A Novel Recommendation-Based Trust Inference Model for MANETs

Hui Xia(✉), Benxia Li, Sanshun Zhang, Shiwen Wang, and Xiangguo Cheng

College of Computer Science and Technology, Qingdao University, Qingdao 266071, People's Republic of China
xiahui@qdu.edu.cn

Abstract. Over the last few years, trust, security, and privacy in mobile ad hoc networks have received increasing attention. The proposed trust-based countermeasures are considered to be promising approaches, which play an important role for reliable data transmission, qualified services with context-awareness, and information security. The foundation of these countermeasures is trust computation. In order to address this issue, we first study trust properties, and subsequently abstract a novel recommendation-based trust inference model. Two trust attributes called the subjective trust and the recommendation trust, are selected to quantify the trust level of a specific entity. Recommendations provide an effective way to build trust relationship, by making use of the information from others rather than exclusively relying on one's own direct observation. To compute the subjective trust and the recommendation trust precisely, some comprehensive factors are introduced. Furthermore, the concept of belief factor is proposed to integrate these two trust attributes. The aim of this trust model is, the network can itself detect, prevent and exclude the misbehaving entities, and obtain strong resistibility to malicious attacks as well. The effectiveness and resistibility of the model are analyzed theoretically and evaluated experimentally. The experimental results show that this new mechanism outperforms existing mechanisms.

Keywords: Mobile ad hoc networks · Trust-based countermeasure
Trust computation · Trust inference model · Recommendation trust
Belief factor

1 Introduction

A mobile ad hoc network can be seen as an implementation of the perception layer, which is at the most front-end of information collection and plays a fundamental role in the internet of things (IoT). This type of network can offer a high quality of service, and a high level of flexibility for data perception, collection, transmission, process, analysis and utilization. The recent proliferation of mobile entities (e.g. mobile phones) has given rise to numerous applications. Various data collected by underlying mobile entities can be further processed, mined and analyzed for the sake of multifarious promising services with intelligence. As we become increasingly reliant on intelligent and interconnected devices in every aspect of our lives, critical security issues involved

S. Chellappan et al. (Eds.): WASA 2018, LNCS 10874, pp. 893–906, 2018.
https://doi.org/10.1007/978-3-319-94268-1_82

in this type of wireless network are raised as well, and remain serious impediments to widespread adoption. In recent years, trust, security and privacy in mobile ad hoc networks have received increasing attention [1]. The existence of malicious entities can make a seriously damage on the availability and correctness of network services. In order to address the abovementioned problem, several security extensions and detection systems have been proposed in the literature to counter various types of malicious attacks [2, 3].

Cryptography-based solutions (PKI) is based on a centralized server [3], while have clear deficiencies: (*a*) these solutions cannot recognize the malicious entities since they all have been authorized identities, thus are vulnerable to suffer from DoS/DDoS attacks, internal attacks, privacy breach and impersonation attacks; (*b*) most cryptographic operations consume a significant amount of bandwidth, and cause a high network overhead to be incurred, and are therefore not suitable for resource-constrained networks. In contrast, trust-based countermeasures are considered to be more acceptable as promising approaches [4, 5], which play an important role for reliable data transmission and fusion, qualified services with context-awareness and information security. For instance, these countermeasures have been widely used to neutralize packet dropping attack, exclude misbehaving entities from the network and guarantee security interactions between entities.

The trust computation is the foundation of those countermeasures, which plays an important role to initialize a trusted network system (e.g. the network can itself detect, prevent and exclude the misbehaving nodes [6, 7], and obtain strong resistibility to attacks as well [8, 9]). And the feedback of trust information can be applied to traditional network services with unique security assurances at different levels [10]. The trust mechanism can help entities overcome perceptions of uncertainty and risk in consumption on network services and security applications (e.g. routing function) [11, 12]. However, the computational model is often very complicated. And the selection rules of the trust decision attributes and the calculation methods of weights have not been solved effectively. Moreover, most of these proposed models have poorly capability to resist various types of attacks. The basis of some countermeasures may be exploited to fulfill new attacks. As mentioned above, how to design an effective and efficient trust-based framework is a challenging task in such networks.

