International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 23797-23814

http://www.ripublication.com

TV-DSR : Trust Vector Based DSR Protocol For Secure Routing In Mobile Adhoc Networks

Jayalakshmi V
Research and Development Center,
Bharathiar University,
Coimbatore, India
jayasekar1996@yahoo.co.in
Dr. Abdul Razak T
Department of Computer Science,
Jamal Mohamed College,
Tiruchirappalli, India
abdul1964@yahoo.com

Abstract

In a mobile ad hoc network (MANET), a source node must depend on other nodes to forward its packets on multi-hop routes to the destination. Due to the openness in network topology and absence of a centralized administration in management, MANETs are very susceptible to various attacks from malicious nodes. In order to enhance the security of network and protect the nodes from vulnerabilities, this paper presents a vector trust management model to evaluate the trustworthiness of a node. The trust value of a node is calculated based on the nodes historical behaviors and the trust aggregation method is designed to provide fast trust propagation to each node which does not have a trust value. We have also integrated the proposed vector trust management model into the popular DSR routing protocol. Our novel on-demand trust-based unicast routing protocol for MANETs, called as Trust Vector based DSR routing protocol (TV-DSR), provides a flexible and feasible method to choose the route that meets the security requirement of data packets transmission. Extensive experiments have been conducted to evaluate the efficiency and effectiveness of the proposed mechanism in malicious node identification and attack resistance. The results show that TV-DSR improves packet delivery ratio and reduces average end-to-end latency when compared to the standard DSR routing protocol.

Keywords: DSR; Trust; Malicious node; MANET; Vulnerabilities;

Introduction

Mobile ad hoc networks (MANETs) are spontaneously deployed over a geographically limited area without well-established infrastructure. In most MANET routing schemes, security is an added layer above the routing layer. As nodes may not aware to which nodes it is connected with or which nodes connected to them. Therefore access to resources or information can be shared among both trusted and non-trusted nodes. The networks work well only if the mobile nodes are trusty and behave cooperatively. There is a common assumption among routing protocols and applications for ad hoc networks that all nodes are trustworthy and cooperative [1] i.e., all nodes behave in accordance with the defined specifications of such protocols and applications. Nevertheless, this hypothesis is invalid due to constrained resources and malicious behaviors among nodes, e.g., selfish nodes deny relaying the packets of other nodes, and malicious nodes disturb the network. Several attacks, such as man-in-the-middle, black hole, and DoS, may target a MANET. Thus, the aforesaid assumption may lead to unpredicted consequences, namely, low network efficiency and high vulnerability to attacks. Furthermore, other factors such as reliability and bandwidth are occasionally included in discovering routes aside from determining the shortest distance. Assigning a local trust level to a node pair can not only alleviate the negative effects caused by misbehaviors but also make communication occur only among trustworthy neighbors with respect to the fact that the exchange of information with compromised nodes which can weaken the performance of ad hoc networks. Therefore, incorporating a relationship of trust into MANET nodes is important. According to Denning [2], "Trust cannot be treated as a property of trusted systems but rather it is an assessment based on experience that is shared through networks of people." As in real life, two entities with no previous mutual experience put confidence in each other's competence so as to realize their respective goals. These shared experiences lead to trust development and decays with time and frequency of interactions. . The inherent freedom in self-organized mobile ad hoc networks introduces challenges for trust management. Some trust management models have been developed for wired networks but they are inapplicable to MANETs because of their dynamic topology and application scenario. In this paper, a trust management model is proposed for MANET with the objectives: a) to protect the network from any attacks from the malicious nodes b) to improve the packet delivery ratio.

AODV [3], DSR [4], and TORA [5] are three well-known reactive routing protocols which are undergoing wide ranging active research. These protocols have been developed for networks where all nodes can faithfully execute them in a generous manner. However, in real life, such an unselfish attitude is difficult to achieve and so, these protocols are more often executed by nodes that divert from the basic requirements of participation. In order to maintain the spontaneous nature of ad hoc networks without making any superfluous assumptions, a trust-based scheme is usually applied to protect these routing protocols. In this paper, a new trust management model is proposed which uses vector trust aggregation method .In this model, to ensure trust worthiness, trust value for each node is calculated accurately by employing different factors namely Weight based Forwarding Ratio Factor, similarity Factor and Time Aging Factor based on the history of interaction between the nodes.

For the trust inference, vector trust is used for aggregation of distributed trust scores. Different from some existing global trust and reputation management schemes [6], Vector Trust is designed to be used in a distributed environment where no centralized server exists. In this kind of environment, the trust computation overhead should be reasonable for each node. Trust Vector Aggregation method requires only localized communication between neighbor nodes. The trust vector captures a concise snapshot of the trusted network from each node's perspectives. An application of the proposed vector based trust management model, a novel reactive routing protocol called Trust Vector based Dynamic Source Routing Protocol (TV-DSR) is proposed on the basis of the standard DSR protocol. The proposed protocol kicks out the malicious nodes and establishes a reliable trusted routing path for packet transmission.

The rest of the paper is structured as follows. Section 2 presents the related work. In section 3, we present the trust calculation methods adopted in this paper. In section 4, we discuss the vector Trust scheme and trust vector aggregation method. In section 5, we present the proposed new TV-DSR protocol. Section 6 presents the simulation results to evaluate the performance of the proposed scheme. Section 7 concludes the paper.

