Trust Based Power Aware Secure Source Routing Protocol using Fuzzy Logic for Mobile Adhoc Networks

V. Jayalakshmi *Member, IAENG* and T. Abdul Razak

***Abstract*— Secure transmission without node failure in Mobile Ad hoc Network is a challenging issue because of the absence of centralized administration, openness in the network topology and limited batter power in the nodes. In order to enhance the security of network and protect the nodes from vulnerabilities, this paper proposes a novel trust based power aware routing scheme which uses fuzzy logic prediction rules to select the most trustable path. 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 battery power. 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 Trust based Power Aware DSR routing protocol (FTP-DSR), provides a flexible and feasible method to choose the route that meets the security requirement of data packets transmission. 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 FTP-DSR improves packet delivery ratio and reduces average end-to-end latency when compared to the standard DSR routing.**

***Index Terms*— DSR, fuzzy logic, malicious node, power aware, trust, vulnerabilities**

I. 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. Trust management in MANETs is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves. Trust management is also required in the collection and distribution of evidences to assess or maintain the levels of trust required for successful task completion. 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, an entity has confidence on another entity without any previous experience in order to achieve their 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 defend the network from any attacks from the malicious nodes and selfish 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 a lot of 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.

The authors [6] assume that nodes often behave maliciously or selfishly caused by their inherent nature as well as environmental or operational conditions. 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

Manuscript received June 07, 2015; revised January 29, 2016

V.Jayalakshmi is with the Research and Development Center, Bharathiar University, Coimbatore, Tamilnadu, India. (E-mail: jayasekar1996@yahoo.co.in).

T. Abdul Razak is with the Department of Computer Science, Jamal Mohammed College, Tiruchirappalli, Tamilnadu, India. (E-mail: abdul64@gmail.com).

performing more energy-consuming defense mechanisms. Note that the association between a node's status and its behavior is based on the assumption that each node has its own inherent nature to trigger bad behavior.

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. 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 Fuzzy based Power aware Trusted Dynamic Source Routing Protocol (FTP-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 proposed trust model which computes trust value, residual energy of each node and fuzzy logic to predict the node behaviour. In section 4 we present the rule based fuzzy system, section 5 describes the most trustable path calculation. In section 6, we present the proposed new FTP-DSR protocol. Section 7 presents the simulation results to evaluate the performance of the proposed scheme. Section 8 concludes the paper.

II. 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. [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, 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. 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 neighbors and remain in active in the network. In [12], 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 [13]. 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 [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. 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. [15] have 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 the routers that make up that path. As another extension to DSR, Guo et al. [16] 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 [17]. 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. Islam Tharwat et al. [18] proposed Agent-based trusted dynamic source routing protocol (ATDSR) for MANETs. This protocol depends on the self-monitoring of each node to find its trust value by installing a multi-agent system (MAS) in each participated node in the network and manages trust and reputation. Jayalakshmi et al. proposed Trust vector based dynamic source routing protocol TV-DSR [19]. In this model, to ensure trust worthiness, trust value for each node is calculated accurately by employing different factors based on the history of interaction between the nodes.

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.

III. Fuzzy Based Power Aware Trust Model

We propose a power aware trust management model using fuzzy logic to secure the routing protocol between source and destination nodes based on the trust value and residual energy of a node in the path. The model considers the problem of different types of attacks due to some misbehaving nodes.

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 $P = (V_S..., V_i ..., V_D)$, *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.

