Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Trust Based Solution for Mobile Ad-hoc Networks

Dr N.Radhika*, Thejiya V
Department of Computer Science
Amrita Vishwa Vidyapeetham, 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. The important applications of ad-hoc networks are military operations, disaster management etc. In all these and other networking applications, security in routing protocol plays a major role to prevent routing attacks. 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. But many of these protocols assume a trusted and cooperative environment. 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. To improve security in Mobile ad-hoc Networks, it is very important to evaluate the trustworthiness of the nodes. Our proposed trust model is designed over ad-hoc On-demand distance vector routing protocol (AODV). Instead of performing signature verification or any other cryptographic schemes at every packet, this model can do trusted route discovery for each packet. 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 neighbours. 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.

Keywords*— Mobile Adhoc Networks, 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. Since the network topology is generally dynamic, the connectivity among nodes varies according to the nodes departure. 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. Security approaches used for fixed networks cannot be applied for ad-hoc networks due to its prominent characteristics. For the design and analysis of secure mobile networks, trust is an important aspect that we need to consider. Routing in MANET is a cooperative process where the routing information is relayed on to the neighbouring nodes. 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. Section II describes the Routing Protocol overviews in mobile ad-hoc networks. Section III presents literature survey about various existing trust based AODV for MANET. Section IV describes the proposed methodology. The paper is concluded in section V and the references to this paper are mentioned at last.

II. ROUTING PROTOCOL OVERVIEWS

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

Table-driven: This table driven routing protocols mainly use proactive schemes. They maintain up to date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables for storing routing information. Any changes in the network topology can be reflected by propagating updates throughout the network for network consistency.

On demand: This type of routing protocol creates routes only when source node requires it. This process will get completed only when a route is found, or all possible route permutations have been examined.

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. When the routes fluctuate frequently, it will result in large network traffic and there occurs the need of larger broadcasts. In order to avoid such broadcasts, the mobile nodes need to consider settling time of routes. So that the nodes can delay the update broadcasts by settling time, during which a better route can be found and this can reduce the network traffic. 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. Due to its proactive nature, it has the advantage of having the routes immediately available when needed. 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. So that this protocol is beneficial for the traffic patterns where a large subnet of nodes are communicating with each other. 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. The protocol does not require an in-order delivery of its messages. 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. It relies on selection of multipoint relays and calculates its route to all nodes through these nodes. 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. To disseminate neighbour information OLSR uses topology control (TC) messages along with MPR.

C. *Cluster Head Gateway Switch Routing (CGSR)*

This protocol differs from other previous protocols because of its addressing and network organization scheme. 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 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. These CMTs are broadcasted periodically by the nodes using DSDV algorithm. When a particular node receives CMT information from its neighbours, it can update its own information too. Each node also maintains a routing table to find the next hop to reach the destination. When transmitting a packet, the node looks at the CMT and the routing table, to determine the nearest CH along the route o destination and to find the next hop to reach this CH.

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 process in TORA can be compared to that of water flowing down from a hill toward a sink node through tubes that can model the routes in the real network. The junction of tubes represent the nodes, the tube themselves represent the route links and the water in the tubes represents the packets flowing between nodes via route links towards destination. 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. 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)*

The main objective of this protocol is to find routes that are longer lived. 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. LITERATURE SURVEY

Most of the mobile ad-hoc networks are designed which is to focus on the efficiency and performance of the networks. The nodes in the ad-hoc networks are mobile and they communicate through direct radio links or by multi hop routing. Since ad-hoc networks can be deployed with relatively less cost, it is used for many commercial purposes. Ad-hoc networks do not have any predefined infrastructure, security in ad-hoc network become a weakness. The ad-hoc on demand distance vector (AODV) routing protocol is used in the proposed work for creating a trust model. Existing routing protocols uses shortest path method to find its destination. But the selected path will not be always best. Such path may be congested and may include malicious nodes also. Trust is an important feature for mobile ad-hoc networks. An untrustworthy node can cause considerable damage to MANET and it can also affect the quality and reliability of data. Therefore, computing the trust value will give a positive influence on the confidence in which each entity conducts transactions with various nodes. There are various trust computing approaches existed for MANET. In this paper we also compare the existing trust based AODV methods in MANET.