Related Work

Several different protocols have been proposed for ad hoc routing. The earlier protocols such as DSDV [7], DSR [4], and AODV [3] focused on problems that mobility presented to the accurate determination of routing information. DSDV is a proactive protocol requiring periodic updates of all the routing information. In contrast, DSR and AODV are reactive protocols, only used when new destinations are sought, a route breaks, or a route is no longer in use.

As more applications were developed to take advantage of the unique properties of ad hoc networks, it soon became obvious that security of routing information was an issue not addressed in these protocols. In [8], Lundberg presents several potential problems including node compromise, computational overload attacks, energy consumption attacks, and black hole attacks. Deng et al. further discuss energy consumption and black hole attacks along with impersonation and routing information disclosure in [9]. Many new routing protocols and extensions to existing protocols have been proposed to address these issues.

In the area of information security, cryptographic primitives are often used to ensure properties such as confidentiality and integrity. Several secure routing protocols with cryptography have been proposed to protect ad hoc networks, such as SAODV and Ariadne, but most of these protocols need centralized units or trusted third-parties to issue digital certificates or monitor network traffic. The common trusted authority actually violates the nature of self-organization. Therefore, these protocols are less practical for MANETs. Moreover, the traditional cryptosystem based security mechanism is typically used to resist the external attacks. They show inefficiency in handling the attacks from the internal malicious nodes. Recently a new class of routing protocols in MANETs has been proposed, called trusted routing protocols, which consist of two parts: a routing strategy and a trust model [10]. The

selection of next hops or forward paths in a routing strategy is made according to the trust model.

Due to the extra information available in DSR, by way of source routing, numerous new security protocols are based on it. In [11], Marti et al. extend DSR by adding 'watchdog' and 'path-rater' mechanisms. One disadvantage of this protocol is that it merely avoids routing through malicious nodes, and it does not do anything to penalize them. This allows a lazy or selfish node not to forward traffic for its neighbors while its neighbors will continue to forward its traffic.

In [12], Hughes et al. propose Dynamic Trust-based Resources (DyTR), which uses trust evaluation as a method of access control to network resources. The authors, however, do not discuss the securing of the trust information exchange.

Pirzada and McDonald develop a protocol based on DSR in [13], their protocol takes advantage of the full route information available in DSR. Unlike other recommendations, however, they only consider trust from direct observations rather than including third party opinions. In their protocol, however, lazy nodes are not penalized and therefore have no incentive to participate.

Trusted-DSR [14] extended from DSR [4] selects a forward path based on a local evaluation of the trust values of all intermediate nodes along the path to the destination. The node trust is calculated through an acknowledged mechanism from destination to source. Every acknowledged packet will increase the sender node's trusts in all the intermediate nodes along the path to the destination, while every retransmission decreases the trusts. But, it is impossible for senders to know which nodes discard packets.

Pirzada et al. [15] evaluated the performance of three trust based reactive routing protocols (trusted AODV, DSR and TORA) by varying the number of malicious nodes and other experiment settings. The results indicate that each trust-based routing protocol has its own advantage. In particular, trust-based AODV routing maintains a stable throughput and surpasses TORA and DSR at higher traffic loads.

Manickam et al. proposed a Fuzzy based Ad hoc on demand Distance Vector (FAODV) Routing Protocol [16]. The authors used fuzzy logic for trust evaluation and setup a Threshold Trust Value (TTV) for trust verification. Fuzzy logic based trust evaluation gives a rational prediction of trust value and an accurate identification of malicious behavior based on fuzzy inference rules. However, the FAODV model only considers the protection method against modification attacks. Furthermore, the trust evaluation process only monitors the node's behavior for route discovery but not for the transmission of data packets.

As another extension to DSR, Guoet al. [17] gave a dynamic trust evaluation scheme based on routing model (Trust-DSR). Five route selection strategies have been proposed, which are based on the trust evaluation of the transmission links. Since its route selection is limited on the routes that obtained from standard DSR, the ultimate selected route is not necessarily the most trusted one Xia et al. proposed Fuzzy Trusted Dynamic Source Routing FTDSR protocol [18].The subjective trust evaluation model proposed by the authors use the credibility of nodes can be evaluated using analytic hierarchy process theory and fuzzy logic rules prediction method. The model can detect malicious nodes only if there are few in the numbers

and also the problem of dynamic modification behaviour is not addressed by the authors.

Trust Calculation

Definition: Adhoc network contains many nodes and these nodes are independent in nature and the network can be considered as a weighted graph $G = (V, E, Tv)$, where V is the set of all nodes, E is the set of all edges and $Tv:Tv(E_{ij}) \rightarrow R \in [0,1]$ denotes the value of the trust of the node. There is an edge between two nodes if they are located within each other's transmission range. A path between the source node V_S and the destination node V_D can be represented as a node sequence $P = (V_S, \ldots V_i, \ldots, V_D)$, *where* $V_i \in V$.

The trust model of an ad hoc network can be represented as the weighted directed graph as in the Fig.1. Each node in the model maintains a trust table which contains the trust values of the neighbouring nodes.

