Trust Evaluation and Dynamic Routing Decision Based on Fuzzy Theory for MANETs

Hongjun Dai, Zhiping Jia and Zhiwei Qin
School of Computer Science and Technology, Shandong University, Jinan, China.P.R.
Email: {dahogn, jzp}@sdu.edu.cn, qzw@mail.sdu.edu.cn

***Abstract*—As a kind of typical embedded system, MANET is a multi-hop self-configuring network with the topology changes dynamically. To model of the security, mobility, and dynamic changes of MANET, trust is used as a novel concept recently. In this paper, based on the classic fuzzy theory, the trust evaluation and the dynamic routing protocols for MANET are represented, to give the modeling of MANET with the fuzzy inference rules, and to improve the routing protocols with fuzzy dynamic programming. The experiments with OPNET show that the novel fuzzy trusted DSR protocols can reduce the Packet Drop Ratio and enhance the throughput with the acceptable End to End Delay in MANET.**

***Index Terms*—embedded system, trust routing of MANET, fuzzy trust evaluation, trust modeling with fuzzy logic, fuzzy dynamic programming, fuzzy trusted DSR**

I. INTRODUCTION

As a kind of typical embedded system, the mobile ad-hoc network (MANET) [2] is a self-configuring network of the mobile devices connected by wireless links, which consists of a lot of low power wireless devices. Each device (called node) in a MANET is free to move in any direction independently, which exchanges the data and link information with each other frequently, to maintain the instant communication by co-operating during the establishment of routes in forwarding packets to the destination. Usually, the nodes can communicate without use of any fixed infrastructure, and they are performed through the multi-hop routing. For the security and variability, current typical routing protocols, such as DSR, AODV, LAR [3], have to be thoroughly designed and analyzed in term of their co-operations with each other, proposed rapid response well in coping with the unstable topology.

Since the network topology changes dynamically due to the arbitrary mobility of nodes and the nodes can participate or withdraw from MANET at any time, it is difficult to measure the security and stability of the dynamical routing traffic information. All nodes behave as the routers to take part in the processes of the routing discovery and maintenance to other nodes at the same time, which need to share the information and the data instantly. Furthermore, as the self-organized multi-hop network, it means two nodes may be out of direct communication range, which requires the inter-mediate nodes to transmit the messages. Frequently, the nodes serve as host and router simultaneously, so MANET is inefficient to deal with the malicious nodes' attacks, which usually relies on the individual security solutions within each node. All these are concluded as the network factors.

On the other hand, each node is a typical embedded system, which still faces the challenges from its own characters, such as limited physical security, flexible node mobility, low manufacturing price, and limited system resources (i.e., processor, power, size, storage). Definitely, these hardware/software constraints of the node are critical to keep the network safe and stable, so there is the increasing concern about the nodes' system security and usability in MANET because the nodes may be deeply affected by the real complex environments and the malicious attacks can also aim to these nodes. All these are concluded as the node factors.

Obviously, it's necessary to keep the nodes and the network active within these two factors, but traditionally, they belongs to network research and embedded system research separately, it's very difficult to calculate both node factors and network factors as a holistic modeling and analysis. Recently, trust is carried out as a set of new theory and has been used into MANET to measure these integrated factors.

In the human society, trust is one of the most common concepts, while trust depends on a host of factors which can't be easily modeled by the computational methods. In the areas of computer science, trust has been used in many fields to mean many different things. For example, it's a descriptor of security and encryption; a name for authentication methods or digital signatures; a measure of the quality of a peer in P2P systems; a factor in game theory; a model for agent interactions; a gauge of attack-resistance; a component of ubiquitous and distributed computing; a foundation for interactions in agent systems; or a motivation for online interaction and recommenders systems [4]. In MANET, Trust can be defined that the current agent has followed the trusted agent's willingness and has the capability to deliver a mutually agreed service in a given context [5]. For example, when a node requests the transmission service from its neighbors, the neighbor

Manuscript received November 12, 2008; revised July 1, 2009; accepted July 15, 2009.

This work was supported in part by the Natural Science Foundation of China (No. 90718032), the China National 863 Project (No. 2007AA01Z105-05) and the China Postdoctoral Science Foundation (No. 20080431169).

doi:10.4304/jsw.4.10.1091-1101

node may have behaved to be damaged, overloaded or compromised maliciously, and leads it's difficult to get the correct data or information by the requesting node. In this case, trust can be used to measure the network conditions and external environments, and also to get the optimal solutions further [24].

There have been some algorithms to evaluate the trust of MANET, such as graph theory [6, 7], Markov Chain [8], Bayesian model [9]. Besides, as a fact that the uncertainty exists in most of the factors, fuzzy theory is suitable for modeling and evaluation of the uncertainty and boundary in MANET.

First, fuzzy logic can be used for the trust modeling of MANET. It uses qualitative terms and linguistic labels to represent trust as a fuzzy concept, and the membership functions describe the degree of a peer which can be labeled as trustworthy or untrustworthy. Fuzzy logic also provides the rules to reason with fuzzy measures. In the modeling of the trust, concepts such as trustworthiness, honesty, and accuracy, are needed to be defined and quantified with the mathematical methods in an interval, fuzzy logic can be used to handle the uncertainty and the imprecision.

Second, the calculated trustworthy value then can be used to the routing protocols for the practical purpose. According to the fuzzy and dynamic features of MANET and the uncertain factors in routing discovery, fuzzy dynamic programming (FDP) [10] can be used into the optimization of the routing protocols. FDP is developed as a process to accept preprocessed inputs and has the outputs which are further de-fuzzy for actual applications. Because the calculation and measurement of trust in this unsupervised ad-hoc environment involves complex aspects such as credibility rating for opinions delivered by a node, the honesty of recommendations provided by a mobile node, or the assessment of past experiences with the node one to interact with. The use of FDP algorithms and models extends fuzzy logic to develop a trust model based on the fuzzy recommendation to solve routing problems.

In this paper, as the extension of the research in [1], based on the classic fuzzy theory, the trust evaluation modeling and the dynamic routing protocols for MANETs are introduced. First, trust evaluation with fuzzy logic is given, directly modeling the nodes with the mathematical formula, then fuzzy modeling the main aspects of MANET with the fuzzy inference rules. Second, the routing decision with fuzzy dynamic programming is discussed, which includes the steps and process to establish the fuzzy trusted routing, to implement the improved DSR protocols (FTDSR), and to take some useful optimizations. The experiments have shown that FTDSR protocols can reduce the packet drop ratio, enhance the throughput with the acceptable end to end delay.

