RECOMMENDATION TRUST PROXY (RTP) BASED SECURITY METHOD FOR BLACK HOLE ATTACK PREVENTION IN MANET

Ankit Gupta[1], Mahesh Malviya[2]
Department of Computer Science and Engineering,
Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India

Abstract: This Research proposes a Recommendation trust proxy (RTP) mechanism which is liable for the trust calculation. The RTP measures an optimal route for communication by analyzing the network parameters like delivery ratio, overhead & delays. After the trust value index is calculated the RTP node issues a certificate to every node in its network array. In this work, approach to detect blackhole nodes for AODV protocol of MANET. To contribute in routing the nodes must have two recommended trust index (RTI) certificates & can be consider as a recommended node by RTP. The directory of this certificate is maintained in a Recommended Trust Index (RTI) Table. This RTI is shared with the data aggregation between node. Enhanced AODV protocol using C++ is written, to simulate the Black Hole attack. In order to test the proposed method, a simulation model was developed. The simulation results show the effectiveness of our scheme compared with conventional scheme.

Keywords- AODV, MANET, REQP, RREP, Black hole attack, Malicious node

I. INTRODUCTION

MANET is formed with wireless mobile nodes without per-established infrastructure. Some packets can be delivered from a source node to a destination node by way of various intermediate nodes, thereby maintaining network connectivity and applicability of MANET depends heavily on cooperation between nodes in such a dynamic environment [2]. A mobile ad hoc network (MANET) is a group of devices or nodes that transmit across a wireless communication medium mainly based on radio frequency without any fixed infrastructure or centralized control. Cooperation of nodes is important to forward packets on behalf of each other when destinations are out of their direct wireless transmission range. There will be no centralized control or network infrastructure for a MANET to be set up, thus making its deployment quick and inexpensive. AODV (Ad hoc on demand distance vector protocol) routing strategy. This approach detects and prevents misbehaving nodes (malicious) capable of launching any of the network layer attacks. This work focus on improving the more secure mechanism to this forged message detection & valid packet dropping by malicious node identification. Better the timing of identification of these misbehaving nodes, it’s easy to identify them but requires some standard protocol parameters [4]. Trust can be consider a well known parameter for node behavior whose value is continuously exchanged between all the adjacent neighbour nodes. The proposed work of RTP & RTI will also categorize the parameters to define maliciousness or unwanted behaviour of the node. These unwanted behavior of node can be find out by the trust value of node which is been participated in data transfer previously. Thus this trust value calculation & the exchange of this trust table needs to be secure. The work categorizes in to two related domain areas first is invalid trust value due to malicious node behavior is legitimate at certain condition. & second is trust packet modification by fabrication (Masquerade) type of attack. MANET applications includes emergency disaster relief, military operations over a battlefield (vulnerable infrastructure), and wilderness expeditions (transient networks), and community networking through health monitoring using medical sensor network (MSN) [1]. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse [2]. In Section 2 of this paper, we summarize the basic characteristic of MANET. In Section 3 we discuss the basic Operation of AODV (Ad hoc On- demand distance Vector Routing) protocol on which we base our work. In Section 4 we describe the effect of black hole attack in AODV. Section 5 presents our proposed work protects against black hole attack. Section 6 discusses the performance evaluation based on simulation experiments and

results. Finally, Section 7 presents conclusion and future work.

II. MANET

MANET is formed with wireless mobile nodes without pre-established infrastructure. Each node in MANET is responsible for relaying packets to other nodes. Some packets can be delivered from a source node to a destination node by way of various intermediate nodes, thereby maintaining network connectivity [10] and applicability of MANET depends heavily on cooperation between nodes in such a dynamic environment[11]

III. AODV

Ad hoc on-demand distance vector (AODV)[4] routing protocol uses an on demand approach for finding route that is, a route is establish only when it is required by a source node for transmitting data packets. It allows all mobile nodes, to pass messages through their neighbors to nodes with which they cannot directly communicate. AODV does this by discovering the routes along which messages can be passed. AODV makes sure these routes do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in routes and can create new routes if there is an error. AODV defines three types of control messages for route.

