IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.

www.ijiset.com

ISSN 2348 – 7968

Trust based solutions using counter strategies for Routing attacks in MANET

Prof. Ramya S Pure[1], Prof. Gouri Patil[2] and Prof. Mohammad Manzoor Hussain[3]

[1] Department of Computer Science and Engineering, G N D E C
Bidar, Karnataka-585403, INDIA

[2] Department of Computer Science and Engineering, G N D E C
Bidar, Karnataka-585403, INDIA

[3] Department of Information Science and Engineering, G N D E C
Bidar, Karnataka-585403, INDIA

Abstract— *A Mobile ad-hoc Network (MANET) is a collection of wireless mobile nodes which are capable of communicating with each other without the help of network infrastructure. MANETs possess unique characteristics of self-organizing and self –configuring. The important applications of ad-hoc networks are military operations, disaster management etc. Routing protocol plays a major role to prevent routing attacks. Security attacks can be launched towards any layer of the protocol stack. Routing in MANET is a challenging task because of its unique characteristics such as dynamic networking topology, limited band width and battery power etc. Now a days, many researches are going on in this area and several efficient routing protocols have been proposed for Mobile ad-hoc Network. They are vulnerable to attacks due to the presence of malicious nodes. Therefore security is an important factor for the establishment of desirable Mobile ad-hoc Networks. The overall performance of MANET depends on the cooperation and trust among the mobile nodes. Our proposed trust model is designed over ad-hoc On-demand distance vector routing protocol (AODV). So that computation overhead can be reduced and also trustworthiness of routing procedure can be guaranteed. The proposed routing algorithm adds a field which stores trust value or node's trust on its neighbors. Based on the trust value, the routing information will be transmitted to highest trust valued node. This method pertaining to mobile ad-hoc networks can provide secured routing and can also improve the network throughput. In this paper, we will also walk through some of the common attacks on the Network layer such as Blackhole attack, Wormhole attack and the Grayhole attack which fall under the category of Denial-of-Service Attack (DoS)*

Keywords— *Mobile Adhoc Networks, Security ,Adhoc on demand distance vector routing, Trust based Adhoc on demand distance vector Routing, Trust based routing request, Trust based routing reply, Trust based warning message*

I. Introduction

Mobile ad-hoc network is a collection of mobile node or terminals that communicate with each other by maintaining connectivity in a decentralized manner. Here each node act as both host and a router. For the mode of operation considered ,ad-hoc networks are peer to peer multi hop wireless networks where packet information are transmitted in a store and forward manner from source to destination via intermediate nodes. Routing in MANET depends on many factors which include topology, selection of routes, initiation of request etc. Mobile ad-hoc networks are prone to many security issues due to their lack of infrastructure. If the routing protocols are not secured enough, a malicious node can easily disrupt its route discovery during the data forwarding phase. For the design and analysis of secure mobile networks, trust is an important aspect that we need to consider.. A secured routing mechanism always relies on the trustworthiness of other nodes. The two primary motivations for this trust model are firstly, it helps to identify malicious entities. Secondly, trust model can improve network performance. In this paper we propose a trust model to maintain a trust relationship among nodes and to make a secured routing decision. We evaluate our trust model using NS2 simulator and the experimental results proves that our trust model is more effective compared to normal AODV. The rest of the paper is structured as follows. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure[2] .Figure 1 is an image of a Mobile Adhoc Network.

ISSN 2348 – 7968

On the other side, the inherent characteristics of MANET leads to some major issues such as routing protocols, power constraints, mobility management, Quality of Service (QoS) topology dynamically, lack of central monitoring and management.

Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the on-going communication .In this paper, we have surveyed the various Dos attacks and their counter strategies. The rest of the paper is organized as follows. Dos attacks like Blackhole , Wormhole and the Grayhole attacks along with proposed strategies for prevention and detection of same

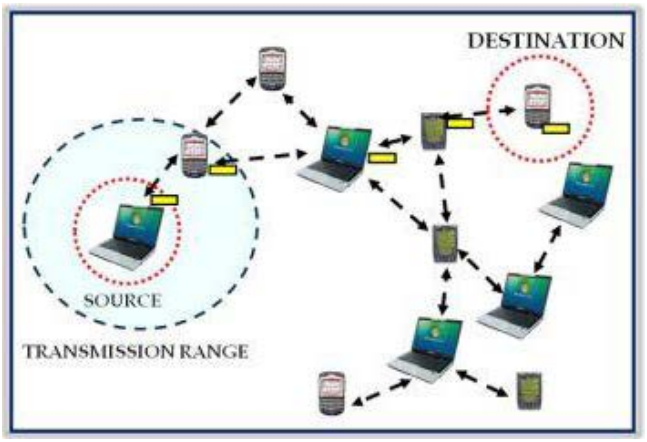

Figure 1: Mobile Adhoc Network

II. Routing in manet

There are many protocols developed for MANETs. They can be mainly classified into two categories:

A. Proactive routing protocol (Table driven): In this routing scheme every node continuously maintains complete routing information of the network. This is achieved by flooding network periodically with network status information to find out any possible change in network topology. Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. A new set of routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm

B.Reactive routing protocol (Demand driven): Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the and security. MANETs often suffer from security attacks because of its features like open medium, changing its

route. Rapidly changing wireless network may break active route and cause subsequent route search.

C.Hybrid routing protocol: Is a combination of good characteristics of the above 2 stated protocols. Efficiency of hybrid protocols may vary with the number of nodes and the amount of traffic decides the reaction to demand.

The main routing protocols coming under table driven category are DSDV, OLSR, WRP and CGSR.

A. Destination sequenced distance vector routing (DSDV)

This table driven routing protocol is based on Bellman-ford routing algorithm. Each mobile node maintains a routing table with a route to every destination in the network and each such entry in routing table is marked with a sequence number. The sequence number allows distinguishing the stale route from new one and also helps to avoid loops during routing. If multiple routes are available for same destination, the most recent sequence numbers is used. If two updates have same sequence number, the route having smaller number of hops is considered. The updates in routing table should be broadcasted periodically in the network.

B. Optimized Link state Routing Protocol (OLSR)

OLSR is an IP routing protocol optimized for mobile ad-hoc networks which can also be used on wireless ad-hoc networks. OLSR inherits the stability of link state algorithm. In pure link state protocol, all the links with neighbour nodes are declared and are flooded in the entire network. OLSR is an optimization of a pure link state protocol for mobile ad-hoc networks. This protocol keeps the routes for all the destinations in the network. OLSR is particularly suitable for large and dense networks and it works completely in distributed manner and thus does not depend upon any central entity. It does not require any reliable transmission for its control messages. Each node sends its control messages periodically and can sustain a loss of some packets from time to time. OLSR performs hop by hop routing. Each node uses its most recent information to route a packet. Therefore when a node is moving, its packets can be successfully delivered to it. OLSR makes use of hello messages to find its one hop neighbours and its two hop neighbours through their responses. The sender can select its multi-point relay (MPR) based on the one hop node that offers the best routes to the two hop nodes

C. Cluster Head Gateway Switch Routing (CGSR)

CGSR uses Cluster Head (CH) which controls the group of ad-hoc nodes so that channel access, routing and bandwidth allocation can be achieved. The selection of CH and

ISSN 2348 – 7968

identification of its cluster is a complex task. When cluster has been identified, distributed algorithm is used for electing the CH. CGSR uses DSDV (Destination sequenced distance vector routing) as the underlying protocol and shares the overhead with the same. This protocol modifies DSDV to use a hierarchical cluster head to gateway routing approach. The gateway nodes are within the communication range of two or more CHs. The packet transmitted is first passed to its CH. From there to the gateway node and then to another CH. This will continues until the packet reaches the CH of destination. Then the packet is transmitted o the destination. For using this routing scheme, each node must maintain a Cluster Member Table (CMT) which stores the destination CH for each nod in the network.

