Volume 3, No. 6, June 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
TECHNICAL NOTE
Available Online at www.jgrcs.info

TRUST BASED SECURE AODV IN MANET

Pankaj Sharma[*1], Yogendra Kumar Jain[2]
[1,2]Department of C.S.E, Samrat Ashok Technological Institute, Vidisha, M.P., India
[1] Pankaj.sati2010@gmail.com
[2]ykjain_p@yahoo.co.in

Abstract- The nature of self-organization and the limitation of individual resources, MANET always confront security and selfishness issues. In this thesis, we design trusted routing protocols using trusted frame works and intrusion detection system (secure protocol) for MANET. Trust combination algorithms and trust mapping functions are provided in this model, where the former can aggregate different opinions together to get a new recommendation opinion. Based on this trust model, we design our trusted routing protocols for MANET called TAODV on top of Ad Hoc On-demand Distance Vector (AODV) routing protocol. We extend the routing table and the routing messages of ADOV with trust information which can be updated directly through monitoring in the neighborhood. When performing trusted routing discovery, unlike those cryptographic schemes that perform signature generation or verification at every routing packet, we just combine the recommended opinions together and make a routing judgment based on each element of the new opinion. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedure can be guaranteed as well. In this thesis, we implement the security and selfishness issues of wireless networks, either in non-cooperative form or in cooperative form. Our results show that the cumulative utilities of cooperative nodes are increased steadily and the selfish nodes cannot get more utilities by behaving selfishly than cooperatively.

Keywords- MANET, AODV, Security, Trusted AODV.

INTRODUCTION

Many security schemes from different aspects of MANET have been proposed in order to protect the routing information or data packets during communications, such as secure routing protocols and secure key management solutions. Due to resource scarcity (battery power, memory, and processing power) of nodes, securing MANET is quite different from traditional schemes that generally involve management and safe keeping of a small number of private and public keys. The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save the node energy. On the other hand, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. However, most of these schemes assume that there are trusted third parties or centralized servers who are responsible for issuing digital certificates and keys or monitoring the behaviors of other nodes. Centralized servers or trusted parties make the network more controllable but they destroy the self organizing nature of MANET and reduce the network scalability. Even some schemes distribute the servers into many nodes; there are still bottlenecks due to centralization. If the scheme distributes the functions of servers into each node of the network, it will introduce significant performance overhead. What's more, by requiring nodes to generate and verify digital signatures all the time, these solutions often bring huge computation overhead [1] and [2] and [3]. Therefore, we need a self-organized light-weight security scheme for mobile ad hoc networks.

In our work to be described in the thesis, we focused on designing a secure routing mechanism for MANET in a self-organized way instead of using centralized servers. Our solution is introducing the idea of "trust" to solve this problem. Based on this trust model, we design our secure routing protocol for MANET according to Ad hoc On-demand Distance Vector (AODV) routing protocol. The new protocol, called TAODV (Trusted AODV), has several salient features: (1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them; (2) a node which performs malicious behaviors will eventually be detected and denied to the whole network; and (3) System performance is improved by avoiding requesting and verifying certificates at every routing step.

LITERATURE SURVEY

Trust is an important aspect of mobile ad-hoc networks (MANETs). It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints, and the independent movement of component nodes. This prevents the direct application of techniques suited for other networks. In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the quality and reliability of data. Therefore, analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with that node. In this work we present a detailed survey on various trust computing approaches that are geared towards MANETs. We highlight the summary and comparisons of trust based AODV in MANET approaches.

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

A secure version of AODV called Secure AODV (SAODV). It provides features such as integrity, authentication, and non-repudiation of routing data. It incorporates two schemes for securing AODV. To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the *double signature*: when a node A generates a RREQ message, in addition to the

regular signature, it can include a second signature, which is computed on a fictitious RREP message towards A itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node A. If one of these nodes then receives a RREQ towards node A, it can reply on behalf of A with a RREP message, similarly to what happens with regular AODV. To do so, the intermediate node generates the RREP message, includes the signature of node A that it previously cached, and signs the message with its own private key.

SAODV does not require additional messages with respect to AODV. Nevertheless, SAODV messages are significantly bigger, mostly because of digital signatures. Moreover, SAODV requires heavyweight asymmetric cryptographic operations: every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature. This gets worse when the double signature mechanism is used, because this may require the generation or verification of two signatures for a single message. In the SAODV operations, SAODV allows to authenticate the AODV routing data. Two mechanisms are used to achieve this: hash chains and signatures [2] and [4] and [12].