RREQ - When one node needs to send a message to another node that is not its Neighbor it broadcasts a Route Request (RREQ) message. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number which serves as a unique ID

RREP - A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ”precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination [8]. The main advantage of this protocol is that routes are established on demand and destination sequence number is used to find the latest route to the destination. The proper maintenance of sequence numbers is crucial to keeping AODV loop-free and thereby avoiding the “counting to infinity” problem. One of the disadvantages of this protocol is that multiple RouteReply packets in response to a single RouteRequest Packet can lead to heavy control overhead. Another disadvantage of AODV is that the periodic beconing leads to unnecessary bandwidth consumption [9].

IV. BLACK HOLE ATTACK

It’s an analogy to the black hole in the universe in which things disappear. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, all the data traffic passing through it.

During the route discovery process, the source node sends route discovery packets (RREQ) to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. As show in figure 2.3 source node ‘A’ want to send data to destination node ‘D’, so node ‘A’ broadcast RREQ message all neighbors nodes ‘B’ and ‘M’ to find shortest or fresh route to destination node ‘D’. ‘M’ is malicious node and cannot check its routing table and immediately reply with false RREP message and cannot broadcast RREQ message to node ‘E’. After receiving RREP message from ‘M’ source node ‘A’ assume route discovery process is complete and shortest path to destination node ‘D’ through node ‘M’ and start to sending data to node ‘M’, and node ‘M’ silently dropped all incoming data to it without informing the source that the data did not reach its intended recipient destination node ‘D’. Thus the packets attracted by the black hole node will not reach the destination. The detection of Black holes in ad hoc networks is still considered to be a challenging task. So during the black hole attack performance of network goes very down, to eliminate the effect of this black hole attack in the network we propose a trust based RTP method to black hole attack prevention in the network.

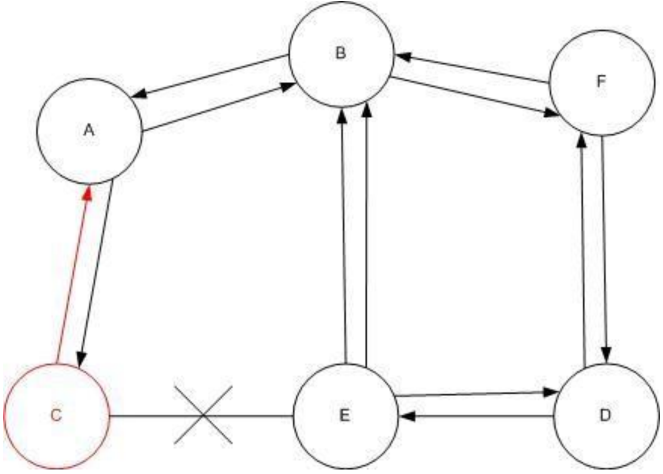


Figure-1 Black hole attack

V. PROPOSED APPROACH & ALGORITHM

Malicious node trust calculation is a critical issue in mobile ad network. For this purpose this work proposes a novel approach for Recommendation Trust Proxy (RTP) Algorithm[2]. In this mechanism route discovery can be achieved through a routing decision based on trust sequence certificate exchange through RTP proxy node which is an additional node in node group having extra responsibility of trust calculation. This RTP node will act as monitoring node for routing decision based on given steps for malicious node detection. To analyze the result of proposed mechanism this work uses AODV routing protocol. In AODV while discovering the route the sender node will send a RREQ packet to each neighbour node & will expect a RREP packet for existence of route. The node behaving as a malicious node will reply fast irrespective of legitimate node, due to this malicious node looks like active shortest link. Thus source node will add this malicious node in its routing table which causes packet drop or denial of service attack. Considering the above problem this work will also adds an additional wait of 20 sec for reply of other nodes. During this wait period RTP proxy node comes into act for authenticity of each neighbour node through trust certificate exchange in a proper sequence. In this approach firstly the trust of each node is calculated through the previous participation of node in data transmission. This trust must be more than minimum threshold which is decided by the node behaviour and issue a specific trust certificate to that node. This certificate is exchange with the entire neighbour nodes in a sequence & routing table of each is updated with the current information. Those nodes who want to participate in data transfer must have at least two trust certificates in a sequence. Now after this routing decision is made on the basis that the node having less than two certificates from previous & next neighbour is identify as the malicious node. After this detection RTP proxy node will transmit a recommendation message of malicious alert & a trust table to entire nodes in a network range. Every node receiving this message must do updates in their routing table with this authenticity detection & deletes the malicious node. RTP algorithm used to identify the malicious behaviour on the basis of trust table which is been continuously updated & analyzing the nodes behaviour. In this every node inside a network must acquire two trust certificates from it's at least two nodes. The node having more than two trust certificate can be able to participate in data transfer. This trust certificates with the nodes parameter is stored in trust value table. This trust value table is recommended by proxy nodes & exchanged between other data aggregation server.

