Intrusion Detection for Mobile Ad-Hoc Network

Deepika Dua[1], Atul Mishra[2]
[1,2]Deptt. of Computer Engineering, YMCA University Of Science And Technology,(Haryana), INDIA
[1]deepikadua876@gmail.com, [2]mish.atul@gmail.com

***Abstract*—Mobile ad-hoc networks(MANET) are the networks which uses the wireless medium for communication ,every node is free to either join or leave the network and the nodes in such a network have no fixed topology, the topology changes with time as the nodes move from one place to another. So in such a network, security can be easily compromised as the attacker can introduce its malicious node in the network and can degrade the network performance. As a result there is a need of an intrusion detection system. This paper describes a scheme that will detect the intrusion in the network and will help improve the network performance in the presence of malicious node.**

***Keywords*—AODV, MANET, Intrusion, Intrusion Detection system, Attacks**

I. INTRODUCTION

Mobile ad-hoc networks are the collection of nodes in the wireless medium which have random motion. Nodes can act both as a transmitter as well as receiver. Nodes can directly forward the data packet to the nodes which are in its radio range, in-fact the communication can be done with the nodes that are not in the radio range of the sender. In this case, nodes rely on other intermediate nodes to forward the packet to the destination. The network in former case is known as the single-hop network and the latter network as multi-hop network. MANETs are decentralized and self organizing networks. Nodes in MANET assume that other nodes in the network cooperate with it to forward the packet. As a result, various attacks can be possible on such a network as the network gets compromised by introducing some misbehaving nodes in the network. Misbehaving nodes are the nodes in the network which drops the packet intentionally or just to save its own resources .The nodes are highly mobile and as a result intrusion detection for wired medium cannot be applied to these kinds of mobile networks. Intrusion detection acts as a second layer of defense in MANETs. It detects for the misbehavior in the network by monitoring the network for any compromise in security like confidentiality, integrity etc. In this paper, watchdog [1] scheme is implemented for detecting the intrusion in the network. The watchdog scheme is a reputation based scheme [2].In reputation based scheme, after the detection of the intrusion, the information is propagated throughout the network so that the misbehaving node can be avoided in future routes. The paper is organized as follows. In section 2, assumptions and a brief introduction of the routing protocol used is present. In section 3, scheme description is present, the methodology used is described. In section 4, simulation environment and results of the simulation are presented. And finally conclusion is presented in section 5.

II. BACKGROUND

A) ROUTING PROTOCOLS IN MANET

Nodes in mobile ad-hoc network behave as a router and helps in forwarding the packet to the destination. Due to the MANET's limitation such as limited battery power, high error rates and continuously changing topology ,routing protocol for wired or infrastructure network cannot be applied to mobile ad-hoc network. The routing protocol for MANETs can be classified into table driven routing protocols [3], on-demand routing protocols [4] and hybrid protocol.

- **Table Driven Routing protocols/Proactive protocol**
  In this every node maintains the routing table containing information about the network topology. Every node updates its routing table if there is a change in network topology and change is propagated throughout the network for consistent and reliable route information. It takes less time to discover the routes but consumes more network bandwidth. Examples of such protocol are Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP).
- **On-Demand Routing protocols/Reactive protocol**
  In On-Demand routing protocol, routes are created only when the source wants to connect to the destination. When source requires a route to destination it initiates a route discovery process by broadcasting route request packet to its neighbors. The route request packet is forwarded by neighbors till it reaches the destination, where destination replies using route reply packet. Route is maintained till source no longer wants to connect to destination or destination becomes unreachable. Examples of such protocol are Ad-hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Temporary Ordered Routing Algorithm (TORA).
- **Hybrid Protocol**
  These protocols combine the features of both Table-driven and On-Demand routing protocols. Example of such protocol is Zone based routing protocol (ZRP).

B) AODV (Ad-Hoc On Demand Distance Vector) routing protocol

It is a routing protocol used for mobile ad-hoc networks. It is a reactive protocol [5] means that the route is build only when source wants to send the data to destination and is maintained as long as source needs it. For freshness of the routes, sequence number is used by AODV. If the sequence number of the current packet received is greater than the last sequence number, then the node updates its routing table and path information. The route is build using route request/route reply query messages. For a source that wants a route to destination, it broadcasts RREQ (route request) packet across the network. All the nodes that receives RREQ packet checks their routing table for the route. If route is present in their routing table, then they reply using RREP (route reply) to the source node. If

no route is present in their routing table, then they forward the packet to their neighbors.