Security Aware Ad hoc Routing (SAR):

SAR protocol integrates the trust level of a node and the security attributes of a route to provide the integrated security metric for the requested route. A Quality of Protection (QoP) vector used is a combination of security level and available cryptographic techniques. It uses the timestamps and sequence numbers to stop the replay attacks. Interception and subversion threats can be prevented by trust level key authentication. Attacks like modification and fabrication can be stopped by verifying the digital signatures of the transmitted packet. The main drawbacks of using SAR are that it required excessive encrypting and decrypting at each hop during the path discovery. The discovered route may not be the shortest route in the terms of hop-count, but it is secure.

Adaptive SAODV (A-SAODV):

A-SAODV optimizes the routing performance of secured protocols with help of a threshold mechanism. ASAODV is a multithreaded application. In that protocol the cryptographic operations are performed by a dedicated thread to avoid blocking the processing of other message and other thread to all other functions. Every node has queue of routing message to be signed or verify and the length of the queue implies the load state of the routing thread. Whenever a node processes a route request and has enough information to generate a RREP on behalf of destination, it first checks its routing message queue length. If the length of the queue is below a threshold then it reply otherwise, it forwards the RREQ without replying. The value of threshold can be changed during execution. The A-SAODV also maintains a cache of latest signed and verified message in order to avoid signing and verifying the same message twice. This adaptive reply decision has a significant improvement on the performance of SAODV.

In this way, the algorithm could adapt itself to the situation and the computing power of the node. An additional external parameter could be used to take into account the previously mentioned external factors (how much a node is willing to collaborate, e.g., depending on its battery state). Another little optimization included in the A-SAODV prototype is a cache of latest signed and verified messages, in order to avoid signing or verifying the same message twice [5] and [9] and [10].

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

The existing AODV has been extended to RAODV by adding two types of control packets: Reliable Route Discovery Unit (RRDU) and RRDU Reply (RRDU_REP). The RRDU messages are control packets sent by the source node along with RRDU-ID, to the destination at regular intervals and RRDU_REP message is the response of RRDU by the destination to the source node. RRDU_REP can only be generated by the destination. There is no impersonation i.e. no node other than the destination, can generate RRDU_REP on behalf of the destination.

Reliability List (RL) field is also adding in the routing table entry. An entry in the RL has Source address, a field called Forward Data Packet Count (FDPC) and RRDU-ID, i.e. the triplet (Source address, FDPC, RRDU-ID). The Routing Table entry format of RAODV is same as that of AODV [13] except for the additional RL field. RAODV uses RREQ, RREP messages for route discovery and RERR, HELLO messages for route maintenance which is similar in AODV. In addition, RAODV also uses RRDU and RRDU_REP to help discover the path and for reliability maintenance. In RAODV the path discovery can be thought of as consisting of two phases. The phase I is same as AODV. Whenever a node wishes to communicate with another node it looks for a route in its table. If a valid entry is found for the destination it uses that path else the node broadcasts the RREQ to its neighbors to locate the destination [2] - [6].

ARAN (Authenticated Routing for Ad-hoc Networks):

ARAN provides authentication, message integrity and non-repudiation in ad-hoc networks by using a preliminary certification process which is followed by a route instantiation process that ensures end-to-end security services. But it needs the use of trusted certification server. The main disadvantage with the protocol is every node that forwards a route discovery or a route reply message must also sign it, which is very power consuming and causes the size of the routing messages to increase at each hop [7, 8].

Moreover, some authentication measures, such as digital signature, can be performed in a more flexible way based on the trust value so the system overhead can be greatly reduced. Based on this trust model, we design our secure routing protocol for MANET according to Ad hoc On-demand Distance Vector (AODV) routing protocol. The new protocol, called TAODV (Trusted AODV).

PROPOSED METHODOLOGY

Several routing protocols have been proposed for mobile ad hoc networks, such as AODV, DSR, and DSDV and so on. In this work, we make some assumptions and establish the network model of Trust AODV (TAODV). We also argue

why we focus our security solution on routing protocol in the network layer instead of link layer. Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel.

We assume that:

a. Each node in the network has the ability to recover all of its neighbors;
b. Each node in the network can broadcast some essential messages to its neighbors with high reliability;
c. Each node in the network possesses a unique ID that can be distinguished from others.