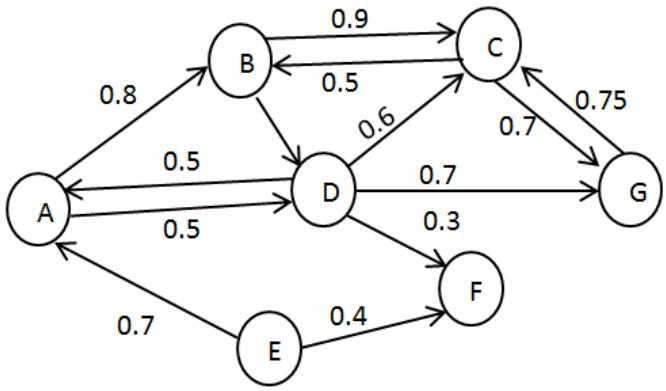

Figure 1: Weighted Graph In The Adhoc Networks

In most existing trust models, direct trust is based on the two neighbour entities historical interactions. In this paper, the trust value is calculated by averaging the weighted forwarding ratio and the similarity factor between the neighboring nodes which forwards packets.

A. Weighted Packet Forwarding Ratio

The ratio of number of packets forwarded correctly to the total number of packets is known as Forwarding Ratio (FR) [19].The packet forwarding ratio at time t is calculated as follows

$$FR(t) = \frac{N_{cor}(t)}{N_{all}(t)} \text{-------(1)}$$

Our proposed model, calculates the trust value with multiple constraints: weight factor assigned to each packet transmitted and time aging factor. Trust normally fades

with time variation. A weight is assigned to each data being forwarded because some malicious nodes may forward data packets if they are of less importance and do not forward data packets of high importance. Based on the above constrains the packet forwarding ratio is modified to compute the trust value. The weighted packet forwarding ratio at time t is given in the equation (2)

$$FR_{(t)} = \frac{\sum_{j=1}^{n} \delta_j}{\sum_{i=1}^{m} \delta_i} \text{--------(2)}$$

δ is the weightage factor for the data based on its importance as shown below in the table 1. *n* is the number of packets correctly forwarded and *m* is the total number of packets forwarded.

Table 1: Weightage of Packets Forwarded

S. No.	**Importance**	**Value**
1.	Important/Rare	>=0.8
2.	Control packets/ Medium	>=0.4 to <0.8
3.	Unwanted	<0.4

The trust information is given by the trust record list which contains monitored node ID, node's trust value, two integer counters of i and j for the number of packets forwarded and the number of packets correctly forwarded without any modifications by the malicious nodes, a packet buffer and weight factor for packet forwarded. It is computed using forwarding count of all packets including the control packets and data packets according to the time t, the trust value of node v_j evaluated by node v_i is calculated by this equation (2).

B. Similarity Factor

Similarity [20] in MANET is a subjective judgment a mobile node makes about another's owned attributes based on its preference and standpoint. Similarity indicates the relationship between user attributes. The mobile nodes having an exactly the same or similar affiliated organization may also have a stronger trust in each other than the ones with different affiliated organizations. Since trust is defined in the context of similarity conditions, the more similar the two users are the greater their established trust would be considered [21]. In order to compute the similarity between users, a variety of similarity measures have been proposed, such as Pearson correlation, cosine vector similarity, Spearman correlation, entropy-based uncertainty and mean-square difference. However, Breese et al in [22] and Herlocker et al. in [23] suggest that Pearson [24] correlation performs better than all the rest.

The notation V_i (a_1, a_2… an) denotes node V_i with n attributes (a_1, a_2,….,a_n). For two nodes V_i and V_j both with n attributes (V_i(a_1, a_2,….,a_n) , V_i(a_1, a_2,….,a_n)), the corresponding attributes have a certain similarity. One node can have more than one

attribute, and these attributes have different numerical ranges. Some are composed of discrete variables, such as velocity and transmission range, where as some are depicted by linguistic description, such as moving direction and affiliated organization. The first step is to assign a unique value to different elements of a given attribute, e.g., the attribute value of velocity is given by its practical value. The established similarity trust between two nodes is defined as the Pearson Correlation [24] given in the equation.

$$ST_{(v_i,v_j)} = \frac{\sum_{k=1}^{n} (V_{i_{a_k}} - \bar{V}_{i_{a_k}})(V_{j_{a_k}} - \bar{V}_{j_{a_k}})}{\sqrt{\sum_{k=1}^{n} (V_{i_{a_k}} - V_{i_{a_k}})^2} \sqrt{\sum_{k=1}^{n} ((V_{j_{a_k}} - V_{j_{a_k}})^2}} \text{---(3)}$$

The Trust value of a node is calculated as follows,

$$TV(t) = \frac{\alpha FR + \beta ST}{2} \text{----------(4)}$$

α and β are the weights for the calculated forwarding ratio and the similarity Trust respectively. The values of α and β are chosen in such a way that $\alpha + \beta = 1$, $0 < \alpha < 1$ and $0 < \beta < 1$.

C. Time Aging Factor

The attenuation rate made by the kth interaction interval compares to the latest interaction interval in the trust computation is defined as the time aging function. Δt is the time interval between the trust calculation and it is 30 s.

$$AF = \frac{f}{(f+1)} \text{-------(5)}$$

$$f = \rho^{n-k}, 0 < \rho < 1, 1 \le k \le n \text{-----(6)}$$

The base coefficient ρ represents the attenuation factor. smaller ρ causes a greater attenuation of *f* and vice versa.

