Proceedings of the 5th WSEAS Int. Conf. on APPLIED INFORMATICS and COMMUNICATIONS, Malta, September 15-17, 2005 (pp77-84)

Modified AODV protocol for prevention of Denial of service attacks in wireless Ad hoc networks

B. MALARKODI, B. VENKATARAMANI AND X.T. PRADEEP
Department of Electronics and Communication Engineering
National Institute of Technology, Tiruchirappalli, INDIA

Abstract: In this paper we analyze attacks that deny channel access by causing pockets of congestion in mobile networks. Such attacks would essentially prevent one or more nodes from accessing or providing specific services. Here we focus on the properties of the most commonly used routing protocol, the AODV, which enables such attacks. We propose a new routing protocol which we call as BT_AODV protocol to mitigate these DOS attacks. We make use of Blacklist table method to isolate the malicious node from the network. The malicious node is circumvented at various stages of the routing protocol. In this method the intruder's node is denied all the services provided by the network. Our analysis and simulation show that providing BT_ AODV protocol with blacklist table method alleviates the effects of such attacks.

Keywords: ad hoc network, malicious nodes, denial of service, intruder

1 Introduction

A mobile ad hoc network is an autonomous system of mobile routers and associated hosts connected by wireless links. There are no mobility restrictions on these routers and they can organize themselves arbitrarily, resulting in rapid and unpredictable change in the network topology. The property of these networks that makes it particularly attractive is that they do not require any prior investment in fixed infrastructure. Instead the participating nodes form their own co-operative infrastructure by agreeing to relay each other's packets.

The dynamic and cooperative nature of MANETs presents substantial challenges in offering secured services. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration and high dependence on inherent node cooperation. As the topology keeps changing, these networks do not have a well defined boundary and thus network based access control mechanism such as firewalls are not directly applicable. It is extremely easy for a malicious node to bring down the whole network. As a result, ad hoc networks are vulnerable to various attacks including eavesdropping, spoofing, modification of packets and denial of service attacks (DOS). DOS attacks can cause a severe degradation of network performance in terms of the achieved throughput and latency. It has been shown that the extent to which performance of the wireless network is degraded by DOS depends on many factors such as location of malicious nodes, their traffic pattern, fairness provided in the network resources.

In this paper we focus on the prevention of DOS attacks in wireless Adhoc networks at the network layer. Ad hoc on demand distance vector (AODV) routing protocol is assumed to be used in the network layer since it offers a no. of advantages such as quick adaptation to dynamic link conditions, low processing as well as memory overhead and low network utilization. However AODV is vulnerable to various kinds of attacks as it allows attackers to easily advertise falsified route information to redirect routes and to launch various kinds of attacks. In each AODV routing packet, some critical fields such as hop count, sequence numbers of source and destination, IP headers as well as IP addresses of AODV sources and destination and RREQ ID are essential to the correct protocol execution. Any misuse of these fields can cause AODV to malfunction. We propose a solution based on black list table for AODV and study its effectiveness.

The paper is organized as follows: section 2 presents a brief review of the previous work on security and intrusion detection in ad hoc networks. In section 3, the details of the Black list table method is

presented. Section 4 presents the simulation results and discusses the effects of the DOS attacks on the network when i)AODV protocol and ii) BT_AODV protocol are used. Section 5 presents the conclusions.

2 Review of the previous work

Security in ad hoc networks has been the focus of attention in recent times [1-4]. In the ad hoc networks presently in operation [5-7], the nodes are required to watch their neighbors for misbehaviour and this not only necessitates promiscuous modes of operation but also overloads the nodes. In [5], a method referred to as Watchdog and path rater approach is proposed to detect and isolate the misbehaving nodes. In this approach, a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. It improves the throughput of the network in the presence of malicious nodes. However, it has the demerit of not penalizing the malicious nodes. In [6], misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially[8]. In [9], a set of techniques referred to as TIARA is proposed to limit the damage sustained by MANET from intrusion attacks and allow continued network operation at an acceptable level during such attack. However the implementation of these techniques requires extensive modification of routing algorithm in MANET. Several cryptographic approaches have been proposed for security in MANET[10-12]. These algorithms have to be implemented between every point to point connection in the MANET and each and every packet requires to be encrypted so that nobody can alter its signatures. Hence they require expensive computation at the nodes. Trust Evaluation method [13] provides an effective security mechanism based on data protection and secure routing. But it relies on global information and hence the reaction time is more. It would be prefereable to reduce the reaction time. In the Reputation scheme [14], the reputation of the nodes is assessed based on their past history of relaying packets, and are used by their neighbors to ensure that the packet will be relayed by the node. Instead of choosing the shortest path to the destination, the source node chooses a path whose next hop node has the highest reputation. As a result, the good nodes (nodes with higher reputations) become overloaded. Once the load on the good nodes is more than what the resources can manage , they start dropping packets and start loosing reputation. As a result, their incoming traffic is reduced to a level at which they can forward all the packets they receive for relaying. Also the number of route discoveries is more with increase in the average hop length.