In TAODV, we also assume that the system is equipped with some monitor mechanisms or intrusion detection units either in the network layer or the application layer so that one node can observe the behaviors of its one-hop neighbors.

In the network layer, a new node model is designed as the basis of our trust model. Some new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing procedures with others. By embedding our trust model into the routing layer of MANET, we can save the consuming time without the trouble of maintaining the expire time, valid state, etc., which is important in the situation of high node mobility and invalidity. Also because of this reason, it is hard to design secure solutions in the transport layer, which is an end-to-end communication mechanism.

Framework of our Trusted AODV:

There are mainly three modules in our whole TAODV system: basic AODV routing protocol, a trust model, and trusted AODV routing protocol. Based on our trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating. The structure and relationship among these components are shown in Fig 4.1 below. The general procedure for establishing trusts relationships among nodes and for performing routing discovery is described as follows.

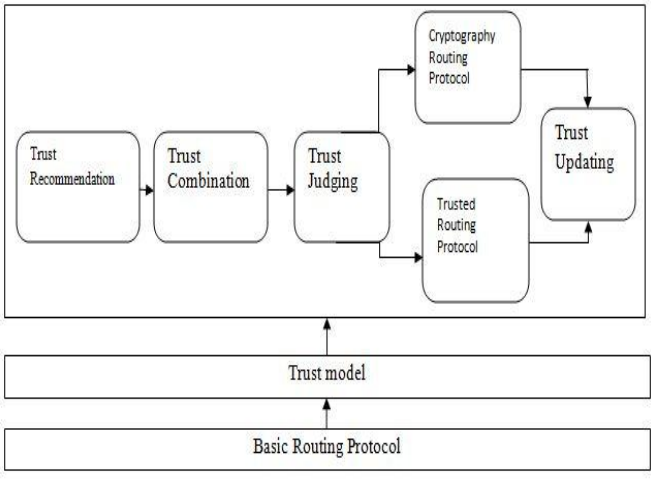


Figure 1: Framework of Trusted AODV

Let us first imagine the beginning of an ad hoc network which contains a few nodes. Each node's opinion towards one another initially is (0, 0, 1) which means total uncertainty. Suppose node A wants to discover a routing path to B. Because the uncertainty element in A's opinion towards others is larger than or equal to 0.5, which means that A is not sure whether it should believe or disbelieve any other nodes, A will use the cryptographic schemes as proposed in SAODV or some other schemes to perform routing discovery operations. After some successful or failed communications, A will change its opinions about other nodes gradually using the trust updating algorithm. The uncertainty elements in its opinions about other nodes will be mostly less than 0.5 after a period of time. By means of this procedure, eventually each node in the network will form more certain opinions towards other nodes eventually after the initial time period.

Once the trust relationship is established among most of the nodes in the network, these nodes can rely on our trusted routing protocol which is based our trust model to perform routing operations. Node A now will utilize the trust recommendation protocol to exchange trust information about a node, B, from its neighbors, then use the trust combination algorithm to combine all the recommendation opinions together and calculate a new option towards B. The subsequent routing discovery and maintenance operations will follow the specifications of our trusted routing protocol. In this framework, the establishment of trust relationships among nodes and the discovery of routing paths are all performed in a self-organized way, which is achieved by the cooperation of different nodes to exchange information and to obtain agreements without any third-party's interventions.

Intrusion Detection (Security Protocol) Algorthm:

The algorithm can be summarized as follows.

a) During route discovery, a source node sends RREQ packets to its neighboring nodes. In these packets, along with the regular information, the node also sends its security related information, such as key information.
b) Once an RREQ packet is received by an intermediate node. The node places the link trustworthiness and QoS information in the RREQ packet and forwards it to its next hop. This process is repeated until it reaches the final destination.
c) At the destination, the node waits for a fixed number of RREQs before it makes a decision. Or else, a particular time can be set for which the destination or intermediate node needs to wait before making a routing decision. Once the various RREQs are received, the destination node compares the various TQI index values and selects the index with the least cost. It then unicasts the RREP back to the source node. When the source node receives the RREP, it starts data communication by using the route.
d) Once the route is established, the intermediate nodes monitor the link status of the next hops in the active routes. Those that do not meet the performance and trustworthiness requirements will be eliminated from the route.
e) When a link breakage in an active route is detected, a route error (RERR) packet is used to notify the

other nodes that the loss of that link has occurred. Some maintenance procedures are needed as in AODV.