Finally, the node V_i computes node V_j' s trust according to history of interactions via the following equation:

$$TV_{ij}(t) = AF \ X \ TV_{ij}(k) \text{-----(7)}$$

Vector Trust Aggregation Method

To propagate the calculated trust information in the network efficiently and accurately, we define the concept of trust vector, trust transfer and most trustable path. This trust aggregation algorithm is designed to provide fast trust propagation to each node.

A. Trust vector

An edge directed from node A to node B if and only if node B is a neighbour node to node A and can do direct transaction/interaction and A has a direct trust rating towards B. The value of the directed edge A to B reflects how much A trusts B .$T_{A,B}$ = 1 indicates A 100% trusts B , $T_{A,B}$ = 0 indicates A never trust B.

Definition: In Vector Trust, a personalized trust is propagated as a vector of trust rating and direction, where trust rating is defined as a real number T, T∈ [0,1] and direction is defined as a directed edge in the trust graph. This directed link with trust rating is called Trust Vector (TV).

If node A has a trust rating 0.8 on B , the trust vector is $T_{A,B}$ = 0.8 as shown in Fig.2

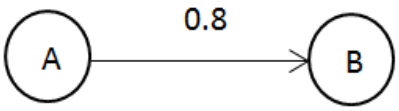

Figure 2: Vector Trust

Suppose *A* wishes to find a trust value for *C* . If *A* and *C* had prior transactions, then *A* can just look up the value of edge $A \rightarrow C$. However, if *A* and *C* have never had a prior transaction, *A* has to infer a trust value for *C* by using trust transfer.

B. Trust Transfer :

If node V_i has a trust rating $TV_{i,j}$ towards node j , node j has trust rating $TV_{j,}k$ towards node k, then node i has indirect trust $TV_{i,k} = TV_{i,j} \times TV_{j,k}$ towards node k.

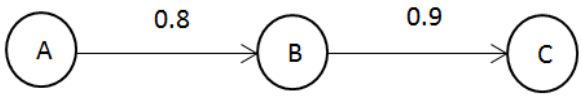

Figure 3: Trust Transfer

As shown by Fig. 3, *A* has indirect trust $T_{A,C}$ toward. *C*. $T_{A,C} = T_{A,B} \times T_{B,C}$ =0.8 × 0.9 = 0.72.

C. Most Trustable Path

There might be many trust paths from node *A* to node *C*. Given a set of paths between *A* and *C*, *A* tends to choose the *Most Trustable Path* (MTP) to finish multihop transactions with an unfamiliar node *C*.

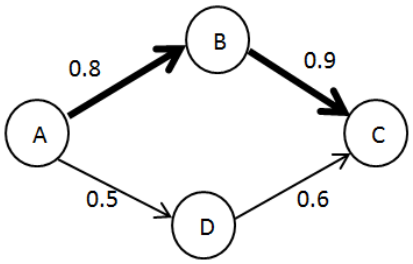

Figure 4: Most Trustable Path

The most trustable path from node *i* to node *k* is the trust path yielding highest trust rating $TV_{i,k}$.

In Vector Trust, the most trustable path can be computed as the maximal product value of all directed edges along a path. And this product will be considered as *A*'s trust rating towards *C* . In the example shown in Fig.4, the MTP is

$A \rightarrow B \rightarrow C$, and *A* infers a trust rating of $T_{A,C} = 0.72$ toward *C* .

For each direct transaction in the system, participating nodes generates a direct trust link and assigns a trust rating based on the calculations used in the section 3 to represent the quality of this transaction. For example, consider a successful transaction between nodes *A* and *B* in which *A* is the neighbor of *B*. After the transaction completes, node *A* assigns a trust rating to reflect the quality of *B*'s service. And a new link starts from *A* with the arrow point to the node *B* will be added in trust graph. *A* stores this rating in its trust table.

The trust table is required for each node. It consist of the destination nodes address as entry, the trust rating, the next hop and the total hops (optional) to reach the destination. Each entry shows only the next hop instead of the whole trust path.

D. Trust Vector Aggregation

In the initial stage of the transmissions in the network, direct trust values calculated by using methods given in the previous section and values are stored in local trust tables. However, the direct trust information is limited and does not cover all potential interactions. For most nodes without adequate direct trust information, they have to use indirect trusts to start the process. An algorithm for *Trust Vector Aggregation* (TVA) is proposed to infer and aggregate trust values. In this algorithm, each trust path is aggregated to MTP with most reliable trust rating towards a target node by the value iteration process. Indirect trust information will be added to a trust table and be updated as the aggregation process evolves. Note that, trust aggregation does not create any new link in the network. Links are created or modified only after direct transactions. The value iteration function used in the Trust Vector Aggregation Algorithm is given in function

$$TV_{ik} = \max(TV_{ij} \; X \; TV_{ik}) \text{ - - - - - (8)}$$

Where $TV_{i,k}$ is the trust rating towards node *k* given node *i* 's local trust table, $TV_{i,j}$ is the direct link trust and $TV_{i,k}$ is the received trust information towards node *k*.

