

Fig. 2. End to End Delay vz Number of nodes

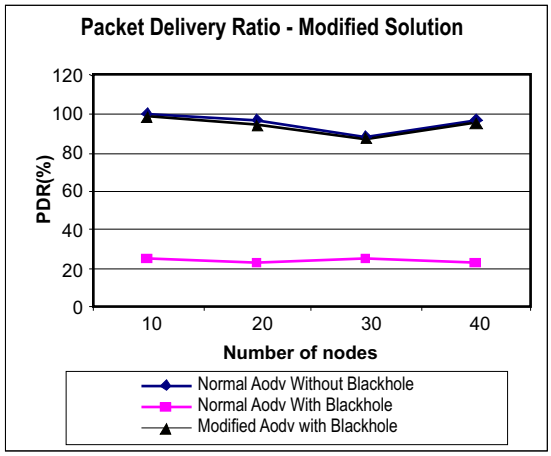

Fig. 3. Packet Delivery Ratio vz Number of nodes

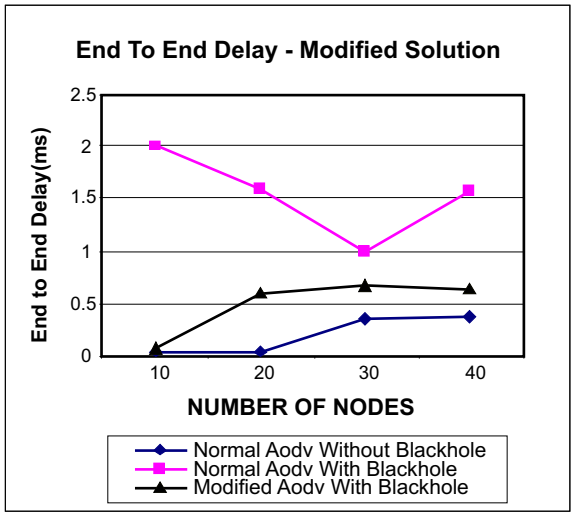

Fig. 4. End to End Delay vz Number of nodes

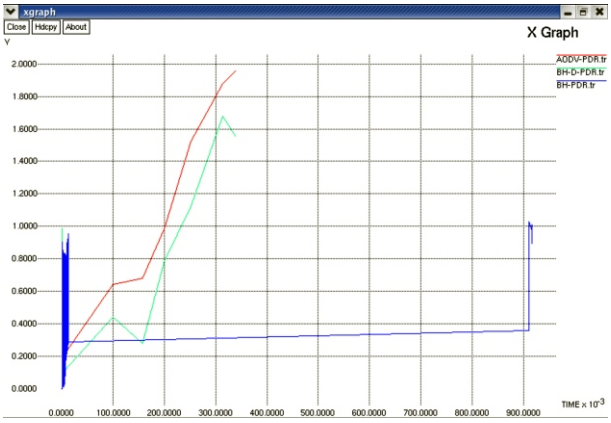

Fig. 5. Trace File Analysis- Packet Delivery Ratio

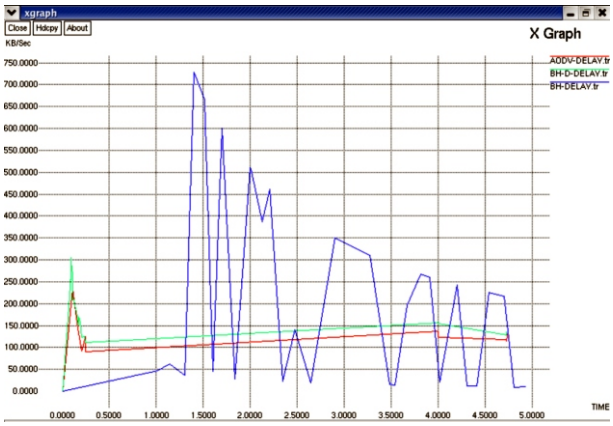

Fig. 6. Trace File Analysis- End to End Delay

VII. CONCLUSION AND FUTURE WORK

In our approach, we have used a simple and effective solution for secure transfer in AODV against Blackhole attack . From the graphs and Trace File analysis we can infer that the packet delivery ratio drops drastically in the presence of blackhole attack and there is a high rise of delay. When our solution is implemented there is a very good increase in the delivery Ratio and minimal increase in the end to end delay. Thus as compared to other approaches , this MSBD Solution is more simple and efficient in implementing. This same algorithm can further be implemented for the other routing algorithms also. In our future work we have planned to focus on the other attacks which affect the network and investigate it based on the impact of node density.

REFERENCES

[1] Hao Yang et al., "Security in mobile ad hoc networks:challenges and solutions", IEEE Wireless Communications, Volume 11, Issue 1, Page(s): 38 – 47, Feb. 2004.

[2] J. Hortelano et al., "Castadiva: A Test-Bed Architecture for Mobile AD HOC Networks", 18th IEEE Int. Symp. PIMRC, Greece, Sept. 2007.

[3] Charles E.Perkins and Elizabeth M.Royer . "Adhoc On-Demand Distance Vector Routing", In Proceedings of the Second IEEE Workshop on Mobile Computing systems and Applications

[4] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007.

[5] C. E. Perkins, S.R. Das, and E. Royer, "Ad-hoc on Demand Distance Vector (AODV)". March 2000, Http://www.ietf.org/internal-drafts/draft-ietf-manet-aodv-05.txt

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc.8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[7] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP' 02), 2002

[8] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," Proc. 2nd ACM Symp. Mobile Ad hoc Networking and Computing (Mobihoc'01), Long Beach, CA, October 2001, pp. 299-302.

[9] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, Apr. 2004.

[10] Kevin Fall and Kannan Varadhan (Eds.), "The ns Manual", 2006, available from http://www-Bash.cs.berkeley.edu/ns/