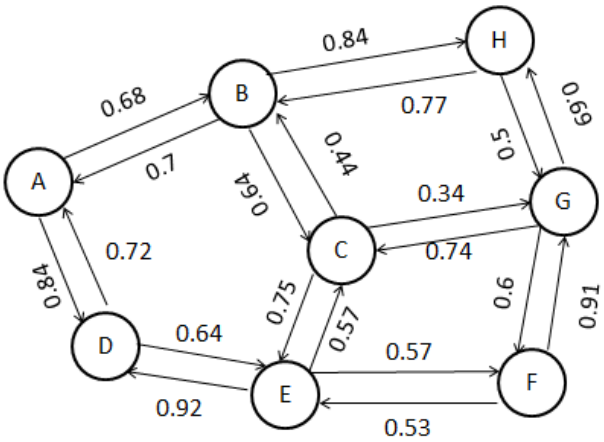

Fig 1. Weighted graph in the Adhoc Networks

Each node in the model maintains a trust table which contains the trust values of the neighbouring nodes. For example, the trust table for the node C is given in Table 1. In each row of the table, NN denotes node C's neighbour that can communicate with C via a single hop; TV_{in} is the trust value that the neighbour node gets about node C; TV_{out} is the trust value that node C has about the neighbour; status indicates whether C considers this neighbour as a malicious node. If the trust value is below the threshold value then the status of the node is malicious. In this example, the threshold value is set as 3.5.

Table I. Node C's trust table

NN	TV_{in}	TV_{out}	Status
B	0.64	0.44	Trusted
E	0.57	0.75	Trusted
G	0.74	0.34	Malicious

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. Trust Calculation

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.

Weighted Packet Forwarding Ratio

The ratio of number of packets forwarded correctly to the total number of packets is known as Forwarding Ratio (FR) [20].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 with multiple constraints: weight factor assigned to each packet transmitted, similarity factor between two nodes and time aging factor. 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)

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

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

Table II. 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 [21] 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 [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, $a_{2,\ldots}$ 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 [24] given in the equation.

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

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 $0 < \beta < 1$.In our experiments, $\alpha = \beta = 0.5$.

Time Aging Factor

The attenuation rate made by the k^{th} 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:

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

B. Residual Battery Power

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 [25]. 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.

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

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. For the MANET in disaster-hit area, Jiahong Wang et al. [26] stated that putting mobile terminals into sleep may bring a MANET-based communication system into a collapsing state.

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

$$\mathrm{E_{SP}\ (node)} = \mathrm{c1 P_{size}} + c2 \quad (9)$$

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

$$\mathrm{E_{RP}\ (node)} = \mathrm{c1 P_{size}} + c2 \quad (10)$$

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

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.

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

The energy value will vary from 1 to 0 with 1 corresponding to full energy level and 0 for all energy depleted (dead node).Comparing residual battery power with the energy threshold η , a node can have either low power or moderate power or high power or very high power.

C. Rule based Fuzzy System

The design methodology of a fuzzy controller is used for the prediction of the node behaviours [18, 21] and obtains a best route. It determines, for each source-destination node pair, the availability of all the paths and the quality of all the routes based on the trust value and energy level of a node .It decides the best route to be used for routing the current traffic. As information related to trust value and energy value are imprecise by nature, a new approach based on fuzzy logic could prove to be efficient. Its primary focus is to translate expert knowledge into natural language. Thus an inference method has been derived which attempts to represent gradual inference rules using fuzzy control techniques. The inference method is essentially based on heuristic rules derived from expert knowledge and human experience. This approach has been used to develop a fuzzy routing system applied to the trust model and QoS parameter namely battery power.

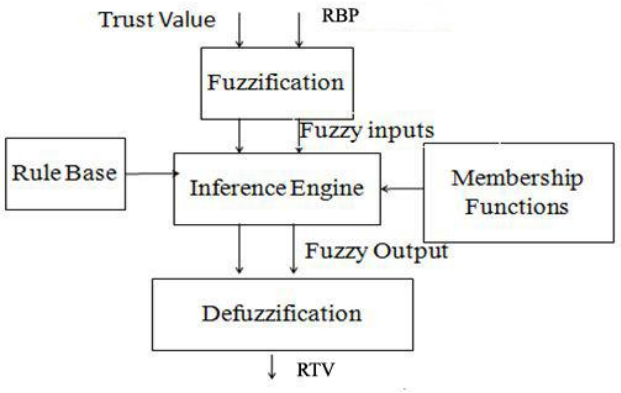

Fig 2. Fuzzy Routing System

TABLE III. RULE BASE FOR INFERENCE ENGINE

Trust / RBP	Very Low	Low	Average	High	Very High
Very Low	Very Low				
Low	Low				
Moderate	Very Low	Low	Moderate	High	High
High	Very Low	Low	Moderate	Very High	Very High
Very High	Very Low	Low	Moderate	Very High	Very High