We therefore focus in this paper on the design of trust inference model. We first study trust properties, and subsequently propose a novel recommendation-based trust inference model to achieve the trust computing problem, where two trust attributes called the subjective trust and the recommendation trust, are selected to quantify the trust level of a mobile entity. The trust information can be used to classify entities as honesty or malevolence.

The remainder of this paper is organized as follows. Section 2 discusses recent works in the literature. In Sect. 3, we describe in detail a trust inference model. Section 4 presents the experimental results and analysis of the performance of this new trust model. Finally, Sect. 5 presents concluding remarks with possible extensions and directions for future research.

2 Related Works

A detailed survey of various trust computing approaches was presented in [4]. According to this survey, distributed trust computations can be classified as neighbor sensing, recommendation-based trust, and hybrid methods (based on direct experience and recommendations from other nodes). Movahedi et al. [5] presented a holistic view on various trust management frameworks geared for MANETs. Besides, they proposed taxonomy for the main identified trust-distortion attacks and they provided a holistic classification of the main evaluation metrics.

Shen and Li [6] presented a hierarchical account-aided reputation management system to effectively provide cooperation incentives. A hierarchical locality-aware distributed hash table infrastructure is employed to globally collect all node reputation information in the system, which is used to calculate more accurate reputations and to detect abnormal reputation information. To complement the insufficiency of identity authentications, Chen et al. [7] presented a novel trust management scheme based on the information from behavior feedback. The successors generate verified feedback packets for each positive behavior and, consequently, the 'behavior-trust' relationship is formed for slow-moving nodes. Shabut et al. [8] proposed a recommendation-based trust model with a defense scheme, which utilized the clustering technique to dynamically filter out attacks related to dishonest recommendations between certain times based on the number of interactions, the compatibility of information and the distance between nodes.

Due to the characteristics of a group communication system (e.g. the existence of selfish nodes and high survival time requirements), Cho and Chen [9] summarised a detailed analysis of trust management for this system. Barnwal and Ghosh [10] proposed an efficient trust estimation scheme to detect the errant/malicious nodes that disseminate incorrect kinematics information to vehicular cyber-physical systems. An attack-resistant trust management scheme was proposed for VANETs in [11], which was not only able to detect and cope with malicious attacks, but it also evaluated the trustworthiness of both data and mobile nodes. Specially, node trust is assessed in two dimensions, i.e. functional trust and recommendation trust.

To secure the data plane of ad-hoc networks, Tan et al. [12] proposed a novel trust management system. In this system, fuzzy logic was employed to formulate imprecise empirical knowledge, which was used to evaluate the path trust value. Together with fuzzy logic, graph theory was adopted to build a novel trust model for calculating the node trust value. Chen and Wang [13] demonstrated a layered trust management model based on a vehicular cloud system. This model could benefit from the efficient use of physical resources (e.g. computing, storage and communication costs) and the exploration of its deployment in a vehicular social network scenario based on a three-layer cloud computing architecture.

Yao et al. [14] proposed the concept of incorporating social trust in the routing decision process and the design of a trust routing protocol based on the social similarity (TRSS) scheme. TRSS is based on the observation that nodes move around and contact each other according to their common interests or social similarities. Based on direct and recommended trust, those untrustworthy nodes will be detected and purged from

the trusted list. Because only trusted node packets will be forwarded, the selfish nodes have incentives to behave well again.

However, there are some problems with the abovementioned trust mechanisms in mobile ad hoc environments, such as the selection of trust attributes, the calculation of their weights and lack of direct interaction experience. Besides, the quality of recommended information is not guaranteed. Moreover, they are weak resistibility to various types of malicious attacks.

3 Trust Inference Model

The concept of trust has appeared in many academic works and can be used to achieve certain missions and system goals. Yan and Wang [15] utilized two dimensions of trust levels to control data access to pervasive social networks in a heterogeneous manner using attribute-based encryption. The trust levels can be evaluated either by a trusted server or by individual entities or by using them both.