A special case needs to be considered. If node A has a direct trust vector to another node *B*, although the trust rating is lower than an indirect path, Vector Trust still considers the direct trust as the most trustable path. That is, in Vector Trust, the direct experience cannot be replaced by indirect trust inference. Evidence is not as valuable as direct experience. However, this criterion can be relaxed or modified depending on needs of applications. We consider the direct trust more important because that Vector Trust is designed as a personalized trust scheme. In personalized trust rating systems, the node has self-policing trust on other peers, and the node tends to believe their own experiences more than recommendations.

Algorithm to detect trusted node

```
//V_i detects trusted node with this algorithm
detection()
{
 for(each node V_j)
 {
   if(TV_ij(t) > threshold)
            V_j is marked as trusted node;
   else
            V_j is marked as malicious nodes;
 }
}
```

Table 2: Different Meaning Of Trust Strategy

Level	**Trust degree**	**Meaning**
1	(Tthreshold,1]	Trusted node
2	[0,Tthreshold]	Malicious node

Proposed TV-DSR Protocol

In this section, we describe the establishment of the proposed new trust vector based DSR protocol called TV-DSR based on the proposed trust model. We also explain the process of the trusted route discovery and trusted route maintenance.

A. Routing Strategy

The procedure for finding the route in the proposed TV-DSR is given as follows:

Step 1: Before a source s sends a data packet to a destination node d, the source looks up in the local routing cache a routing entry to node d. The qualified route should meet the path trust requirement and should have the aggregated trust values for all the nodes in the route.

Step 2: If there is no such route, node s initiates a route discovery process for d.

Step 3: If one or more paths are discovered, a route entry for these paths will be created and inserted into the routing cache of nodes.

Step 4: If there are more than one path which meet the required path trust limit, node s selects the route with the smallest hop count in the qualified routes.

Step 5: If the paths meet the required limit and have the equal hop count, the route with the maximum path trust will be selected as the routing path.

Step 6: In the route discovery process, a forwarding node would detect malicious nodes according to its local trust record list and look for other valid routes in its routing cache.

Step 7: Node s starts to transport data packets.

Step 8: If a qualified route is not selected, node s will return no qualified routes. Go to step 2

In particular, every node maintains a local trust table which contains the trust value of the neighbour node. Before transmitting a packet from the neighbour node, the node compares the trust value with the threshold value, if it is less than the threshold value, then it is considered as the malicious node and is excluded by its neighbour. That is, the packets from a malicious node will not be forwarded by its neighbour node; meanwhile, the neighbour will not send packets to the malicious node except broadcast packets. If a node's trust value is evaluated very low by all its neighbours, any reply it gives to route requests is discarded, and any request it initiates is ignored. In other words, when a node is considered as malicious, it will be excluded from the local network.

B. Route Discovery

Route discovery is the mechanism by which a node wishing to send a packet to a destination node d obtains a source route to d. Route discovery is used only when s attempts to send a packet to d and does not already know a route to d.

Step 1: Source node s initiates a route discovery by broadcasting a ROUTE REQUEST (RREQ) packet that contains the destination address s to its neighbours. The neighbours in turn append their own addresses to the RREQ packet and rebroadcast it. This process continues until a RREQ packet reaches d.

Step 2: Destination node d initiates the decision process backwards to the source node s. Current states select next-hop state using the trust table values and store the chosen state in their route tables. After the vector trust aggregation algorithm finishes, each state obtains its optimal route and the route discovery is implemented.

C. Route Maintenance

Route maintenance is the mechanism by which node s is able to detect, while using a source route to d, if the network topology has changed such that it can no longer use its route to d because a link along the route no longer works. When route maintenance indicates that a source route is broken, s attempts to use any other route it happens to know to d or invokes a route discovery again to find a new route. Route maintenance is used only when s is actually sending packets to d. A link-broken event will trigger a new trust evaluation process and trust route-update process. Also, route maintenance assures the route is integrated and valid in a certain time interval.

Experimental Results

Our protocol in this paper is extended from DSR which is a standard and widely used routing protocol for wireless ad hoc network. To enhance the security of DSR, the vector based trust management model is incorporated in to the protocol and a novel protocol called TV- DSR is proposed. While maintaining the advantage of original protocol, the new protocol is added with security features which mitigate any type of attacks from the malicious nodes. To evaluate the performance of DSR and TV-DSR we have conducted a comprehensive test using NS-2 network simulator [25].

A. Experimental Setup

Ns2 simulator is used to evaluate the performance of the newly proposed protocol under different scenarios. Within a rectangular field of 1000 m × 1000 m, 25 nodes are randomly dispersed and the transmission radius of every node in one hop is fixed at 250 m. The node mobility uses the random waypoint model [26] in which each packet starts its journey from a location to another at a randomly chosen speed. A maximum speed of 0 m/s implies that the MANET is a static network. The fixed simulation parameters in NS-2 are listed in Table 3

Table 3: Simulation Parameters

Parameter	**Value**
simulation time	200 s
number of nodes	25
map size	1000 m×1000 m
mobility model	random way point
traffic type	constant bit rate (CBR)/UDP
transmission radius	250 m
packet size	512 bytes
connection rate	4 pkts/s
pause time	2 s

B. Performance Metrics

We use 3 metrics to evaluate the performance of these routing protocols, in which the first two metrics are the most important for best effort route and transmit protocols.

