Fuzzy Trust Recommendation Based on Collaborative Filtering for Mobile Ad-hoc Networks

Junhai Luo[1,2], Xue Liu[2], Yi Zhang[3], Danxia Ye[1], Zhong Xu[2,4]
[1]School of Computer Science & Engineering,
University of Electronic Science and Technology of China,Chengdu,China,610054
[2]School of Computer Science, McGill University, Montreal, Canada, H3A 2A7
[3]School of Engineering, University of California, Santa Cruz,Santa Cruz, CA 95064
[4]College of Automation, Northwestern Polytechnical University, Xi'an, China, 710072

***Abstract*—Mobile ad-hoc networks (MANETs) are based on the cooperative and trust characteristic of the mobile nodes. Typically, nodes are both autonomous and self-organized without requiring a central administration or a fixed network infrastructure. Due to their distributed nature, MANETs are very vulnerable to various attacks. To enhance the security of MANETs, it is important to rate the trustworthiness of other nodes without central authorities to build up a trust environment. In this paper, we propose a fuzzy trust recommendation based on collaborative filtering, which stimulates collaboration among distributed computing and communicating nodes, facilitates the detection of untrustworthy nodes, and assists decision-making in various protocols for MANETs. Due to the uncertain interaction outcomes, we use fuzzy logic to model trust recommendation in a MANET environment. Our trust model combines direct trust and trust recommendation information based on collaborative filtering to allow nodes to represent and reason with uncertainty and imprecise information regarding other nodes' trustworthiness. Simulation results show that the proposed model is flexible and valid.**

I. Introduction

MANETs are mobile networks which are spontaneously deployed over a geographically limited area, without requiring any pre-existing infrastructure [1]. Due to their distributed nature, MANETs are very vulnerable to various attacks. To enhance security of MANETs, it is important to rate the trustworthiness of other nodes without central authorities to build up a trust environment. Such mechanisms allow a node to evaluate trustworthiness of other nodes, and not only help in malicious node detection, but also improve network performance. In other words, mobile nodes can know whether and how much they can trust other mobile nodes with the help of trust mechanisms. The trust information guides nodes not to take highly risky actions, such as asking or forwarding date packets to the node with low trust value. As a result, the performance and robustness of MANETs will be improved [2].

Recently, various research has focused on building up trust among distributed network nodes to simulate cooperation and improving the performance and security of the network. Most studies use cryptographic primitives to address security attributes including availability, integrity, authentication, confidentiality, authorization, and non-repudiation. These solutions are not always suited to MANETs [3].

In MANETs, a trust relationship formed from direct interactions can be characterized as direct trust; a trust relationship or a potential trust relationship built from recommendations by a trusted node or a chain of trusted nodes, which create a trust path, is called indirect trust [4]. Regarding the aspect of recommendation, a node with high trust value does not correspond to the high or correct recommendation to other nodes. The trustworthiness of the recommendation of a node is different from that of the node itself, especially under some attack conditions, such as malicious collusion attacks. So, the hypothesis that nodes with the high trust value will give honest recommendations is questionable. The trust model in a MANET environment is hard to assess due to the uncertainties involved. The theory of fuzzy logic extends the ontology of mathematical research to be a composite which leverages quality and quantity, and which contains certain fuzziness. Introducing fuzzy logic into the research of trust management by combining the collaborative filtering, we try to solve the issues associated with uncertainty in a MANET trust management.

The rest of the paper is organized as follows. After this introduction, the second section describes and comments on related work that has been done in the field of trust model and computation. The background about trust relationship, fuzzy logic, and design consideration in this work is described in section III. Three kinds of similarity measurements are discussed in section IV. The fuzzy trust-based filtering and recommendation is addressed in section V. Section VI describes the simulation framework and results. Section VII outlines the conclusions and future work.

II. Related Work

Establishing security associations based on distributed trust models among nodes is an important consideration while designing a secure routing solution in MANETs [5]. Not much work has been done to develop a trust model to build up, distribute and manage trust levels among the ad-hoc nodes. Some of the proposed schemes talk about the general requirements of trust establishment. Some of the algorithms think about the direct and recommendation trust to come up with trust computations.

In [6], the authors propose a CONFIDANT protocol based on the dynamic source routing (DSR) protocol. CONFIDANT extends reactive routing protocols with a reputation based system in order to isolate misbehaving nodes. Each node monitors the behavior of its next hop neighbors in a similar way to watchdog. The monitoring mechanism is implemented by a neighborhood watch concept where the no-forwarding behavior of the nodes are monitored and reported. The information is given to a reputation system that updates the rating of the nodes.