3.1 Concept of Trust

In accordance with prior related studies, 'trust' helps humans overcome perceptions of uncertainty and risk when engaging in social activities and sharing social resources. But what is 'trust'? How should one describe and quantify it? Trust is a very complicated concept that relates to the confidence, belief, reliability, honesty, integrity, security, dependability, ability and other characters. According to the method for establishing trust relationships in a human society, building trust relationships in mobile ad hoc networks has a similar process. Therefore, it is a challenging issue to model, manage and maintain trust. For a specific network environment, a high level of trust for a service provider denotes that this provider does not only follow the willingness of a requesting entity, but it also effectively provides a mutually agreed upon service (e.g. to transmit information efficiently).

The concept of trust involves two kinds of participants (i.e. trustor that giving the evaluation and trustee that being evaluated), and the policies are designed by the trustor in the decision-making process.

3.2 Overall Design of Trust Model

In the variety of trust management trust models, the recommendation-based method accounts for a large percentage, which is a common evaluating criterion based on the recommended experiences from reliable recommenders. In order to gain the trust of a specific entity, the two most important steps are: the selection and the synthesis of trust attributes.

We abstract a novel trust inference model to mobile ad hoc networks, where two attributes, called subjective trust (ST) and recommendation trust (RT), are selected to quantify the trust level for a specific entity. The subjective trust of the trustee relative to the trustor is calculated based on the evaluation of historical interactions between them, whereas the recommendation trust of the trustee is computed based on all referenced

reliable evaluations from neighbors in numerous interactions. Recommendations provide an effective way to build trust relationship, by making use of the information from others rather than exclusively relying on one's ow direct observation. The aim of this trust model is that the network can detect, prevent and exclude the misbehaving nodes and it can establish a trusted network system.

3.3 Synthesis of Trust

In the trust system of human society, after each interaction, both participants will make an evaluation for this interaction to the other. A lower interaction evaluation (*IE*) makes decrement in the trust level and vice versa. Two basic factors, called the interaction period and the interaction amount, are introduced to estimate the quality of an evaluation for a specific interaction.

Interaction Period (*IP*): The attenuation of trust is well known. The researches based on economic theory show that, when calculating the rating of an object, the evaluations of historical interactions should be properly attenuated. Using a similar way used by human societies, the evaluations for the recent interactions are more credible, and should be given greater weights on the synthesis of multiple evaluations. In order to achieve this purpose, we will introduce a proper time attenuation function.

Interaction Amount (*IA*): Similar to the vector *IP*, the interaction amount is another noteworthy vector. A larger scale interaction makes a bigger impact on the trust evaluation and reflects an entity's performance more exactly, which should also be given a greater weight for the synthesis of multiple evaluations. A trustor will pay more attention to a larger scale interaction in the future.

In a mobile ad hoc network, the metric TV_{ij} represents the trust value of a specific node j from the perspective of an evaluating node i. This metric can be calculated via synthesizing the abovementioned trust attributes using the following equation:

$$TV_{ij} = \alpha ST_{ij} + \beta RT_{ij} \tag{1}$$

where ST_{ij} and RT_{ij} represent the subjective trust and the recommendation trust levels for node j as derived from node i. The weights α and β ($\alpha, \beta \geq 0$, $\alpha > \beta$ and $\alpha + = 1$) are called confidence factors. In general, subjective trust should be given a greater weight unless there are rarely interactions between two sides. The detailed calculation process will be shown in the following Subsect. 3.3.3.

3.3.1 Calculation of Subjective Trust

You can find that this trust attribute appears in all trust models. There is variety of evaluation methods (e.g. a statistical approach) to characterize this attribute from different aspects. However, the most central part is still the subjective measure of trustee's historical behaviors using mathematical methods.

To simplify the discussion and implementation, we establish a simple inference method. Assume that there are n-th number of interactions between couple of nodes, i.e. node i and node j. And IE_k, IP_k and IA_k, ($\forall k(1 \leq k \leq n)$) represent the interaction evaluation, the interaction period and the interaction amount of the k-th interaction,

respectively. Then we put forward a quality model to synthesize the abovementioned interaction factors.

