VOL. 10, NO. 18, OCTOBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ENERGY BASED TRUSTEDSOURCE ROUTING PROTOCOL FOR MOBILE ADHOC NETWORKS

V. Jayalakshmi[1] and T. Abdul Razak[2]
[1]Research and Development Centre, Bharathiar University, Coimbatore, India
[2]Department of Computer Science, Jamal Mohamed College, Tiruchirappalli, India
E-Mail: jayasekar1996@yahoo.co.in

ABSTRACT

Secure transmission in Mobile Ad Hoc Networks has proven to still be a challenging task due to the openness in network topology and absence of a centralized administration. In order to enhance the security of network and protect the nodes from vulnerabilities, this paper proposes a novel energy based trusted routing scheme to select the most trustable path based on the route trust and also the energy level of nodes in the route. The path obtained by using this scheme not only includes the nodes with high trusted values but also excludes the nodes which have low residual energy. We have integrated the proposed model into the popular DSR routing protocol. Our novel on-demand trust-based source routing protocol for MANETs, called as Energy based Trusted DSR routing protocol (ET-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 ET-DSR protocol selects trustworthy and energy based and improves the overall performance of the protocol in presence of malicious nodes.

Keywords: DSR, energy, malicious node, MANET, security, trust.

INTRODUCTION

Mobile ad hoc network is a collection of mobile nodes without any centralized infrastructure in which each node act as a host as well as a router. Nodes in the network must rely on other nodes in the network to communicate. 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. AODV [2], DSR [3], and TORA [4] are three well-known reactive routing protocols which are undergoing wide range of active research. These protocols have been developed for networks assuming that all nodes participating in the network are reliable and trust worthy without any malicious intentions.

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. To save battery, bandwidth, and processing power, nodes should not forward packets for others. Without countermeasures, the effects of misbehaviour have been shown to dramatically decrease network performance. Depending on the proportion of misbehaving nodes and their strategies decrease in network throughput, packet loss, denial of service and network portioning may occur. These detrimental effects of misbehaviour can endanger the entire network.

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 the routing protocols. Trust management is required in the collection and distribution of evidences to assess or maintain the levels of trust required for successful task completion. The inherent freedom in self-organized mobile ad hoc networks introduces challenges for trust management. The nodes often behave maliciously or selfishly caused by their inherent nature as well as environmental or operational conditions [5]. That is, other than being affected by their given nature, nodes are also affected by operational conditions. For example, a node is much more likely to be selfish to save its own energy particularly when the energy level is low. Further, a node can be compromised. We relate the energy level of a node with the rate at which the node may be compromised. That is, a node is more likely to be compromised when its energy level is low and vice versa since a node with high energy is more capable of defending itself against attackers by performing more energy-consuming defence mechanisms. Note that the association between a node's status and its behaviour is based on the assumption that each node has its own inherent nature to trigger bad behaviour.

Some trust management models have been developed for wired networks but they are inapplicable to MANETs because of their dynamic topology and application scenario. Our work takes into account the dynamically changing conditions in MANET environments. In this paper, a novel trust management scheme is proposed which uses not only the trust value of a node but also the residual energy level of a node. 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 [6]. The residual energy of a node is calculated to mitigate the attacks from the selfish nodes. The nodes with low energy will not forward the packets in order to save their battery power. The most trustable path is obtained by considering both the calculated trust value and also the residual energy of a node. An application of the proposed energy based trust model, a novel reactive routing protocol called Energy based Trusted Dynamic Source Routing Protocol (ET-DSR) is proposed on the basis of the standard DSR protocol. The proposed protocol kicks out the malicious nodes and also the selfish nodes which have low battery power and establish 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 method for obtaining residual energy of a node. In section 5, the algorithm for obtaining the most trustable path is given. In section 6, we present the proposed new ET-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 [3], and AODV [2] focused on problems that mobility presented to the accurate determination of routing information. 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.* [9] further discuss energy consumption and black hole attacks along with impersonation and routing information disclosure.