Algorithm

```
S: Source, D: Destination, W: Watcher Node, MN: Mobile
Node, RT: Record Table, TC: Trust Certificate;
Initiate AODV Transmission ()
S wants to communicate with D.
   RTP Starts new process for data transmission.
   For directional routing the node must transmit        the
packet in specific range
   S broadcast the RREQ //after every 3 sec for latest updates
          //During this period RTP Start sensing the network
   D replies with RREP
          //Malicious node Reply very fast without
          checking its RT
   RTP Initiates if (Reply< Set Timestamp)
         MN uses RTP to contain RT
             //Stores trust value of its all preceding
               and successor nodes
    //Condition Check
    If (Node=New node)
      Assign initial Trust Value=0;
Else //For existing node Calculate threshold & trust by
Historical Data Analysis
If (Trust value>= Threshold) // Check
      Behaviour Ok;
Else
     Verify Malicious behavior;
RTP Issues Trust certificate //To every successor node
If (TC>=2) //Verify trust certificate, Count must be more that
2
     Not malicious node;
End if (TC<2)
     Black hole node;
Remove Entry from RT
Exchange Trust Value Table between other nodes.
Send Message to delete entries from other nodes RT
Exit RTP;
```

VI. SIMULATION OF BLACKHOLE ATTACK

Routing protocol AODV is under the analysis for this paper. The Linux UBUNTU OS10.10 is used to run the Simulating Software NS2 (Network Simulator 2) version 2.34 for the performance evaluation. The performance is observed at various pause time and intervals with the number of nodes. In this situation 30 nodes will be simulated which move randomly 4500m X 3200 m range. There are modifications done to the original AODV.CC and AODV.H files of the NS2 to simulate the Black Hole behaviour.

TABLE SIMULATION PARAMETERS

Examined Protocol	AODV
Simulation time	100 seconds
Number of Nodes	30
Transmission Range	250m
Movement Model	Random way point
Propagation model	Tow-Ray Ground Reflection
Traffic Type	CBR(UDP)
Payload size	512 bytes
Maximum speed	20m/s
Malicious nodes	1

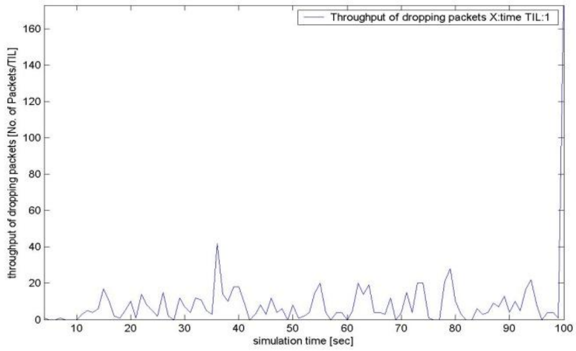
VII. V. RESULTS

The result of the simulation were analysed for various time span, the performance of the AODV goes down to 40% - 60%. This means packets are dropped and the performance of the network decreased to very high level. The performance graphs is plotted on the trace graph and the performance is analysed from this though graphs.

Throughput: it indicates the fraction of channel capacity used for successful data transmission.

Average End-to-End Delay: End-to-End Delay can be defined as the time a packet takes to travel from source to destination. Average End-to-End Delay is the average of the end-to-end delays taken over all received packets.

Node Mobility: Node mobility indicates the mobility speed of nodes



.