In this model, fuzzy inference engine is used as shown in the fig 2. The fuzzy input parameters for the inference engine are trust value and Residual battery power. The values of different criteria are mapped into linguistic values that characterize the level of satisfaction with the numerical value of the objectives. The linguistic variables for the fuzzy trust parameter are very low, low, average, high and very high based on the computed trust value. The linguistic variables for the other fuzzy parameter namely residual battery power are very low, low, moderate, high and very high. The membership functions express a fuzzy status for each value of each measurement, which allows building the rules required for inference engine. The membership functions express a fuzzy status for each value of each measurement, which allows the manager to build the rules required for inference engine. As an example, we illustrate in Table III the rule base for inference engine which provides the trust values of nodes and residual batter power (denoted by RBP) for node. The output variable of the inference engine is the Reliable Trust value (RTV), a fuzzy variable. In order to get the crisp, the fuzzy output variable RTV is defuzzyfied by using the center-of-gravity method. The RTV value helps us to predict the behaviour of the node.

IV. MOST TRUSTABLE PATH COMPUTATION

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*.

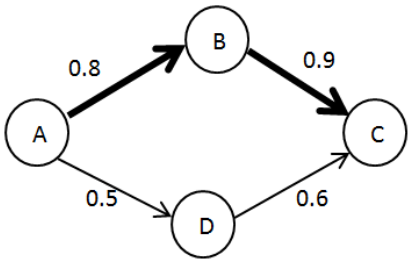

Fig 3. Most Trustable Path

For example, if node A wants to send packets to the neighboring 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 trusted path yielding highest trust rating $TV_{i,k}$.

In Vector Trust [27], 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.2, 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 server B will be added in trust graph and also the residual battery energy is also computed and then 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 re labels 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, RTV, 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

Power Aware Most Trustable Path

The value of trusted power aware path should not be more than the calculated values of the trusted intermediate nodes. So at time t, the trusted power aware path TPAP (t) is equal to the maximal product value of all directed edges along a path as given in the equation.

$$PathRTV_{SD}(t) = \prod (\{ RTV_{ij}(t) \mid v_i, v_j \, \varepsilon \, TPAP \; and \; v_i \rightarrow v_j \}) \quad (12)$$

In which, V_S is the source node, V_D is the destination node of route RTV, v_i and v_j are any two adjacent nodes along the path TSP, and $v_i \rightarrow v_j$ means that v_j is the next-hop node of v_i. Trusted stable path denotes a joint probability at which packets will be forwarded if they are sent along the routing path. The trusted power aware route is the trusted reliable value experienced by the last packet which has arrived along the route. Since network load conditions will change from time to time during the connection, the trust and residual power will also change accordingly. By using the latest arrived data packet to calculate RTV (t), the scheme is adaptive to changing network conditions and the source will be correctly informed in a timely manner for a 'Handoff' so the packet losses can be minimized to a larger extend. The paths are then ordered in decreasing order of route quality and, for each individual traffic relation. The best path with minimum number of hops is selected to route the packets for the next time period.

V. Proposed FTP-DSR Protocol

In this section, we describe the establishment of the proposed new power aware trusted DSR protocol using fuzzy logic called FTP-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 FTP-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 RTV than reliability threshold η.

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 reliable trust value calculated using fuzzy logic 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, the RBP and RTV of the node. Before transmitting a packet from the neighbour node, the node compares the RTV value with 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 RBP values when compared to the energy threshold are made in to sleep node. If a node's RTV 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 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. 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.