Trusted Routing Operations in TAODV:

Routing Table Extensions:

We add three new fields into each node's original routing table: positive events, negative events and opinion. Positive events are the successful communication times between two nodes. Similarly negative events are the failed communication ones. Opinion means this node's belief towards another node's trustworthiness as defined before.

Routing Message Extensions:

We extend the original AODV routing messages by appending some trust information fields. Two main types of extended messages are TRREQ (Trusted Routing REQuest) and TRREP (Trusted Routing REPly).

In trusted routing discovery procedures, every routing request and reply carries trust information, including opinions towards originator node S and destination node D, which will be employed to calculate the credibility of S and D. When a node is required to provide its certificate information, it will fill the fields of trust information with its own signature, as proposed by some traditional security solutions for MANETs.

Trust Updating Policies:

Opinions among nodes change dynamically with the increase of successful or failed communication times. When and how to update trust opinions among nodes will follow some policies, which are derived as follows:

a. Each time a positive event occurs from node A to node B, B's number of successful events in A's routing table will be increased by 1.
b. Each time a negative event occurs from node A to node B, B's number of failed events in A's routing table will be increased by 1.
c. Each time when the field of the successful or failed events changes, the corresponding value of opinion will be recalculated using the evidence space to the opinion space.
d. Each time when the new opinion has been obtained through combination, the corresponding number of successful or failed events will be mapped back using the opinion space to the evidence space.
e. The positive events include successful data or routing packets forwarding, keeping message integrity, and passing cryptographic verification, and so on.

Trust Recommendation Protocol:

Existing trust models seldom concern the exchange of trust information. However, it is necessary to design an information exchange mechanism when applying the trust models to network applications. In our trust recommendation protocol, there are three types of messages: Trust Request Message (TREQ), Trust Reply Message (TREP), and Trust Warning Message (TWARN). Nodes who issue TREQ messages are called Requestor. Those who reply TREP messages are called Recommender. The recommendation target nodes are called Recommendee. Any node may be a Requestor, a Recommender, or a Recommendee.

Figure 2: Trust Routing Step at Current Node

Theoretical Analysis:

From the performance point of view, our trusted routing protocol introduces less computation overheads than other security solutions for MANETs. Our design does not need to perform cryptographic computations in every packet, which will cause huge time and performance consumption. After the trust relationships are established, the subsequent routing operations can be performed securely according to trust information instead of acquiring certificate authentication all the time. Therefore, TAODV routing protocol improves the performance of security solutions. Unlike some previous security schemes, whose basis of routing operations is "blind distrust", TAODV does not decrease the efficiency of routing discovery and maintenance. In detail, we analyze the computation overhead of TAODV from two aspects. One is the cost of each trust combination and update operation. The other is the number of trust combination and update operations when given a certain volume of data load.

The cost of trust combination is O(v), where v is the number of a node's neighbors. Each trust combination needs a constant number of multiplications, where the length of factor is 16 bit. Hence the overall cost of each trust combination requires O (16^2v) bit operations. For security solutions employing digital signature authentication, we use the RSA signature scheme for example to measure the computation cost of signature generation and verification. In general when using a 2k-bit RSA signature, the generation of signature requires O(k^3) bit operations and the verification requires O(k^2) bit operations, where k is recommended at least to be 1024 bits for most security applications. We can conclude from this aspect that TAODV achieves better computation performance compared to the pure signature authentication solutions.

On the other hand, we compare the times of performing digital authentication and trust updating when given a certain traffic volume. The digital authentication scheme usually needs to generate or verify signature for every routing message. While in TAODV protocol, with the help of expiry time of trust values, the trust updating times can be significantly reduced. Let us assume that the total number of routing packets propagated in the whole network is n, the

average packet transmission interval is t, and the average expiry time of a trust value is e. Obviously the number of times in performing digital authentication is a constant value n because the generation or verification is required for each packet. The number of times in performing trust updating can be obtained by Eq. (1.1 and 1.2) in the following. The policy for updating trust used in this equation is that we combine periodical update and on-demand update together. When nodes in the MANET all have high mobility, the routing messages are sent in a high-frequency way. If the average packet sending interval t is smaller than the average expiry time, we update trust values periodically. When the nodes in the MANET stay in more stable positions, the average packet sending interval t is long. If the average packet interval value t is larger than the expiry time, we update the trust in an on-demand way.