$\forall k(1 \leq k \leq n)$, ST_{ij}^{k} can be calculated by using (2):

$$\begin{cases} ST_{ij}^{0} = Threshold, & if\ k = 0 \\ ST_{ij}^{k} = \sum_{m=1}^{k} W_m IE_m, & if\ 1 \leq k \leq n \end{cases} \tag{2}$$

where ST_{ij}^{k} represents the subjective trust for node j, which can be derived from node i after the k-th interaction and W_m represents the weight of IE_m. As shown in Eq. (2), the final subjective trust is a weighted average value of all the interaction evaluations that occurred during different interaction periods. We set a value interval for the variables, IE_m and ST_{ij}^{k} (i.e. $0 \leq IE_k, ST_{ij}^{k} \leq 1$). At the beginning of an experimental simulation, we initially set the subjective trust value to 0.5 (i.e. the threshold value).

The two factors (i.e. *IP* and *IA*) are involved into calculating the weight W_m. A rational solution is carried out using the following equation:

$$W_m = \frac{\rho_{m,k} IA_m}{\sum_{m=1}^{k} \rho_{m,k} IA_m} \tag{3}$$

where $\rho_{m,k}$ represents the time attenuation function. An effective attenuation approach could be used to accelerate the convergence rate of a computing process and to guarantee that this process reaches a stable state. To effectively calculate the subjective trust, the recent interaction should be given a bigger weight. In other words, the value of the attenuation function increases as the interaction period becomes closer to the recent time, i.e. $\sum_{1 \leq m \leq k, m=1}^{k} \rho_{m,k} = 1$ and $\rho_{1,k} < \rho_{2,k} < \ldots < \rho_{k,k}$.

To address the above issues, we introduce a simple model that considers the interaction period through the following equation:

$$\rho_{m,k} = \frac{T_m}{\sum_{m=1}^{k} T_m} \tag{4}$$

where T_m denotes the beginning time of the m-th interaction period.

Then, Eq. (3) can be transformed via Eq. (4). We can obtain two conclusions: (*a*) if the interaction amount for a specific interaction period is small, then it is difficult to obtain a high weight is obtained for this interaction evaluation in the calculation of subjective trust. The benefit of this new approach is that this design could prevent a dishonest node from cheating in a future large interaction if it has obtained a high trust level based on a number of small, honest interactions; (*b*) compared to the historical interactions, the evaluation of the latest interaction is more important and credible. In other words, the calculation of subjective trust is more likely to reflect the recent behaviors of a specific node.

3.3.2 Calculation of Recommendation Trust

If a node wants to interact with another node in an unfamiliar environment, it should first estimate a trust level for this other node. The calculation of trust should rely on the experience-based recommendations from all the referenced and reliable third parties. Even there are direct interactions between a pair of nodes; the trust estimation should also consider the reliable recommendations to overcome the subjectivity. In other words, an effective trust mechanism should use trusted neighbors to scout the behaviors of a specific node. Due to a large number of false recommendations and dishonest recommendations derived from variety of malicious attacks, like ballot stuffing, bad mouthing, conflict and collusion, how to establish a recommendation-based trust model is a challenging issue in such a network.

Each physical neighbor of a specific node can obtain a subjective trust of this node, and the credibility of recommended information derived from such neighbors will directly affect the accuracy of the composition of the recommendation trust. The computational method is based on the following intuitive ideas:

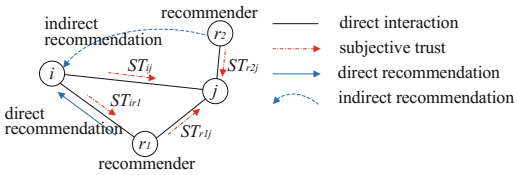

Fig. 1. Calculation of recommendation trust

As shown in Fig. 1, it is assumed that, after k-th interaction between node i and node j, node i can will calculate a value of subjective trust ST_{ij}^{k} for node j based on the ST model. Nodes r_1 and r_2 are two types of neighboring nodes that have previous interactions with node j and their historical evaluations of subjective trust for node j are $ST_{r_1j}^{n}$ and $ST_{r_2j}^{m}$ respectively.