The rest of the paper is organized as follows. An overview of related work is given in Section II. In Section III, the fuzzy trust evaluation model about each node is introduced, including direct trust evaluation according to the features of the node and trust evaluation with fuzzy logic to model the node, the network and the environment. In Section IV, how to make the routing decision with FDP is discussed in detail, from the basic trust abstraction based on FDP, to get the trusted routing model with FDP, and then about the optimal equation solutions for trusted routing model. In Section V, the practical trust routing algorithm with FDP is given, focus on each step of the algorithm, on how to make the multi-stage decision, then it represents the process to establish the fuzzy trusted DSR, gives two useful optimization methods for FTDSR. The simulations and experiments with OPNET are described and analyzed in Section VI. The conclusions are given in Section VII.

II. Related Works

Trust is an abstract matter in the everyday life, but its relevant research on computer science is a new subject. This causes a lack of coherence in its definitions between different fields in computer science. Generally, the notion of trust used throughout this paper is defined as: trust is the degree of belief about the future behavior of other entities, its calculation is based on the past experience with and the observation of the others related actions [11]. For MANET, trust is interpreted as a relation among entities that participate in various protocols [12].

Most studies of trust value management [13-15] have proposed several trust management approaches. [16, 17] proposed the collaborative reputation mechanisms to establish reputation ratings for nodes. [18] proposed a strategy-proof trust management from a node's previous honor. Although the management brings low overhead, the honor definition for changing trust values has not been defined. [19] presented an authentication service to achieve network security by discovering and isolating dishonest users, but the rules of changing a node's trust state between good and bad trust values ware not well defined. In [20, 21], several trust relationships are defined for a context-aware management protocol, but they may cause error trust relationship. [22] proposed a method to manage multicast key trees that match the network topology and thus reduced the communication overhead of rekeying. However, the impact factors of the key management server were not considered due to node mobility. [23] proposed a two-step secure authentication approach for multicast MANETs with Markov chain. A node's trust value is analyzed from its previous trust manner that was performed in this group. The proposed trust model is proven as a continuous-time Markov chain model.

By monitoring the transmission behavior, several trust based security routing algorithms have been proposed to evaluating node's reputation.

[25] proposed a Secure and Objective Reputation-based Incentive (SORI) scheme to encourage packet forwarding and discipline selfish behavior. The scheme, however, does not prevent a malicious node from selectively forwarding packets or from other malicious behavior. Token-based mechanism [26] is a unified network layer security solution in MANETs. In this scheme, each node carries a token in order to participate

in network operations, and its local neighbors monitor any misbehavior in routing or data packet forwarding functions. Sprite [27] is a simple, cheat-proof, credit-based system for MANETs, which uses credit to provide incentives for mobile nodes to cooperate and report actions honestly.

As an extension to DSR, [17] proposed a new security routing protocol-CONFIDANT. Similarly with the Watchdog Path-rater (WP) mechanism, it firstly introduces a monitor to get trustee's transmission state, with the help of reputation system and trust manager component, it then implements the evaluation and update of the trust rating. However, when the time expires, the node will again turn to be a legitimate participant, which may continue its misbehavior. What's more, introducing recommendation trust will make the trust evaluation time-consuming and cause much more overhead, which also increase its complexity. [29] gave a trust evaluation scheme dynamically based on routing model (Trust DSR). Five routing selection strategies have been proposed, which are based on the trust evaluation of the transmission links. Because its routing selection is limited on the routes that obtained from standard DSR, the ultimate selected route is not necessarily the most trusted one.

Some research has used fuzzy theory into trust evaluation and routing decision for MANET. RFSTrust [30], a trust model based on fuzzy recommendation similarity, is proposed to quantify and to evaluate the trustworthiness of nodes. Fuzzy logic provides a natural framework to deal with uncertainty and the tolerance of imprecise data inputs for the subjective tasks of trust evaluation, packet forwarding review and credibility adjustment. [31] proposed a Fuzzy based Ad hoc On-demand Distance Vector (FAODV) Routing Protocol. The authors used Fuzzy Logic at trust evaluation and setup a Threshold Trust Value (TTV) for trust verification. Fuzzy Logic based trust evaluation can give a rational prediction of trust value and give an accurate identification of malicious behavior based on fuzzy inference rules. However, the FAODV model only gives the protection method against modification attacks and the trust evaluation process only monitors the node's behavior for routing discovery but not for the transmission of data packets.

Above all, although there have been some research about trust modeling, trust evaluation and trust routing protocols, the research combined fuzzy theory and trust in MANET is still a new topic. To get more trusted routing algorithms, it is feasible to use FDP into trust computing fields too.

III. FUZZY TRUST EVALUATION

In MANETs, trust is represented by the relationships interacted with each other. This can be abstracted as the associations between a trusting node and a trusted node. Trust relationships are determined by the rules to evaluate the evidence with a quantitative way, generated by the previous behaviors of a node. Accordingly, fuzzy logic is the process to formulate the mapping from a given input to a logical output, which provides the basis from the decisions made, or the patterns discerned. Because of the mobility of the nodes and the time-varying of the wireless channels, the trust in MANET has the natural uncertainty and incompleteness, then the evaluation models of trust focus on the collection and the quantization of the dynamic information. The trust associations between two nodes can be classified into three categories: direct interaction, association through other nodes' recommendations (indirect association), and review through the history records.

A. Direct Trust Evaluation

Let DT_{ij} present the direct trust value from node i to node j, then DT_{ij} can be got from the history records and context information between the two nodes. According to [9, 31], a simple formula can be concluded as F.3-1.

$$DT_{ij} = \rho \frac{1+\sum_{k=1}^{I} S_k}{2+\sum_{k=1}^{I} N_k} + (1-\rho)\frac{\alpha E_p + \beta C_q + \gamma M_t}{\alpha+\beta+\gamma} \qquad 3\text{-}1$$

S_k presents during the recent I times interactions, the real total service count at the kth time between node i and node j. N_k presents the expected service count of node i at the kth time. Node i often makes observation at different time instances. Let S_k denote the time when node i make observation of node j. At time k, node i observes that node j performs the action times upon the request of performing the action times. Obviously, $N_k \geqslant S_k$. These history factors describe that the observation has been made for a period of time, and it should carry less importance than the observation made recently.

E_p, C_q, M_t presents the node information at the current time. E_p is the energy consumption information, which represents the power resources as the mobile embedded system; C_q is the processor utilization percentage, which represents the calculation resources; M_t is the memory utilization percentage, which represents the storage resources. α, β and γ are all positive integers, which represents the weight values of the three aspects. $\rho \in [0,1]$, is the variable coefficient. The proportion of the history records and the node condition can be tuned with it to let the formula more practical.