A. Secure Ad-hoc on demand distance vector Routing (SAODV)

The secure version of AODV is called secure AODV (SAODV). It supports various features like authentication, integrity etc. In order to maintain the collaborative feature of AODV, SAODV includes another feature which allows intermediate nodes to reply to RREQ message. This is called double signature. Which it means in addition to regular signature, it includes a second signature. Intermediate nodes can store this second signature in their routing table along with other routing information. If one of the nodes receives a RREQ message it can reply with RREP message similar to AODV. To achieve that intermediate node generates the RREP message which includes the signature of source node and signs the message with its own private key. As compared to AODV, SAODV does not require any additional messages. And the messages of SAODV are bigger in size because of digital signatures. It also requires heavy weighted asymmetric cryptographic operations. That is every time when a node generates a routing message, it must generate a signature and every time when it receives a routing message, it must verify a signature. These cause difficulties when double signature mechanism is used because it requires generation or verification of two signatures for a single message. SAODV allows to authenticate AODV routing data.

B. Security Aware Ad hoc Routing (SAR)

SAR incorporates security levels of nodes into traditional routing metrics. The important goal of SAR is to characterize and represent the trust values and trust relations associated with ad-hoc nodes and use these values for making routing decisions. In this case source node specifies the desired level of security in the RREQ and broadcast the packet. The intermediate node will forward the packet only if it can provide security or has the required authorization or trust level otherwise it will drop the RREQ message. If an end to end path has acquired security, the intermediate node will send a suitable modified RREP. In order to provide the integrated security metric for the requested route, SAR protocol integrates the trust level of a node and security attributes of a route. Addition to the security level and cryptographic techniques, a quality of protection (QoP) vector is used. It uses sequence number and time stamp to avoid replay attacks. The various attacks like modification, fabrication etc. can be stopped using digital signatures of the transmitted data. One of the drawbacks of SAR is that it requires encryption and decryption at each hop during the path discovery. The discovered route will be secure but it may not be the shortest route in terms of hop count.

C. Adaptive SAODV (A-SAODV)

ASAODV is a prototype implementation of SAODV. In this protocol, the intermediate node replies to RREQs only if it is not overloaded. Each node has a queue of routing messages to be signed or verified. Optimization is included in this protocol to avoid signing or verifying the same message twice. The routing performance of secured protocols is optimized using this A-SAODV protocol. It is a multithreaded application. The cryptographic operations are performed by a dedicated thread to avoid blocking or processing of messages and creates other thread to all other functions. Every node has queue of routing message and it has to be signed and verified. The length of queue denotes the load state of the routing thread. When a node processes a route request and it has necessary information to generate RREP, it first checks its routing message queue length. If the length of queue is below certain threshold, it replies otherwise it forwards the RREQ message without replying. In ASAODV the threshold value changes during execution. The same mechanism can be applied while generating a RREQ message in order to decide between a single signature and a double signature.

D. Reliable Ad-hoc On-demand Distance Vector Routing (RAODV)

The original AODV protocol has been extended by adding route discovery unit (RRDU) and reliable route reply unit (RRDU_REP). RRDU messages are send by source node to the destination at regular intervals along with the RRDU-ID.RRDU_REP is the response message of RRDU from destination node to source node. The RRDU_REP message can only be generated by the destination. The routing table format of RAODV is same as that of AODV except for the additional RL (Reliability List) field. An entry in RL field consists of source address, forward data packet (FDPC) and RRDU-ID. Similar to AODV, RAODV uses RREQ, RREP messages for route discovery and RERR, HELLO messages for route maintenance. It also uses RRDU and RRDU_REP messages for discovering the path and for maintaining reliability. The table 1 below shows the routing table entry of RAODV.