D. Wireless Routing Protocol (WRP)

In this routing protocol, each node maintains four tables which include distance table, routing table, link cost table, MRL (Message retransmission list table). The MRL record about the details of the message that need to be retransmitted and also about neighbours acknowledgement during retransmission. For this, each entry in the MRL has a sequence number of the update message, retransmission counter and list of updates sent to the update message. Nodes discovers each other through hello message and when they receives a hello message from a new node, it adds the new node to its routing table and sends the new node ,a copy of its routing table. A node has to send messages to its neighbours within a certain time to ensure connectivity. If a node does not have any messages to send, it must send periodically a hello message to ensure its connectivity. Otherwise the neighbouring nodes might consider the absence of messages as the failure of link.
The various Source initiated on demand Routing protocols are AODV, DSR, TORA, ABR and SSR.

E. Ad-hoc On demand Distance Vector Routing (AODV)

AODV protocol is a significant improvement over DSDV. The nodes which are not in a particular path do not maintain routing information and also they do not participate in the routing table exchanges. So the number of broadcasts required to create routes via AODV is minimized. When the source node needs to send a message to destination node, the source node sends a route request (RREQ) message to all its neighbours. This will continue until the destination or the neighbouring node finds a route to the destination. Similar to DSDV, AODV also uses sequence number to ensure that all routes are loop free and they contain the most recent information. Each node has a broadcast ID which is incremented each time, the node initiates a RREQ. The nodes IP address together with broadcast ID identifies every RREQ. When the initiator node send RREQ message, the intermediate nodes verifies only if they have a route to destination with sequence number greater than or equal to that contained in the RREQ. When RREQ message reaches destination, it sends back a unicast route reply (RREP) message to the neighbour from which it receives the first copy of RREQ. The RREP message continues to travel back along the reverse path till it reaches the initiator. There is also a route timer associated with a route entry.

F. *Dynamic Source Routing (DSR)*

This is an on-demand routing protocol based on source routing. The mobile nodes maintain all source routes in a cache. The cache will get updated when new routes are discovered. This protocol has two phases: route discovery and route maintenance. When a mobile node has a message to send, it checks the cache to find whether it has route to the destination. If there is any active route to destination, it is used to send message. Otherwise they initiates route discovery by broadcasting a route request packet. The route request contains the destination address, source address and a unique ID. Each node that receives the route request message checks whether it has route to the destination. If it does not, it adds its own address to the route record of packet and then rebroadcasts the packet. When route request reaches the destination, a route reply is generated. Now the route record indicates all the hops taken to reach the destination. The route maintenance is done using acknowledgements or route error packets. The acknowledgments are used to verify that the route links are operating without any faults. When a node receives a route error packet, it removes the hop that has error from its cache.

G. *Temporarily Ordered Routing Algorithm (TORA)*

TORA is a loop free and highly adaptive distributed algorithm based on link reversal. It can also exhibits multipath routing capability. The main advantage of TORA is that, it can operate smoothly in a highly dynamic environment. This protocol has three main phases which includes route creation, route maintenance and route erasure. A separate directed acyclic graph (DAG) is maintained by each node. When a route to a particular destination is required, the initiator will broadcasts a QUERY packet containing destination address. This query message will propagate through network till it reaches the destination or any intermediate node that contains route to destination. This node can respond to an UPDATE message that contains its own height with respect to the destination. When a node receives the UPDATE message, it in turn sets its height to a value greater than that of its neighbours from which UPDATE message has been received. When a node finds a network partition, it generates a CLEAR packet that can reset the routing state and removes invalid routes from the network. In the case of route creation and maintenance phases, the mobile nodes use a height metric to establish a DAG which is rooted to destination. Then links are assigned in upstream or downstream direction according to the height of neighbours. When a node moves, DAG becomes invalid.

ISSN 2348 – 7968

TORA is partially proactive and reactive. It is reactive because its route creation is done on demand and proactiveness is due to its multiple routing option available during link failures.