U= nt/e……t<e……..Equation 1.1
U= n…….t>=e……..Equation 1.2

We now assume that the total number of routing packets is 1000 and the average expiry time is 10s. It can be concluded that when the network has a high throughput it is quite efficient in using TAODV routing protocol. Comparing to those solutions that perform signature authentication not only for routing packets but also for data packets, the computation overheads of our solution will be largely reduced because we do not perform trust updating when transmitting data packets if we have established trust routes between the source nodes and From the security point of view, our design will resist the nodes' misbehaviors finally and reduce the harm to the minimum extent. When a good node is compromised and becomes a bad one, its misbehavior will be detected by its neighbors. Then with the help of the trust update algorithm, the opinions from the other nodes to this node will be updated shortly. Thus this node will be denied access to the network. Similarly, a previously bad node can become a good one if the attacker leaves the node or the underlying links are recovered. In this situation, our design allows this node's opinion from other nodes' points of view to be updated from (0, 1, 0) to (0, 0, 1) after a period of expiry time.

From the flexibility point of view, TAODV gives each node the flexibility to define its own opinion threshold. The default opinion threshold is 0.5, which can be increased by a node to maintain a high security level and also can be decreased to meet demands of some other applications.

Based on this trust model, we design our trusted routing protocols for MANET called TAODV on top of Ad Hoc On-demand Distance Vector (AODV) routing protocol. We extend the routing table and the routing messages of ADOV with trust information which can be updated directly through monitoring in the neighborhood. The more the positive events are collected, the higher the belief value in the opinion will be. Besides, we also present a trust recommendation protocol. When performing trusted routing discovery, unlike those cryptographic schemes that perform signature generation or verification at every routing packet, we just combine the recommended opinions together and have a judgment on each element of the new opinion. Only if the uncertainty value in the opinion is higher than a threshold, will the cryptographic routing scheme take effect. When nodes have conducted more and more number of communications, the uncertainty value will become lower and lower, which means the belief or the disbelief value will dominate the trust judgment, so that the chance of performing cryptographic routing behaviors will get lower and lower. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedures can be guaranteed as well. We compare the performance of our TAODV protocol with Normal AODV protocol.

SIMULATION ENVIRONMENT AND RESULTS

Simulation Environment:

In this thesis we implement Trusted AODV using Network Simulator 2 version 2.34. In MANETs, the entity mobility models typically represent nodes whose movements are completely independent of each other in un- cooperative fashion, e.g. the Random Way Point (RWP) model. The results of these runs were averaged to produce the graphs shown below. The table provides a summary of the chosen simulation parameter values.

In the application layer, the nodes communicate using five constant Bit Rate generators (CBR) over UDP with random source and destination pairs. Each generator produces 1000 data packets of 1024 bytes each at the rate of 8 packets per second.

Besides, in all node movement scenarios, a node chooses a destination and moves in a straight line towards the destination at a speed uniformly distributed between 0 m/s and some maximum speed. Once the node reaches its destination, it waits for a pause time before choosing another random destination and repeats the process. This is called the random waypoint model. The maximum speed was limited to 10 m/s and ran simulations for constant node speeds of 0, 1, 5 and 10 m/s, with pause time fixed at 10 seconds.

Table: 1

Parameters	Values
Examined Protocol	AODV, TAODV
Traffic type	Constant Bit Rate (UDP)
Transmission range	100 m
Packet size	1024 bytes
Data rate	100 kb/s
Pause time	10 s
Minimum speed	1m/s
Simulation time	900s
Area	100X100 m

Results on Malicious Nodes and Intrusion Detection :

There are the 500 nodes simulated, some variable percentage of the nodes is selfish means malicious node. A malicious node is one that agrees to participate in forwarding packets but then haphazardly drops all data packets that are routed through it. The percentage of the selfish nodes was varied from 0% to 33% in 10% increments. Also, a random number generator to designate selfish nodes randomly was developed. In the meantime, the same seed across the 0% to 33% variations of the selfish nodes parameter was used.