Figure-2 Throughput of dropping packets without Black hole attack

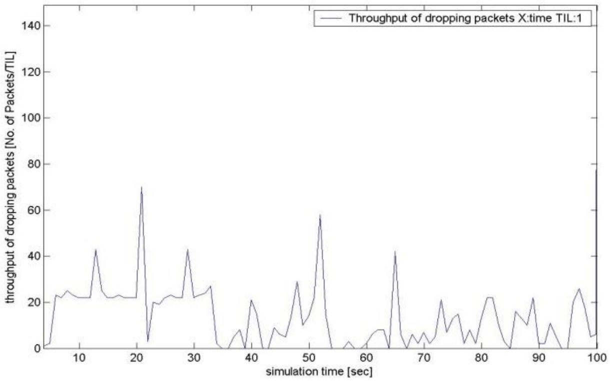


Figure-3 Throughput of dropping packets with Black hole attack

Figure 2 and Figure 3 shows the effect of throughput for AODV protocol when node mobility is increased. The result shows the cases, without black hole and with black hole attack on AODV. It has been measured that throughput decreases with black hole nodes in the Ad hoc network on AODV routing protocol as compared to without blackhole nodes.

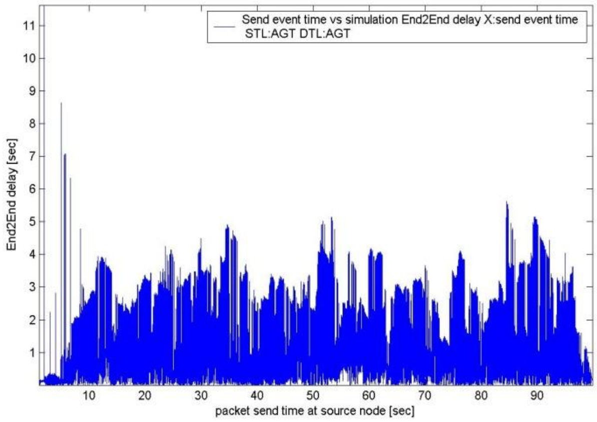


Figure -4 End-to-End Delay without Black Hole Attack

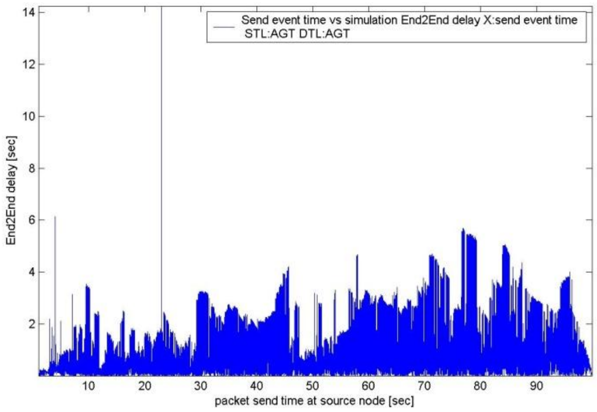


Figure -5 End-to-End Delay with Black Hole Attack

From the figure 4 to 5 it can be observed that, there is slight increase in the average end-to-end delay without the effect of black hole, as compared to the effect of black hole attack, This is due to the immediate reply from the malicious node i.e. the nature of malicious node here is it would not check its routing table