Some of the nodes may be made into sleep mode because of their low RBP level. 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.

VI. 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, the energy level of a node is also taken into consideration using fuzzy logic for finding the reliable route and this trust based power aware management model is incorporated in to the protocol called as FTP- 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 and FTP-DSR we have conducted a comprehensive test using NS-2 network simulator [28].

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 [29] 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

B. Performance Metrics

We use the following 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.
4. Network throughput: throughput indicates the amount of digital data transmitted per unit time from source to destination.
5. Path Optimality: the ratio of the total number of hops in the shortest paths to the total number of hops in the paths taken by data packets to reach its destination.
6. Probability of Detection: The ratio between the number of nodes whose behavior (malicious or benevolent) is identified correctly, to the actual number of such nodes present in the network.

C. Scenario I: Varying Node Speeds

In the first scenario, we compare FTP-DSR with DSR as the maximum speed of nodes varies from 0 to 30 m/s. and the number of malicious nodes are 5. As shown in Fig. 4a, the delivery ratio of DSR declines remarkably as nodes speed up, whereas the delivery ratio of FTP-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. FTP-DSR has higher delivery ratios than 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. Fig. 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. FTP-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.

TABLE IV. 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	20 joule

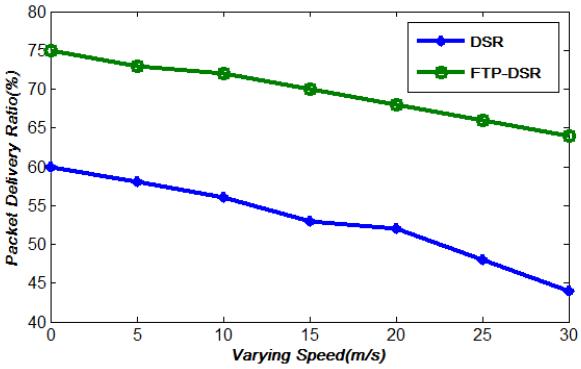

Fig 4a. Packet Delivery Ratio vs varying speed

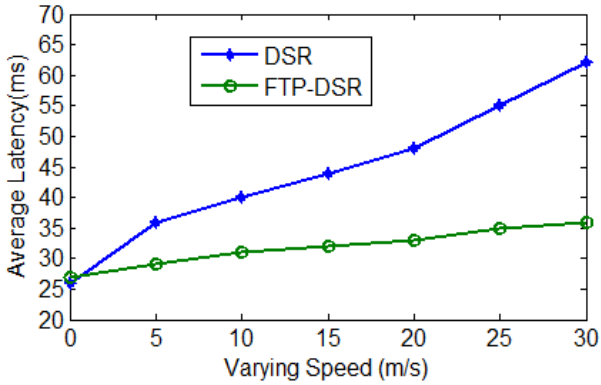