B. Trust Evaluation with Fuzzy Logic

When node i ask node j for the packet transmission of the data or link information, node i has the difficulty to evaluate whether node j can provide the service at that time or whether the service provided by node j is security and trustworthy. Then, this situation can be judged and monitored by node i from the history interaction records of node j.

Let $C(t)$ represents the capability of the requested node (node j) on providing packets transfer services at time t, which includes the remnant utilization ratio of battery, local memory, CPU cycle, and bandwidth at that point. Let $H(t)$ represents at time t, the history behaviors to offer certain services between the past time intervals, such as packet-drop ratio. Let $TL(t+1)$ refers to the node's trust

level at time *t+1*. Assume the fuzzy member function of *C(t)* consists of three fuzzy sets: *LOW(L)*, *Medial(M)* and *High(H)*. The fuzzy membership function of *H(t)* and *TL(t+1)* consists of four different levels of fuzzy sets: *LOW(L)*, *Medial(M)*, *High(H)* and *VeryHigh(VH)*. According to the social control theory [28], the fuzzy inference rules are given in Table I.

TABLE I. FUZZY RULES ON TRUST LEVEL TL(T+1)

C (*t*) \ H (*t*)	L	M	H	VH
L	L			
M	L	M		H
H	L	M	H	VH

The rules in Table I establish a mapping from $H \times C$ to *TL*. It is based on the analysis of the node's current condition and historic behaviors. When an overloaded node lacks the CPU cycles, buffer space or available network bandwidth to forward packets, it will be also untrustworthy in next time interval because of such a low capability level, even if its historic trust level is very high. This is only the first basic rule in Table I, and then the inference relationship can be concluded with R_l:

$$R_l = H_t \times C_t \times TL_{t+1} \quad 3\text{-}2$$

and for $\forall\ h \in H, c \in C, u \in TL$,

$$R_l(h,c,u) = H(h) \wedge C(c) \wedge TL(u) \quad 3\text{-}3$$

For all the *n* rules we have the fuzzy inference relationship as F.3-4

$$R(h,c,u) = \bigvee_{l=1}^{n} R_l(h,c,u) \quad 3\text{-}4$$

For each pair of given input H^* and C^*, use the general total relationship *R*, the output can be calculated:

$$TL^* = (H^* \times C^*) \circ R \quad 3\text{-}5$$

Then, with the maximal membership degree approach, the trust value $u^* \in [0,1]$, can be calculated with the de-fuzzy methods.

This is the basic models with two aspects *C(t)* and *H(t)*.While in the real world, the environments of the MANET are also the important factors. Let *E(t)* represent the environment factors, such as temperature, moisture, and lighting, most of these factors have been classified in Table II. Respectively, the improved results can be modeled and calculated with the similar process and the similar formula above.

TABLE II. MAIN FACTORS WITH TRUST EVALUATION

Items	Contents
C(t)	Power supply Battery condition CPU cycle Local memory Backup of important data Safe system checking Data recovery mechanism Encryption Security of system software System operation log
H(t)	Communication bandwidth Channel frequency Encryption Route table maintenance Real-time route discovery Route backup log
E(t)	Temperature Moisture Lighting Anti-lightning Error-proof setting

IV. FUZZY DYNAMIC ROUTING DECISION

Trust is a natural fuzzy concept, which poses a fuzzy constraint on the trusted routing decision-making, so the different nodes might provide diverse routings about the same nodes, i.e., different nodes would have the different and even opposite trust evaluations toward a same node. Based on fuzzy model, each node can calculate the trust value for its neighbors and maintain in its neighbor route table. Minimal values for trust can occur as a result of more malicious behavior than legitimate behavior of a neighboring node. As the trusted routing process is also fuzzy, FDP is proposed to make the trust routing decision in MANET.

A. Trust Abstraction based on FDP

In the usual dynamic programming (DP), the solutions of the given questions are abstracted as the decision processes, then this process is divided into several associated phases and there have been several designed feasible plans in each phase. The objective of the decision is to select the most suitable plans in each phase, to get the best overall effect of the whole decision process. In FDP, as the extension of DP, the decision is confined with fuzzy constraints in each phase during the process to solve the questions. Because the trust evaluation of each node has the natural fuzzy features, the process of routing discovery is suitable for FDP accordingly.

Based on FDP, The decision model in MANET can be described as:

(1) During the whole decision process, the system may appear to be different states. Suppose the total count is *l*, then the state set is $E=\{e_1,e_2,\ldots e_l\}$

(2) The system should receive the external inputs to be configured or controlled, and then the current states are adjusted to approach the pre-determined object. Suppose the input set is $U=\{u_1,u_2,\ldots u_m\}$

(3) Suppose the whole decision process is fulfilled in the period of [*0, T*], a number of moments are inserted to divide the whole decision process into several phases. For example, the total of the moment is *n-1*($0=t_0<t_1<\ldots<t_{n-1}<t_n=T$), so the total of the phases is *n* and in each phase, the time period is (t_{k-1}, t_k] *(k=1,2,…n)*. Suppose at the *k*($0<k<=n$) phase, the system input is $u(t_k) \in U$.

(4) suppose at the *k-1* moment (that is at the end of (t_{k-2}, t_{k-1}]), the system state is $e(t_{k-1})$ and at the *k* moment (that is (t_{k-1}, t_k]), the system has received the input $u(t_k)$, then at the end of the *k* moment, the system state $e(t_k)$ only has relations with $e(t_{k-1})$ and $u(t_k)$, that is

$$e(t_k) = f(e(t_{k-1}), u(t_k)), k = 1,2,\ldots,n \quad 4\text{-}1$$

Suppose the state migration has no relation with the environment of the current moment, it is allocated with a migration matrix:

$$S(u)=\begin{bmatrix} S_{11} & S_{12} & ... & S_{1m} \\ S_{21} & S_{22} & ... & S_{2m} \\ ... & ... & & ... \\ S_{l1} & S_{l2} & ... & S_{lm} \end{bmatrix}$$

(5) In the matrix, $S_{ij} \in E$. S_{ij} means if the system is in the state $e_i \in E$, if there is the input $u_j \in U$, then the system has the migration to S_{ij}. That is:

$$S_{ij} = f(e_i, u_j)(i=1,2,...,l;\ j=1,2,...,m) \qquad 4\text{-}2$$

If the initial state of the system is $e(t_0)$, the objective of the FDP is a fuzzy set of E, that is in the moment $t_n=T$, $B_n \in F(E)$. Suppose at the phase $(t_{k-1}, t_k]$, the actual system input is u_j, then the actual fuzzy constraint set based on U is $C_k \in F(U)$.