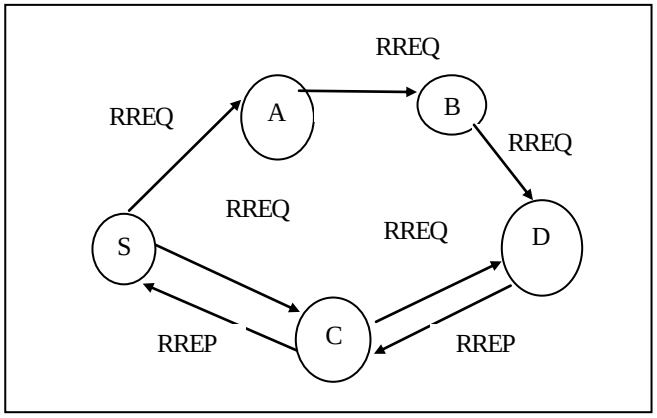


Figure 1: Propagation of route request and route reply from S to D

Figure 1 shows if source S wants to find the route to the destination D.S sends the RREQ to A and C. If A and C have the route in their cache, they will reply the route else they further forward the RREQ to their neighbors. RREQ would be forwarded till it reaches destination. Destination D replied the route using RREP.RERR is the error message used to inform about the link breakage. If the link gets down between the two nodes, then both the nodes initiates a RERR message to inform the nodes about the link breakage.

III. SCHEME DESCRIPTION

An analytical study of watchdog [1] technique is carried out where in this technique is implemented on AODV protocol. Watchdog detects the node as misbehaving by a node listening to its neighbor's transmission of packets. A buffer is maintained and all the packets are stored in the buffer. If a node forwards the packet to its neighbor, then that packet gets deleted from the buffer else a failure counter is maintained and its value gets increased every time a node fails to forward the packet. When the counter value reaches a particular threshold value, then that node is declared as malicious. Now, path rater comes into role. It finds the new route to the destination which excludes that malicious node, if the malicious node is not in all the routes to the destination. This scheme has several weaknesses as described by Marti et al[1].It fails to detect the misbehavior in the presence of 1) Receiver collision ,2) Ambiguous Collisions ,3) Limited Transmission Power ,4)Collusion , 5)Partial Dropping.

IV. SIMULATION RESULTS

A) SIMULATION CONFIGURATION

The experimental study is carried out on Network Simulator 2 (NS-2) version 2.35 running on Linux operating system Ubuntu version 12.10.The hardware platform consist of Core 2 Duo T6500 processor with 4-GB RAM. For plotting graph trace graph version 202 is used. Number of nodes taken are 10 in a flat space with a size of 500x500 m. Physical layer as well as Mac 802.11 are included in wireless extension of NS-2.35.Transmission protocol UDP with constant bit rate traffic (CBR) is used with the packet size of 512B and packet interval of 0.25.

B) ASSUMPTIONS

The assumptions taken here are

- All the links are assumed to be bi-directional.
- Both the sender and receiver are assumed to be non-malicious.
- The wireless interfaces in which nodes can overhear the communication of other nodes which are within its range, also known as promiscuous mode operation.

C) SIMULATION SCENARIOS

For simulation three scenarios have been taken:-

Scenario 1: In this scenario, normal traffic flow is simulated using AODV protocol with the assumption that no node is malicious.

Scenario 2: In this, a malicious node is inserted between the route from source to destination. The malicious node drops all the packets that it receives from the sender.

Scenario 3: In this scenario, watchdog is implemented and IDS performance is evaluated.

D) PERFORMANCE EVALUATION

Scenario 1

In the first case, normal traffic flow is considered with no malicious node in the path from sender to receiver using AODV protocol and throughput is calculated. Figure 2 shows the topology taken where source node is 0 and destination node is 6. Figure 2 shows the network topology where source node 0 wants to connect to the destination node 6.The path chosen here to destination is via the nodes 1 and 3.Source node 0 forwards the packet to its neighbor node 1, which again routes the packet towards node 3, which finally forwards the packet to destination node 6.