Our aim in this paper is to arrive at a simple protocol which strikes a balance between computational complexity and power consumption.

3 Blacklist table method for DOS attacks

One of the methods proposed to detect a malicious node is to count the no. of route requests and data packets from a node over a particular time interval and check if it exceeds a threshold [9]. However, it is not clear how the malicious nodes forging the source addresses are detected and prevented. One possible solution is to encrypt the source addresses in each and every packet. However this calls for large computational resources in the nodes. In order to minimize this, we propose the following procedure:

1. The source nodes are required to declare the type of traffic during each session. The individual nodes notify the congestion status periodically. The average no. of packets for each of the sessions and the average time of a session are computed a priori for different hops and congestion levels using queueing theory and are stored in a table referred to as traffic characteristics table. From this table, the threshold values for number of packets and observation interval, are read.
2. When the no. of packets exceeds the threshold, the source node is required to authenticate the number of packets transmitted using any one of the authentication mechanisms proposed in [10-12] An encrypted reply may not be received either because a malicious node did not forward the authentication request or because the source itself is the malicious node. To sort out this, an encrypted message is sent to the adjacent nodes about the reputation of the above node. Based on the reply received, a particular node may be declared to be a malicious node.
3. The malicious nodes are entered in a table referred to as Blacklist table. Only the authenticated nodes

are allowed to make entry in the Blacklist table. This prevents the malicious node from making false entry in the table.

4. Once the malicious node is detected, it is isolated from the rest of the network so as to prevent further harm. The node is circumvented at various stages of the routing protocol. This is done by comparing the possible malicious node address with the entries in the Blacklist Table.

Choice of threshold values for the number of packets and observation interval plays a crucial role. Choosing small threshold will result in frequent exchange of authentication request and reply messages resulting in increase in overhead traffic and computation time. Fixing large threshold values will result in slower detection of malicious nodes. The traffic characteristics table is used in order to strike a balance between the two.

In order to ascertain the efficacy of the above four step procedure, the following issues need to be addressed.

1. Identification of the models for the source traffic in the ad hoc network: The traffic in the ad hoc network may be compressed audio, video and files of data. However, the majority of the traffic is likely to be internet traffic and in this case self similar traffic model may be used. Using this, the distribution of the no. of packets/session may be computed.
2. Computation of the end to end delay: The path between the source and destination of the nodes in the ad hoc network may be treated as a network of queues and the delay distribution may be computed.
3. Validation of the packet count and delay distributions obtained through steps 1 and 2 by simulation. After validation, construct the traffic characteristics table.
4. Simulation of the ad hoc network with the malicious nodes and study the extent to which the traffic characteristics table and black list table are effective in circumventing the malicious nodes and minimizing the overhead traffic and computational complexity.

The work on the computation and validation of the traffic characteristics table is under progress. In this paper, assuming the traffic characteristics table to be available, we study the efficiency of the black list table scheme.

The proposed blacklist table method has several advantages over the reputation scheme method. For example DOS is completely conquered in Blacklist table method. Also the bottleneck of good nodes never occur as network seen by any node is just same except that malicious node is completely ignored.

One of the merits of this method is that it doesn't need any acknowledgements to be exchanged between nodes. Such acknowledgements increase the traffic volume. Unlike the Reputation scheme, the poor nodes with lack of resources are never dropped from the network. Another advantage of this method is that number of RREQ required are less compared to the Reputation Scheme.