Based on the conditions of the recommender(s) (i.e. whether there are previous interactions with the monitored node), the recommended experience can be divided into directly recommended experience d_RE_{ij} and indirectly recommended experience in_RE_{ij}.

This concept of credibility factor reflects the credibility of the recommended experience given by a recommender. Two computational approaches are presented to estimate the credibility factor of these two different types of recommended experiences, respectively. Moreover, we set a recommended threshold value d, which makes this recommendation mechanism more reasonable.

Directly Recommended Experience

If the recommender has historical interactions with the monitoring node, according to the transferable property of trust, this monitor can use recommended experience directly.

The value of the directly recommended experience for node j is an average of recommended experiences provided by multiple recommenders (e.g. node r_1 as shown in Fig. 1.). This operation is carried out using the following equation:

$$d\_RE_{ij} = \sum_{l=1}^{n} \left(\frac{ST_{ir_l}}{\sum_{l=1}^{n} ST_{ir_l}} \times ST_{r_l j} \right) \tag{5}$$

Indirectly Recommended Experience

If the recommender has no historical interactions with the monitor, while they have a common set of evaluated nodes, then this monitor can still effectively use recommended experience.

It is assumed that a monitor node i and a recommender node r have a consistent view if they have a higher similarity rating on a public node set (denoted by $Set(i, r)$). The deviation of their trust evaluation about a public node set is defined using the following equation:

$$Diff_{ir} = \frac{\sum_{k \in Set(i,r)} |ST_{ik} - ST_{rk}|}{|Set(i,r)|} \tag{6}$$

where $|Set(i,r)|$ represents the number of public node sets. The credibility of this type of recommended experience can be obtained as $CR_{ir} = 1 - Diff_{ir}$. The value of this variable also needs to satisfy the recommended threshold for the synthesizing operation. Then, we can obtain the following equation:

$$in\_RE_{ij} = \sum_{s=1}^{m} \left(\frac{CR_{ir_s}}{\sum_{s=1}^{n} CR_{ir_s}} \times ST_{r_s j} \right) \tag{7}$$

The concept of the recommended threshold can be used to counter slander attacks from malicious nodes. Furthermore, the interaction amount (IA) between a recommender and a specific node makes a great impact on the estimation of recommendation trust. A larger interaction amount results in a more credible recommendation. The IA can be considered as another weighting factor and is used to optimize the calculation of recommendation trust. Equations (5) and (7) can therefore be derived into the following equations:

$$d\_RE_{ij} = \sum_{l=1}^{n} \left(\frac{ST_{ir_l} \times IA_{r_l j}}{\sum_{l=1}^{n} ST_{ir_l} \times IA_{r_l j}} \times ST_{r_l j} \right) \tag{8}$$

$$in\_RE_{ij} = \sum_{s=1}^{m} \left(\frac{CR_{ir_s} \times IA_{r_s j}}{\sum_{s=1}^{m} CR_{ir_s} \times IA_{r_s j}} \times ST_{r_s j} \right) \tag{9}$$

Such assignments and the abovementioned recommended credibility mechanism can effectively prevent malicious nodes from providing false recommended experience, which is used to raise or decrease the trust level for a specific node.

Finally, we can calculate the recommendation trust for a specific node from the monitor's point of view using the following equation:

$$RT_{ij} = \omega_1 d\_RE_{ij} + \omega_2 in\_RE_{ij} (\omega_1 + \omega_2 = 1) \tag{10}$$

where ω_1 and ω_2 are the weighting factors for the two types of recommended experiences.

$$\omega_1 = \frac{\sum_{l=1}^{n} IA_{rij}}{\sum_{l=1}^{n} IA_{rij} + \sum_{s=1}^{m} IA_{rsj}} \quad \omega_2 = \frac{\sum_{s=1}^{m} IA_{rsj}}{\sum_{l=1}^{n} IA_{rij} + \sum_{s=1}^{m} IA_{rsj}} \tag{11}$$

