Towards Neutral Trust Management Framework in Unstructured Networks

Ruidong Li

National Institute of Information and Communications Technology, Japan
Email: lrd@nict.go.jp

Jie Li

Graduate School of Systems and Information Engineering, University of Tsukuba, Japan
Email: lijie@cs.tsukuba.ac.jp

***Abstract*—Free-rider problem greatly influences the performance of unstructured networks (like ad-hoc or peer-to-peer networks). To solve such problem, we focus on trust management framework, which is intended to stimulate nodes to cooperate with each other. Currently, the existing trust management framework can be classified into trust establishment framework and reputation-based framework. However, none of them was explicitly designed with the considerations on neutrality, which is indispensable issue when devising a network system. In this paper, we investigate the relation between neutrality and trust definition, and then focus on trust management of one kind of typical unstructured networks, mobile ad hoc network (MANET). We propose a neutral trust management framework of MANET from the several aspects of neutrality characteristics, objectiveness, fairness and variegation. Then, we perform analysis on our proposed framework, which shows our proposal can achieve neutrality under the location-dependent attack of free-rider.**

I. Introduction

Unstructured networks [14] are those networks that have no hierarchy, and in which all users are equally sharing duties or responsibilities. That is, users can choose whether to participate in the operation of the network or not. Also there is a cost associated with choosing to participate. Typical examples of unstructured network are mobile ad hoc networks (MANETs) and peer-to-peer (P2P) network. In a MANET, the users who participate can obtain the service from the network and at the same time, they should forward packets for other users. Similarly, in a P2P network, file sharing protocols depend on the cooperation of the users to succeed.

To make these unstructured network run regularly, the free-rider problem should be solved. Free-rider is defined as the users who obtain the services from the network but does not contribute to the same degree to the community. The free-rider utilizes file-sharing applications to download content from others but does not upload to the same degree in a P2P network, or obtains service from network and refuses to forward packets for other nodes in a MANET. To solve such problem and stimulate the cooperation of users, trust management framework has been researched, which aims to establish and manage trust relations between different users. Basically, trust management framework is designed based on one specific *trust* definition, and mainly has two components, trust calculation and trust propagation.

978-1-4244-5113-5/09/$25.00 ©2009 IEEE

Currently there are two categories of trust management frameworks for unstructured networks. One is *reputation-based framework* [1], [2], [7], [8]. The other is *trust establishment framework* [10], [11], [12], [13]. By the reputation-based frameworks [1], [2], [7], [8], *trusts* for other nodes are evaluated objectively by direct observations and second-hand information. In this category of frameworks, the method to establish a reputation-based framework is mostly Bayesian approach based on Beta distribution [2], [5], [7], [13]. For the trust establishment framework [10], [11], [12], [13], *trusts* for neighbors are evaluated based on direct observations and trust relations between two nodes without previous direct interaction are established through combination of the opinions of intermediate nodes. The difference for the methods in this category of frameworks is mainly on implementation of calculation method for trust and trust propagation method.

However, these existing trust management frameworks lack the considerations on neutrality explicitly, which are important and indispensable issues for network protocol design [3], [15]. Network neutrality is vital to ensuring that users can obtain services free from discrimination or interference. WE can see that the core concept of network neutrality is free from bias. In this paper, we firstly investigate the relation between neutrality and trust definition, and it is discovered that neutrality can be expressed from four aspects: objectiveness, fairness, variegation and privacy preserving. Then, we mainly focus on one of typical unstructured networks, MANET, to design a neutral trust management from the first three aspects, which can be regarded as the first step towards neutral trust management framework. In the existing trust management framework, the fairness characteristic of trust propagation in reputation-based framework and the objectiveness of trust calculation method in trust establishment framework express neutrality to some extent. Based on this findings, we design a neutral trust management framework for MANETs. To the best of our knowledge, we are the first to investigate neutrality of trust management framework. Some analysis results show the reasonability of our proposal.

The remainder of the paper is organized as follows. In Section II, the relation between neutrality and trust definition will be provided. Section III describes the proposed neutral trust management framework for one kind of unstructured

network, MANET. We provide performance evaluations to compare the proposed neutral trust management with the existing frameworks in Section IV. Finally, we conclude our work in Section V.