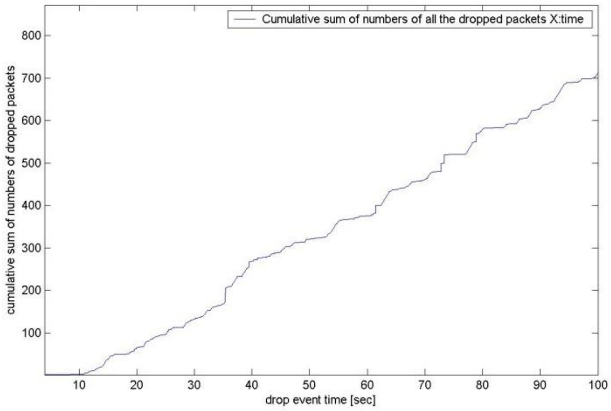


Figure-6 Average packet dropping ratio without Black Hole Attack

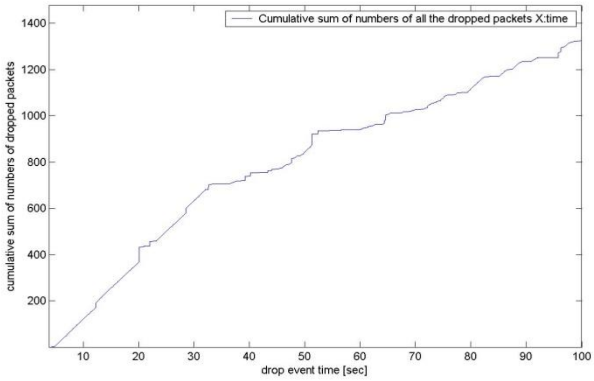


Figure-7 Average Packet dropping Ratio With black hole attack

It is observed from the figure 8 that, average packet dropping ration between the nodes is more without the black hole attack, as compared to the Average Packet dropping ratio between the nodes with the effect of black hole attack. This is due to the malicious nodes provides the path with fewer number of nodes, or smaller path.

VIII. CONCLUSION

Wireless Ad-Hoc Networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. In this paper the effect of packet delivery ratio, Throughput, and End-to-End Delay has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio, Throughput, and End-to-End Delay, as shown in fig. 2-7. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of Cooperative Black holes in ad hoc networks is still considered to be a challenging task.

REFERANCES

[1] G. D He, C Chen, S Chen, J Bu & A B. Vasilakos, "ReTrust: Attack Resistant & Lightweight Trust, Management for Medical Sensor Network" in IEEE Transaction on IT in vol:-16, No 4, July 2012

[2] Ankit Gupta (Author himself) and Mahesh Malviya, "A Novel Recommendation Trus Proxy (RTP) Based Pre-emptive Malicious Node Detection Mechanism for AODV in MANET",International Journal of computer Science and Management Research (IJCSMR) Vol 2 Issue 6 June 2013 ISSN 2278-733X

[3] F. Bai, N. Sadagopan, and A. Helmy, "Important: A framework to systematically analyze the impact of mobility on performance of routing protocols for ad hoc networks," in IEEE INFOCOM, April 2003.

[4] S. Djahel, F Na¨ıt-abdesselam, Z. Zhang" Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION, 6 June 2010.

[5] C. Perkins, "(RFC) Request for Comments – 3561", Category: Experimental, Network, Working Group, July 2003.

[6] C. E. Parkins and E. M. Royer. "Ad hoc On-Demand Distance ", Proceeding of IEEE workshop on mobile computing System and Applications 1999, pp,90-100, Ferbary1999

[7] M. Rastogi, K. K. Ahirwar, A. Bansal H. "Traffic Generator Based Performance Evaluation of Proactive and Reactive Protocols of Mobile Ad-Hoc Networks" International Journal of Scientific & Technology Research Vol. 1, Issue 4, MAY 2012.

[8] http://moment.cs.ucsb.edu/AODV/

[9] C. Siva Ram Moorthy, B. S. Manoj: Ad hoc Wireless Network Architectures and Protocols, Prentice Hall, 2004.

[10] F. Bai, N. Sadagopan, and A. Helmy, "Important A frame-Work Systematically Analyze the Impact of Mobility on Performance of Routing Protocols for Ad Hoc Networks", IEEE INFOCOM, pp.383-403, April 2003.

[11] S. Djahel, F.Nait-Abdesselam, and Z. Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", IEEE Communications Surveys and tutorials, Vol. 13, No.4,pp. 658-672 November 2011.

Mr. Mahesh Chandra Malviya received his BE and Mtech degree in Computer Science & Engg from University of Rajiv Ghandi Bhopal. He is currently Asst. Professor & Head of Department of Computer Science & Engineering in Jawaharlal Institute of Technology "Vidhya Vihar" Borawan, (M.P), India. His research interest in network security and moblie technological

Mr Ankit Rajendra Gupta pursing his ME in software Engg. And received his BE in Computer Science & Engg from University of Rajiv Gandhi Bhopal. He is currently software developer in Quicsolv Technology at lead position. Interested research area is Mobile networking, Big data, Java framework.