According to the given conditions above, the FDP can be described as:

Given $e(t_0)$, then

$$U^* = \{u \mid u = (u(t_1), u(t_2), ..., u(t_n), e(t_n))\}$$

Of course, U^* can be calculated with

$$e(t_1) = f(e(t_0), u(t_1)), e(t_2) = f(e(t_1), u(t_2))$$
$$....., e(t_n) = f(e(t_{n-1}), u(t_n))$$

Let $D \in F(U^*)$, if $u=(u(t_1), u(t_2), \ldots, u(t_1), e(t_n))$, then

$$D(u) = C_1(u(t_1)) \wedge C_2(u(t_2)) \wedge ... \wedge C_n(u(t_n)) \wedge B_n(e(t_n))$$

So the FDP can be abstracted to findk $u^* \in U^*$, for the result of

$$D(u^*) = \bigvee_{u \in U^*} D(u) \qquad 4\text{-}3$$

and $u^*=(u^*(t_1), u^*(t_2), \ldots, u^*(t_1), e^*(t_n))$ is the optimal equation solution.

B. Trusted Routing Model with FDP

Distinguished from the traditional routing model in LAN networks, MANET is regarded as a time-invariant finite-state deterministic system under the definite control. Each node has a certain state from the delivered packets' perspective and the migration between two states can be conceived from two nodes' interaction. The input control variables for each state are the output links with neighbor nodes, and then the process of routing discovery equals a multi-stage state migration from initial state to terminate state. The result is to get a trustworthy critical path from source node to destination node. In order to model the trusted routing in such environments, three basic definitions are given below:

Definition 1. *State Set* X= $\{\sigma_1, \sigma_2, ..., \sigma_l, \sigma_{l+1}, ..., \sigma_n\}$, where σ_i, $i=1,2,\ldots n$, represents node i in an ad hoc network with the scale n, it's a finite set.

Definition 2. *Goal Set* T= $\{\sigma_{l+1}, ..., \sigma_n\}$, which is a specified non-fuzzy subset of X, it represents the destination's neighbor states.

Definition 3. *Input Set* U= $\{\alpha_1, ..., \alpha_m\}$, where α_j, $j=1,2,\ldots m$, equals to m links in the network. Because the trust condition of the links is fuzzy by nature, set U is a fuzzy set.

Let x_t be the state of the packet being delivered at time t, t=0,1,2,…, which ranges over X, and let u_t, t=0,1,2,…, be the input control variable at time t, which ranges over U. Define the temporal evolution of the system to be a state formula F.4-4.

$$x_{t+1} = f(x_t, u_t) \qquad 4\text{-}4$$

where $t=0,1,2,\ldots$, and f is a given fuzzy function from $X \times U$ to X, which means that when the packet at time t arrives at state x_t, with the choosey input u_t, then the state will be transferred to state x_{t+1}. Because the input u_t is an alternative from the fuzzy set U, and we assume the final goal G is to induce the system state into goal set T, so the discovery of trusted routing turns out to find an optimal decision D by decision making in a fuzzy environment. Suppose the decision process starts from the initial state σ_1 and ends with σ_n, according to the definition of goal set T, the process actually would finish once the system enters T, the end time t can be given by:

$x_t \in T$, with $x_t \notin T$

For $t<N$, where N is the *hop-count*.

With these conditions, fuzzy decision is defined as an intersection of the given goals and constraints, while the fuzzy logic has presented the malicious behaviors based on trust evaluation model, which constitutes the fuzzy constraints as input variables to this model.

C. Optimal Equation Solutions

According to the features of the MANET topology and the mobility of the wireless communication, an undirected graph can be used to abstract the node relations. As the models described above, the state migration graph can be concluded as Fig.1, which can be conceived as a typical fuzzy system.

In the state migration graph, a trusted transfer path is needed to be found from initial state S to destination D. The intermediate states among them can transfer mutually according to the established migration graph. Take state 4 and state 5 as an example, state 4 may migrate to state 2, 3, 5, 6 and 7, while state 5 may migrate to state 1, 2, 4, 7 and 8. Moreover, when state 4 is migrated to state 5, it will be constrained by its trust degree on state 5 with the given value 0.8 (suppose 0 represents complete distrust,

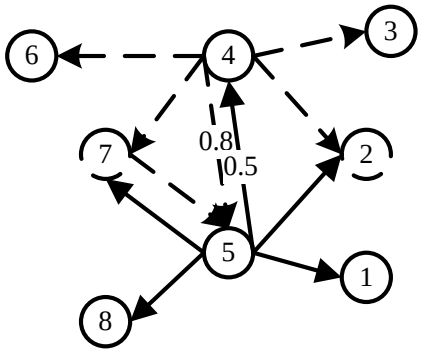

Figure1. Part of a state migration graph with 8 nodes.

and 1 represents absolute trust in the coming time interval). When the state migration process reaches state 4, it will make a decision to choose which state can be the successor under the constraint *C* and the general trust goal *G*.

According to the fuzzy dynamic programming theory [10], in this fuzzy system, for each decision at the certain stage, its membership function could get its corresponding maximal value. Let $\mu_D^M(\sigma_i)$ denotes the i_{th} component of the optimal goal attainment vector, and $\mu_C(\alpha_j \mid \sigma_i)$ is the value of the membership function of the constraint *C* in state σ_i for input α_j, with $\mu_C(\alpha_j \mid \sigma_i)$ =1 for *i=l+1,…,n*; and then the decision can be made as the following equation:

$$\mu_D^M(\sigma_i) = \vee_j(\mu_C(\alpha_j \mid \sigma_i) \wedge \mu_D^M(f(\sigma_i, \alpha_j)))$$

where *i =1,2,…n; j=1,2,…m.*

Also according to [10], an optimal policy π must exist in the finite policy space within *l* stages, modifying from the traditional backward iteration algorithm.

V. Fuzzy Routing Algorithm

Fuzzy routing protocols consider much uncertain network status as the factor in making routing decisions. The fuzzy routing algorithm monitors the congestion status of active routings and feeds the network status to the fuzzy logic controller in order to make the best routing decision.

A. Trust Routing Algorithm with FDP

The improved routing algorithm is presented as Trust Routing algorithm based on FDP, which is described in Fig.2.

B. Multistage Decision Making

The backward iteration process initiates from the destination state. Each state involved in each decision stage besides the destination can be divided into three sub-states.