II. Design Requirements of Neutral Trust Management Framework

Network neutrality is defined as service acquisition free from discrimination or interference [3], [15] in this paper. To achieve network neutrality is a big problem, since it is a concept related to sociality, context. On the other hand, trust management framework is based on the concept "Trust", which can be defined as the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context [6]. Therefore, the neutrality of this belief and the neutrality of influence of this belief are the points we should focus on, when we design a neutral trust management.

We herein firstly investigate the relation between neutrality and trust definition, since it becomes clear that a neutral belief is the cross point of neutrality and trust. In the world, different users has different beliefs. Trust definition is the basis for trust management framework, which reflects the composition of trust. After the trust is defined exactly in a unstructured network, the trust management framework will shape the value of network according to this definition, whatever it is neutral or biased. If the behaviors of users follow the value of network, the users can obtain service from network regularly. Otherwise, they will be exempted from the network. Thus, to find a neutral trust definition is the first step towards neutral trust management framework.

Neurility means no bias. On the contrary, *Trust* means preference on one kind of network value. They seems to be contrast concept. The relation between neutrality and trust definition is clarified in Fig.1. Since bias can be expressed as the acceptance extent, we denote neutrality as the degree of consensus, which is a value between 0 and 1. Here, 0 means completely no consensus, which is antisocial, and 1 indicates complete consensus. From Fig. 1, we can see that when acceptance ratio of trust definition is low, the neutrality is also low. If the acceptance ratio of trust definition becomes higher, the expressed neutrality will also becomes higher.

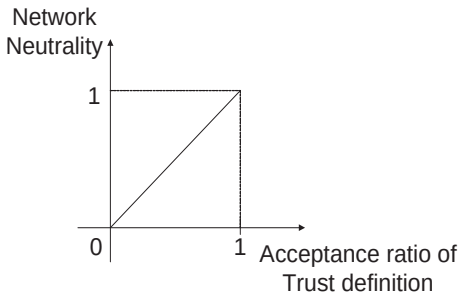

Fig. 1. Neutrality Vs. Acceptance ratio of Trust definition

Besides the trust definition as described in the above, the neutrality of trust calculation and trust propagation are also important to design a neutral trust management framework. Meanwhile, we identify the main characteristics of neutrality as objectiveness, fairness, variegation, and privacy preserving. Therefore, neutral trust management design requirements are summarized in Fig. 2. Since the biased procedure is contrary to neutrality, objectiveness can be seen as one component of neutrality. Fairness should be the basic thing of neutrality. Because of trust definition is various from one to another, variegation should be one component of neutrality. When enforcing trust to different users, the disclose of their identities also violates the neutrality. As in Fig. 2, the main components of trust management framework are shown in the left part, while the main components of neutrality are illustrated in the right part.

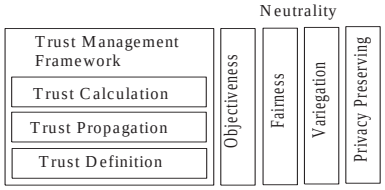

Fig. 2. Neutral Trust Management Design Requirements

In this paper, we will focus on one of typical unstructured networks, mobile ad hoc network (MANET), to design a neutral trust management frameworkand mainly from the first three aspects, objectiveness, fairness, variegation.

III. Proposed Neutral Trust Management Framework in MANETs

Trust in a MANET is simply defined as a *belief level* that one node can put on another node for a specific action according to previous direct or indirect information of observations on behavior, which is similar to [9]. The *belief level* is defined as the probability that one node believes that another node is willing to and able to obey the protocol and act normally in this paper. Herein, we only concentrate on one or two specific action(s). This means that trust is not defined complexly based on multidimensional and comprehensive actions, but is formed based on the simple specific action(s). Under this situation, neutrality can be simply expressed as the selection between action and no such action, which make trust formation procedure has no variegation for different nodes.

In MANETs, the main behavior of free-rider is to refuse to forward packets for others. There are only two options for each mobile node, forwarding packets or refusing to forward. Obviously, forwarding packets meets the social requirements and can get consensus of all users, compared with refusing to forward, since cooperation is the basic function of the system. It corresponds to the point (1, 1) shown in Fig. 1. Therefore, trust here is simply the belief level on the nodes performing forwarding behavior.