The salient features of the proposed Blacklist table method are:

1. detection and circumvention of node is done at the network layer
2. A good node can enter into the network without any prior authentication and can enjoy the facilities of the network
3. subsequent increase in the average throughput of the network
4. the network performance is not degraded even when the malicious node transmits data at high speed
5. Since authentication is required less frequently, computational complexity is reduced very much.

3.1.Circumvention Of Malicious node from the Network using AODV protocol

In the AODV routing protocol, proceedings involving malicious node have to be terminated in three sections: 1. Handle Data 2. Handle Request 3. Handle Route Reply.

1.Handling the Data Requests:

In this section, when data packets are received by a particular node, it takes decision about the processing of the data. These decisions are: whether the node is the destination or an intermediate node; in case of the latter, forwarding the packet to next hop towards destination or to send the route error message if the route is broken.

Here the circumvention should be done when the node detects that the source node message is malicious. Also when the destination node is malicious, we have to send route error message back to the source of the message, so that it stops sending further data to that destination.

While transmitting the data, the node checks whether the destination node is malicious or not. And

if it finds that destined node is indeed a malicious node then it just drops the packet. Also it compares the next hop address towards destination with the node address entries in the blacklist table. If it matches then node drops the packet and sends route error message so as to inform the source node to initiate new route discovery.

2.Handle Request :

A node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node, or if a previously valid route to the destination expires or is marked as invalid. In this case, node sends the request only if it finds that the destination node is not the malicious one.

When a node receives a RREQ, it first creates or updates a route to the previous hop without a valid sequence number. First, it increments the hop count value in the RREQ by one. Then the node searches for a reverse route to the Originator IP. If need be, the route is created, or updated using the Originator Sequence Number from the RREQ in its routing table. If a node does not generate a RREP and if the incoming IP header has TTL larger than 1, the node updates and broadcasts the RREQ to address 255.255.255.255 on each of its configured interfaces.

While handling the route request packets, the request is not processed if the source or destination node is found to be malicious node. This is most important condition because once the route for particular destination is removed, the malicious node tries to reestablish the connection. So it sends route request packets for the route discovery. Circumvention of malicious node at this stage is helpful for preventing malicious node from degrading the network performance.

While relaying the route request packets also, node has to make sure that source and the destination nodes are not the malicious nodes.

3.Handle Route Reply :

A node generates a RREP if either:

- it is itself the destination, or
- it has an active route to the destination, the destination sequence number in the node's existing route table entry for the destination is valid and greater than or equal to the Destination Sequence Number of the RREQ. When generating a RREP message, a node copies the Destination IP Address and the Originator Sequence Number from the RREQ message into the corresponding fields in the RREP message. Once created, the RREP is unicast to the next hop toward the originator of the RREQ, as indicated by the route table entry for that originator.

If route reply is to be generated by the destination, it ensures that the originator node is not malicious node by comparing the source address with Blacklist Table entries.

If the node generating the RREP is not the destination node, but instead is an intermediate hop along the path from the originator to the destination, it updates the forward route entry by placing the last hop node (from which it received the RREQ, as indicated by the source IP address field in the IP header) into the precursor list for the forward route entry -- i.e., the entry for the Destination IP Address. In this case the route reply packet is to be relayed only if the node from which route reply has been initiated or relayed is not the malicious node. If the source or destination nodes are found to be malicious then it simply drops the request. In another case if the next hop is found to be malicious then it not only drops the packet but sends route error packet indicating broken link.

Thus we achieve complete circumvention of the malicious node from the network.

4 Simulation results

4.1. Network Scenario

In this section we quantify and evaluate attacks at the *network* layer. The simulation package, GloMoSim[15] is used to analyze and evaluate the performance of AODV and BT_AODV. GloMoSim is a library based sequential and parallel simulator for wireless networks. It is designed as a set of library modules each of which simulates a specific wireless communication protocol in the protocol stack. the library has been developed using PARSEC, a C based simulation language developed by parallel computing laboratory at UCLA.