In [7], Josang propose a trust model based on subjective logic, which introduces the concepts of evidence space and opinion space to describe and measure trustworthiness. Based upon the beta distribution function that describes the posteriori probability for binary events, the author calculates the trustworthiness for every possible event from every entity.

Watchdog and Pathrater mechanisms [8] are two extensions to the DSR algorithm. The watchdog mechanism, based on promiscuous mode operation of the ad-hoc nodes, has been the fundamental assumption in many trust computational models. The pathrater mechanism uses the knowledge form the watchdog extension to choose a path that is most likely to forward data packets.

Buttyan and Hubaux introduce a virtual currency called Nuglets, which is used to charge/reward the packet forwarding service [9]. A credit counter can implement the nuglets. There are two models in nuglets, packet purse model and packet trade model.

Some mechanisms are proposed to give incentives to the nodes for acting unselfishly. He, Wu & Khosla propose a secure and objective reputation-based incentive (SORI) scheme to encourage packet forwarding and discipline selfish behavior [10]. The scheme, however, does not prevent a malicious node from selectively forwarding packets or from other malicious behavior.

CORE [11] is a generic mechanism by which each on observations in a similar manner to watchdog. CORE can be integrated with many network functions, such as packet forwarding and delay. CORE stimulates node cooperation by using a collaborative monitoring technique and a reputation mechanism. CORE makes use of a node's own experience and other nodes experiences as well (called subjective and indirect reputation respectively). The combined experiences are described by a function. If the observed behavior is different from the outcome of this function, then the rating of the observed nod is altered.

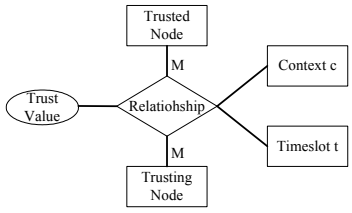
III. BACKGROUND

A. Trust Relationship

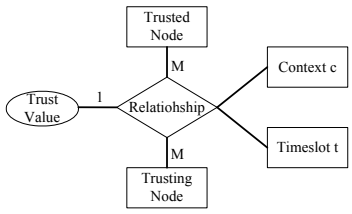
In MANETs, an important notion of network security is trust, which represents a node's individual assessment of the reliability, honesty, etc., for a given context *c* at a given timeslot *t*. The concept of trust in the realm of network privacy corresponds to a set of relationships among nodes. The node to be assessed for trustworthiness will be called trusted node and the node assessing the trusted node's trustworthiness will be called trusting node [12]. Nodes which share information about their past experiences with the requesting node are called recommending nodes. Trust influences decisions like access control, choice of public keys etc. Trust is realized by the trust relationship. Trust has no meaning without a relationship. A trust relationship is an association between a trusting node and a trusted node in MANETs. Trust relationships are determined by rules that evaluate the evidence in a meaningful way generated by the previous behaviors of a node. The contact between the trusting node and the trusted node is formed by the three means, i.e., direct personal contact or interaction with one another, association through other nodes' recommendations, and contact through reviewing the history records.

In Figure 1, there is a M: M (many-to-many) trust relationship between the trusting node and the trusted node for context *c* at timeslot *t* [13]. In a relationship, there is a trust vale that denotes the degree of the relationship from the trusting node to the trusted node. The trust value is also unique for context *c* at timeslot *t*. For a given trusting node and a given trusted node in a given trust relationship, there is a M: M: 1 (many-to-many-to-one) relationship between the trusting node, the trusted node, and the trust value for context *c* at timeslot *t*.

However, the trust value is dynamic in different context *c* and timeslot *t*. The trust vale ascribed to a node is based on each individual's own experience with that node: positive experiences lead to positive trust and negative ones to distrust. Although based on the known outcomes of previous experiences, there is inherent uncertainty regarding the level of trust ascribed to the node. For example, there is no guarantee that a previously reliable node will continue to be so. Fuzzy logic offers the ability to handle uncertainty and imprecision effectively, and is therefore suited to reasoning about trust. Inference using fuzzy logic copes with imprecise inputs, such as assessments of quality, and allows inference rules to be specified using imprecise linguistic term, such as "very high quality" or "slightly late".