1. Packet delivery ratio: the fraction of the data packets delivered to destination nodes to those sent by source nodes.
2. Average end-to-end latency: the average time taken by the data packets from sources to destinations, including buffer delays during a route discovery, queuing delays at interface queues, retransmission delays at MAC layer and propagation time.
3. Routing packet overhead: the ratio of the number of control packets (including route request/reply/update/error packets) to the number of data packets.

C. Scenario 1: Varying Node Speeds

In the first scenario, we compare TV-DSR with DSR as the maximum speed of nodes varies from 0 to 30 m/s. As shown in Fig. 5 a, the delivery ratio of DSR declines remarkably as nodes speed up, whereas the delivery ratio of TV-DSR decrease gently. The differences become more apparent at higher speeds. The node in DSR only implements the traditional routing protocol, which only maintains one shorter route to a destination and is unable to improve packet delivery in case of route break. TV-DSR has higher delivery ratios than DSR because it obtains a more accurate trust value for node which elevates the probability of successful delivery.

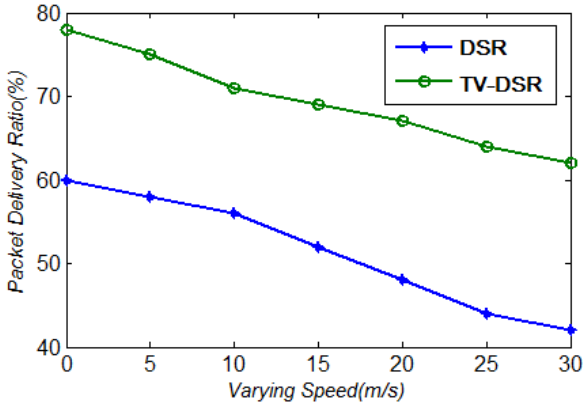

Figure 5a: Packet Delivery Ratio vs Varying Speed

Fig. 5b illustrates that the average end-to-end latency in these protocols rise with the increase of maximum speed. At higher speeds, route entries become invalid more quickly and thus source nodes initiate more route rediscoveries before sending data. At the highest speed of 30 m/s, the average latency reaches their peaks, respectively. TV- DSR has a lower average latency than DSR when the speed is greater than 5 m/s because it avoids malicious nodes more accurately, thus reducing the risk of adding delay for resenting the failed routing packets.

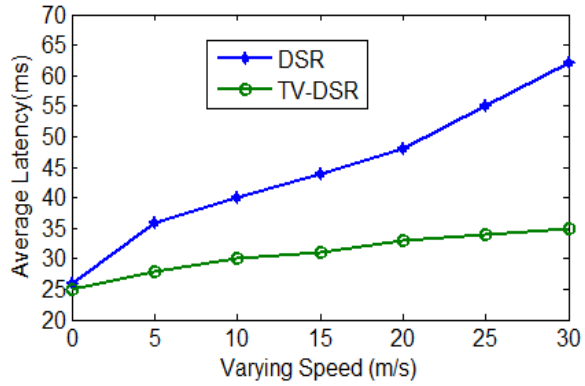

Figure 5b: Average Latency vs Varying Speed

In Fig. 5c, the routing packet overhead in these protocols rises with the increase of maximum speed. When the speed is smaller than 13 m/s, the overhead in TV-DSR remains comparatively higher than that in DSR. The reasons for different period are: (i) More RREQ and RREP packets need to be sent for qualified routes to meet trust requirement in TV-DSR and meanwhile, trust requirement is not considered in DSR; the additional route update and maintenance packets increase the amount of control packets and the routing packet overhead in TV-DSR. Along with the speed increasing, there is an opposite impact. As the nodes move faster, the number of interactions between the nodes increases gradually. The trust is transferred to the entire network. For the low credibility of the nodes, in the route discovery process of the future, the network does not need to send route query packets to them again, and this reduces the routing overhead. But in DSR, along with the increase of maximum speed, the routing routes break down easily, leading to send more route request and route maintenance packets.

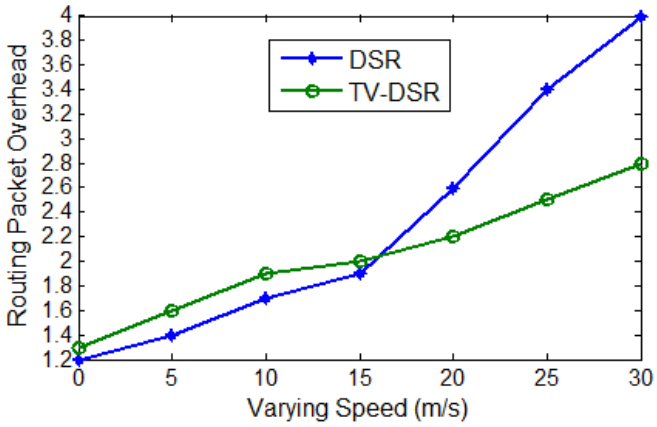

Figure 5c: Routing Packet Overhead vs Varying Speed

D. Scenario 2: Varying Number of Malicious Nodes

In scenario 2, the proposed protocol is evaluated by varying number of malicious nodes. When there are no malicious nodes, the packet loss rate is about 3% in DSR, and TV- DSR. As shown in Fig. 6a. the delivery ratios in the protocols degrade sharply as the number of malicious nodes increases. The delivery ratio of DSR drops from 97 to 35% as the number of malicious nodes varies from 0 to 10. Malicious nodes essentially limit interactions between nodes in the network.