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 [10], 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 [11]. 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 [12], Marti *et al.* extend DSR by adding 'watchdog' and 'path-rater' mechanisms. This protocol avoids the malicious nodes in routing and it does not impose any penalty to them. This allows a lazy or selfish node not to forward packets for its neighbours and remain in active in the network. In [13], Hughes *et al.* propose Dynamic Trust-based Resources (DyTR), which uses trust evaluation as a method of access control to network resources. In this work, the trust information is not exchanged securely. Pirzada and McDonald develop a protocol based on DSR in [14]. The authors consider only the direct trust and the recommendation trust based on the third party opinion is not considered. In their protocol, lazy nodes which do not participate in the transmission are not penalized. Trusted-DSR [15] 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. 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. Jensen *et al* [16] has also proposed trust-based route selection in dynamic source routing (DSR). Each router is assigned a trust score based on past experience, and the trustworthiness of a candidate path is a function of that of the routers that make up that path. As another extension to DSR, Guo *et 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 author uses the credibility of nodes can be evaluated using analytic hierarchy process theory and fuzzy logic rules prediction method. The dynamic modification behaviour is not addressed by the authors.

In the proposed trust based routing protocols in the literature, the energy level of the node is not taken as the parameter to evaluate the trust worthiness of a node. In this paper, we consider the residual battery power of a node in obtaining the trusted path since the nodes with low energy may be compromised.

TRUST MODEL

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 Figure-1. Each node in the model maintains a trust table which contains the trust values of the neighbouring nodes.

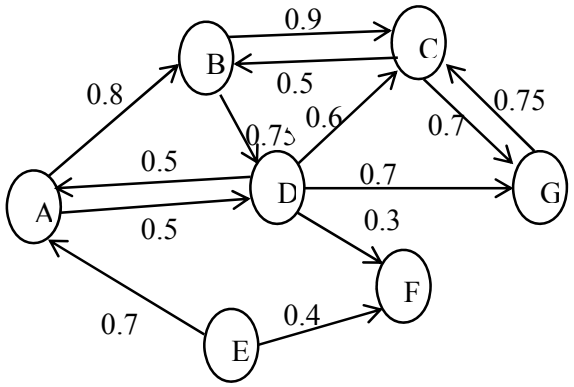

Figure-1. Weighted graph in the ad hoc networks.

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 neighbouring nodes which forwards packets.

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

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

Our proposed model, calculates the trust value based on weight factor assigned to each packet transmitted. 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 constrain 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).

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

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).

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. 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 [21] and Herlocker *et al*. in [22] suggest that Pearson [23] 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 ($V_i(a_1, a_2,\ldots,a_n)$, $V_i(a_1, a_2,\ldots,a_n)$), 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 [23] given in the equation.

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

The Trust value of a node is calculated as follows,

$$TV_{ij}(t) = \frac{\alpha FR + \beta ST}{2} \quad (4)$$

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 $0 < \beta < 1$.

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 15 s.

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

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

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:

$$TV_{ij}(t) = AF \; X \; TV_{ij}(k) \quad (7)$$

RESIDUAL ENERGY MODEL

The nodes in the network may be in various states namely compromised or malicious, selfish or trustworthy. The energy level of node is associated with its state. Depending on the amount of remaining energy, each node acts differently. The rate of energy consumption is also affected by the node's status. Thus, these parameters are linked and affect the node's lifetime considerably.

Energy dissipation rate in a given node can be measured by the metric known as the drain rate [24]. Each Node V_i monitors its energy consumption caused by the transmission, reception, and overhearing activities and computes the energy drain rate, denoted by DR_i for every t seconds sampling interval by averaging the amount of energy consumption and estimating the energy dissipation per second during the past t seconds. In this work, t is set to 15 seconds.

$$DR_i = E_{SP} + E_{RP} + E_{DP} + E_{IS} \quad (8)$$

Where E_{SP}, E_{RP} and E_{DP} stands for energy expended on sending, receiving and dropping packets respectively. E_{IS} is the energy consumed by node when it is in idle state or wait state. In the sleep mode, the node consumes less energy and it is not taken for the consideration in this work.

The energy exhausted in sending a data-packet of size P_{size} bytes from anode can be modled as

$$E_{SP}(node) = c1P_{size} + c2 \quad (9)$$

The energy exhausted in receiving a data-packet of size P_{size} bytes from anode can be modled as

$$E_{RP}(node) = c1P_{size} + c2 \quad (10)$$

Where c1 and c2 are the incremental costs and fixed costs incurred in sending the packets.