As is shown in Fig.3, when the intermediate states receive the ROUTE DECISION (RDE) packet that

Assumptions: each node in the network maintains a trust table about its neighbor's trust values

Input: each state's trust table $N(\sigma_i)$, X, T

Output: optimal policy $\pi(\sigma_1)$ from σ_1 to σ_n

1 $\mu_D^M(\sigma_n) = 1;\ \mu_D^M(\sigma_m) = 0; m = 1,2,...,n-1.$

2 *t=1;* $A = T;$

3 destination σ_n broadcasts optimal goal value $\mu_D^M(\sigma_n)$;

4 while (*t*<*n*)

5 {for all $\sigma_i \in X$ {

6 if (σ_i be triggered && $\mu_D^M(f(\sigma_i, \alpha_j)) \neq 0$)

7 {calculate:

$$\mu_D^M(\sigma_{it}) = \vee_j(\mu_C(\alpha_j \mid \sigma_i) \wedge \mu_D^M(f(\sigma_i, \alpha_j)));$$

8 if ($\mu_D^M(\sigma_{it})$ <= $\mu_D^M(\sigma_{i(t-1)})$) delete σ_i from *A*;

9 else store: $\pi(\sigma_{it}) = u_i^* = \alpha_j$, where α_j makes the maximum value $\mu_D^M(\sigma_{it})$, in state σ_i 's route table; add σ_i into A;}} /*end if, end for*/

10 if (A $\neq \Phi$) {

11 all the states in A broadcast their corresponding optimal goal value; *t=t+1*; }

12 else {

13 if ($\mu_D^M(\sigma_1) == 0$) no trusted routing to the state σ_n;

14 else

$$\pi(\sigma_1) = (\sigma_1, f(\sigma_1, u_1^*), f(f(\sigma_1, u_1^*), u_2^*), ..., \sigma_n);$$

15 break;}} /*end while*/

16 return $\pi(\sigma_1)$;

Figure2. Steps of Trust Routing algorithm based on FDP

contains the optimal goal value $\mu_D^M(x_t)$ from the pre-stage states, it will be transferred from *Sleep (S)* sub-state into *Decision (D)* sub-state. If the received value is larger than the optimal goal value of pre-stage, the state will enter the *Ready (R)* sub-state, otherwise it will return to *Sleep(S)*. After a broadcast of the new RDE packet, the *Ready(R)* sub-state will also turn to *Sleep(S)*, waiting for new arrival RDE packets. Because one state always has several neighbors, a state need to make an iteration decision until obtains the best choice.

Take state 4 and state 5 in Fig.1 as an example, suppose at time *t*, both of them gets their optimal values, then they will broadcast corresponding RDE packets to their neighbor states. States 2 and 7 will receive two RDE packets; moreover, state 4 and 5 will exchange their RDE packets mutually.

This may cause two problems:

a) Time synchronization and asynchronization

In order to avoid the message confliction problem, we adopt the synchronous decision and asynchronous delivery mechanism. At the end time *t* of a stage, all states in set *A* make decisions simultaneously and within

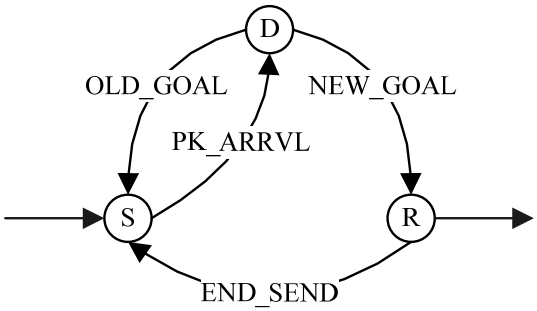

Figure3. Sub-state migration graph

certain *time interval* (*TI*) the decision states will broadcast their optimal goal value one after another to its neighbors, a state which receives a RDE packet will wait a certain time *TI* until get enough RDE packets from other neighbor states and then make an integrated decision.

b) Route cycle problem

In Fig.1, suppose state 4's successor is state 7, state 7's successor is 5, then it can be concluded that $\mu_D^M(4) \geq \mu_D^M(7)$, $\mu_D^M(7) \geq \mu_D^M(5)$, which indicates $\mu_D^M(4) \geq \mu_D^M(5)$. If state 5's successor is 4, it must fit the equation $\mu_D^M(5) \geq \mu_D^M(4)$, this condition can work only in the precondition $\mu_D^M(4) = \mu_D^M(5)$, however, according to the algorithm, if $\mu_D^M(4) = \mu_D^M(5)$, the RDE packet will be dropped. So it is unable to form a routing cycle. Moreover, the desertion of the packets with equal optimal goal values can decrease the invalid messages in the network and reduce the overhead of network nodes.

C. Establish Fuzzy Trusted DSR

According to the Trust Routing Algorithm with FDP described above, the process to establish a fuzzy trusted MANET protocol is generally as the following, with an abbreviation FTDSR.

Assumptions:

(1) The links between two nodes are bidirectional; this assumption is often valid [32].

(2) Besides the route table needed in standard DSR protocol, each node in our model additionally owns a trust table with items defined as follows:

N_ID(i) is the identification (ID) of node *i*'s neighbor;

T_IN(i) is the trust value that the neighbor node gets about node *i*;

T_OUT(i) is the trust value that node *i* has about its neighbors. All the trust values are obtained from the trust evaluation model shown in section III.

(3) The packets that contain the trust values are kept from modified by malicious nodes, just like the RDE packet.

The routing establishment process mainly includes routing discovery and routing maintenance. FDP is mainly used for the discovery process, and no much change should be made for the maintenance of DSR.

Routing discovery:

Step 1: Source node *S* initiates a routing discovery by broadcasting a ROUTE REQUEST (RRQ) packet that contains the destination address *D* to its' neighbors. The neighbors in turn append their own addresses to the RRQ packet and rebroadcast it. This process continues until a RRQ packet reaches *D*.

Step 2: Terminate node *D* initiates the decision process backwards with the trust routing algorithm with FDP (as described in Fig.2). Current states select next-hop state with the current trust table items and store the chosen state in their route tables. After finishing the process of the algorithm, each state obtains its optimal route and the routing discovery is completely implemented.

Route maintenance:

Route maintenance assures the route is integrated and valid in a certain *time interval* (*TI*); a link-broken event will trigger a new trust evaluation process and trust route-update process. Also, when a route table item overwhelms the *maximum valid time*, a new routing discovery will also restart.

D. Two Optimization methods for FTDSR

Basically, FTDSR is a more complex process than the common routing algorithms such as DSR, AODV. While the routing decision should be rapid enough and fulfill the throughout requirements, so some optimization could be taken to get more practical usability. Of course, there is certain performance loss after the optimization and they should be used into different conditions.