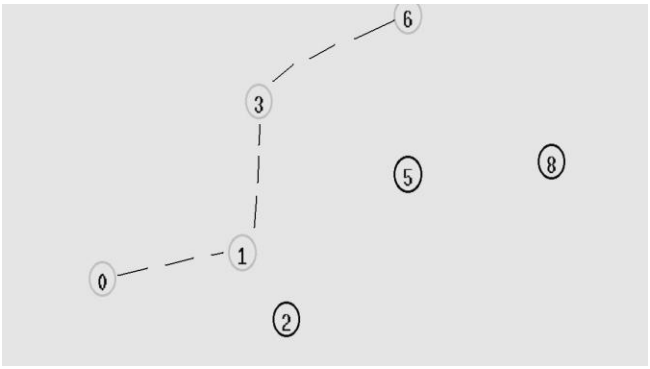
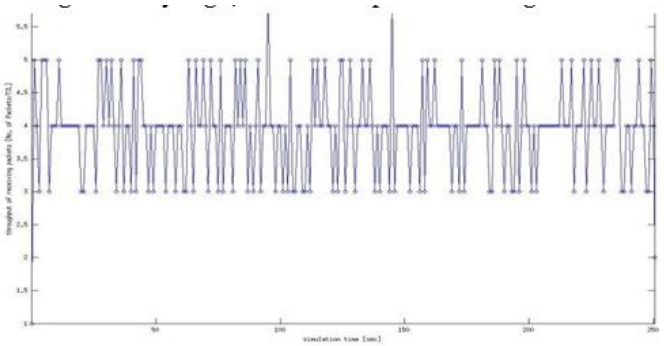


Figure 2: Topology taken in scenario1

Figure3 shows the graph of throughput of receiving packet vs. simulation time. Here throughput is calculated by number of packets received every time interval divided by its length. With time, throughput of packet receives vary as the traffic is busty in nature. As a result, the rate at which the throughput changes is very high, when more packets are Figure 3:



Throughput of receiving packet vs. simulation time received per unit time throughput increases and with decrease in number of packets, graphs of throughput also decreases. Figure4 shows the throughput of packet drop vs. simulation time. As there is no misbehavior in the network, almost all packets reached the destination, so throughput of dropped packets is zero and is depicted by straight line in the graph.

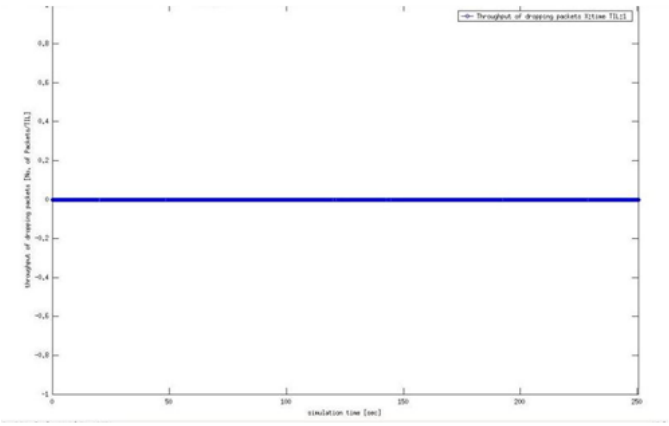


Figure 4: Throughput of drop packet vs. simulation time

Scenario 2

In this case, a malicious node is introduced in path from source to destination. Malicious node taken in this scenario is node 3.This node drops all packets that reach to it. Now again the performance is evaluated. Figure 5 shows the network topology where node 3 is malicious. The packets are coming to node 3 but it is not forwarding the data packets.

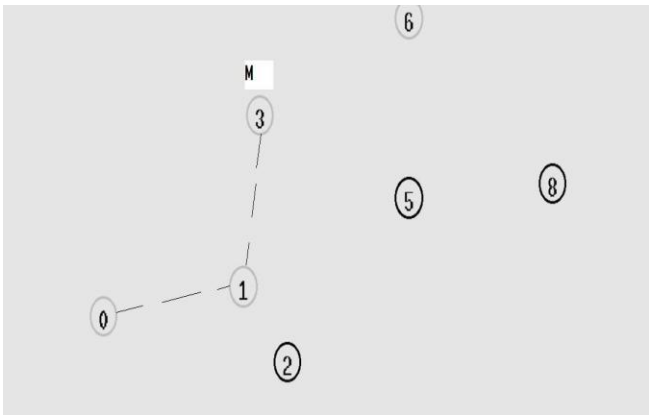


Figure 5: Topology with malicious node in path

The figure 6 shows the throughput of receiving packet. The received numbers of packets are almost zero as the malicious node dropped all the packets and doesn't forward at all.