Selfish Nodes (Malicious) Graph in AODV:

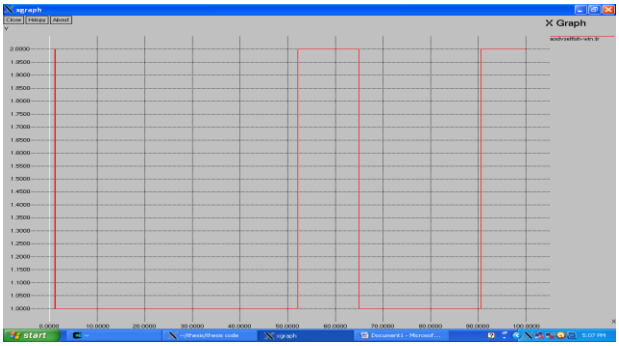


Figure. 3 End to end delay (s) vs. number of nodes

That means for example that the group of the selfish nodes in the 20% case is a superset of the group of the selfish in the 10% case. Thus, that ensures that the impediments present in lower percentage selfish nodes runs are also present in higher percentage selfish nodes runs. After using the trusted frame work and IDS in AODV then the overall system called Trusted AODV. The graph 3 and 4 described the selfish nodes and intrusion detection system in AODV respectively.

Intrusion Detection System graph in AODV:

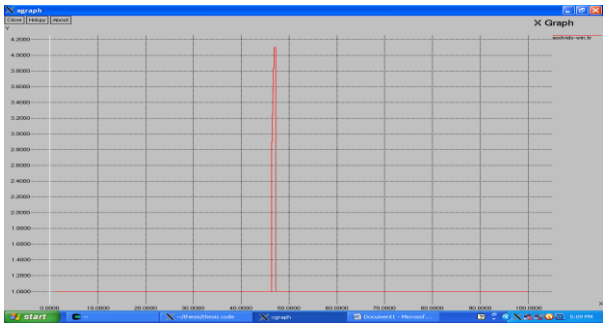


Figure. 4 End to end delay (s) vs. number of nodes

Combined Gragh for Results analysis:

The graph (Figure 5) described the results analysis based on normal AODV and Selfish AODV (Malicious nodes affected AODV) and intrusion detected AODV.

End to end delay (s) vs. number of nodes

Figure. 5 Graph of Normal AODV, Selfish AODV and IDS AODV

Performance Analysis:

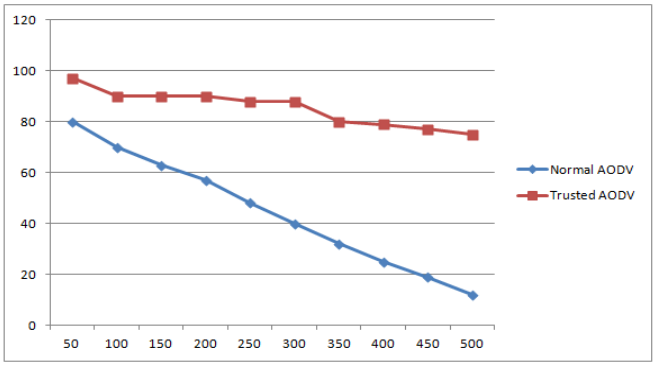
In order to compare the performance of Trusted AODV (TAODV) and normal AODV, both protocols are run under identical mobility and traffic scenarios. First, an analysis of normal well-behaved AODV network is done. Then, some uncooperative nodes are introduced to the normal AODV network and analysis of the performance is done. Following that, the newly designed Trust-based scheme is added to normal AODV, to TAODV become, and performance is compared to normal AODV. A comparison between both of these protocols using the metrics explained is presented.

Experiment on: Packets Delivery Ratio:

In this experiment, the packets reached metric for the normal AODV routing protocol and the TAODV is measured with node varies 1 to 100 and also 100 to 500. The speed of the nodes and the percentage of selfish nodes participating in the mobile ad hoc network are varied to compare the results.

From the graph figure 6, it is clear that with increasing the percentage of selfish nodes in the network, there is a remarkable fall in normal AODV's number of packets reached metric. The different bars show a network of 500 nodes with different percentages of selfish nodes, from 0% up to 30%, and moving at different speeds. Here are some points that can be observed in this graph:

a. In the case that there are no selfish nodes in the mobile ad hoc network, both normal AODV and trusted AODV have almost identical number of packets reaching their destinations. This proves that the trusted AODV protocol is as normal AODV efficient as in delivering the packets and discovering routes to any destination.
b. It can be noted that in both normal AODV and trusted AODV when the nodes' speed rises, the number of packets reached diminishes as the network in general gets more fragile.
c. Also, as the percentage of selfish nodes participating in the network increase, the number of packets reached decreases because these selfish nodes tend to drop packets that they beforehand promised to forward. The outcome of dropping packets affects the normal AODV protocol during the full life of the network, but in case of trusted AODV, it is just affected partially as by time the selfish node will be identified and weeded out of the network.
d. The increase in the number of packets reached in the case of using trusted AODV is attributed to that each node uses its local table of other nodes' the trust values in the selection of the next-hop node for establishing the data route.