(a): Trust Relationship for Context c at Time t



(b): Trust Relationship for Context c at Time t with Cardinality

Fig. 1. Trust Relationship

B. Fuzzy Logic for Trust

For every element x in the set of X, there is a mapping $x \mapsto \mu(x)$, in which $\mu(x) \in [0,1]$. The set $\Delta = \{(x, \mu(x))\}$ is defined a fuzzy set for trust in MANETs. $\mu(x)$ is defined as the membership function for every x in Δ. A membership function defines the degree to which a fuzzy variable is a member of a set. Full membership is represented by 1, and no membership by 0.

Fuzzy logic is derived from fuzzy set theory dealing with reasoning that is approximate rather than precisely deduced from classical predicate logic. Fuzzy set theory defines fuzzy operators on fuzzy sets. The problem in applying this is that the appropriate fuzzy operator may not be known. For this reason, Fuzzy logic usually uses IF/THEN rules, or constructs that are equivalent, such as fuzzy associative matrices. Rules are usually expressed in the form:

IF variable IS set THEN action

For example, an extremely simple temperature regulator that uses a fan might look like this:

(R1) IF temperature IS very cold THEN stop fan
(R1) IF temperature IS cold THEN turn down fan
(R1) IF temperature IS normal THEN maintain level
(R1) IF temperature IS hot THEN speed up fan

Rules are applied in parallel and the conclusion membership degrees are aggregated by superimposing the resultant membership curves [14]. A Mamdani Min-Max approach is applied to inference, such that the membership degree of rule conclusions is clipped at a level determined by the minimum of the maximum membership values of the intersections of the fuzzy value antecedent and input pairs [15].

C. Design Considerations

There are five topics that are important to address in any MANETs trust model [16]:

1) The trust model should be without infrastructure. Because the network routing infrastructure is formed in an ad-hoc fashion, the trust management can not depend on, e.g., a trusted third party (TTP). There is no public key infrastructure (PKI), where some center nodes monitor the network, and publish illegal nodes periodically. In a MANET, there are no certification authorities (CA) or registration authorities (RA) with elevated privileges etc.
2) The trust model should be anonymous because of the anonymity of mobile nodes in MANETs.
3) The trust model should be robust. That is, it can be robust to all kinds of unfriendly attacks and the network itself should not be susceptible to attacks by unfriendly nodes. Moreover, in the presence of malicious nodes, they attempt to subvert the model in order to get the unfairly good trust value.
4) The trust model should have minimal control overhead in accordance with computation, storage, and complexity.
5) The trust model should be self-organized. MANETs are characterized to have dynamic, random, rapidly changing and multi-hop topologies composed of relatively bandwidth-constrained wireless link between nodes. Furthermore, evidence is uncertain and incomplete generated by the nodes on the fly without lengthy processes.

IV. Similarity Functions

Those nodes in the open, self-organization and distribution MANETs may collude each other or take "bad-mouthing manner" to attack the trust model so as to maximize their own benefits, such as packet-forwarding, power-control or control overhead etc. For instance, a node may take a collusion with a group of nodes in order to be given the unfairly high reputation value by them, which will have a effect on inflating the node's reputation, so allowing the node to receive more services from other nodes in MANETs at a normal price than it deserves. In other side, a node may collude with some nodes to "bad-mouth" other nodes that it want to slander and isolate. In this way, those conspiring nodes make some unfairly negative evaluation to reduce the reputations of the target nodes in MANETs.

Suppose that $N_s = [N_1, N_2, N_3, \cdots, N_n]$ denotes the set of nodes with which both node A and the recommender B make some interactions. The vector $V_A = [\overline{v}_{A_1}, \overline{v}_{A_2}, \overline{v}_{A_3}, \cdots, \overline{v}_{A_n}]$ denotes trust rating vector that node A makes rating to each node N_j in N_s set to form, where $\overline{v}_{i_j}$ is the average evaluation from node i to node j. The trust evaluation from node B to each node N_j in N_s set forms a vector $V_B = [\overline{v}_{B_1}, \overline{v}_{B_2}, \overline{v}_{B_3}, \cdots, \overline{v}_{B_n}]$. The credibility of recommendations of node B can be computed by the similarity of the trust rating information between node A and Node B. There are three commonly used methods to measure the similarity between vectors listed as follows [17]:

1) Cosine-based similarity: In this case, the trust ratings of every node are thought of as a vector in the m dimensional space. If a node does not evaluate a node, then the default rating is set. The similarity between two nodes is measured by computing the cosine of the angle between these two vectors. Formally, in the ratings matrix, similarity between nodes i and j, denoted by $cos(i, j)$ is given by

$$\cos(\overrightarrow{i}, \overrightarrow{j}) = \sin(i, j) = \frac{\overrightarrow{i} \bullet \overrightarrow{j}}{\left\| \overrightarrow{i} \right\| * \left\| \overrightarrow{j} \right\|} \qquad (1)$$

where "$\bullet$" denotes the dot-product of the two vectors.
2) Correlation-based similarity: In this case, the similarity between two nodes i and j is measured by computing the Pearson-r correlation. Let the set of nodes who both make ratings nodes i and j is denoted by U, then the correlation similarity is expressed by

$$\cos(\overrightarrow{i}, \overrightarrow{j}) = \sin(i, j) = \frac{\sum_{u \in U} (R_{u,i} - \overline{R_i})(R_{u,j} - \overline{R_j})}{\sqrt{\sum_{u \in U} (R_{u,i} - \overline{R_i})^2 (R_{u,j} - \overline{R_j})^2}} \qquad (2)$$

where $R_{u,i}$ is the rating of node u to node i, $\overline{R_i}$ and $\overline{R_j}$ are the average ratings of nodes i and j separately.
3) Adjusted cosine similarity: In the case of using basic cosine measure, the node-specific rating bias of each node

is not taken into account. The adjusted cosine similarity offsets this drawback by subtracting the corresponding node's average from each co-rated pair. Formally, the adjusted cosine similarity between node i and node j is given by

$$\cos(\overrightarrow{i},\overrightarrow{j}) = \sin(i,j) = \frac{\sum_{u\in U}(R_{u,i}-\overline{R_u})(R_{u,j}-\overline{R_u})}{\sqrt{\sum_{u\in U}(R_{u,i}-\overline{R_u})^2(R_{u,j}-\overline{R_u})^2}} \quad (3)$$

where $\overline{R_u}$ is the average ratings of the u-th node.

V. Fuzzy Trust-Based Filtering & Recommendation

In this section, we first describe a similarity model based on collaborative-filtering between a node and a node set in a genre. We then introduce a fuzzy trust recommendation framework, the recommendation algorithm based on collaborative-filtering for MANETs.

A. Collaborative Filtering

In a collaborative filtering, suppose that there are N nodes denoted as $n_i, i = 1,2,\cdots,N$, and $N \times N$ node-node trust rating matrix. Rating of a node to a node is denoted by $r[i,j], i = 1,2,\cdots,N \quad and \quad j = 1,2,\cdots,N$. The collaborative filtering for MANETs in this paper is originated from user-based [18] collaborative filtering which is one of the most successful personalized recommendation technology in e-commerce application. The basic assumption is that nodes have similar trust preferences on some node may also have similar preferences on other nodes. Thus the algorithm provides recommendations or predictions to the target node based on the opinions of other like-minded nodes. The foundation of collaborative filtering is built on the basis of similarity. The target node's evaluations are similar to that of its nearest-neighbors. In other words, the target node's rating for a node can be predicted by combining the ratings of the target node's nearest-neighbors.

Collaborative filtering recommendation mainly includes three steps described as follows.

1) Representation, a node trust rating matrix R,$R = (r_{ij})$ is used to represent node ratings. The evaluations of nodes are shown by a $N \times N$ matrix R.
2) Neighborhood formation, to find the set of the K most similar nodes-nearest-neighbors, all the similarities between nodes in the model are computed. The K most similar nodes-nearest-neighbors are sorted by similarity.
3) Recommendation generation, based on the nearest-neighbor set, the predicted ratings of the node unrated by the target node can be computed, and the recommendations are generated. Suppose that the nearest-neighbor set of node i is NNS_i, the predicted rating of node i on node k is T_{ik}, $cos(i,j)$ is the similarity between node i and node j, which is traditionally calculated as Pearson's correlation coefficient, $\bar{R_i} = \sum_k R_{i,k}$ and $\bar{R_j} = \sum_k R_{j,k}$ are the average trust ratings of node i and node j. Based on Resnick's standard predication formula, T_{ik} can be estimated as below 4:

$$T_{ik} = \bar{R_i} + \frac{\sum_{j\in NNS_i} cos(i,j) * (R_{j,k} - \bar{R_i})}{\sum_{j\in NNS_i} |cos(i,j)|} \quad (4)$$