Fig 4b. Average Latency vs Varying Speed

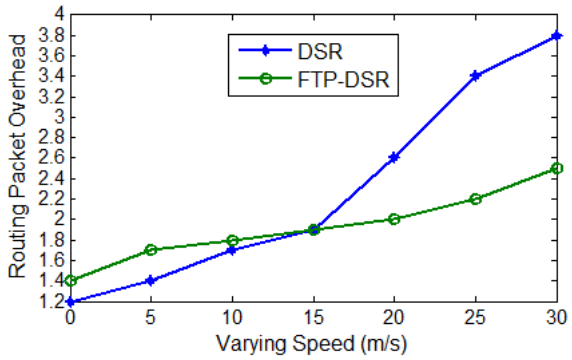

Fig 4c. Routing Packet Overhead vs Varying Speed

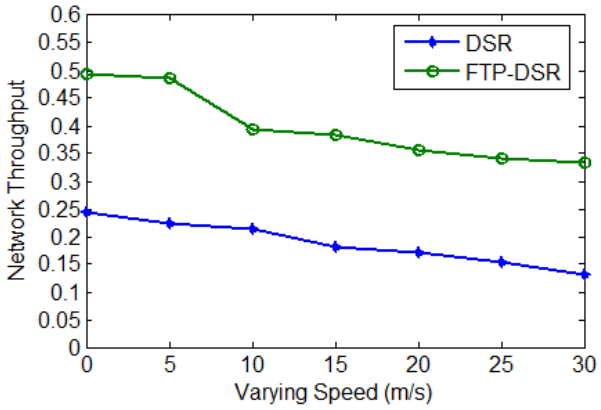

Fig 4d. Network Throughput vs Varying Speed

In Fig. 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 FTP-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 FTP-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 FTP-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. Fig. 4d illustrates that, comparing with the dispersed value; our proposed protocol gives obvious higher throughput than the traditional DSR protocol. In the Fig. 4d for example, at the speed of 10 (m/s) in the simulation, the throughput of DSR is 0.21packets per second, and FTP-DSR is 0.394 packets per second. Our approach improves the throughput by 83%.

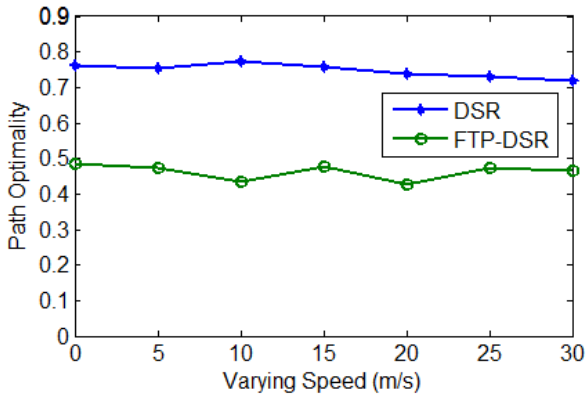

Fig 4e. Path Optimality vs Varying Speed

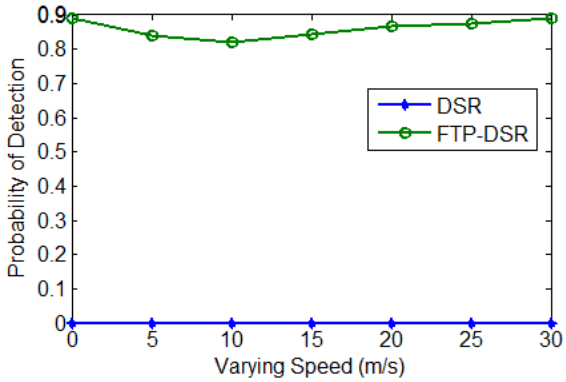

Fig 4f. Probability of Detection vs Varying Speed

As shown in Fig. 4e, the path optimality of these protocols degrades as the speed increases. FTP-DSR has smaller path optimality than DSR. It is observed that the actual routes may not be the best available routes due to the 'trust' factor that in FTP-DSR, where source nodes make routing selection considering hop count and route trust. Sometime only longer routes have satisfied trust requirements. They reduce the path optimality. The detection ratios of FTP-DSR increase with node speed as shown in Fig. 4f. We can observe that when the nodes move faster, the interactions among nodes increase gradually. This leads to higher detection ratios of malicious nodes because FTP-DSR makes a better identification rate for node's attributes based on historical behavior information, nodes' residual battery level and fuzzy logic rules prediction mechanism.

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 FTP-DSR. As shown in Fig. 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.