Packet Delivery Ration vs. Number of Nodes

Figure 6 Packet Delivery Ratio Graph where node varies 1 to 500

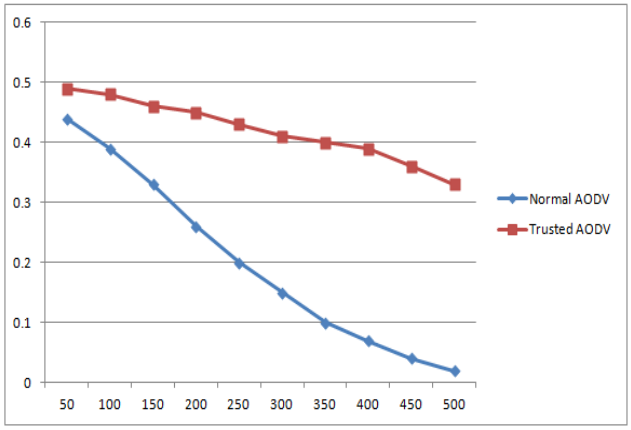
e. Thus, the number of packets reached is reduced to 380 packets with normal AODV, when 30% of the nodes are selfish and moving at speed of 10 m/s. However,

the number of packets reached is reduced to only 680 packets with trusted AODV, in the same circumstances. This proves that the trusted AODV increases the number of packets reached by 300 packets over normal AODV routing protocol.

Experiment on: Average Latency:

In this experiment, the average latency of data packets for the normal AODV routing protocol and the trusted AODV is measured. The percentage of selfish nodes participating in the mobile ad hoc network is varied to compare the results. The figure 7 shows the results of the average latency of data packets metric of both protocols: normal AODV and trusted AODV with different percentage of selfish nodes.

From the graph it is clear that the newly proposed trusted AODV protocol has a higher average latency of data packets than the normal AODV routing protocol. This is due to the fact that in the trusted AODV, at each hop and before sending or forwarding data packets Also, as the percentage of selfish nodes increase in the mobile ad hoc network, the trusted AODV protocol can end up choosing a longer selfish-free route to the destination with extra number of hops, maximum two extra hops, as each extra hop costs 2 ms.



Average Latency vs. Number of Nodes Varies

Figure: 7 Average Latency Graph where Number of Node varies 1 to 500

Network Throughput:

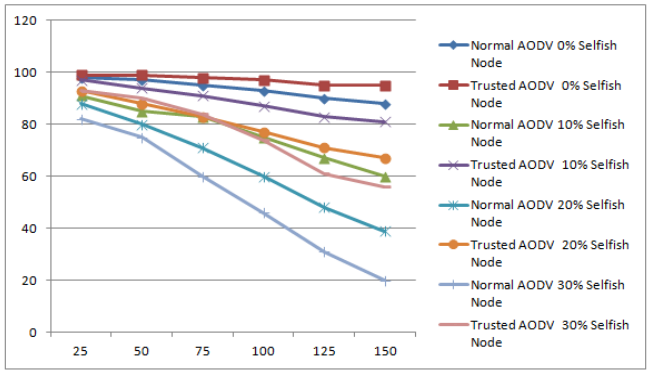
The below figure 8 shows the results of the network throughput of both protocols: normal AODV and TAODV with different node speed and different percentages of selfish nodes. From the 6.7 graph it is clear that the lack of cooperation has fatal effect on the efficient working of the network. This graph shows the dramatic fall in normal AODV's network throughput with increasing percentage of selfish nodes. The different curves show a network of 150 nodes with different percentages of selfish nodes, from 0% up to 30%, and moving at different speeds. Here are some points that can be observed in this graph:

In the case that there are no selfish nodes in the mobile ad hoc network, both AODV and TAODV have almost identical network throughput values. This proves that the TAODV protocol is as efficient as AODV in delivering the packets and discovering routes to any destination.