We set $f(r_i,n_j) = cos(i,j) = W_{ij}$, then the Equation 4 is re-denoted as:

$$T_{ik} = \bar{R_i} + \frac{\sum_{j\in NNS_i}(R_{j,k} - \bar{R_i}) * W_{ij}}{\sum_{j\in NNS_i} |W_{ij}|} \quad (5)$$

B. Local Trust Representation

In MANETs, each node i can store the number of the successful packet-forwarding transactions it has had with node j, S_{ij}, and the number of the failed packet-forwarding transactions it has had with node j, F_{ij}. We define a local trust value:

$$C_{ij} = \frac{S_{ij} - F_{ij}}{\sum_j S_{ij} - F_{ij}} \quad (6)$$

This ensures that all values will be between -1 and 1. If a node doesn't make any transactions with other nodes in MANETs, it will assign a zero score to all other nodes . In this case, we set $C_{ij} = pr_j$, meaning that the node chooses to trust the pre-trusted nodes. So the formula 6 is redefined as:

$$C_{ij} = \begin{cases} C_{ij} = \frac{S_{ij}-F_{ij}}{\sum_j S_{ij}-F_{ij}} & if \ \sum_j S_{ij} - F_{ij} \neq 0 \\ pr_j & \text{otherwise} \end{cases} \quad (7)$$

C. Fuzzy Trust Recommendation

we associated a trapezoid membership function (TMF) that enables us to specify a range for a give trust level instead of giving it a particular discrete value. A TMF shown in Figure 2 is defined as (a_1,a_2,a_3,a_4), where $a_1 \leq a_2 \leq a_3 \leq a_4$. The TMF, denoted as $\mu(x)$, is defined as follows:

$$\mu(x) = \begin{cases} 1 & a_2 \leq x \leq a_3 \\ 0 & x = a_1 \quad or \quad x = a_4 \\ \frac{x-a_1}{a_2-a_1} & a_1 < x < a_2 \\ \frac{x-a_4}{a_3-a_{a4}} & a_3 < x < a_4 \end{cases} \quad (8)$$

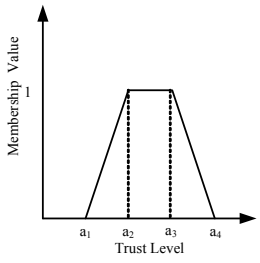


Fig. 2. Trapezoid Membership Function

In order to use fuzzy inference to determine trust, we must define trust as a fuzzy variable, with an associated set of fuzzy trust level that quantifies the behavior trust of a node in MANETs. The universe of discourse (UoD) is $[-1,1]$, which ranges over a set of linguistic label values from high distrust to high trust as illustrated in Table I. We define these fuzzy

TABLE I
FUZZY TRUST LEVELS

Trust Level	Description	TMF
HD	High Distrust	$[-1,-0.8,-0.6]$
D	Distrust	$[-0.8,-0.6,-0.4,-0.2]$
UD	Undistrust	$[-0.4,-0.2,0]$
UT	Untrust	$[0,0.2,0.4]$
T	Trust	$[0.2,0.4,0.6,0.8]$
HT	High Trust	$[0.6,0.8,1]$
U	Unknown	$[0,0,0,0]$

trust levels: high distrust (HD), distrust (D), undistrust(UD), untrust(UT), trust(T), high trust (HT), and unknow (U).

Suppose that there are two linguistic fuzzy trust labels, i.e., a and b, which are represented by using TMFs. Then, there are some operations [19] defined as follows:

1) Addition: $(a_1,a_2,a_3,a_4)+(b_1,b_2,b_3,b_4)=(a_1+b_1,a_2+b_2,a_3+b_3,a_4+b_4)$
2) Substraction: $(a_1,a_2,a_3,a_4)-(b_1,b_2,b_3,b_4)=(a_1-b_1,a_2-b_2,a_3-b_3,a_4-b_4)$