In this paper, the notation, $\{subject : object, action\}$, is used to denote the trust relation from a subject node to an object node on a specific action. As an example of utility of

the above notation, $T\{subject : object, action\}$ in this paper is used to denote the *trustworthiness* from a subject node to an object node on the specific action, $action$.

In reputation-based frameworks, the second-hand information has been utilized to form the trustworthiness from one node to another node, which show its fairness for all users. On the other hand, in trust establishment framework, both trust value and confidence value have been considered when evaluating trustworthiness, which reflects its objectiveness. In this paper, we absorb these good points of existing frameworks when designing trust calculation method and trust propagation method in MANETs.

In the proposed framework, subject node evaluates *trust* for object node based upon modified Bayesian approach [2]. It is assumed that subject node believes that object node behaves normally with probability θ. Using modified Bayesian approach [2], there are several distributions such as Beta, Gaussian, Poisson, Binomial etc., which can be used to represent θ. Among these distributions, Beta distribution is the most promising one since it is flexible and simple and its conjugate is also a Beta distribution [2], [5], [7], [13]. Here, θ in the proposed framework is also assumed to follow Beta distribution [4], which is provided as follows.

$$\begin{aligned} Beta(\theta, \alpha, \beta) &= \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \\ \forall\ 0 &\leq \theta \leq 1, \alpha \geq 0, \beta \geq 0 \end{aligned} \quad (1)$$

From equation (1), we can see that there are two parameters to characterize a Beta distribution, which is very suitable for trust management. That is, α and β are used to denote magnitude of *normal behaviors* and *misbehaviors*, respectively. Here, normal behavior means forwarding packets for other nodes. In contrast, misbehavior means refusing to forward packets for others. In this paper, we use ITF to denote *initial trust form* that is formed by the collected raw data. $ITF\{i : j, action\}$, the *initial trust form* from node i to node j on a specific action, $action$, is defined as $(\alpha_{ij}, \beta_{ij})$. Here α_{ij} and β_{ij} are used to describe the number of normal behaviors and the number of misbehaviors of node j observed by node i, respectively. At the same time, second-hand information S_{kj} is similarly defined as the pair $(\alpha_{kj}, \beta_{kj})$.

When forming trust, initially θ is uniform distributed between 0 and 1, which can be described as $Beta(\theta, 1, 1)$. Then if there are s observations with normal behaviors and f observations with misbehaviors, α and β are updated by $\alpha = w_1^{t_d} * (\alpha - 1) + 1 + s$ and $\beta = w_1^{t_d} * (\beta - 1) + 1 + f$, when s observations with normal behaviors, f observations with misbehaviors are collected during period t_d, and w_1 is discount factor using to expire old observations.

According to analysis in [2], if one node performs more normal behaviors, θ will converge to a larger constant near 1 and this node is more trustable. Otherwise, θ will converge to a lower constant near 0 and the node is untrustable.

A. Proposed Neutral Framework Overview

Here we provide the skeleton for the proposed framework as in Figure 3, which is composed of four steps, $S1$, $S2$, $S3$, $S4$ as below. The characteristics of neutrality mentioned in Section 2 have been integrated into the proposed framework naturally.

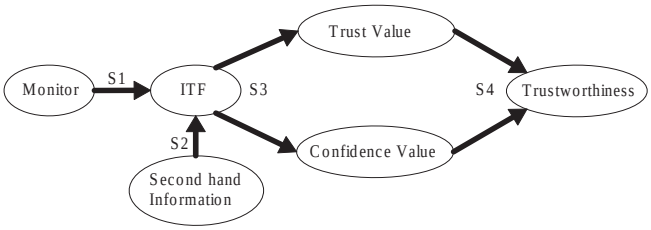

Fig. 3. Proposed neutral trust management framework

Step S1: Update ITF through Direct Information. Node in the network monitors the behavior of its neighbors using watchdog mechanism [10].