It can be noted that in both AODV and TAODV when the node movement speed rises, the network throughput diminishes as the network in general gets more fragile.

Also, as the percentage of selfish nodes participating in the mobile ad hoc network increase, the throughput decreases because these selfish nodes tend to drop packets that they beforehand promised to forward. The outcome of dropping packets affects the normal AODV protocol during the full life of the network, but in case of TAODV, it is just affected partially as by time the selfish node will be identified and weeded out of the network.

The increase of throughput of the network in the case of using TAODV is attributed to that each node uses its local table of other nodes' trust values in the selection of the next-hop node for establishing the data route.



Throughput (%) vs. Node Speed (ms)

Figure 8: Effects of Selfish nodes on Network Throughput

CONCLUSION AND FUTURE WORKS

The performance of Ad-hoc On Demand Vector (AODV) protocols has been modified by including the source route accumulation feature. As low transmission power of each ad-hoc node limits its communication range, the nodes must assist and trust each other in forwarding packets from one node to another. However, this implied trust relationship can be threatened by malicious nodes that may modify or disrupt the orderly exchange of packets. Security demands that all packets be authenticated before being used.

Based on this trust model, we design trusted routing protocols using trusted frame works and intrusion detection system (secure protocol) for MANET. We extend the routing table and the routing messages of ADOV with trust information which can be updated directly through monitoring in the neighborhood. The more the positive events are collected, the higher the belief value in the opinion will be. Besides, we also present a trust recommendation protocol. When performing trusted routing discovery, unlike those cryptographic schemes that perform signature generation or verification at every routing packet, we just combine the recommended opinions together and have a judgment on each element of the new opinion. In this way the computation overhead can be largely reduced, and the trustworthiness of the routing procedures can be guaranteed as well. Through simulation we can see that the bad nodes are clearly separated from the good nodes.

Although a comparison of the performance between AODV and TAODV routing protocols under different environments was achieved, the experiments did have a number of limitations.

Adapting our model to counteract more malicious attacks in MANETs, and attacks aiming at trust model itself, for example, fabricating trust recommendations and conspiring to rate each other high scores among malicious nodes, should be also taken into consideration.

TAODV still has some imperfect points. For example, it cannot synchronize the trust level settings on different nodes when multiple paths cross with each other, in which case some node's access violation ratio is not 0. As a future work, we will focus on designing the synchronization control mechanism to solve this problem.

A public key verification mechanism, such as certificate-based authentication, is needed for improvement of TAODV, in order to verify the binding between the node's identity and its public key.

REFERENCES

[1]. Dalip Kamboj and Pankaj Kumar Sehgal, "A Comparative Study of various Secure Routing Protocols based on AODV", International Journal of Advanced Computer Science and Applications,Vol. 2, No. 7, 2011, pp 80-85.

[2]. G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010, pp 815-819.

[3]. Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443.

[4]. R. S. Mangrulkar, Pallavi V Chavan and S. N. Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT", International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010, pp 36-39.

[5]. Shilpa S G, Mrs. N.R. Sunitha, B.B. Amberker, "A Trust Model for Secure and QoS Routing in MANETS", INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711) VOL.1 NO.5MAY 2011, pp 22-31.

[6]. Suchita Gupta, Ashish Chourey, " PERFORMANCE EVALUATION OF AODV PROTOCOL UNDER PACKET DROP ATTACKS IN MANET", International Journal of Research in Computer Science eISSN 2249-8265 Volume 2 Issue 1 (2011) pp. 21-2.

[7]. A.Menaka Pushpa M.E., "Trust Based Secure Routing in AODV Routing Protocol", IEEE2009.

[8]. Songbai Lu1, Longxuan Li and Kwok-Yan Lam, Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", IEEE 2009 International Conference on Computational Intelligence and Security, pp 421-425.

[9]. Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009.

[10]. Jun Pan and Jianhua Li, "MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Networks", IEEE 2009.

[11]. Wenchao Huang, Yan Xiong, Depin Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation", IEEE 2009 International Conference on Computational Science and Engineering, pp 809-816..

[12]. A.H Azni, Azreen Azman, Madihah Mohd Saudi, AH Fauzi, DNF Awang Iskandar, "Analysis of Packets Abnormalities in Wireless Sensor Network", IEEE 2009 Fifth International Conference on MEMS NANO, and Smart Systems, pp 259-264.