$c1 = Power_{packet} / BR$

$c2 = (Power_{MAC} \times MAC_{size} + Power_{packet} \times P_{Header})/BR$

$Power_{packet}$ is the power at which the data packets are transmitted/received , $Power_{MAC}$ is the power at which the MAC packets are transmitted/received, MAC_{size} is the size of the data packets in bytes ,P_{Header} is the size of the data-packet trailer and header in bytes and BR is the transmission or receiving rate in Bytes/sec.

The residual battery power at node V_i RBP_i can be calculated as follows:

$$RBP_{t_i} = \frac{P_t(V_i) - DR_i}{P(V_i)} \quad (11)$$

$P(V_i)$ be the initial power level of node V_i, DR_i is the draining rate of the node V_i and $P_t(V_i)$ is the power of the node V_i at time t.

The energy value will vary from 1 to 0 with 1 corresponding to full energy level and 0 for all energy depleted (dead node). In order to isolate the selfish nodes in the trusted path, the nodes which have more residual battery power are chosen for the transmission. The energy

threshold η is used. Node should have more residual battery energy (RBE) than energy threshold η to transmit the packet to the next node in the route. And those nodes having equal RBE than energy threshold η are made to go into sleep mode. This selecting criterion helped to prolong the network life by avoiding the link breakage. The calculated RBP value is stored in the local trust table along with the trust values for the neighbouring nodes.

MOST TRUSTABLE PATH ALGORITHM

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 multi hop transactions with an unfamiliar node *C*.

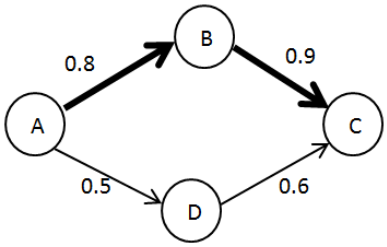

Figure-2. Most trustable path.

For example, if node A wants to send packets to the neighbouring nodes B and D. First it checks the trust value of the nodes. The trust value of B is high when compared to node D. After selecting the trusted node, it checks the RBP value of the node with the energy threshold η. If it is more, then that node is selected for sending the packets. The most trustable path from node*i* to node*k* is the trust path yielding highest trust rating $TV_{i,k}$.

In Vector Trust [25], 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 Figure-2, the MTPis

$A \rightarrow B \rightarrow C$, 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 neighbour 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 server *B* will beaded in trust graph and also the residual battery energy is also computed and its value is also stored along with the trust value in the trust table. So, each transaction in the system can either adds a new directed edge in the trust graph, or relabels the value of an existing edge with its new trust value or a compound value of both old and new trust ratings.

The trust table is required for each node. It consists of the destination nodes address as entry, the trust rating, residual battery energy, 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.

$$TV_{ik} = \max(TV_{ik}, TV_{ij} X TV_{ik}) \quad (12)$$

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*.

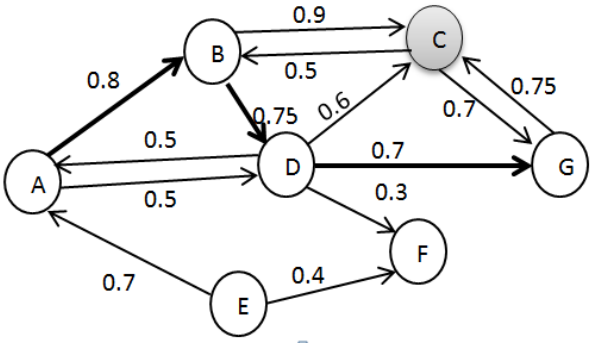

Figure-3. An example network with 7 nodes.

In the above network with 7 nodes, A is the source node and G is the destination node. There are 3 paths exists in the Figure-5. A→B→C→G, the computed trust rating for this path is 0.504, the path A→D→G has the trust path rating of 0.35 and the path A→B→D→G has the trust path rating of 0.42.

Though the path A→B→C→G gives the higher trust ratings than the other computed paths, the node C is having less RBE than energy threshold η and is made to go into sleep mode.