Two general optimization algorithms are carried here.

a) Avoid second decision-making

In FTDSR, there is a necessary inverse iteration process (as the de-fuzzy process) to get the routing path. Because of the asymmetric features between two neighbor nodes, the trust value from node *i* to node *j* may not equal the trust value from node *j* to node *i*. This causes it useful to re-calculate and re-activate the nodes which have previously finished the routing decision, and to make the second decision. In a complex MANET with many (i.e., more than 100) nodes, this may happen frequently because so many nodes can communicate each other directly. Although this second decision-making process is more accurate to find the most trustworthy path, it brings much more pressure to the in-time decision and the huge throughout processing.

Note that only line 6 and line 7 make the changes, add the function **Decision_Flag() to avoid the second decision.**

6 if (σ_i be triggered && $\mu_D^M(f(\sigma_i, \alpha_j)) \neq 0$ && **Decision_Flag(σ_i)==0**)

7 {calculate:

$$\mu_D^M(\sigma_{it}) = \vee_j(\mu_C(\alpha_j \mid \sigma_i) \wedge \mu_D^M(f(\sigma_i, \alpha_j)));$$

Decision_Flag(σ_i)=1;

Figure4. Algorithm Changes in FTDSR-I

So the approach to avoid the second decision-making is a useful way to accelerate the decision response. Use a flag function to mark the nodes whether it has made the decisions, only few changes is made to the algorithm in Fig.2 and Fig.4 shows the improved process. This improvement is named as FTDSR-I.

b) Heuristic decision with threshold value

when the node is in the state of calculation and decision, among all of the succeeding nodes which have passed trust value just now, there are may be more than one node have the same trust values, then one node is selected without any decision in FTDSR, just shown as α_j in Line 9, Fig.2. To be more trustworthy, the nodes, with the biggest trust value (the node with the biggest μ_c) in the positive routing directions, can be selected as the next-hop from the current node. Compared with FTDSR, this can improve the trust value in the each separate hop, which means the trust value in the critical routing path can be more average and stable.

In the implementation, the changes for the algorithm in Fig.2 are mainly added the steps to make a maximal comparison. This is shown in Fig.5, named as FTDSR-II respectively.

Note that from line8, another branch statement is added and the maximum path is selected

8 if ($\mu_D^M(\sigma_{it}) <= \mu_D^M(\sigma_{i(t-1)})$) delete σ_i from *A*;

else

9 IF more than one α_j could satisfy the optimal goal $\mu_D^M(\sigma_{it})$;

10 store:

$$\pi(\sigma_{it}) = u_i^* = \alpha_{jk} \mid \alpha_{jk} \to \max(\mu_C(\alpha_{jk} \mid \sigma_i))$$

in state σ_i 's route table; add σ_i

else

11 store: $\pi(\sigma_{it}) = u_i^* = \alpha_j$, where α_j makes the maximum value $\mu_D^M(\sigma_{it})$, in state σ_i 's route table; add σ_i into A;}}

/*end if, end for*/

Figure5. Algorithm Changes in FTDSR-II

VI. Simulations and Experiments

In the experiments, OPNET is used to perform the simulations. A mobile ad hoc network with 20 nodes is distributed randomly in the range of 1000m×1000m area. Each node has the constant movement speed of 1 m/s and the direct radio transmission range of each node is set to be 250m. The simulation continues for 100s each time. The details of the simulation parameters are shown in Table III.

To get the different level of the performance, various numbers of the malicious nodes are set to run the simulations. In the experiments, it is assumed that the malicious nodes percentage is 12% (2 malicious nodes, some nodes may be out of the communication range), 25%, and 35% respectively. After the implementation of the protocols through FTDSR family (including FTDSR, FTDSR-I, FTDSR-II), the performance is compared with DSR and TDSR [29], from the aspects of Packet Drop Ratio, End to End Delay and Throughput. All data can be got from the simulator directly and the trend is shown in the following figures.

TABLE III. SIMULATION PARAMETERS

Parameter	Value
Simulator	OPNET
MAC layer	802.11
Frequency of operation	2.4GHz
Number of mobile nodes	20
Mobility model	Random waypoint
Terrain range	1000×1000 m^2
Transmission range	250m
Channel bandwidth	1 Mbps
Movement speed	1m/s
Application traffic	CBR(UDP)
Simulation time	100s
Propagation mode	Free space
Packet size	512 Bytes
Maximum connection	10
Maximum malicious nodes	7(35%)
Type of attack	Coordinated attack

A. Packet Drop Ratio

The packet drop ratio indicates the data transmission performance of the MANET routing protocols. The basic character of the malicious nodes is to take the attack by dropping packets deliberately or forcedly when they are overloaded. Fig.6 shows the experiment results of the packets drop ratio under DSR, TDSR, FTDSR, FTDSR-I, and FTDSR-II respectively.

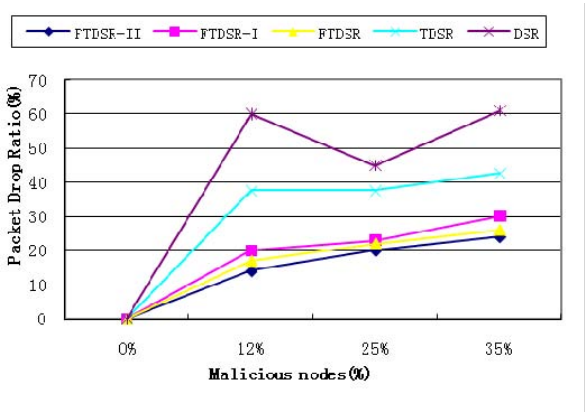

Figure6. Packet drop ratio with various malicious nodes

It can be found that FTDSR protocol maintains a lower drop ratio and the curve fluctuates smoother than others. This is mainly because the traditional DSR protocol only considers the hop count as the source for routing selection, and TDSR chooses the optimal trusted route limited on DSR. While FTDSR has used the FDP algorithm at trust evaluation and routing decision process, this can eliminate malicious nodes' influence and mitigate the attack caused by packet-drop. Take the cases with 12% malicious nodes as an example, the packet drop ratio of FTDSR is 17%, TDSR is 37.5% and DSR is 60%. When the malicious nodes increase from 25% to 35%, the packets dropped by FTDSR increase only 4% while DSR increase 15%.

Compared with FTDSR family, the results also have shown that FTDSR-II is more trustworthy than FTDSR, while FTDSR-I has the trust loss than FTDSR.

B. End to End Delay

End to End Delay (ETE Delay) refers to the time taken for a packet to be transmitted across a network from source to destination. In order to choose the most trusted path, the unique backward decision process in FTDSR is implemented which is more complex than DSR and TDSR. Furthermore, the most trusted route is not always the shortest path.