Mobility and randomness of the topology complicates the analysis. In order to keep our analysis simple, we test various attack scenarios for a static 12 x 12 grid topology, consisting of 144 nodes. Each node is separated from its neighbor by 350 meters. The topological structure of the network is shown in fig.1

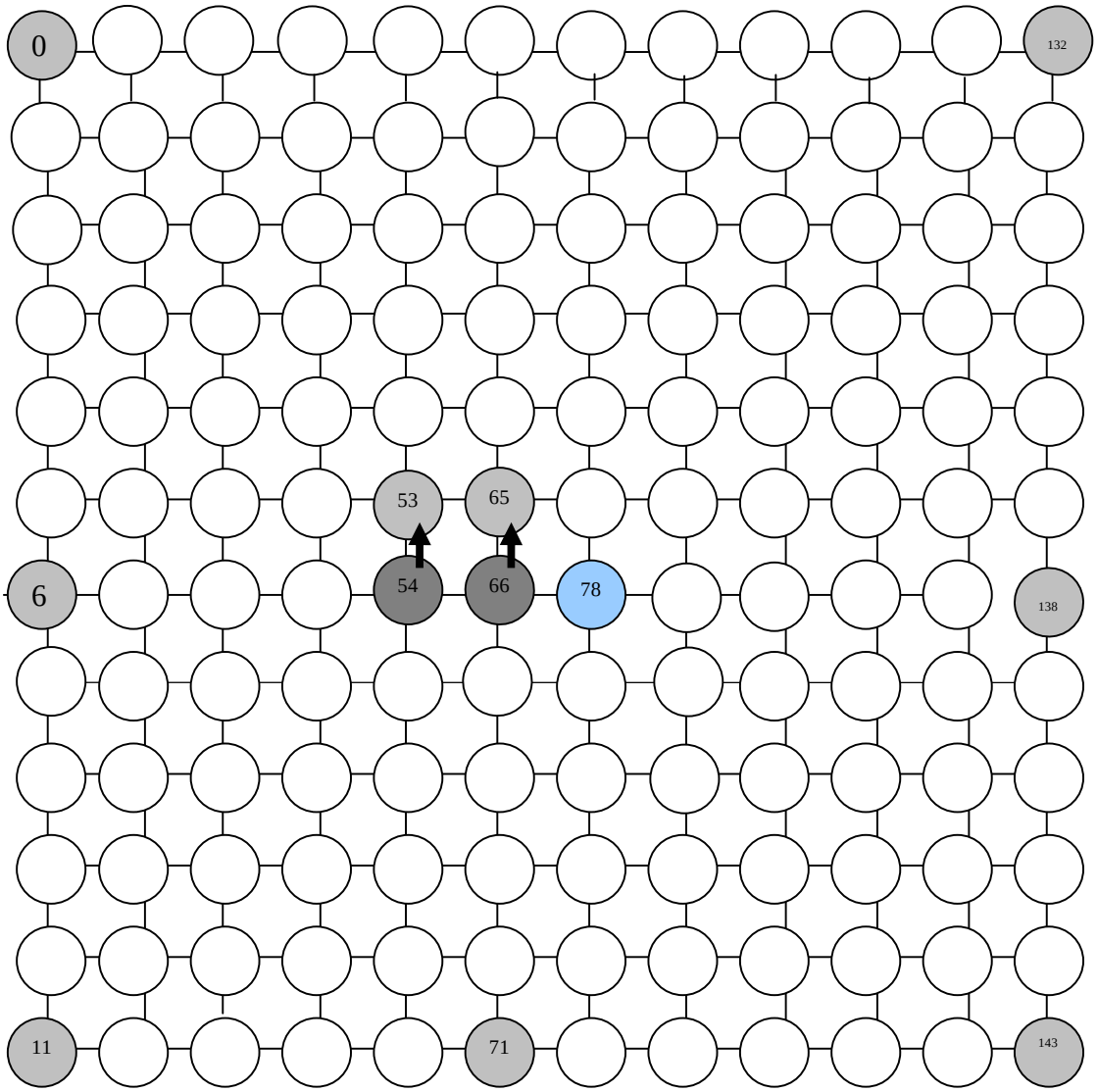

Fig .1. Network Layout

Network Layout:
Server Node: 78
Client Nodes: 1, 6, 11, 60, 71, 132, 138, 143,
Malicious nodes: 1 hop attack 65, 66
2 hop attack 53, 54,56

The metric for quantifying the effects of DoS attacks are the achieved throughputs as seen by 8 clients from a particular server. The clients are placed at the corners (nodes 1,11,132 and 143 as in figure 1 and mid-way (nodes 6,60,71 and 138 in fig.1) along the edges of the grid. The server is placed approximately at the center of the grid i.e. Node 78. The malicious nodes are 66 for 1 Hop attack and 54 for 2 Hop attack.