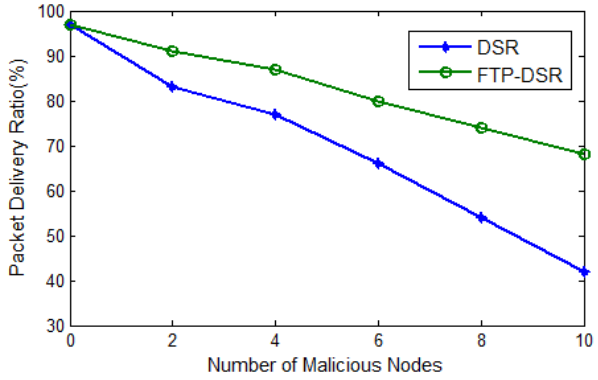

Fig 5a. Packet Delivery Ratio vs Number of Malicious Nodes

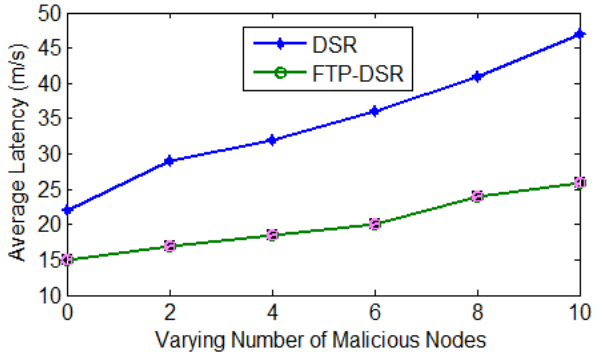

Fig 5b. Average Latency vs Number of Malicious Nodes

As shown in Fig. 5b, the average latency in FTP-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 FTP-DSR when compared to DSR. As a result, in the process of establishing a trusted route with nodes with high energy level, the network will be able 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 (40% of the whole nodes), the routing packet overhead of FTP-DSR is approximately 2.8 as shown in Fig. 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 FTP-DSR is bigger than in DSR, the reason is that, the increased control packets in FTP-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 FTP-DSR is smaller than DSR, because of the huge damage on routing path from malicious nodes.

As shown in Fig. 5e, DSR exhibits the best path optimality with the increase number of malicious nodes. As malicious nodes increase, the path optimality of FTP-DSR decreases. DSR only implements the traditional routing protocol, which only maintains one shorter route to a destination, while FTP-DSR is able to detect and filter out malicious nodes and selfish nodes. The detection ratios of FTP-DSR and DSR are shown in Fig. 5f. FTP-DSR declines with the increase number of malicious nodes. It is obvious that the more malicious nodes are, the more serious their damage is, and the detection is harder.