Besides, we find a phenomenon that, the number of recommenders is also an important factor for calculating the recommended trust on the basis of a variety of researches. A larger number of recommenders yielded a more accurate recommended experience. We can design a function $\phi(x)$ that considers the number of recommenders as follows:

$$\phi(n+m) = e^{-1/(n+m)}, \lim_{n\to\infty} \phi(n+m) = 1 \tag{12}$$

where $(n + m)$ represents the number of recommenders. Without considering the abovementioned factor, multiple malicious nodes can easily raise each other's trust through complicity. Therefore, this mechanism can be used to counter collision attacks from malicious nodes.

Then, Eq. (10) should be optimized and derived as follows:

$$RT_{ij} = \phi(n+m) \times (\omega_1 d\_RE_{ij} + \omega_2 in\_RE_{ij}) (\omega_1 + \omega_2 = 1) \tag{13}$$

It hints that if a node wants to raise its recommendation trust, it must deal with a large number of honest nodes.

3.3.3 Calculation of Confidence Factors α and β

The primary remaining problem in calculating the trust is how to legitimately calculate the confidence factors α and β. The process of calculating trust must consider the confidence level of the subjective trust and the recommendation trust.

In general, if a monitor is familiar with the behavioral performance of a specific node, then it is supposed to be more convinced with the calculation of subjective trust. On the contrary, if there are rarely interactions between them, then the synthesis of trust is supposed to mainly rely on the recommended experience.

Based on the abovementioned analysis and taking the influence of the interaction amount into consideration, a simplified approach based on game theory is proposed to determine the values of confidence factors α and β using the following equation:

$$\alpha = \frac{IA_{ij}}{IA_{ij} + \sum\limits_{p \in SetC} IA_{ip}} \quad \beta = \frac{\sum\limits_{p \in SetC} IA_{ip}}{IA_{ij} + \sum\limits_{p \in SetC} IA_{ip}} \tag{14}$$

SetC includes two types of nodes: (1) direct recommenders. In other words, for a specific interaction period, these nodes not only directly interact with a monitor i, but they also interact with a specific node j. (2) Set(i, r), which was discussed in Subsect. 3.3.2, for node r represents an indirect recommender.

3.4 Trust Table

Each node can calculate the trust values of its neighbours and establish a trust table to record and update this information as shown in Table 1.

Table 1. The trust table for a special node i

Neighbour ID(i)	TV	Property flag
k	0.92	0
m	0.73	0
j	0.23	1
…	…	…

The vector *TV* denotes a neighbor's trust value on the node i's point of view, and *Property Flag* indicates whether this neighbor is a malicious node or not. With the help of the trust model, if a particular node is detected as a malicious node by all its neighbors, then this node will be logically excluded from the local network and prevented from engaging in any activity with the local network (e.g. data forwarding).

4 Trust Model Performance

To verify the validity and accuracy of our trust mechanism, compared with the BFT [7], the RT [8], the Tan [12] and the TRSS [14], we have conducted a comprehensive test using NetLogo [16]. NetLogo is an agent-based programming language and integrated modeling environment, which can simulate the large-scale dynamic environment and interaction process between agents.

In this simulator, 200 agents were arranged, and a simulation time of 3000 steps was used for simulation scenario. Two types of behaviors were launched by agents (i.e. trustworthy behaviors and malicious behaviors). In trustworthy behaviors, a specific agent provides reliable service in an interaction. While in malicious behaviors, a specific agent provides untrustworthy service (i.e. launching various types of attacks). The dynamic environment contained 20% malicious agents and each malicious agent provided bad services (e.g. launched malicious behaviors) in the entire simulation time over a rate of 80% in the following experiments. Figure 2, 3, 4 and 5 show the simulation results during the simulation.