H. *Associative Based Routing (ABR)*

ABR is free from loops, deadlocks and packet duplicates. This protocol uses a new routing metric called association stability which is characterized by connection stability of one node with respect to another node over time and space. If association stability is high, it means that there is a low state of node mobility. A new route is selected based on the degree of association stability. Similar to most other protocols, each node in ABR periodically transmits a beacon signal to broadcast its existence. The three phases of ABR are route discovery, route reconstruction (RRC) and route deletion. In route discovery phase, a broadcast query awaits reply (BQ-REPLY). All nodes other than the destination that receive the BQ (Broadcast query message) append their addresses and the associativity ticks with their neighbours along with Qos information to the BQ message. The destination can select the best route from all the packets received by examining the associativity ticks along the path. Then the destination node send back he REPLY packet to the source along the selected path. The nodes propagating the REPLY message mark their route as active routes. The RRC phase kicks when there exist a movement of nodes along the path. When source node moves, a BQ-REPLY is initiated and when destination moves, the immediate upstream node erases its route. It then checks whether the destination is still reachable or not by localized query (LQ). If the destination receives the LQ packet, it sends back a REPLY message with best practical route. Otherwise the initiating node times out and the process backtracks to the next upstream node. This is done by sending RN [0] message to the next upstream node, which erases the invalid route and then invokes the LQ [H] process. If this process backtracks to more than halfway to the source node, the LQ process is discontinued and then a new BQ process gets initiated at the source. When route is no longer needed, the source node broadcasts a route delete (RD) message so that routing table of all the nodes gets updated.

I. *Signal Stability-Based Routing (SSR)*

SSR is another on-demand routing protocol that selects routes depending on the signal strength between nodes. SSR can be divided into two cooperative protocols: the dynamic routing protocol (DRP) and static routing protocol (SRP).The DRP protocol is responsible for maintaining signal stability table (SST) and routing table(RT). The SST keeps the record of the signal strengths of the neighbouring nodes. The strength of the signal is recorded as either strong or weak channel and all the transmissions are processed by DRP. After updating the table entries, the DRP passes its received packet to SRP. Now SRP processes the packet as follows: It passes the packet to the stack, if it is the intended receiver otherwise it looks at the destination in the RT. These route requests are propagated throughout the network. They are forwarded to the next hop only if they were received over a strong channel and were not previously processed. The DRP now sends a route-reply message back to the initiator through the reverse route. The DRP of all the nodes along the reverse path updates their RTs accordingly. The route search packets that arrives at the destination have to choose paths that have strong stability. But there is a chance that a no route exists with all strong channels. In that case, the source has a time out associated with the route search. When a link fails, the intermediate node informs the source through an error message. The source sends erase message to inform other nodes about the broken link. The source then reinitiates the route search process to find a new path the destination.

III. SECURITY CONCERNS

Security is an essential component for the widespread use of MANET. The unique characteristic of MANET i.e. dynamic and continuously changing network topology, resource constraints such as limited battery power and bandwidth makes it difficult to use the existing security schemes for the conventional networks directly for MANETs [4]. An attacker by passively or actively attacking on MANET can violate one or the entire security goal such as availability, confidentiality, integrity, authentication, non-repudiation and access control [5]. TABLE-I shows the classification of attacks with their characteristic feature and few examples. Both the type of attacks can be launched on any of the layers of protocol stack.
Figure 2 shows various examples of the attacks at different layers.