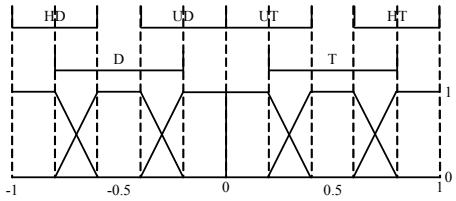


Fig. 3. Description of Fuzzy Trust Level

D. Fuzzy Inference

As above mentioned, let $x_i \quad (i=1,2,\cdots m)$ be the input variable. The inference rule is expressed as follows:

$$\begin{array}{c} R_1 \quad If \;\; x_1 \; is \; A_j^1, \; x_2 \; is \; A_j^2, \; \cdots \; x_m \; is \; A_j^m \\ Then \; y=\varpi_j \quad (i=1,2,\cdots,m) \end{array} \tag{9}$$

where A_j^m is fuzzy set of jth rule defined in ith input variable and ω is the "non-fuzzy" real number value. Let x_i^0 denote the input value to the reasoning model. Therefore, the membership degree d of the rule is computed as:

$$d_j=\prod_{i=1}^{m}\mu_{A_j^i}(x_i^0) \tag{10}$$

where $\mu(\bullet)$ is the membership function shown in Figure 3. The output of the fuzzy inference model is denoted as:

$$W=\frac{\sum_{i=1}^{m} d_i\varpi_i}{\sum_{i=1}^{m} d_i} \tag{11}$$

where the output W is used as the similarity of collaborative filtering for the trust model in MANETs. In this paper, we let the correlation coefficient value r or both the correlation coefficient value r and the number of rated nodes n in Equation 5 be the input of the fuzzy model [20]. The flowchart of trust recommendation based on collaborative filtering of the fuzzy reference is shown in Figure 4.

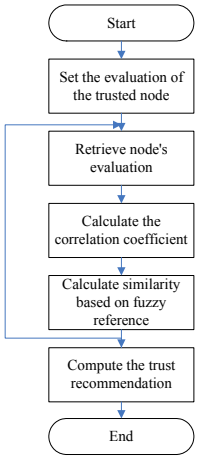


Fig. 4. Flowchart of Collaborative Filtering Based on Fuzzy Reference

VI. PERFORMANCE EVALUATION

A. Metrics

The following metrics are considered:

(1) Throughput. One of metrics is the result of the total throughput of a network with n mobile nodes [6]. That is, the data forwarded to the correct destination for each node i is denoted as follow:

$$Throughput=\frac{\sum_{i=1}^{n} Packets_{Received}}{\sum_{i=1}^{n} Packets_{Originated}} \tag{12}$$

As opposed to the throughput, packet loss and retransmissions are taken into account. The goodput is directly influenced by packet loss. Packet loss can occur due to general network conditions causing link errors or unreachable nodes, but packets can also be lost because an intermediate node intentionally drops them. The latter is the only form of packet loss directly attributable to malicious behavior. We therefore use the number of intentionally dropped packets as a metric, both in absolute numbers and relative to the number of packets originated.

(2) Mean absolute error (MAE). This measures the quality of the recommender model, and it denotes statistical accuracy and decision support accuracy for trust recommendation in MANETs. MAE is one of the statistical accuracy metrics. It is easy to be understood, and is the most common method of evaluating the quality of recommendation. Suppose the set of trust recommendation is $\{Tr_1,Tr_2,\cdots,Tr_N\}$, corresponding the set of real evaluations $\{Rr_1,Rr_2,\cdots,Rr_N\}$, MAE is defined as follows:

$$MAE=\frac{\sum_{i=1}^{N}|Tr_i-Rr_i|}{N} \tag{13}$$

B. Simulation Setup

We perform our simulation on a NS-2 simulator. Various network scenarios are analyzed to prove the accuracy of the model and its characteristics. Every plot is taken as an average of ten different runs. In this experiment, the area, where the nodes are placed randomly, is chosen to maintain the network density and connectivity as constant and balanced. The size

of the area is $1000m \times 1000m$, and AODV is used as the underlying routing protocol.

The fixed parameters for the simulation are shown in Table II [6]. The radio range and sending capacity are chosen to represent an off-the-shelf device. The speed of the node is uniformly distributed between 5m/s and 20m/s. The MAC layer protocol simulates the IEEE 802.11 distributed coordination function (DCF), and assumes a fixed transmission range model, when two nodes can directly communicate only if they are in each other's transmission range. The mobile nodes use the random waypoint as the movement model. The traffic is produced using a traffic generator, which generates constant bit rate (CBR) sessions. The data packet size is 64 bytes, and no fragmentation is used.