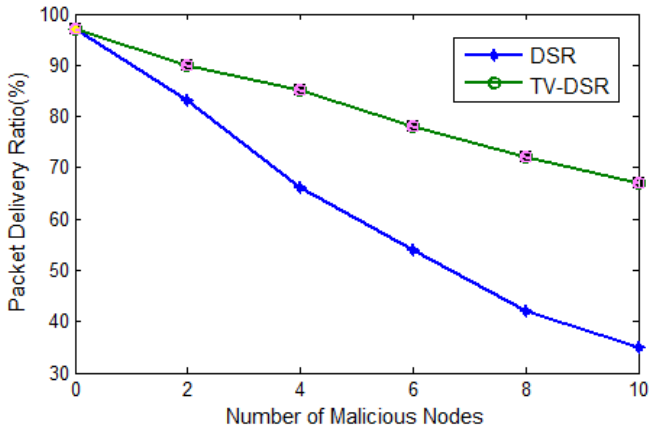

Figure 6a: Packet Delivery Ratio vs Number of Malicious Nodes

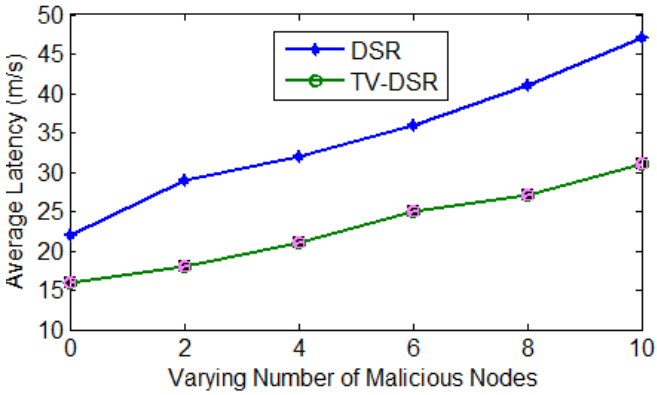

Figure 6b: Average Latency vs Varying Number of Malicious Nodes

As shown in Fig. 6b, the average latency in TV-DSR ascends slowly with the increase in number of malicious nodes, but the average latency in DSR arises sharply. This average latency is mainly caused by queuing delays and retransmission delays. But there is an apparent reduction in the average latency with TV- DSR when compared to DSR. As a result, in the process of establishing a trusted routing route, the network will be possible to avoid the suspect and malicious nodes. This can contribute to effectively reduce the end-to-end latency.

When the number of malicious nodes increases to 10 (33% of the whole nodes), the routing packet overhead of TV-DSR is approximately 2.8 as shown in Fig. 6c. The value is smaller than the routing packet overhead in DSR. When the number of malicious nodes is smaller than 5, the routing packet overhead in TV-DSR is bigger than in DSR, the reason is that, the increased control packets in TV-DSR is primarily due to its route discovery mechanism that broadcasts more RREQ and RREP packets to look for trustworthy routes to destinations. When the number of malicious nodes is bigger than 5, the routing packet overhead in TV-DSR is smaller than DSR, because of the huge damage on routing path from malicious nodes.

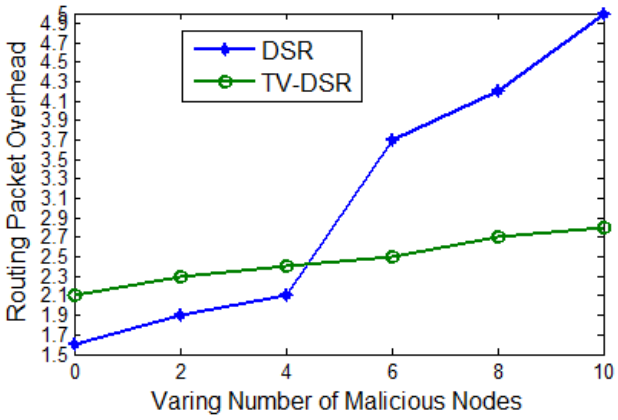

Figure 6c: Routing Packet Overhead vs Varying Number of Malicious Nodes

The experimental results in scenarios 1 and 2 shows that TV-DSR performs better than DSR, as TV-DSR gives higher delivery ratio, minimizes average latency and decreases the control packet overhead.

Conclusion

In this paper, a novel vector trust management model has been proposed. First, to establish a new trust evaluation model, the trust value is calculated based on the factor namely forwarding ratio with weight assigned to each packet based on the importance of the packets. The nodes which do not have any direct trust value, vector trust aggregation method is used to infer the trust for the other nodes in the network. Then taking the trust value as the input, a trusted routing model is proposed. The proposed trust vector based Dynamic Source Routing protocol called as TV-DSR is on the basis of the standard DSR protocol, which can eradicate the untrustworthy nodes such that a reliable passage delivery route is obtained. Performance comparison of standard DSR and proposed TV-DSR shows that TV- DSR is able to achieve a significant improvement in the packet deliver ratio in the presence of malicious nodes.