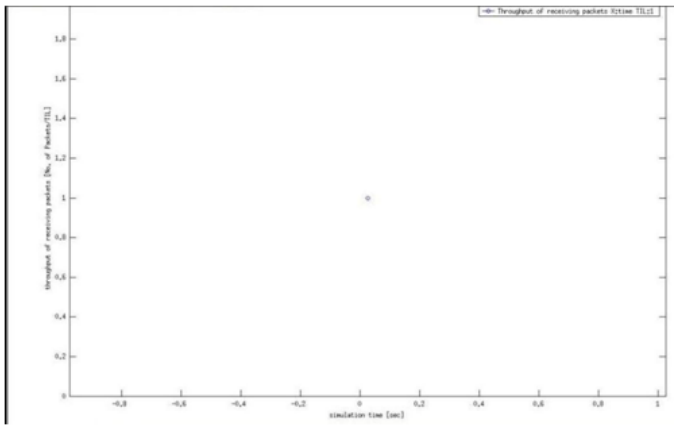


Figure 6: Throughput of received packet vs. simulation time

Figure 7 shows the throughput of packet drop vs. simulation time. As a single node is malicious, so all the packets coming to that particular node gets dropped. When more packets come to malicious node during the simulation period, throughput increases and when arrival of packets decreases throughput of dropping packet also drops.

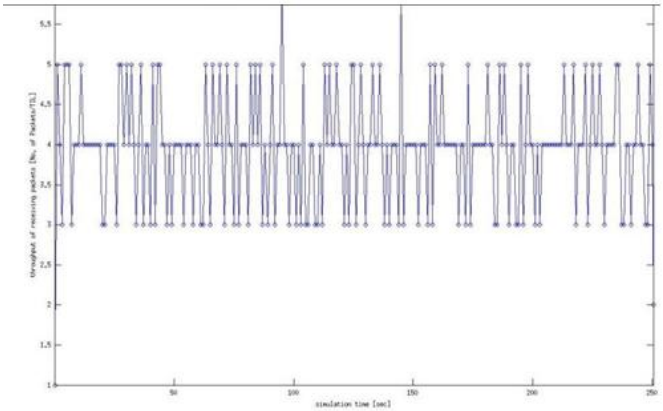


Figure 7: Throughput of packet drop vs. simulation time with misbehavior in network

Scenario 3

In this case, IDS is introduced in the system. So, now when the malicious node drops the packet more than a threshold, IDS detects it and declares the node as malicious and a new route is calculated and now packets are re-routed to the new route. Figure 8 shows the new route taken when the IDS detects node 3 as misbehaving. Node 1 acts as a watchdog for node 3 .Node 1 listens to node 3 transmission of packets by promiscuously listening to it. When node 3 is detected as misbehaving then a new route is calculated excluding the misbehaving node 3 from the route and packet is re-routed to destination node 6.

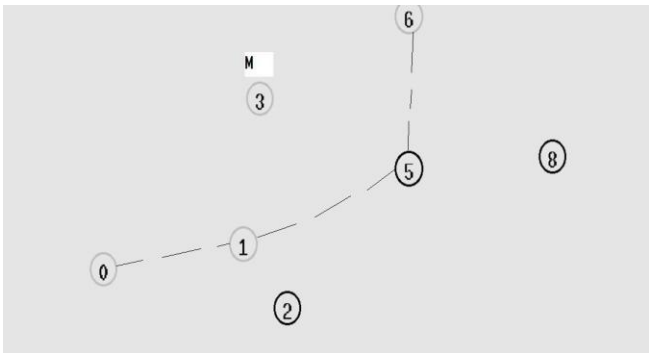


Figure 8: Route taken in presence of IDS

Figure 9 shows the throughput of packet received vs. simulation time. Initially ,when the network gets started and no node is malicious ,packets gets received and slope gets up but when a malicious node gets introduced in the network throughput of received packet decreases but When the IDS detects the misbehavior in network, it re routed the packet and hence the throughput gets increased again.