The end to end latency of FTDSR turns to be averagely 26% longer than DSR and TDSR. And because FTDSR-I has avoided the second-decision making process, its delay is less than FTDSR. While the calculation in FTDSR-II is more complex than that in FTDSR, so its delay is longer generally.Fig.7 shows the result.

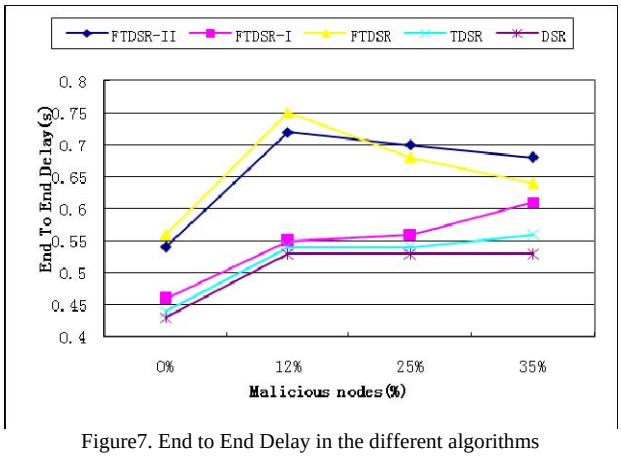

Figure7. End to End Delay in the different algorithms

C. Throughput

In MANET, throughput is the average rate of successful message delivery over a communication channel. These data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually the sum of the data rates that are delivered to all terminals in a network, which can be analyzed mathematically by means of queuing theory, where the load in packets per time unit.

In this experiment, the path's time-average throughput in the destination node is given the statistics, which is measured in packets per second. Fig.8, Fig.9 and Fig.10 show the throughput to the destination under the conditions of 12%, 25%, and 35% malicious nodes respectively. According to the distribution values in each figure, it can be found that FTDSR can get an obvious higher throughput than DSR and TDSR. Take fig.8 as an example, in the end of the simulation, the throughput of TDSR is 0.14 packet per second, and FTDSR is 0.22 packet per second, FTDSR improves the throughput by 57%. Because FTDSR-II has more consideration about the stability of the trust value, it can generally get the higher throughput than FTDSR.

VII. CONCLUSIONS

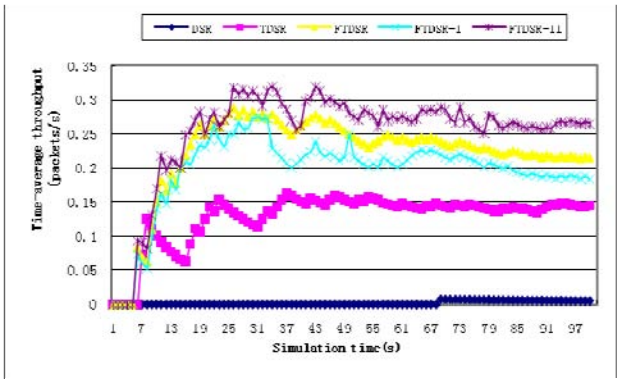

Figure8. Throughput with 12% malicious nodes

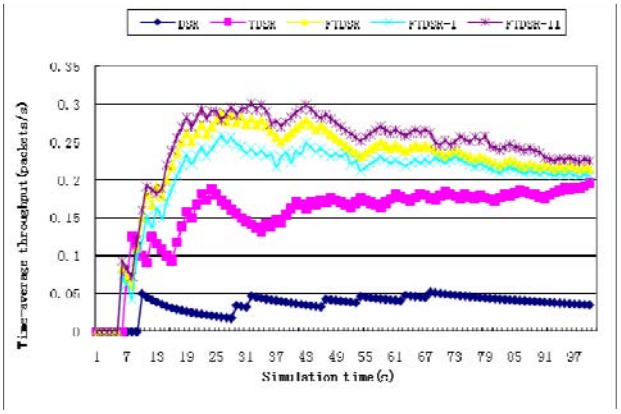

Figure9. Throughput with 25% malicious nodes

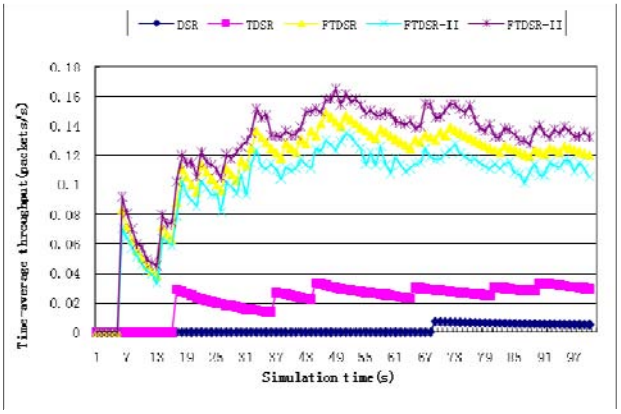

Figure10. Throughput with 35% malicious nodes

MANET is a multi-hop self-configuring network without any fixed infrastructure to communicate. Its topology changes dynamically and each node faces challenges from its processor, power, size, storage etc. Because the uncertainty exists in all of the evaluation factors, fuzzy theory is suitable for the evaluation of the uncertainty and the boundary.

In this paper, based on the classic fuzzy theory, the trust evaluation modeling and the dynamic routing protocols for MANET are introduced and verified. First, it has introduced the fuzzy trust evaluation model about each MANET node, including direct trust evaluation according to the features of the node and trust evaluation with fuzzy logic to model the node, the network and the environment. Second, the routing decision with fuzzy dynamic programming is discussed, focus on each step of

the algorithm and how to make the multi-stage decision, then it represents the process to establish the fuzzy trusted DSR, and gives two optimization methods for FTDSR. The experiments use OPNET to simulate a MANET environment. The result has shown that FTDSR protocols can improve the network security, reduce the Packet Drop Ratio, and enhance the throughput with the acceptable End to End Delay.

In the future work, more optimization should be done to improve the efficiency of the FDP for the better use in the real MANET environments.

REFERENCES

[1] Q. Zhiwei, J. Zhiping, and C. Xihui, "Fuzzy Dynamic Programming Based Trusted Routing Decision in Mobile Ad Hoc Networks," in Embedded Computing, 2008. SEC '08. Fifth IEEE International Symposium on, 2008, pp. 180-185.

[2] M. Conti and S. Giordano, "Multihop Ad Hoc Networking: The Theory," Communications Magazine, IEEE, vol. 45, pp. 78-86, 2007.