Step S2: Distribute and process second-hand information. This is the trust propagation procedure described in Fig. 2. In this step, the second-hand information can be formed periodically between neighbors and then used by other nodes to achieve fairness as shown in Fig. 2 for all nodes. That is, the direct observations obtained by one node k about a neighboring node, node j, can be used by another node i as second-hand information about the behaviors of node j. We say node k's direct observations about node j are second-hand information. After the formation of second-hand information, it will be flooded in the network. Due to the watchdog mechanism, the behaviors (of node j) observed by any two neighbors of node j will never overlap each other. That is, if both node k and i are the neighbors of node j. The behaviors covered by the direct observations of node k on node j and the observations of node i on node j will not overlap each other.

Step S3: Evaluate trust and *confidence value* evaluation. This is part of trust calculation procedure illustrated in Fig. 2. To achieve objectiveness as shown in Fig. 2, one node forms the elementary opinion for another node, which consists of two parameters: *trust value* and *confidence value*, based on ITF obtained through steps S1 and S2. The former parameter corresponds to the subject's estimate of the object's trust for a specific action based on the ITF. A high *trust value* means that the subject node trusts that the object node can perform an action well, such as forwarding packets, issuing certificates. On the other hand, the *confidence value* means the accuracy of the calculated *trust value*. A high *confidence value* represents that the object node has passed a large number of tests which have been given by the subject and other nodes in the network. Obviously opinions

with a high confidence are more useful in making decisions. Therefore, the *confidence value* is also referred to as the quality of the opinion.

Step S4: Evaluate *trustworthiness*. This is also part of trust calculation procedure shown in Fig. 2. Since two parameters are difficult for opinion comparison [13], two parameters formed in S3 by one node are combined into a whole opinion, *trustworthiness*, to another node.

B. ITF Update through Direct Information

This is the first step for the proposed framework. At this step, the ITF is firstly initialized as $(1, 1)$. Then each node in the network observes the behaviors of its neighboring nodes, and update the ITF in succession.

When an observation for j is obtained by i, the ITF should be updated. Let $s \in \{0, 1\}$ be the set of symbols for observations. That is, if the observation is normal behavior, $s = 1$; otherwise $s = 0$. In this situation, the ITF should be updated as follows:

$$\begin{aligned} \alpha_{ij} &= w_1^{CT-t_{last}} * (\alpha_{ij} - 1) + 1 + s \\ \beta_{ij} &= w_1^{CT-t_{last}} * (\beta_{ij} - 1) + 1 + 1 - s \\ (0 &\leq w_1 \leq 1) \end{aligned} \quad (2)$$

where w_1 is a discount factor between 0 and 1, CT is current time, and t_{last} is the time point that last update was performed. $w_1^{CT-t_{last}}$ is the factor to expire old observations exponentially. In equation (2), we use $\alpha_{ij} - 1$ and $\beta_{ij} - 1$, because they are the actual number of observations on the behaviors and the minimum value for both α_{ij} and β_{ij} is 1. Here we utilize memoryless characteristic for exponential distribution. That is, at any time point, the influence of the observations will decrease exponentially at the same speed. It shows the fairness from time aspect, since the nodes' past status cannot represent its current status and the past is given up at the same speed.

At the same time, to achieve fairness from space aspect besides time aspect as described above, second-hand information is shared between different nodes. It is obtained every period T. One piece of this information only represents the observation information during one period. At the beginning of every period, second-hand information, S_{kj}, is initialized as $(0, 0)$, because this information only needs to express the number of observations. If node k obtains an observation for j, the S_{kj} should be updated. Here also let $s \in \{0, 1\}$ be the set of symbols for observations. That is, if the observation is normal behavior, $s = 1$; otherwise $s = 0$. The S_{kj} should be updated as follows:

$$\begin{aligned} \alpha_{kj} &= w_1^{CT-t_{last}} * \alpha_{kj} + s \\ \beta_{kj} &= w_1^{CT-t_{last}} * \beta_{kj} + 1 - s \qquad (0 \leq w_1 \leq 1) \end{aligned} \quad (3)$$

The second-hand information will be reset every period, T. When one period T reaches, it will be kept as a record for second-hand information. At the same time, the S_{kj} will be reset to (0, 0).

C. Second-hand Information Distribution and Processing

After the formation of second-hand information, it should be distributed and processed by other nodes throughout the network to achieve fairness from space aspect. Here we provide the detailed method for second-hand information distribution and processing.