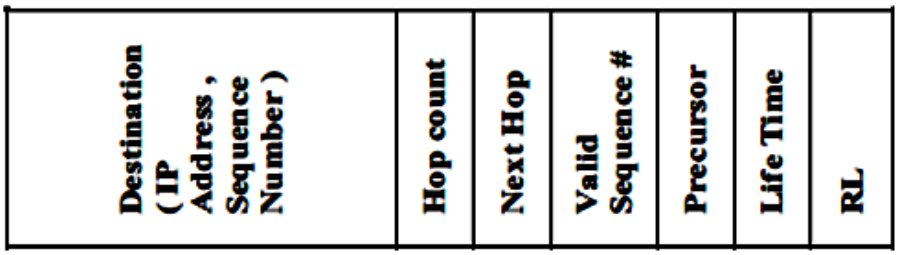

Fig 1: Routing Table Entry of RAODV [4]

E. *ARAN (Authenticated Routing for Ad-hoc Networks)*

ARAN uses public key cryptographic mechanisms to defeat all identified attacks. Therefore it requires the use of a trusted certificate server. This protocol introduces authentication, message integrity and non-repudiation to routing in an ad-hoc environment, as a result of minimum security policy. ARAN consists of certification process followed by a route instantiation process which can guarantee end to end authentication. This protocol is simple compared to most non-secured ad-hoc routing protocols. The route discovery in ARAN is done by broadcasting route discovery message from a source node that to the destination. Only authorized nodes participate at each hop between source and destination. So that it can be used in open environments. The main disadvantage of this protocol is that every node which forwards route discovery message or reply message should sign it. It causes high power consumption and also results in the increase of message size at each hop. ARAN is an on-demand protocol which incurs no traffic has on the existing route for its life time, the route will get simply deactivated in the routing table.

IV. PROPOSED METHODOLOGY

There are several protocols proposed for MANET such as AODV, DSR, OLSR etc.. In this work we consider AODV protocol for establishing a trust based network model.

In our proposed model, TBAODV(Trust based ad-hoc On-demand distance vector routing) we assume that the system is equipped with some intrusion detection units in the network or application layer so that each nodes can observe the behaviour of its one-hop neighbour. A new model is designed in the network layer as a part of our trust model. In order to store opinion about other node's trustworthiness, positive and negative evidences when it performs routing procedures with others etc. some new fields are added into a node's routing table. Our Proposed trust model can save time without maintaining expiring time, valid state etc. There are three modules in the proposed TBAODV system. They are basic AODV routing protocol, a trust model and a trusted AODV routing protocol. The TBAODV consist of various procedures such as trust combination, trust recommendation, trust judging, cryptographic routing behaviours, trust routing and trust updating. Once the trust relationship among nodes is established in networks, these nodes rely on our trust model to perform routing operations. Consider for example that the Node A and B are communicating with each other. Node A will utilize the trust based protocol to exchange trust information about node B from its neighbours. Then it uses trust combination algorithm to combine all recommendation opinions together and calculate a new option to node B. The route discovery and maintenance operations will also follow our trust based protocol.

A. *Secured Trust based Routing Algorithm:*

The algorithm works as follows.

1) A source node sends RREQ packets to its neighbours during its route discovery. Packets consists of additional information like security related information, key information etc.

2) When RREQ packet is received by a node. The node places its QoS information and trustworthiness information in RREQ packet and forwards it to next hop. This process will get repeated until it reaches its final destination.

3) Before making decision, the node waits at the destination for a fixed number of RREQ packets. Once the RREQ packets are received, the destination node compares the various TQI index values and selects the least cost index value. It then unicast the RREP packet back to the source node. When the source node receives the RREP packet, it starts data communication by using the route.

4) When the routes get established, the intermediate nodes will monitor the link status of next hop in the active routes. Those nodes that do not have trustworthiness requirements, it will be eliminated from the route.

5) If any link error or breakage is detected in an active route, a route error (RERR) packet is send to notify other nodes.

B. *Trusted routing operations in TBAODV*

1)Routing table extension

The three new fields are added to routing table of each node. They are positive events, negative events and opinion. Positive events are those events which has successful communication time between each node. Negative events are failed communication events. Opinion means a node's belief toward trustworthiness of another node.

2)Extension of Routing Message

In our method, we extend the existing AODV by adding some trust information fields. The two important messages that we add includes Trust based Routing Request (TBRREQ) and Trust based Routing Reply (TBRREP).In this trust based routing procedure, every routing request and routing reply includes trust information. It also includes opinion of source node towards the destination node.