We use FTP application clients in GloMoSim for the TCP connections. Each client sends 20 packets of fixed size to the server by establishing a TCP connection with it. The simulation time is 1000 seconds. The attack is simulated as a Constant Bit Rate (CBR) application client using UDP. The rate at which the attacker sends data is different for various attacks that we have simulated. The attacker node sends data

continuously to one of its neighbors. We should note here that malicious node chooses its victims to be the ones very nearer to it. In mobile environments routing information may be changing. Thus if the victim node is at far distance from malicious node, the malicious node has to change routing information frequently. So it is *more difficult for malicious nodes to launch a DoS attack on a specific node that is at a large distance from them***.**

We have extended GloMoSim to include a modified AODV protocol which includes Blacklist Table Method. (BT_AODV). Since we simulate a simple grid topology, we ensure that slot reuse is maximized. Through the comparison of performance of the network in presence of DoS attacks with original AODV and modified AODV, we aim to characterize the effects of NETWORK layer fairness on a node's ability to withstand DoS attacks

4.2 Performance under 1-hop attack at low data rate

Objective

The objective of this experiment is to show that a service is vulnerable to an attack from any of its 1-hop neighbors. The attacking node creates congestion by continually transmitting packets in the neighborhood of the service. For example, Node 66 in fig. 1 sends data continuously to one of its neighbors i.e. node 65 (as shown by the arrow) at data rate of 100 packets per second or less.

The simulation results on the performance of the network using AODV with and without malicious node as well as that using modified AODV (BT_AODV) with malicious node, are shown in fig.2

Observations

a) Under the attack when the original AODV is used, throughputs of all nodes go down to considerable level except for node 60. This is because of the server's inability to receive data or to transmit TCP ACK packets.

b) Under the attack, with the modified AODV throughput does not suffer degradation in throughput in most cases.

c) One of the nodes (Node 6) does not get any bandwidth even with modified AODV. This is because the attacking node lies on the path from node 6 to the server. Packets from Node 4 suffer large queuing delays at node 66, thereby causing the degradation in throughput.

d) The throughput of node 60 is even greater than original AODV when modified AODV is used. The reason for this is that, when path to server via malicious node is removed, the packets are routed through node 60 and hence its throughput is increased.

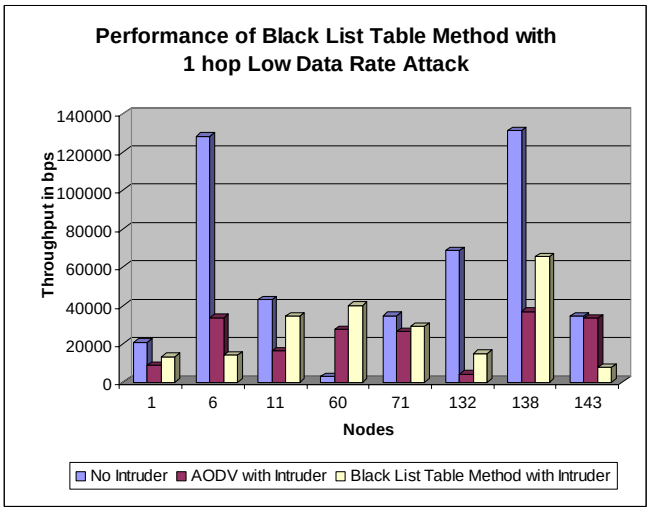

Fig 2 . One hop low data rate attack

Discussion

We notice that node 66 i.e. malicious node was able to capture the media completely when the original AODV was used. However, the degradation in the case of modified AODV is not severe. Thus, AODV using *Blacklist Table method* is *necessary* in preventing attacks that capture the channel. Furthermore, our inability to provide any bandwidth to Node 6, even through using a modified AODV, proves that there should be other prevention mechanism for such attacks.

4.3. Performance under 1-hop attack at high data rate

The objective of this experiment is same as 1-hop attack at low speed except that here the malicious node transmits the data packets at very high rate i.e. at 1000 packets per second. The simulation results are shown in fig. 3.

Observations

a) Under the high speed attack the network performance degrades completely. For all the nodes the throughput goes down to ***zero.***

b) With the Blacklist Table method the throughput is completely restored.