Considering the other two paths, the path with more trust rating is chosen as the most trustable path to transmit packets to the destination.

Algorithm for selecting the most trusted path

1. Arrange the trusted paths TP = TP_1, TP_2, TP_3..TP_n in the decreasing order of trust values and increasing order of hop counts
2. Initialize j=1 (choose the first path with the highest trust value)
3. For $\forall$ nodes V_i in the path P_j,

If $RBP_{V_i} > \eta$ then select the path for secure transmission

4. Else select the next path in the list by incrementing j value
5. Go to step 2
6. If all paths are exhausted then wait for another path
7. If no paths are left then there is no possible to route transmission securely

PROPOSED ET-DSR PROTOCOL

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

Routing strategy

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

Step 1: Before a source s sends a data packet to a destination node (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 all the nodes in the route should have greater RBE than energy threshold r_t.

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

Step 3: If one or more most trustable paths are discovered with nodes with high residual energy, 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 and battery life, 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 and maximum residual energy will be selected as the routing path.

Step 6: In the route discovery process, a forwarding node would detect malicious nodes and selfish 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 and the RBE of the node. Before transmitting a packet from the neighbour node, the node compares the trust value and RBE with the threshold value, if it is less than the threshold value, then it is considered as the malicious and selfish 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. The nodes with low RBE values when compared to the energy threshold are made in to sleep node. 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.

Route maintenance

Route maintenance is needed for two reasons:

Mobility

Connections between some nodes on the path are lost due to their movement,

Energy Depletion

The energy resources of some nodes on the path may be depleting too quickly.

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. Some of the nodes may be made into sleep mode because of their low RBE level. When route maintenance indicates that a source route is broken, s attempts to use any there 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, along with the computed trust value [6], the energy level of a node is also taken into consideration for finding the reliable route and this energy based trust management model is incorporated in to the protocol called as ET-DSR. 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 and also from the selfish nodes. To evaluate the performance of DSR, TV- DSR and ET-DSR we have conducted a comprehensive test using NS-2 network simulator [26].

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 [27] 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 initial energy of all the nodes is 120J. The transmission power is

200mW and the receiving power is 100mW. The simulation parameters in NS-2 are listed in Table-3.

Table-2. 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
Energy of each node	Joule

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.

a) **Packet delivery ratio:** the fraction of the data packets delivered to destination nodes to those sent by source nodes.
b) **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.
c) **Routing packet overhead:** the ratio of the number of control packets (including route request/reply/update/error packets) to the number of data packets.

Scenario 1: Varying node speeds

In the first scenario, we compare ET-DSR with TV-DSR and DSR as the maximum speed of nodes varies from 0 to 30 m/s. As shown in Figure-4a, the delivery ratio of DSR declines remarkably as nodes speed up, whereas the delivery ratio of ET-DSR and 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. ET-DSR has higher delivery ratios than DSR and TV-DSR because it obtains a more accurate trust value for the node and also the nodes with low residual battery level are not chosen for the transmission which elevates the probability of successful delivery.

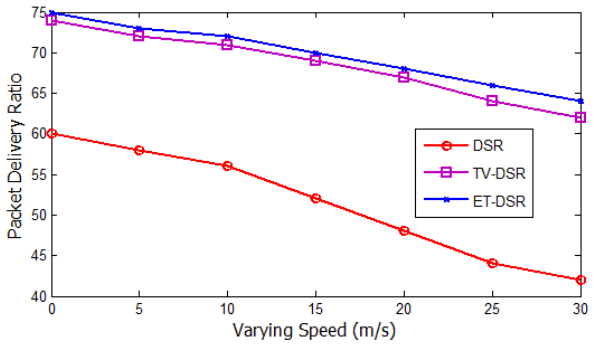

Figure-4a. Packet delivery ratio vs varying speed.

Figure-4b 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. ET-DSR has a lower average latency than DSR when the speed is greater than 5 m/s because it avoids malicious nodes and selfish nodes more accurately, thus reducing the risk of adding delay for resending the failed routing packets.