3)Trust Updation

With the increase of success or failed communication time, the opinion among node will change dynamically. To know when and how to update trust opinion among nodes, they have to follow some rules which is derived below.

1) When a positive event occurs from Node A to node B, the successful events of Node B in A's routing table is increased by one.

2) When a negative event occurs from node A to node B, the number of failed events of node B in node A is increased by one.

3) When a new opinion has been obtained from combination, the corresponding successful and failed events will be mapped back using opinion space to the evidence space.

4) The positive events consists of successful data or routing packets which can maintain data integrity, cryptographic verifications etc.

4)Trust based Protocol

The existing trust model considers the exchange of trust information. In our trust recommendation model there are three types of messages. They are Trust based Routing Request(TBRREQ) , Trust based Routing Reply(TBRREP) and Trust based warning message(TBWARN).The nodes that issues TBRREQ message is called Requestor and those who reply with TBRREP message is called recommender. The target nodes of recommender are called recommendee. There is no restriction on which node is to be considered as all these entities. So any nodes can be requestor, responder and recommender.

5)Analysis of the trust model

Compared to other security solutions of MANET, our trust based model has less computation overhead. And also our method does not perform cryptographic computations in every packet which can cause more time and performance consumption. After establishing the trust relation, the subsequent routing operations can be performed securely according to the trust based information instead of going for certificate authentication all the time. Therefore our proposed TBAODV can improve the performance of security solutions. We also analyze the computation overhead of TBAODV from two aspects. One is based on cost of each trust combination and update operation. Other one is based on the number of trust combination and update operations when a certain volume of data is given. The computation cost of trust combination stage is O(v).Each trust combination requires a constant number of multiplications where its length factor is 16 bit. Hence the overall cost of trust combination is O (16^2v) bit operations. For security solutions which use digital signature authentication, the RSA signature scheme is used to measure the computation cost of signature generation and verification. When 2k-bit RSA signature is used, the generation of signature requires O(K^3) bit operations and the verification requires O(k^2) bit operations where k is the recommended to be at least 1024 bits for most security applications. From this aspect we can conclude that TBAODV has better computation performance compared to other signature authentication solutions. We also compared time when certain volume of data is given, to perform digital authentication and trust updation. The digital authentication method needs to verify signature for every routing message. In case of TBAODV protocol, with the help of expiry time of trust values, the trust updation times can be reduced. Assumption is made on the total number of packet propagation in whole network as n, the average packet transmission time as t and the average trust value time as e. In case of digital authentication and verification is required for each packet so the time required is n. The time required for performing trust updation can be obtained from the following equations.

$T = n\ t/e$ when $t < e$ (1)

$T = n$ when $t >= e$ (2)

The policy for updating trust used in the above equations is that we combine periodic update and on-demand update together. If nodes in the MANET have high mobility, the routing messages are sent at high frequency. We update the trust values when the average packet sending interval t is smaller than average expiry time. The average packet sending interval t is long, when the nodes in the MANET stay in a more stable position. When the average packet interval value t is larger than the expiry time, we update the trust in an on-demand way. We assume that the total routing packets is 1000 and average expiry time is 10s. In order for the network to have high throughput it is recommended to use TBAODV routing protocol. Compared to existing solutions that perform signature authentication for both routing packets and

routing packets, the computation overhead of our proposed solution is reduced because proposed system do not perform trust updation during transmission as trust routes between source nodes are established. Our design can also resist the nodes misbehaviour. When a good node is compromised and become a bad node, its misbehaviour can be detected by neighbouring nodes. After that with the help of trust based algorithm, opinion from other node to this node will be updated periodically. TBAODV also gives flexibility for each node to define its own opinion threshold. Based on this trust model, we design our trust based routing protocol TBAODV on top of Ad hoc on-demand distance vector routing protocol. We also extended the routing table and routing message of AODV with trust information which can be updated directly by monitoring the neighbourhood. If large number of positive events is collected, then the belief value in the opinion will be increased. We also present a trust recommendation protocol. Unlike the cryptographic schemes that perform signature verification for every routing packet we combine the recommended opinions together and did a judgment on each opinion during trusted route discovery. If the uncertainty value of opinion is higher than a threshold value, cryptographic routing effect will take the role. When nodes have performed many communications, the uncertainty will decrease which means the belief or disbelief value dominates the trust value calculation. So the probability of performing cryptographic routing will get lower. In this way the computation overhead can be reduced largely and trustworthiness of routing can be guaranteed.