Discussion

We observe that when a malicious node sends data at very high rates, the network comes to standstill. No messages are transmitted or received by the nodes.

The reason for this is that all the media is captured by the malicious node. The *Blacklist Table Method* provides an excellent solution for this kind of attacks.

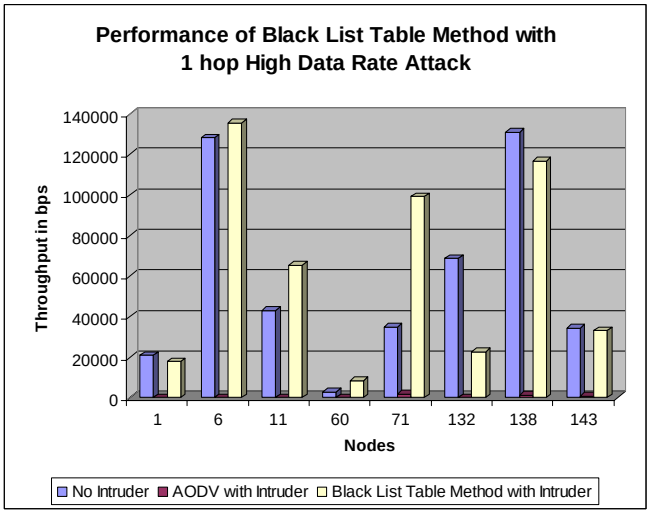

Fig 3. One hop High data Rate Attack

4.4. Performance under 2-hop attack

Objective

The objective of this experiment is to show that a service is vulnerable to an attack from a node that is two hops away from it. For example, Node 54 in fig. 1 sends data continuously to one of its neighbors (as shown by the arrow from node 54 in fig 1.).

We experiment with 2 different scenarios; (a) Node 54 sends data to node 66 (that is in the neighborhood of the service) and (b) in the other case to a different neighbor. The simulation results for case (a), where receivng node is in the neighborhood of the service are shown in fig.4 and for case (b), where receiving node is any other neighbor node are shown in fig 5.

Observations

a) We observe that even if the attack is from 2-hops away from the server, the degradation in the throughput with original AODV is very high.

b) When the original AODV is used and the attack is launched through node 66, the *average throughput* of the server goes down. This is because the server has to wait for the duration indicated in the CTS messages sent by node 66 before it can receive data from any neighbor. Furthermore, the TCP ACK packets that it has to send get delayed resulting in timeouts at the client's TCP Layer.

c)For 2 hop attack launched through node in the neighborhood of server, the degradation in the throughput is completely restored by using *Blacklist Table Method*.

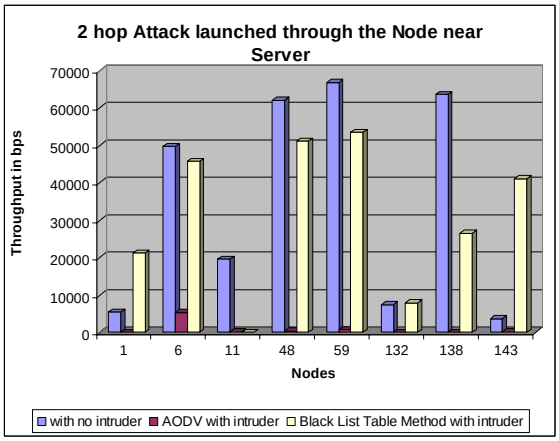

Fig 4: 2 hop attack launched through the Node near server.

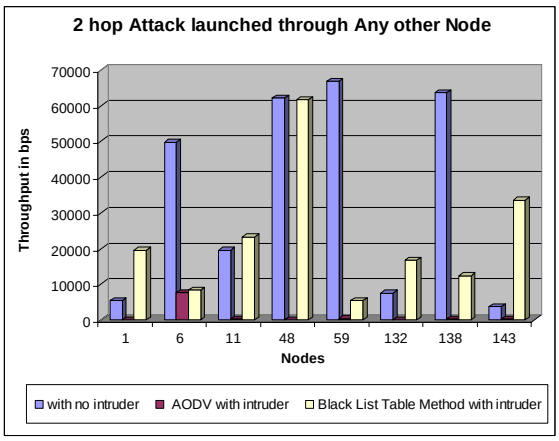

Fig 5: 2 hop attack launched through any Other node

d) For the attack launched through any other neighbor, the throughput is not degraded when we use *Blacklist Table Method*.