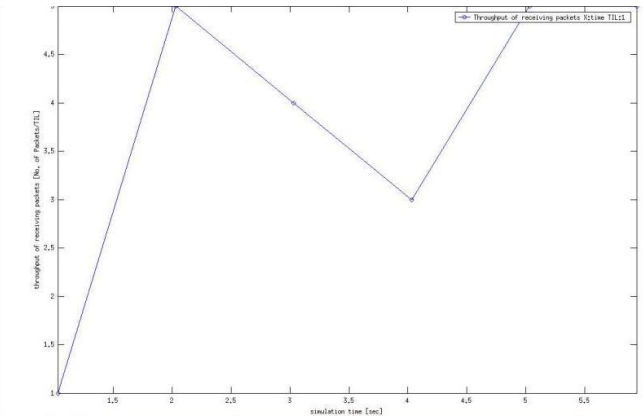


Figure 9: Throughput of packet received vs. simulation time with IDS

Figure 10 shows the throughput of packet drop vs. simulation time. As there is malicious node in the network, packet gets dropped by the malicious node and graph of packet drop gets increased but when the IDS detect the misbehavior, the packet drop decreases.

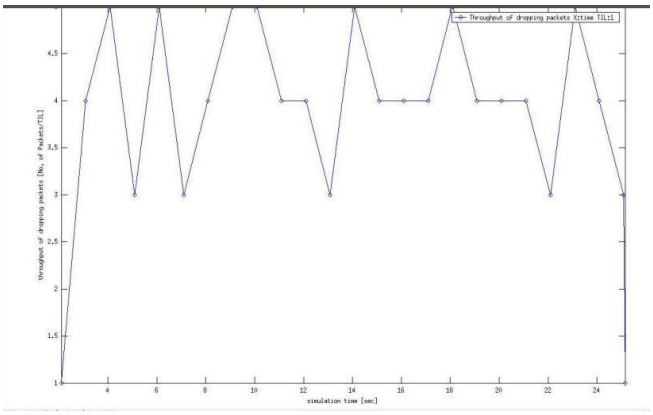


Figure 10: Throughput of packet drop vs. simulation time with IDS

Table 1 shows the statistics of the number of packets sent, number of packets received and percentage of packets received and drop in all three scenarios i.e. in absence of malicious node, in its presence without IDS and with IDS. The statistics shows that with the presence of IDS in the network, the network performance gets improved.

Table 1: Statistics of simulation data

	Number of packets sent	Number of packets received	Percentage of packets received	Percentage of packet drop
Absence of malicious node	1000	997	99.69	0.30
Presence of malicious node without IDS	1000	13	1.3	98.69
Presence of malicious node with IDs	1000	889	88.9	11.1

V. CONCLUSION

Malicious nodes can easily enter the mobile ad-hoc network and can lead the whole network to fail. The scheme presented in this paper detects the intrusion in the network and a new route is established which don't contain misbehaving node. So, the overall performance of the network gets improved. The result shows the benefits of introducing intrusion detection system.

REFERENCES

[1] S. Marti, T.J.Giuli, K.Lai ,and M.Baker,"Mitigating routing misbehavior in mobile ad hoc networks,",in Proc. 6Th Annu.Int. Conf. Mobile Comput. Netw.,Boston,MA,2000,pp.255-265.

[2] K.Liu, J.Deng, P.K.Varshney, and K.Balakrishnan , "An acknowledment-based approach for the detection of routing misbevaior in MANETs,"IEEE Trans Mobile Comput.,vol.6,no.5,pp.536-550 ,May 2007

[3] U.Venkanna, R.Leela Velusami,"BLACKHOLE ATTACKAND THEIR COUNTER MEASURE BASED ON TRUST MANAGEMENT IN

[4] MANET: A SURVEY",in Proc. of1nt. Con/, on Advances in Recent Technologies in Communication and Computing 2011,pp 232-236

[5] Bindhu.R ,"Mobile Agent Based Routing Protocol with Security for MANET ," in International journal of applied engg research, Vol 1, No1, 2010 ,pp 92-101