For future work, ,in order to avoid node failures because of the depletion in a node, residual power of nodes will also be considered along with the calculated trust value . The proposed trust model will be incorporated into other protocols namely AODV and TORA

References

[1] Ramana KS, Chari AA, Kasiviswanth N. Trust based security routing in mobile adhoc networks.International Journal on Computer Science and Engineering 2010;2(2):259–63

[2] D.Denning,"A New Paradigm for Trusted Systems," Proc. ACM New Security Paradigms Workshop, pp. 36-41, 1993

[3] C.E. Perkins, E.M. Royer, S.R. Das, Ad-hoc on-demand distance vector routing, in: Proceedings of International Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, Louisiana, USA, February 1999, pp. 90–100.

[4] D. Johnson, D. Maltz, Dynamic source routing in ad hoc wireless networks, in: I. Tomasz, K. Hank (Eds.), Mobile Computing, first ed., Kluwer Academic Press, 1996, pp. 153–181.

[5] Vincent D. Park, M. Scott Corson, Temporally-Ordered Routing Algorithm (TORA) version 1: functional specification, Internet- Draft, draft-ietf-manet-tora-spec- 00.txt, November 1997

[6] Kamvar SD, Schlosser MT, Molina H-G (2003) The eigentrust algorithm for reputation manage- ment in p2p networks. In: Proceedings of the 12th international conference on world wide web (WWW2003), Budapest, Hungary, May 20–24, 2003, pp 640–651

[7] E.M. Royer, C.K. Toh, A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Communications Magazine 6 (2) (1999) 46–55.

[8] J. Lundberg, Routing Security in Ad hoc Networks, Technical Report Tik110.501, Helsinki University of Technology, 2000.

[9] W.L.H. Deng, D.P. Agrawal, Routing security in wireless ad hoc networks, IEEE Communications Magazine (2002) 70–75.

[10] N. Griffiths, A. Jhumka, A. Dawson, R. Myers, A simple trust model for on-demand routing in mobile ad-hoc networks, in: Proceedings of International Symposium on Intelligent Distributed Computing (IDC 2008), 2008, pp. 105–114.

[11] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, Mobile Computing and Networking (2000) 255–265.

[12] T. Hughes, J. Denny, P.A. Muckelbauer, J. Etzl, Dynamic trust applied to ad hoc network resources, in: Proceedings of the Autonomous Agents and Multi-Agent Systems Conference, 2003, pp. 273–280.

[13] K. Meka, M. Virendra, S. Upadhyaya, Trust based routing decisions in mobile ad-hoc networks, in: Proceedings of the Workshop on Secure Knowledge Management (SKM 2006), 2006.

[14] C.D. Jensen, P.O. Connell, Trust-based route selection in dynamic source routing, Proceedings of International Conference on Trust Management (2006) 150–163.

[15] A.A. Pirzada, C. McDonald, A. Datta, Performance comparison of trust-based reactive routing protocols, IEEE Transactions on Mobile computing 5 (6) (2006) 695–710.

[16] J. Manickam, Leo Martin, S. Shanmugavel, Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET, Advanced Computing a A novel trust based security framework to identify 2003.

[17] Guo, W., Xiong, Z.W., Li, Z.T.: 'Dynamic trust evaluation based routing model for ad hoc networks'. Proc. Wireless Communications, Networking and Mobile Computing, September 2005, vol. 2, pp. 727–730

[18] Xia, Hui, et al. "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory." Wireless Sensor Systems, IET1.4 (2011): 248-266

[19] Xia, Hui, Zhiping Jia, Xin Li, Lei Ju, and Edwin H-M. Sha. "Trust prediction and trust-based source routing in mobile ad hoc networks." *Ad Hoc Networks* 11, no. 7 (2013): 2096-2114

[20] Wang, Jian, Yanheng Liu, and Yu Jiao. "Building a trusted route in a mobile ad hoc network considering communication reliability and path length." Journal of Network and Computer Applications 34.4 (2011): 1138-1149.

[21] Ziegler, C.N. and Lausen, G. "Analyzing Correlation Between Trust and User Similarity in Online Communities". Proc. of the 2 nd International Conference on Trust Management, 2004

[22] Breese, J. S., Heckerman, D. and Kadie, C. "Empirical analysis of predictive algorithms for collaborative filtering". Proc. of the 14 th Conference on Uncertainty in Artificial Intelligence, 1998

[23] Herlocker, J. L., Konstan, J. A., Borchers, A., and Riedl, J. "An Algorithmic Framework for Performing Collaborative Filtering". Proc. of the 22nd ACM SIGIR Conference on Research and Development in Information Retrieval, 1999

[24] Pearson K. "Mathematical contribution to the theory of evolution: VII, on the correlation of characters not quantitatively measurable". Phil. Trans. R. Soc. Lond. A, 195, 1-47, 1900.

[25] http://www.isi.edu/nsnam/ns/

[26] Bettstetter, C., Resta, G., Santi, P.: 'The node distribution of the random waypoint mobility model for wirelessad hocnetworks',IEEE Trans.Mobile Comput., 2003, 2, (3), pp. 257–269