C. 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.

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

For comparing the performance of Trust based AODV (TBAODV) and normal AODV, both protocols are made to run with identical mobility and traffic. Initially, analysis of normal AODV network is done. Then, some malicious nodes are introduced to normal AODV and performance analysis is done.

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. 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.

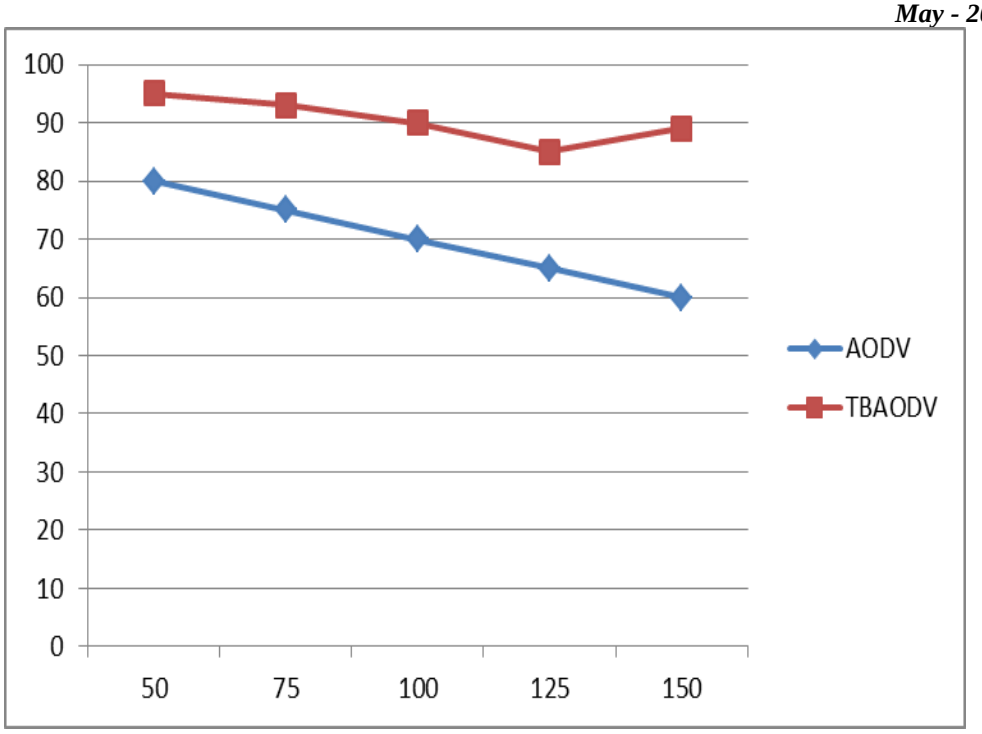

Fig 2: Packet Delivery Ration Vs. Number of Nodes

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 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.