As described in the previous subsection, a node forms the second-hand information every period T. Here how to select T is a problem. T should be larger than the time needed to flood the message in the whole network. That is, if the time that a message can reaches every node in the network is estimated to be ET, it is necessary to set $T >= ET$. This mechanism is to make publishing message not so frequent that each node is busy for receiving this kind of information. On the other hand, because T is larger than ET, a node must have a record of another node when they want to establish trust relation between them.

The formed second-hand information should be flooded throughout the network. We consider the situation that a node receives a published second-hand information. The algorithm it will perform is provided as below.

$Algorithm:$
$if(it\ has\ not\ been\ received\ before)$
$\{receive\ this\ information$
$\quad update\ ITF;$
$\quad distribute\ such\ message\ to\ its\ neighbors.$
$\}$
$\}else\{$
$drop\ the\ message.$
$\}$

In the above algorithm, the node firstly should check whether it has received this information before when receiving a piece of second-hand information. If it has, only drop this information. Otherwise, it will receive this information, update ITF, and then distribute this message to its neighboring nodes.

D. Trust and Confidence Value Evaluation

In proposed framework, elementary opinion from the subject node, node i, to the object node, node j, is composed of *trust value* and *confidence value*. To achieve objectiveness as shown in Fig. 2, here both trust value and confidence value have been included into the trust calculation procedure. The definitions for them are similar to [13]. *Trust value* is to specify the trust estimation of node i to node j. *Confidence value* is to describe the accuracy of the evaluated *trust value*. The simple trust value cannot reflect the accuracy of the formed trust, which shows its subjectiveness. In the reputation-based frameworks, confidence value has not been included into opinion formation. Some notations are defined as follows.

- $t\{i : j, action\}$: *Trust value* that node i puts on node j for a specific action $action$. It has the property $0 \leq t\{i : j, action\} \leq 1$.

- $\sigma\{i : j, action\}$: Standard deviation of *trust value* from node i to node j on a specific action $action$.
- $c\{i : j, action\}$: *Confidence value* of *trust value* from node i to node j on a specific action $action$. It also has the property $0 \leq c\{i : j, action\} \leq 1$

Here we investigate calculation method for these parameters. Since the relation between the characteristic of Beta function and the trust is clarified in the first part of this Section, the *trust value* can be calculated as the expectation value of $beta(\theta, \alpha, \beta)$, which is the Dirac of Beta distribution.

$$t\{i : j, action\} = E(Beta(\theta, \alpha, \beta)) = \frac{\alpha}{\alpha + \beta} \tag{4}$$

Here if $t\{i : j, action\}$ approaches to 1, it means that node i trusts node j to perform the action $action$. On the contrary, if $t\{i : j, action\}$ approaches to 0, it means that node i distrusts node j to perform the action $action$.

The other important parameter, $c\{i : j, action\}$, is used for characterizing the statistical reliability of the computed $t\{i : j, action\}$. It is a value between 0 and 1. Similarly to [13], $\sigma\{i : j, action\}$ and $c\{i : j, action\}$ are calculated as formula (5) and (6), respectively.

$$\begin{aligned} \sigma\{i : j, action\} &= \sigma(Beta(\theta, \alpha, \beta)) \\ &= \sqrt{\frac{\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)}} \end{aligned} \tag{5}$$

$$\begin{aligned} c\{i : j, action\} &= 1 - \sqrt{12}\sigma(Beta(\theta, \alpha, \beta)) \\ &= 1 - \sqrt{\frac{12\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)}} \end{aligned} \tag{6}$$

Here if $c\{i : j, action\}$ approaches to 1, it means that the evaluated *trust value* from node i to node j on the action $action$ is believable because enough observations on behaviors have been collected. On the contrary, if $c\{i : j, action\}$ approaches to 0, it means that the evaluated *trust value* is untrustworthy because of the lack of observation collection.

Here, both trust value and confidence value have been considered into trust formation, which show the objectiveness of our proposed framework.

E. Trustworthiness Evaluation

In previous subsection, node i obtains the elementary opinion for node j as a pair of parameters (t, c). But having two parameters is difficult for opinion comparison as indicated in [12]. In this subsection, we combine such two parameters into one parameter, *trustworthiness*, which can be utilized to judge whether a node is a good guy or not more easily . We use $T\{i : j, action\}$ to represent the *trustworthiness* from node i to node j on a specific action $action$ as described in Section 2.A. Similarly to [13], the obtained $T\{i : j, action\}$ has the following properties.