ISSN 2348 – 7968

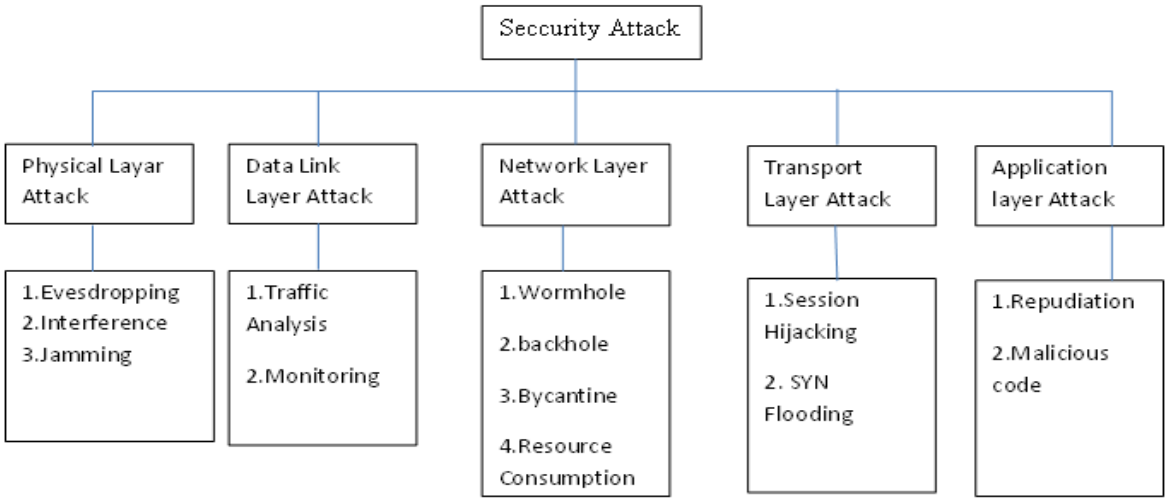

Figure 2: Attacks on different layers of protocol attack

IV.DOS ATTACKS

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection. Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider.

A. Blackhole attack

Black hole attack is one of the kinds of Denial Of Service (DoS) attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [26]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets 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 RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply. The attacker now drops the received messages instead of relaying them as the protocol requires

Operation of Black Hole Attack: In the figure 4, imagine a malicious node "3". When node "1" broadcasts a RREQ packet, nodes "2", and "3" receive it. Node "3", being a malicious node, does not check up with its routing table for the requested route to node "4". Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node "1" receives the RREP from "3" ahead of the RREP from "2". Node "1" assumes that the route through "3" is the shortest route and sends any packet to the destination through it. When the node "1" sends data to "3", it absorbs all the data and thus behaves like a Black hole[24]. In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number. Upon receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with and RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets

will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination

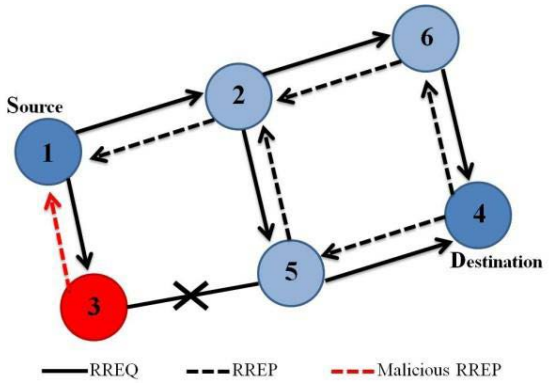

Figure 3: Blackhole attack

B. Wormhole Attack

The Wormhole attack, is a kind of tunnelling attack which is dangerous and damaging to defend against even though the routing information is confidential, authenticated or encrypted [11].Under this attack two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbours. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there [12]. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through thewormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network [14]. On receiving this false information, other nodes may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from establishing links between the source and the destination [16]. More the number of end-to-end paths passing through Wormhole Link, stronger the attack.

O**peration of Wormhole attack:** Consider Figure 5 in which node A sends RREQ to node H, and nodes C and G are malicious nodes having an out-of-band channel between them. Node C “tunnels” the RREQ to G , which is legitimate neighbour of H [18]. H gets two RREQ –A-C-G-H and A-B-D-F-H. The first route is shorter and faster than the second, and chosen by H. Since the transmission between two nodes has rely on relay nodes, many routing protocols have been proposed for ad hoc network. In a wormhole attack, attackers “tunnel” packets to another area of the network bypassing normal routes as shown in Figure 5. The resulting route through the wormhole may have lower hop count than normal routes [19]. In with this leverage, attackers using wormhole can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DOS attack . The entire routing system in MANET can even be brought down using the wormhole attack [13].Malicious nodes C and G along with the Wormhole link are not visible in the route, and also the Wormhole attacker is hidden from the higher layers.