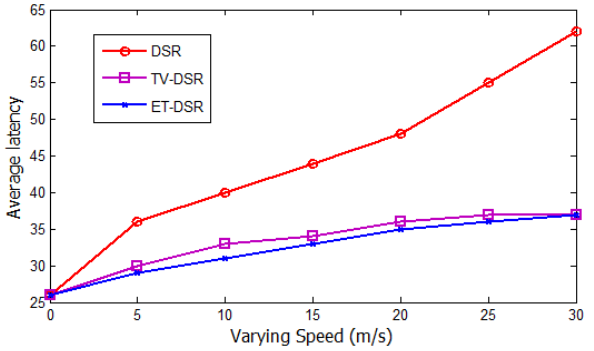

Figure-4b. Average latency vs varying speed.

In Figure-4c, 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 ET-DSR and 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 and energy requirement in ET-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 ET-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 and route is chosen considering both the trust value and the energy level of node so there is no link

failure. 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.

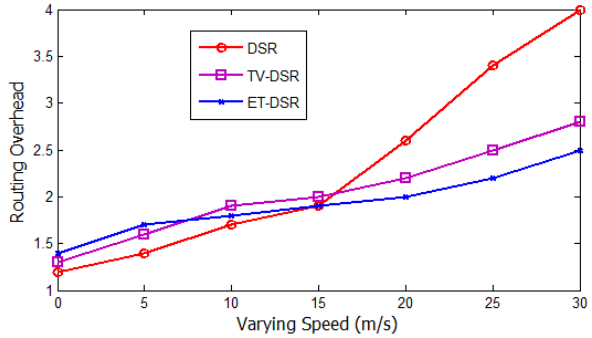

Figure-4c. Routing packet overhead vs varying speed.

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, TV-DSR and ET-DSR. As shown in Figure-5a, 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.

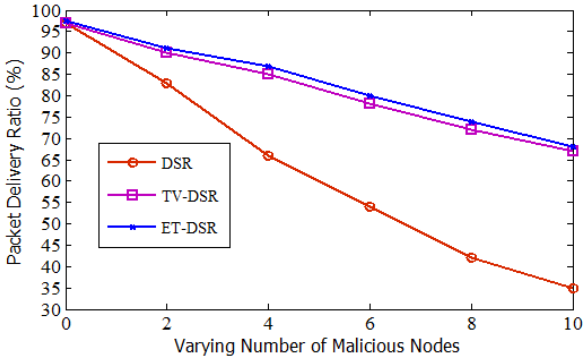

Figure-5a. Packet delivery ratio vs number of malicious nodes.

As shown in Figure-5b, the average latency in ET-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 ET-DSR and TV-DSR when compared to DSR. As a result, in the process of establishing a trusted routing route with nodes with high energy level, the network will be able to avoid the suspect and malicious nodes. Additionally in the proposed ET-DSR protocol, the nodes with low energy level are not selected which extend the life time of the network and the path. So there is a reduction in the number of RREQ sent. This can contribute to effectively reduce the end-to-end latency

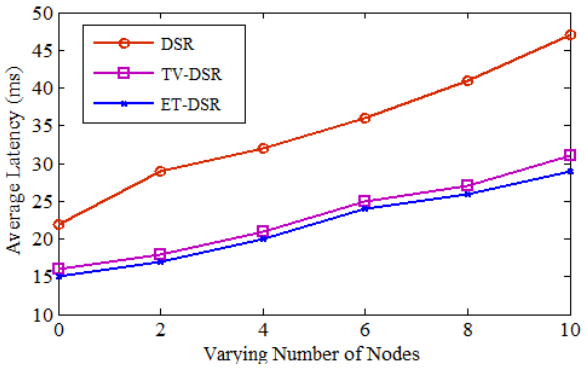

Figure-5b. Average latency vs number of malicious nodes.

When the number of malicious nodes increases to 10 (40% of the whole nodes), the routing packet overhead of ET-DSR is approximately 2.8 as shown in Figure-5c. 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 ET-DSR is bigger than in DSR, the reason is that, the increased control packets in ET-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 ET-DSR is smaller than DSR, because of the huge damage on routing path from malicious nodes.