- $0 \leq T\{i : j, action\} \leq 1$.
- $T\{i : j, action\}$ is induced from $t\{i : j, action\}$ and $c\{i : j, action\}$, but there are some rules for the calculation. Given a pair of *trust value* and *confidence value*, if the *confidence value* is high, *trust value* plays more important role for the *trustworthiness* formation. Thus under this situation, $t\{i : j, action\}$, should be put larger weight than *confidence value* $c\{i : j, action\}$. On the contrary, if the *confidence value* is low, obviously the *confidence value* is more important than *trust value* when forming the opinion. Therefore, $t\{i : j, action\}$, should be put less weight than *confidence value* $c\{i : j, action\}$.

Similarly to [13], the value of *trustworthiness* can be defined as

$$T\{i : j, action\} = 1 - \frac{\sqrt{\frac{(t-1)^2}{x^2} + \frac{(c-1)^2}{y^2}}}{\sqrt{\frac{1}{x^2} + \frac{1}{y^2}}} \tag{7}$$

where t denotes $t\{i : j, action\}$, c represents $c\{i : j, action\}$, x and y are constants. The research in [13] shows that the most appropriate values for the *trustworthiness* parameters are $x = \sqrt{2}$ and $y = \sqrt{9}$. Therefore, in this paper, we also set x be $\sqrt{2}$ and y be $\sqrt{9}$.

F. Fuzzy Decision Making

To show the variegation of the formed trustworthiness, we classified the calculated trustworthiness into several trust levels when performing decision making as in Table I. In contrast with [13], a threshold is used to determine whether a node is good or bad, which is not reasonable especially under the complex environment. In many comprehensive scenarios, trust cannot be determined very exactly, since multi-dimensional trust exists. Under such case, it is necessary to introduce fuzzy decision making to achieve variegation characteristics of neutrality shown in Fig. 2. As in Table I, the nodes holding trustworthiness between 0.4 and 0.6 is at trust level 3, which is not determined as simply good or bad.

TABLE I
TRUST LEVELS

Trust Level	Trustworthiness
5	$0.8 \leq T \leq 1$
4	$0.6 \leq T < 0.8$
3	$0.4 \leq T < 0.6$
2	$0.2 \leq T < 0.4$
1	$0 \leq T < 0.2$

VI. PERFORMANCE EVALUATION

Here, we investigate one kind of attack performed by free-rider, location-dependent attack. By this attack, when the free-rider has no packet to send, it will move to one location and is not willing to forward packets for other nodes. However, when it has many packets to send, it will move to another location and perform normal behaviors, which make it be able to gain good opinion in this new environment. Thus all the neighboring nodes in this new location are willing to forward packets for this free-rider. This free-rider contributes less to network and get much more from network.

To the whole network, the resource consumed should equal to the resource provided by all the nodes in the system. If some nodes contribute less to the system and get more from the network, the additive resource obtained by it should be provided by other nodes. It is obviously not neutral for the nodes that contribute more and get little. The reason that this attack can be effective is because the behaviors at one location cannot influence the opinion formation at another location.

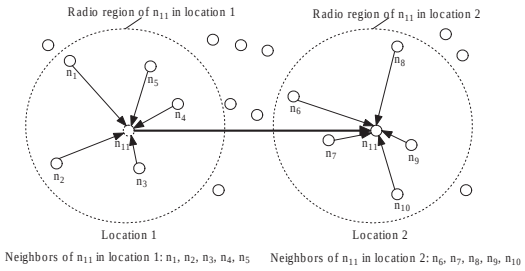

Fig. 4. Location-dependent attack

An example for location-dependent attack is given in Fig. 4. In this Figure, n_{11} is assumed to be an free-rider. At location 1, n_{11} forwards the packets from all the neighbors with high drop ratio 90%. But when it is desired to send some packets, it moves to location 2, where it forwards the packets for these new neighbors with drop ratio 10%. Here the opinion from nodes $n_6, n_7, n_8, n_9, n_{10}$ to n_{11} have not been influenced by the misbehavior information at location 1.