TABLE II
SIMULATION PARAMETERS

Parameter	Value
MAC	802.11
Area	$1000m \times 1000m$
Speed	$[5, 20]$
Radio range	250m
Placement	Uniform
Movement	Random waypoint
Application	CBR
Sending capacity	2Mbps
Packet size	64B
Simulation time	900s

C. Simulation Results

In the first experiment, to determine the best similarity measure among the three methods, i.e., cosine-based, correlation-based, and adjusted cosine-based, The MAE values corresponding three similarity measures with different sizes of neighborhood nodes can be computed. The experimental results are shown in Table III, where NN is the neighborhood nodes and SM is the similarity measurement. As shown in Figure 5, given the same number of neighborhood nodes, using the adjusted cosine similarity measurement always results the lowest MAE values. It means that adjusted cosine measure is better than the others.

TABLE III
MAE VALUES

NN \ SM	Cosine-based	Correlation-based	Adjusted cosine-based
5	1.332	1.335	1.283
10	1.313	1.322	1.302
15	1.286	1.280	1.278
20	1.302	1.300	1.279
25	1.288	1.302	1.288
30	1.294	1.295	1.293
35	1.331	1.332	1.300
40	1.279	1.299	1.279
45	1.336	1.299	1.289
50	1.291	1.333	1.290

In the second experiment, our network consists of good nodes (normal nodes participating in the network to forward packets and update routing) and malicious nodes (adversarial nodes, participating in the network to undermine its performance). We have N=100 total number of mobile nodes in MANETs. Among them, we change the total number of malicious nodes from 1 to 12. In this experiment, the malicious nodes perform gray hole attack [21], i.e., randomly drop 65-75% packets passing through them. Two systems are compared: (1) baseline scheme that does not build or utilize trust record; (2) the system using collaborative filtering-based model for fuzzy trust recommendations. Figure 6 shows the average packet drop ratios of good nodes. The simulation time is 900 seconds. We can see that malicious nodes can significantly degrade the performance of the baseline system. Even with 4 attackers (4% of total nodes), the packet drop ratio can be as high as 25%. Obviously, using the proposed mechanism to build and utilize trust records can greatly improve the performance. In particular, it takes more than 12 attackers (12% of total nodes) to cause 20% average packet drop ratio.

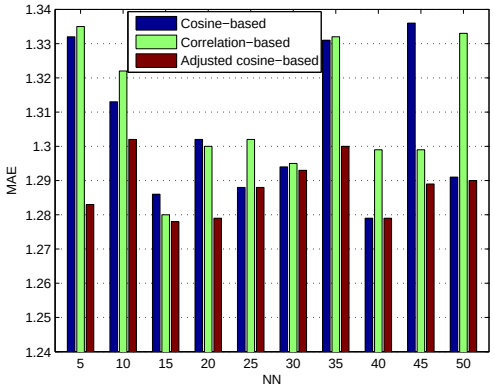


Fig. 5. Comparison of MAE Values

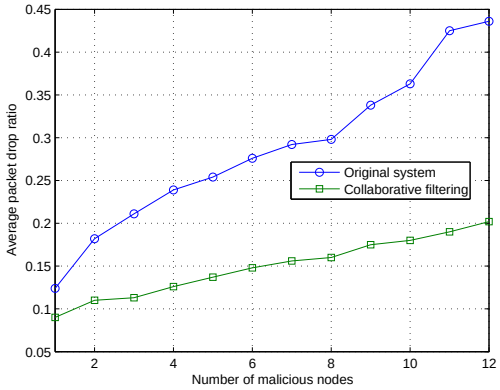


Fig. 6. Average Packet Drop Ratio with Different Number of Malicious Nodes

VII. Conclusion and Future work

Mobile ad-hoc networks (MANETs) exhibit new vulnerabilities to malicious attacks or denial of cooperation due to their characteristics. Mobile nodes need to be equipped with efficient facilities to calculate and evaluate trust and credibility values of other nodes in MANETs. The subjectivity and uncertainty contained in the individual notions and definitions of trustworthiness and credibility need a flexible and adjustable model. It needs to deal with cooperation risk measurement relying on the approximate estimation of a node's behavior instead of detailed and crisp data. In this paper, we have proposed a fuzzy trust recommendation based on collaborative filtering for MANETs. Such approximations are comprised in linguistic terms such as "high", "unreliable", and "unknow". Fuzzy logic is be used to represent trust and select appropriate nodes for cooperation. Our trust model combines direct trust and trust recommendation information based on collaborative filtering to allow nodes to represent and reason with uncertainty and imprecise information regarding other nodes' trustworthiness. Simulation results show that the proposed model is flexible and valid. There are some areas of ongoing work, including additional experimentation and integration with existing models of trust for MANETs. We plan to validate our model in a MANETs environment to assess the framework accuracy on a long term basis.