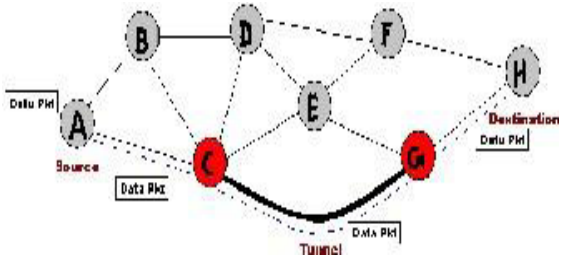

Figure 4: Wormhole attack

C. Grayhole Attack

Grayhole attack is an extension of Blackhole attack in which a malicious node is exceptionally unpredictable. Gray hole attack has two phases [11]. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainty [14]. A Gray hole may exhibit its malicious behavior in different ways [11]. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A Gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult and thus degrading network performance [27]. 1. Operation of Grayhole Attack: Figure 6 shows a MANET using AODV routing protocol. Node 3 and 5 initially behaves as ordinary nodes and forwards all packets coming from other nodes. After some time, these same nodes (3 and 5) behave maliciously and starts dropping packets send via

ISSN 2348 – 7968

node 1 and 7 towards the destination. After some time, node 3 and 5 acts as normal nodes. Thus behaving maliciously for a certain period of time. Due to lack of security mechanism in AODV, malicious nodes can perform many attacks just by not following the protocol rules.

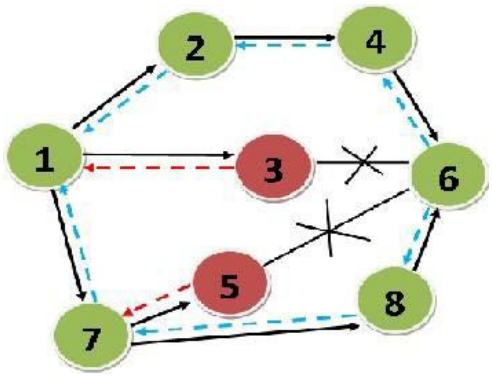

Figure 5: Grayhole attack

IV. EXPERIMENTAL ANALYSIS

We implemented our trust based model, TBAODV in the network simulator, NS2. The nodes communicated across each other using five constant bit rate (CBR).In movement scenario, a node moves towards the destination at a uniform speed. The maximum speed was limited to 10 m/s and we ran the simulation for constant bit rate of 1, 5 and 10 m/s. In order to analyse the performance of our TBAODV, we compared it with the performance of normal AODV. First we analyse the normal AODV. Then some uncooperative nodes are added to AODV network and performance analysis is done. After that our proposed model TBAODV was added to the normal AODV. This protocol was simulated with 1 to 100 nodes and also 100 to 150. The number of packets reached is same as normal AODV. So we can say that TBAODV is as similar as AODV in delivering packets. And when we increase the number of selfish nodes, the number of packets received at the destination decreases because of packet drop rate. In our proposed method, it had partially affected because the selfish nodes are discovered at each time. In our model, the number of packets reached is more compared to AODV. That is due to the use of local table at each node which consists of trust values for establishing the route. The average latency of data packets is higher in TBAODV compared to normal AODV. And also in the case of normal AODV, throughput has a sudden decrease when number of selfish node is increased. From our work, we can conclude that our proposed model, TBAODV is more efficient than normal AODV.

1)Packet Delivery ratio: Here the packet delivery ratio for normal AODV and TBAODV is measured with number of nodes varying from 1 to 150.We changed the speed of nodes and the number of selfish nodes to compare the results.

TABLE I
SIMULAION PARAMETRS

Parameters	***Values***
Protocol Analysed	AODV
Traffic	UDP
Packet size	1024 bytes
Data rate	100 kb/s
Minimum speed	1 m/s
Simulation time	800s
Area	100 x 100 m
Transmission range	100 m

In both AODV and TBAODV have almost identical number of packets received the destination. This shows that the TBAODV is almost same as normal AODV in case of efficiency in delivery of packets and finding routes to the destination. In both AODV and TBAODV, when speed of node increases, the number of packets reached at the destination decreases. When malicious nodes are added, the number of packets reached at the destination decreases because of the packet drop. In the case of TBAODV, it is affected partially, as the malicious node will be identified and isolated from the network.