Here, we investigate how trustworthiness value changes with the drop ratio of the free-rider in location 1. It is assumed that the drop ratio of n_{11} to the packets for forwarding at location 1 ranges from 10% to 90%. But n_{11} forwards packets at location 2 with drop ratio 10%. Then we can obtain the results as in Fig. 5. From Fig. 5, we can see that there are much difference on the opinions to n_{11} between nodes at location 1 and nodes at location 2 by trust establishment framework. However, by the proposed framework or reputation-based framework, nodes at location 1 and location 2 can hold the same opinion, since the proposed framework and reputation-based framework hold fairness characteristic. Thus, the location-dependent attack can be inhibited by them, and the neutrality has been achieved by the proposed framework under the attack from free-rider.

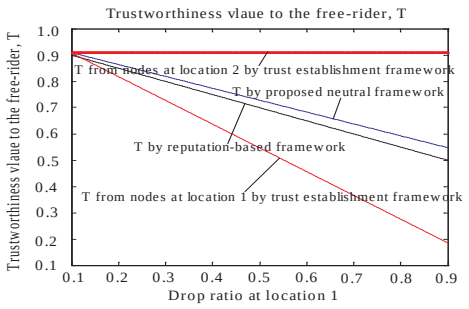

Fig. 5. Trustworthiness Vs drop ratio at place 1

VII. Conclusions

To inhibit the free-rider problem in unstructured network and guarantee the neutrality of the network at the same time, a neutral trust management framework is required. To march towards such a neutral framework, we clarify the relation between neutrality and trust definition, and make clear the design requirements for it. Then we take one of typical unstructured network, MANETs, as example, and design a neutral trust management framework on a MANET. In the proposed framework, three aspects of neutrality, objectiveness, fairness and variegation have been included into the design. Meanwhile, performance analysis have been performed under location-dependent attack performed by free-rider, which shows the neutrality of the proposed framework.

In the future, we will incorporate privacy preserving issue into the proposed framework and generalize the proposed framework from trust definition.

References

[1] S. Buchegger, and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," *Proceedings of ACM MobiHoc 2002*, Sept. 2002, Atlanta, USA.

[2] S. Buchegger, and J.-Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-Hoc Networks," *Proceedings of P2PEcon 2004*, Harvard University, Cambridge MA, USA, June 2004.

[3] J. Crowcroft, "Net neutrality: the technical side of the debate: a white paper", ACM Computer Communication Review, 2007.

[4] A. Davison, "Statistical Models," *Cambridge University Press, Cambridge Series in Statistical and Probabilistic Mathematics*, June 2003.

[5] S. Ganeriwal and M. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004)*, Washington, D.C., USA, Oct. 25, 2004.

[6] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications", IEEE Communications Surveys and Tutorials, Fourth Quarter 2000.

[7] A. Jϕsang, and R. Ismail, "The Beta Reputation System," *Proceedings of the 15th Bled Conference on Electronic Commerce*, Bled, Slovenia, 17-19 June 2002.

[8] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," *Proceedings of 12th International World Wide Web Conferences*, May 2003.

[9] R. Li, J. Li, P. Liu, and H.-H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," 2007 IEEE 65th Vehicular Technology Conference VTC 2007 Spring (IEEE VTC 2007 Spring), pp. 56-60, 23 - 25 April 2007.

[10] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proceedings of MobiCom 2000*, Aug. 2000, pp. 255-265.

[11] Y. Sun, Z. Han, W. Yu and K. J. Ray Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks," *Proceedings of the IEEE Infocom 2006*, Apr. 2006, Barcelona, Spain.

[12] G. Theodorakopoulos, and S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," *IEEE Journal on Selected areas in Communications*, Special Issue on Security in Wireless Ad-Hoc Networks, Feb. 2006.

[13] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs," *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005)*, Alexandria, VA, USA, November 7, 2005.

[14] G. Theodorakopoulos and J. S. Baras, "Malicious Users in Unstructured Networks," *MIT Press*, 1995.

[15] X. Yang, G. Tsudik, X. Liu, "A Technical Approach to Net Neutrality", Fifth Workshop on Hot Topics in Networks (ACM HotNets-V), Irvine, 2006.