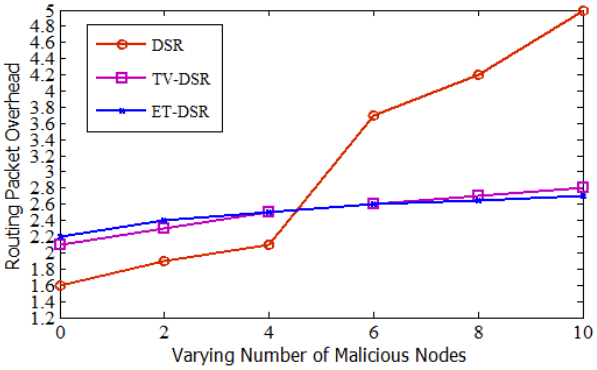

Figure-5c. Routing packet overhead vs nmber of malicious nodes.

The experimental results in scenarios 1 and 2 show that ET-DSR performs better than TV-DSR DSR, as

ET-DSR gives higher delivery ratio, lower end to end delay and less packet overheads.

CONCLUSIONS

In this paper, a novel energy based trust management model has been proposed. First, to establish a new trust evaluation model, the trust value is calculated based on the factors namely weighted forwarding ratio and the similarity factor. The residual energy level of each node is obtained. Then taking the trust value and the RBP as the input, a trusted routing model is proposed. The proposed energy based trusted Dynamic Source Routing protocol called as ET-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. In this protocol, a source establishes optimal trustworthy paths in a single route discovery. This protocol provides a flexible and feasible approach to choose a better path in all path candidates with trust constraint. Performance comparison of standard DSR,TV-DSR and proposed ET-DSR shows that ET-DSR is able to achieve a significant improvement in the packet delivery ratio in the presence of malicious nodes and selfish nodes.

For future work, to derive a more accurate trust value we plan to incorporate other influencing trust decision attributes to the trust model. Apart from the energy as a QoS metric, other criterion can be used to determine the optimum route to set up Route. The weighted average of the criteria into consideration when selecting a route in future works. The proposed trust model will be incorporated into other protocols namely AODV and TORA.

REFERENCES

[1] Ramana K. S, Chari A A, Kasiviswanth N. 2010. Trust based security routing in mobile adhoc networks. International Journal on Computer Science and Engineering. 2(2): 259-63.

[2] 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. pp. 90-100.

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

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

[5] Cho Jin-Hee, Ananthram Swami and Ray Chen. 2012. Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks, Journal of Network and Computer Applications. 35.3: 1001-1012.

[6] Jayalakshmi V., Abdul Razak T., TV-DSR. 2015. Trust Vector Based DSR Protocol For Secure Routing In Mobile Adhoc Networks. International Journal of Applied Engineering Research. 10(9): 23797-23814.

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

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

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

[10] Arshad Junaid and Mohammad Ajmal Azad. 2006. Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks, Sensor and Ad Hoc Communications and Networks. SECON'06.3rd Annual IEEE Communications Society on. Vol. 3. IEEE.

[11] 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). pp. 105-114.

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

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

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

[15] C. D. Jensen, P.O. Connell. 2006. Trust-based route selection in dynamic source routing. Proceedings of

International Conference on Trust Management. 150-163.

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

[17] Guo W., Xiong Z. W., Li Z. T. 2005. Dynamic trust evaluation based routing model for ad hoc networks. Proc. Wireless Communications, Networking and Mobile Computing, September. 2: 727-730.

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

[19] Xia Hui, Zhiping Jia, Xin Li, Lei Ju and Edwin H. M. Sha. 2013. Trust prediction and trust-based source routing in mobile ad hoc networks, Ad Hoc Networks. 11(7): 2096-2114.

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

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

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

[23] Pearson K. 1900. 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.

[24] Kim D. , Garcia-Luna-Aceves J. J., Obraczka K., Cano J. C. and Manzoni P. 2003. Routing mechanisms for mobile ad hoc networks based on the energy drain rate. Mobile Computing, IEEE Transactions on. 2(2): 161-173.

[25] Zhao H. and Li X. 2013. Vector Trust: trust vector aggregation scheme for trust management in peer-to-peer networks. The Journal of Supercomputing. 64(3): 805-829.

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

[27] Bettstetter C., Resta G., Santi P. 2003. The node distribution of the random waypoint mobility model for wireless ad hoc networks. IEEE Trans. Mobile Computing. 2(3): 257-269.