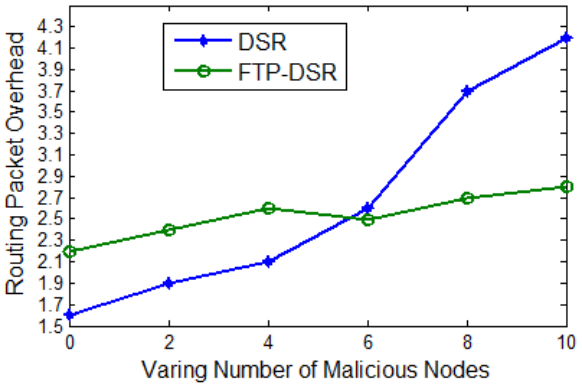

Fig 5c. Routing Packet Overhead vs Number of Malicious Nodes

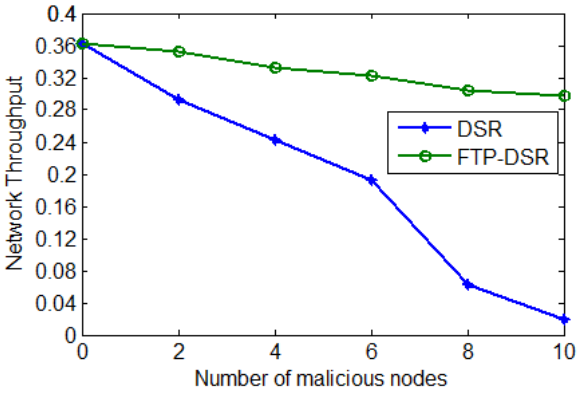

Fig 5d. Network Throughput vs Number of Malicious Nodes

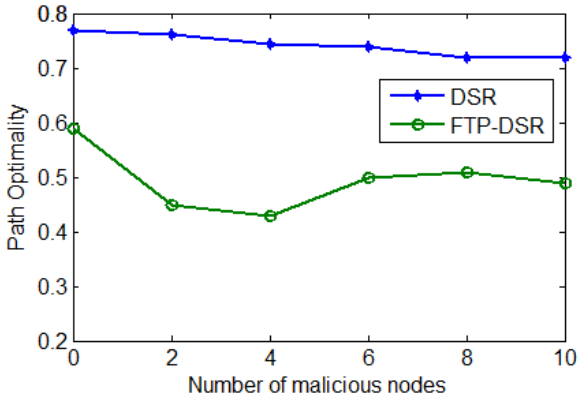

Fig 5e. Path Optmality vs Number of Malicious Nodes

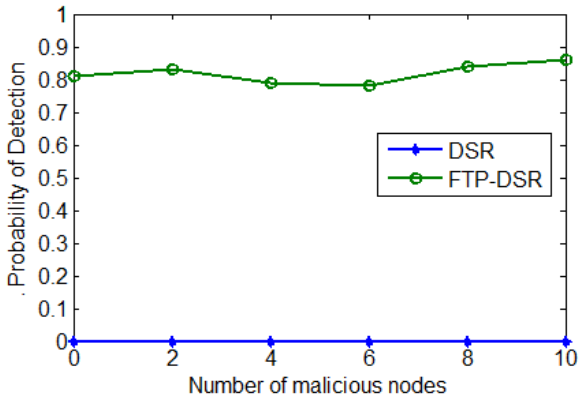

Fig 5f. Probability of Detection vs vs Number of Malicious Nodes

The experimental results in scenarios 1 and 2 shows that FTP-DSR performs better than DSR, as FTP-DSR gives higher delivery ratio, network throughput and detection ratio for malicious nodes.

VII. Conclusion

In this paper, a novel power aware 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 battery power level of each node is obtained. Then taking the trust value and the RBP as the inputs to the fuzzy system, a trusted routing model is proposed. The proposed trust based power aware Dynamic Source Routing protocol using fuzzy logic called as FTP-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 and proposed FTP-DSR shows that FTP-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 will be taken 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 KS, Chari AA, Kasiviswanth N. "Trust based security routing in mobile adhoc networks".International Journal on Computer Science and Engineering,, 2(2), pp.259–63,2010.

[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, pp. 90–100, 1999.

[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, pp. 153–181, 1996.

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

[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) ,pp. 46–55, 1999.

[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, pp. 70–75,2002

[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), pp. 105–114, 2008.

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

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

[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 and P.O. Connell, "Trust-based route selection in dynamic source routing", Proceedings of International Conference on Trust Management, pp. 150–163, 2006.

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

[16] 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, vol. 2, pp. 727–730, September 2005.

[17] 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 ,pp. 248-266,2011

[18] Abdel-Halim, Islam Tharwat, Hossam Mahmoud Ahmed Fahmy, and Ayman Mohammad Bahaa-Eldin. "Agent-based trusted on-demand routing protocol for mobile ad-hoc networks." Wireless Networks 21, 2 , 467-483,2015.

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

[20] 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.

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

[26] Jiahong Wang, Yuhiro Yonamine, Eiichiro Kodama, and Toyoo Takata, "Supporting User Communication in Disaster-Hit Area Using Mobile Ad Hoc Networks," IAENG International Journal of Computer Science, vol. 42, no.2, pp152-159, 2015.

[27] Zhao, H., & Li, X. (2013). "VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks" The Journal of Supercomputing, 64(3), 805-829, 2013.

[28] Network Simulator, The Information Sciences Institute **(ISI),** University of Southern California, http://www.isi.edu/nsnam/ns/.

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