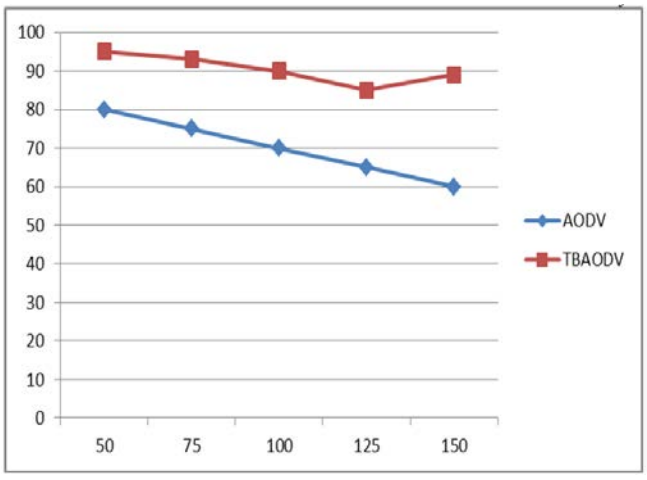

Figure 6: Packet Delivery Ration Vs. Number of Nodes

2) Average Latency: Here the average latency of normal AODV and TBAODV has been measured. The number of malicious nodes are varied to compare the results. From the graph it is very clear that TBAODV has a higher latency of data packets compared to normal AODV. This is because in TBAODV, at each hop and also before sending packet data

ISSN 2348 – 7968

the trustworthiness of each node is calculated. When the number of malicious node increases, the TBAODV will choose a longer selfish free route to destination with extra hops.

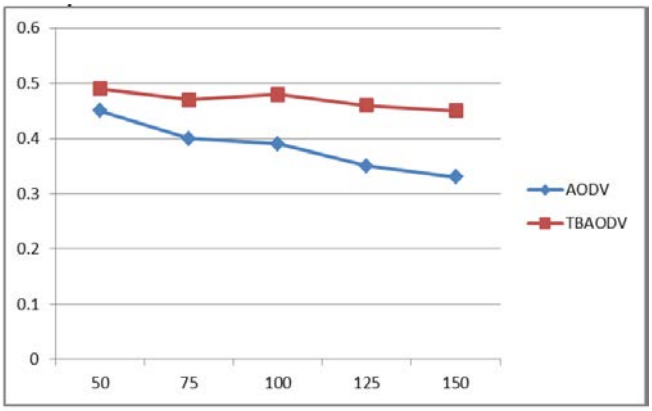

Figure 7: Average Latency Vs. Number of Nodes Varies

3) Network Throughput: The graphical result shows the throughput of normal AODV and TBAODV with varying speed and different number of malicious nodes. It shows that there is a sudden decrease in network throughput with the increase of malicious nodes. When there are no selfish nodes in the network, both AODV and TBAODV have almost identical network throughput values. From this we conclude that, TBAODV is as efficient as AODV in delivering the data packets. Also in both AODV and TBAODV when the speed of node increases the network throughput decreases. When the number of malicious node increases, the throughput decreases because of the packet drop ratio during data transfer. The packet drop affect normal AODV. But in the case of TBAODV, it will get affected only partially as the malicious node will be identified and thrown out of the network.

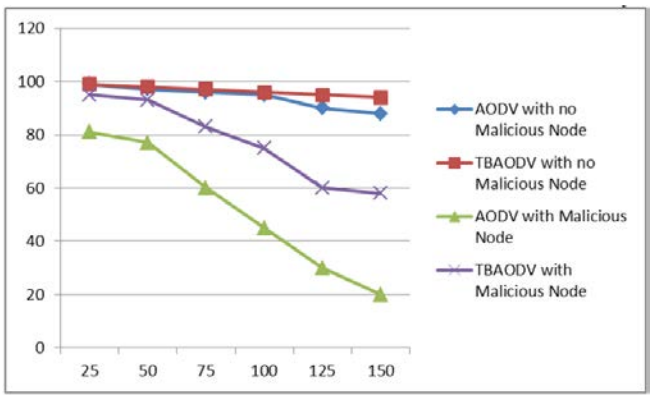

Figure 8: Throughput (%) Vs. Node Speed (ms)

Algorithm for different functions used in packet transmission and reception in NS2 simulator is as follows.