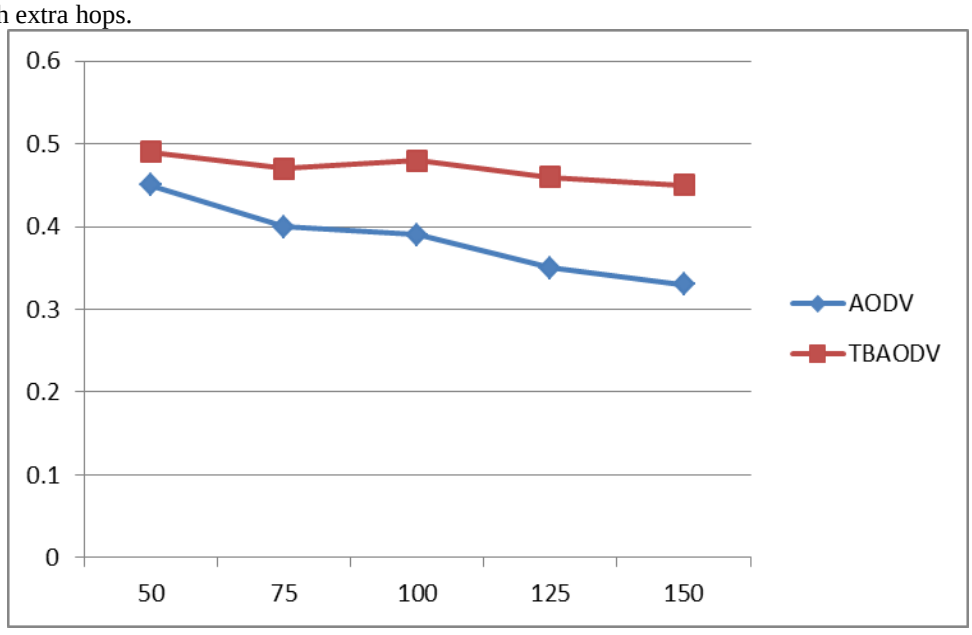

Fig 3: Average Latency Vs. Number of Nodes Varies

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.

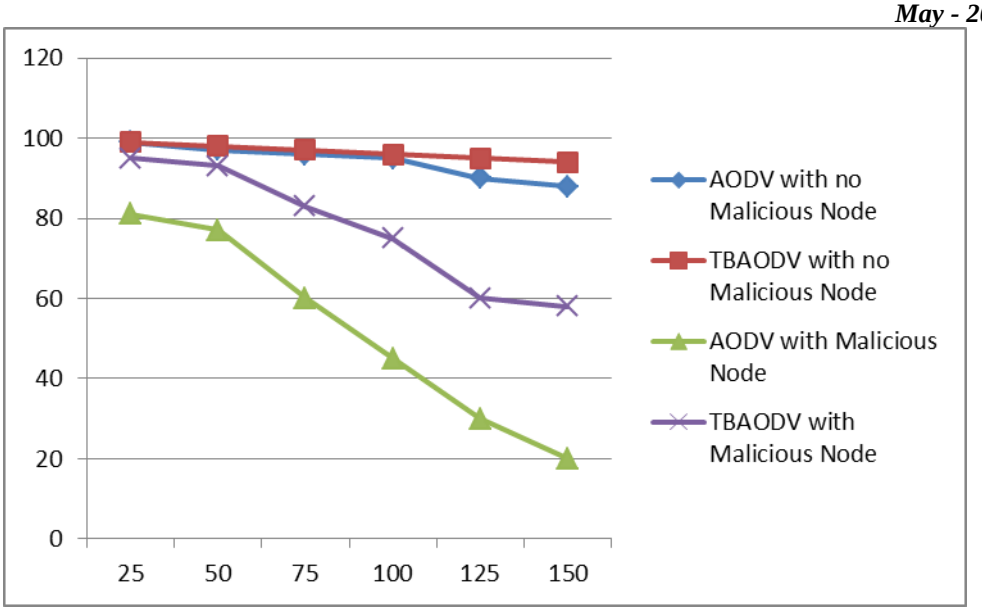

Fig 4: Throughput (%) Vs. Node Speed (ms)

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

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.

ACKNOWLEDGMENT

We make use of this opportunity to express our sincere gratitude to all those who have helped us to complete this work successfully. We wish to place on record our deep sense of gratitude to Dr.Latha Parameswaran, Ph.D., Chairperson, Dept. of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, for her generous guidance, help and useful suggestions. We express our sincere gratitude to Dr.Vidya Balasubramanian, Ph.D., Assoc.Professor, Dept. of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, for her stimulating guidance, continuous encouragement and supervision throughout the course of present work. We also would like to extend our thanks to M.Rithwik and A.K.Sumesh, Dept. of Computer Science and Engineering, Amrita Vishwa Vidyapeetham, and other colleagues for their insightful comments and constructive suggestions to improve the quality of this work. Last but not the least; we would like to express our sincere thanks to our friends for their valuable suggestions and helpful discussions.

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, 2008.

[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,