[3] A. Boukerche, "Performance comparison and analysis of ad hoc routing algorithms," in Performance, Computing, and Communications, 2001. IEEE International Conference on. , 2001, pp. 171-178.

[4] Chang. E, Dillon T, and Hussain. F, "Trust and reputation for service oriented environment", John Wiley and Sons, 2005.

[5] J. Golbeck, "Computing with Trust: Definition, Properties, and Algorithms," in Securecomm and Workshops, 2006, 2006, pp. 1-7.

[6] U. Maurer, "Modeling a public key infrastructure," in Proc. Eur. Symp. Res. Comput. Security, vol. 1146, Lecture Notes in Computer Science, 1996, pp. 325-350.

[7] M. K. Reiter and S. G. Stubblebine, "Resilient authentication using path independence," IEEE Trans. Comput., vol. 47, no. 12, pp. 1351 - 1362, Dec. 1998.

[8] C. Ben-Jye and K. Szu-Liang, "Markov Chain Trust Model for Trust-Value Analysis and Key Management in Distributed Multicast MANETs," Vehicular Technology, IEEE Transactions on, vol. 58, pp. 1846-1863, 2009.

[9] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in Proc. ACM Security for Ad-Hoc and Sensor Netw., 2004, pp. 66-67.

[10] M. Alkan, A. M. Erkmen, and I. Erkmen, "Fuzzy dynamic programming," in Electrotechnical Conference, 1994. Proceedings. , 7th Mediterranean, 1994, pp. 723-726 vol.2.

[11] A. Boukerch, L. Xu, and K. El-Khatib, "Trust-based security for wireless ad hoc and sensor networks," Computer Communications, vol. 30, pp. 2413-2427, 2007.

[12] G. Theodorakopoulos, and J. Baras, "Trust evaluation in ad-hoc networks," Proceedings of ACM workshop on Wireless security, USA, 2004, pp. 1-10

[13] G. Suryanarayana, M. H. Diallo, J. R. Erenkrantz, and R. N. Taylor, "Architectural support for trust models in decentralized applications," in Proc. 28th Int. Conf. Softw. Eng., May 2006, pp. 52-61.

[14] L. Xiong and L. Liu, "Building trust in decentralized peer to peer electronic communities," in Proc. 5th Int. Conf. Electron. Commerce Res., Oct. 2002, pp. 1-15.

[15] E. Kotsovinos and A. Williams, "BambooTrust: Practical scalable trust management for global public computing," in Proc. ACM Symp. Appl. Comput., Apr. 2006, pp. 1893-1897.

[16] G. Zacharia and P. Maes, "Trust management through reputation mechanisms," Appl. Artif. Intell., vol. 14, no. 9, pp. 881-907, Oct. 2000.

[17] S. Buchegger and J. L. Boudec, "Performance analysis of the confidant protocol: Cooperation of nodes-Fairness in dynamic ad hoc networks," in Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput., Jun. 2002, pp. 226-236.

[18] H. Sun and J. Song, "Strategy proof trust management in wireless ad hoc network," in Proc. Can. Conf. Elect. Comput. Eng., May 2004, vol. 3, pp. 1593-1596.

[19] E. C. H. Ngai, M. R. Lyu, and R. T. Chin, "An authentication service against dishonest users in mobile ad hoc networks," in Proc. IEEE Aerosp. Conf., Mar. 2004, vol. 2, pp. 1275-1285.

[20] C. Candolin and H. H. Kari, "Distributing incomplete trust in wireless ad hoc networks," in Proc. IEEE Southeast Conf., Apr. 2003, pp. 68-73.

[21] D. K. Chiu, C. Wang, H.-F. Leung, I. Kafeza, and E. Kafeza, "Supporting the legal identities of contracting agents with an agent authorization platform," in Proc. Int. Conf. Electron. Commerce, Aug. 2005, vol. 113, pp. 721-728.

[22] Y. Sun, W. Trappe, and K. J. Ray, "A scalable multicast key management scheme for heterogeneous wireless networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 653-666, Aug. 2004.

[23] A. A. Pirzada and C. McDonald, "Trust establishment in pure ad hoc networks," Wirel. Pers. Commun., vol. 37, no. 1/2, pp. 139-168, Apr. 2006.

[24] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," Computer Communications, vol. 31, pp. 4343-4351, 2008.

[25] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks," Wireless Communications and Networking Conference 2004 WCNC 2004, 21-25 March 2004, vol. 2, IEEE, pp. 825-830.

[26] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: self-organized network-layer security in mobile ad hoc networks," IEEE J. Selected Areas Commun.24 (2) (2006) 261-273.

[27] S. Zhong, J. Chen, and Y.Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks, " INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, 30 March–3 April 2003, vol. 3, IEEE, pp.1987-1997.

[28] M. A. Caloyannides, "Online monitoring: security or social control?," Security & Privacy, IEEE, vol. 2, pp. 81-83, 2004.

[29] Guo Wei, Xiong Zhongwei, and Li Zhitang, "Dynamic trust evaluation based routing model for ad hoc networks", Proc. of the Wireless Communications, Networking and Mobile Computing 2005, Sept.2005, Vol.2, pp.727-730.

[30] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," Computer Networks, vol. In Press, Corrected Proof, 2009.

[31] Manickam, J. Martin Leo, and Shanmugavel. S, "Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET", Advanced Computing and Communications 2007, Dec.2007, pp.414-421.

[32] Khayata R.E., Puig C.M., Zweig J.M, "A distributed medium access protocol for wireless LANs", *Signals, Systems and Computers 1994*, Nov.1994, Vol.1, pp.238-242.

Hongjun Dai received the B.S. degree in computer science and technology and the PH.D degree in computer application from Zhejiang University of China in 2002 and 2007, respectively.

He is currently a Full Lecturer at the School of Computer Science and Technology, Shandong University, Jinan, China. His research interests include component-based software, multi-core computer architecture, and trust computing for embedded systems and MANETs.

Zhiping Jia received the B.S. degree and the M.S. degree in computer technology from Shandong Industry University of China in 1989 and 1992 respectively, and the PH.D degree in control theory and engineering from Shandong University of China in 2007.

He is currently a Full Professor at the School of Computer Science and Technology, Shandong University, Jinan, China. His research interests include control engineering, embedded system, real-time system, distributed computing, and trust computing.

Zhiwei Qin received the B.S. degree in computer science and technology from Shandong Normal University of China in 2004, and received the M.S. degree in computer architecture from Shandong University of China in 2009.

He is currently a PH.D Candidate of Department of Computing at the Hong Kong Polytechnic University, China. His research interests include multi-core embedded software and systems, trust computing for MANETs.