Discussion

We notice that when using the original AODV a service is affected even if the attacking nodes are 2-hops away. From the observation (b) above, we find that throughput of server node 78 is affected because node 66 keeps sending CTS messages in response to 54's RTS messages. The same thing is repeated when the attack is launched through any other neighbor. All the requests from malicious node are turned down in the blacklist table method so the throughput of server 78 is not affected.

From the above statistics, we observe that in the original AODV protocol the malicious node i.e. node

66 was successful in lunching DoS attack. All the packets had been transmitted to receiving node and almost null packets had been dropped.

But the BT_AODV protocol circumvented the malicious node from the network. Here we observe that only the no of packets limited by threshold value has been transmitted by malicious node to the receiving node. All other packets are dropped or left waiting. Also the no. of route requests given by malicious node has been increased because the route from malicious node to receiving node has been deleted.

5 Conclusion and future work

In this paper, we have studied through simulation how the weakness in AODV routing protocol can be exploited to launch DoS attacks in wireless ad hoc environment in various ways. The proposed Blacklist method is simulated using GloMoSim and its effectiveness is also studied. Our simulations and analysis show that, Blacklist Table Method is certainly necessary to alleviate the effects of various types of DoS attack. Using BT_AODV protocol the malicious node gets completely isolated from the network and it is unable to take part in any of the proceedings of the network layer.

In this paper, we assumed that a malicious node would not tamper with the AODV protocol. Also we have considered that authentication system exists in network. In future, this system can be incorporated with the routing protocol so as to present a complete solution to DoS attacks. Fixing the threshold and finding the total time required for data transmission depend on the type of traffic. The work on the computation and validation of the traffic characteristics table is under progress.

References:

[1] L.Zhou L.Haas *Securing Ad hoc networks IEEE network* vol.13, no 6,Nov.-Dec.1999 pp.24-30.

[2] Y.Zhang, W.Lee *Intrusion detection in wireless Adhoc network* ,ACM MOBICOM,2000,pp 275-283

[3] Konrad wrona, *Distributed security: Adhoc networks and Beyond;* Adhoc network security, Pampas workshop, RHUL, Sep. 16-17. 2002.

[4] Y.Zhang,W.Lee *Intrusion detection techniques for mobile wireless networks* wireless network 9,2003, pp.545-556

[5] S.Marti,T.J.Giulli,K.Lai and M.Baker *mitigating routing misbehavior in mobile adhoc network* Mobile computing and networking,2000,pp. 255-265

[6] S.Buchegger and J.Y.L.Boudec *Performance analysis of the CONFIDANT protocol*, Mobihoc 2002 pp. 226-236

[7] R.M.P.Michiardi,*A collaborative reputation mechanism to enforce node cooperation in mobile adhoc network* communication and multimedia security, IEEE 2002

[8] Y.Huang and W.Lee *A cooperative IDS for adhoc network* Security of adhoc and sensor networks ACM 2003,pp.135-145

[9] Amitabh mishra and Animesh Patcha *Intrusion detection in wireless adhoc network* IEEE wireless communication Feb2004,pp.48-60

[10] Yin Chun Hu,Adrian Perrig, David B.Johnson *Ariadne: a secure on-demand routing protocol for adhoc network* MOBICOM02 sep23-26 2002,pp.12-23

[11] Manel Zapata *Secure Adhoc (SAODV)routing*, IETF MANET mailing list available at ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10 mail,Oct 8,2001

[12] Yuh-Min Tseng *Efficient authenticated key agreement protocols resistant to a DOS attacks* published online 28 Feb 2005 in wiley Interscience.

[13] Zheng Yan and peng Zhang *Trust Evalution based security solution in Adhoc network, pp 1-14*

[14] Prashant Dewan, Partha Dasgupta,Amiya Bhattacharya *On using Reputation in Adhoc network to counter malicious nodes* Proceeding of Parallel and distributed system, 10th International Conference on (ICPAD'S 04) July2004, pp 665 - 672

[15] http://pcl.cs.ucla.edu/projects/glomosim: GloMoSim user manual