VIII. Acknowledgments

This work was supported in part by the National Study-abroad Scholarship of China under the Grant No. 27U38009 and the NSERC Discovery Fund under the Grant No. 341823-07.

References

[1] R. Badonnel, R. State, O. Festor, and A. Schaff, "A framework for optimizing end-to-end connectivity degree in mobile ad-hoc networks," *J. Netw. Syst. Manage.*, vol. 13, no. 4, pp. 479–497, 2005.

[2] Y. L. Sun and Y. Yang, "Trust establishment in distributed networks: Analysis and modeling," *Communications, 2007. ICC '07. IEEE International Conference on*, pp. 1266–1273, 24-28 June 2007.

[3] T. Anker, D. Dolev, and B. Hod, "Cooperative and reliable packet-forwarding on top of aodv," *Modeling and Optimization in Mobile, ad-hoc and Wireless Networks, 2006 4th International Symposium on*, pp. 1–10, 03-06 April 2006.

[4] Z. Wu and A. C. Weaver, "Application of fuzzy logic in federated trust management for pervasive computing," in *COMPSAC '06: Proceedings of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06)*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 215–222.

[5] J. N. Al-Karaki and A. E. Kamal, "Stimulating node cooperation in mobile ad-hoc networks," *Wirel. Pers. Commun.*, vol. 44, no. 2, pp. 219–239, 2008.

[6] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad-hoc networking & computing*. New York, NY, USA: ACM, 2002, pp. 226–236.

[7] A. Josang, "A logic for uncertain probabilities," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 9, no. 3, pp. 279–311, 2001.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM, 2000, pp. 255–265.

[9] L. Buttyan and J.-P. Hubaux, "Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks," Tech. Rep., 2001.

[10] 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 IEEE*, vol. 2, pp. 825–830 Vol.2, 21-25 March 2004.

[11] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V., 2002, pp. 107–121.

[12] S. Schmidt, R. Steele, T. S. Dillon, and E. Chang, "Building a fuzzy trust network in unsupervised multi-agent environments," in *OTM Workshops*, 2005, pp. 816–825.

[13] F. K. Hussain, E. Chang, and T. S. Dillon, "Trust relationships and reputation relationships for service oriented environments," in *AICCSA '06: Proceedings of the IEEE International Conference on Computer Systems and Applications*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 508–510.

[14] N. Griffiths, K.-M. Chao, and M. Younas, "Fuzzy trust for peer-to-peer systems," *Distributed Computing Systems Workshops, 2006. ICDCSW Workshops 2006. 26th IEEE International Conference on*, pp. 73–73, 04-07 July 2006.

[15] E. H. Mamdani and S. Assilian, "An experiment in linguistic synthesis with a fuzzy logic controller," *Int. J. Hum.-Comput. Stud.*, vol. 51, no. 2, pp. 135–147, 1999.

[16] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *WWW '03: Proceedings of the 12th international conference on World Wide Web*. New York, NY, USA: ACM, 2003, pp. 640–651.

[17] C. Piao, J. Zhao, and J. Feng, "Research on entropy-based collaborative filtering algorithm," in *ICEBE '07: Proceedings of the IEEE International Conference on e-Business Engineering*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 213–220.

[18] J. O'Donovan and B. Smyth, "Trust in recommender systems," in *IUI '05: Proceedings of the 10th international conference on Intelligent user interfaces*. New York, NY, USA: ACM, 2005, pp. 167–174.

[19] F. Azzedin, A. Ridha, and A. Rizvi, "Fuzzy trust for peer-to-peer based systems," *Proceedings of World Academy of Science, Engineering and Technology, 2007. PWASET 2007.*, pp. 123–127, 2007.

[20] T. Watanabe, S. Katayama, and R. Fujioka, "Improvement of collaborative filtering based on fuzzy reasoning model," *Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on*, vol. 6, pp. 4790–4795, 8-11 Oct. 2006.

[21] Y. Sun, W. Yu, Z. Han, and K. Liu, "Trust modeling and evaluation in ad-hoc networks," *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, vol. 3, pp. 1862–1867, 28 Nov.-2 Dec. 2005.