1) Initialize trust value as 50 for each and every nodes using assign_trust_value () function.

2) In order to print trust value we use print_trust_value () function.

3) Then source node will broadcast request to all neighbouring nodes using send_request () function. Hop count is also initialized in this function.

4) Neighbouring nodes will receive the request message and then it will check whether it is destination or not. If it is the destination it will send send_reply () function otherwise it will forward request to its neighbouring nodes. This will check the receive_request () function.

5) After confirming that it is not the neighbouring node, it will forward the request further to its entire neighbouring node using forward_request () function. Hop count is increased at each node.

6) If it is the destination, it will send reply using send_reply () function. Then trust value 100 is assigned all nodes in the path of source to destination. Now source becomes destination of current node.

7) After receiving the reply, decision will be taken on whether the index node is the destination node or not using receive_reply () function. If it is not the destination, it will forward the reply.

V. CONCLUSION AND FUTURE WORK

In this paper, we propose a trust based solution for AODV protocol. Due to the low transmission power of ad-hoc node, trust among nodes is important for forwarding packets from one node to another. This proposed protocol extends the routing table and the routing messages of AODV with trust information. This trust information gets updated after monitoring the neighbouring nodes. Instead of performing signature verification at every routing packet, we combine the opinions from different nodes so that the computation overhead can be minimized and also trustworthiness of routing procedures can be guaranteed. Based on this trust factor, routing takes place. This saves nodes transmission power by avoiding unnecessary transmission and also its bandwidth. Frequently changing topology of MANET forms the basis for the need of design of most of the routing protocols but security issues have been left ignored. This paper provides brief view about routing as well as security concerns for MANET. We described operations of DoS attacks like Blackhole, Wormhole and Grayhole attacks and surveyed some of the existing solutions for each of them.

REFERENCES

[1] Zheng Yan, Peng Zhang, Teemupekka Virtanen, “Trust Evaluation Based Security Solution in Ad Hoc Networks”, Nokia Venture Organization, Nokia Group, Helsinki, Finland, 2002 IEEE.

[2] Jared Cordasco Susanne Wetzel, "Cryptographic Versus Trust-based Methods For MANET Routing Security," Department of Computer Science Stevens Institute of Technology Hoboken, New Jersey USA, Electronic Notes in Theoretical Computer Science , pp.131–140, 20

[3] Yan Lindsay Sun, Wei Yu, Zhu Han, K. J. Ray Liu, "Information Theoretic Framework of Trust Modelling And Evaluation for Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, Vol.24,February 2006.

[4] Sandhya Khurana, Neelima Gupta, Nagender Aneja, "Reliable Ad-hoc On-demand Distance Vector Routing Protocol", The International Conference on Systems (ICONS 2006)", and The First International Conference on Mobile Communications and Learning , 2006 IEEE.

[5] Okeke, S. S. N, Nwabueze, C. A, "mobile ad hoc network architecture and implementationAnalysis", Natural and Applied Sciences Journal Vol.11, 2008.

[6] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE communications surveys & tutorials, vol. 14, 2012.

[7] Mehdi Maleknasab, Moazam Bidaki, Ali Harounabadi, "Trust-Based Clustering in Mobile Ad Hoc Networks: Challenges and Issues", International Journal of Security and Its Applications Vol.7, pp.321 342, 2013.

[8] Sujata Wasudeorao Wankhade, P. R. Deshmukh, "Comparison of AODV and RAODV Routing Protocols in Mobile Ad Hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1,08.

[9]Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[10] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS",

[11] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[12] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[13] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-InternetCommunication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[14] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[15] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[16] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[17] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[18] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[19] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[20] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[21] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

ISSN 2348 – 7968

[22] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi- path," IEEE Wireless Commuunication. and Networking Conference, 2005.

[23] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[24] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[25] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[26] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp.21-26.

[27] Gao Xiaopeng and Chen Wei,"A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", 2007 IFIP International Conference on Network and Parallel Computing – Workshops, 2007, pp.209-214.