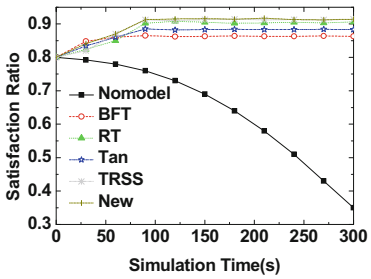

Fig. 2. Satisfaction ratios of network interaction

As shown in Fig. 2, the satisfaction ratios of network interaction perform as a function of the simulation time. The *x*-axis of this figure stands for the number of simulation steps. The satisfaction ratios for all trust models rise in the initial stage of simulation, after that, remain stable. While this ratio of no-model decreases gently in the entire simulation time. Trust models can take advantage of the trust concept, gradually detect malicious agents in the simulation process, and guarantee the interactions occurring only between the trustworthy agents. A longer the existing time of malicious node will lead a greater damage on the simulation environment. Our model has a better performance.

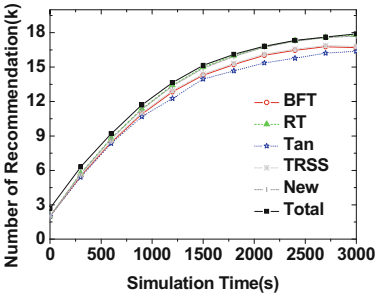

Fig. 3. Number of good recommended experience

Figure 3 illustrates the correction rate of the recommended experience, where *y*-axis is the number of the recommended experience. We can see that, with the increase of total number of recommended experience in network, the number of bad recommended experience is very small, and decreases as time passes. With the help of trust mechanisms, the network can identify its inherent malicious nodes. When calculating a specific node's trust level, the proportion of good recommended experience provided by malicious nodes will be neglected, and the malicious nodes will be slowly removed from the set of recommending nodes. Almost all the recommended experience is good recommended experience, so the plot representing the good recommended experience is almost coincident with the one representing the total recommended experience. Due to the effective and consummate recommendation trust evaluation rules in our new model, the performance outperforms existing mechanisms.

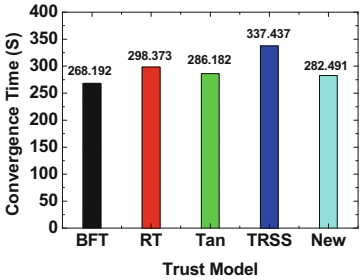

Fig. 4. Convergence time

Figure 4 shows the comparison of the convergence time of different trust models. Our new trust mechanism has a faster convergence time. The reason is that the new proposed mechanism adopts an iterative calculation method, and the update process of trust level is only related to the current trust information.

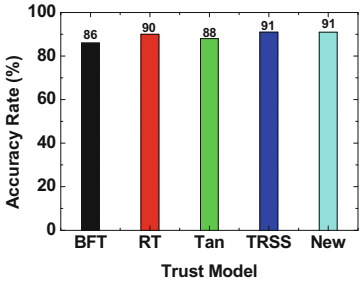

Fig. 5. Accuracy detection ratio of malicious agents

Figure 5 shows the comparison of the accuracy detection rate of malicious agents. The simulation environment can gradually identify its inherent malicious agents benefit from the trust mechanism. In the process of trust calculation, the proportion of recommendation experience provided by malicious agents will be neglected. These malicious agents will be slowly removed from the local network area. Due to the effective and consummate trust evaluation rules in our new trust model, its performance is better than the others.

5 Conclusions and Future Work

Unlike wired networks, which have a higher level of security for gateways and routers, mobile ad hoc networks are vulnerable to various attacks due to their inherent features. It is relatively easy for multiple malicious entities to bring down the whole network in several network services. Trust-based countermeasure is considered to be more

acceptable as a promising approach. Therefore, we carry out a detailed study of the various trust-based countermeasures and abstract a novel recommendation-based trust inference model which is used to establish a trusted network. Two trust attributes called the subjective trust and the recommendation trust, are selected to quantify the trust level of a specific entity. The subjective trust of a specific entity is calculated based on its historical behaviors, whereas the recommendation trust is computed based on all the reliable recommendations. The convincing experimental results show that our new model performs better than the other trust-based countermeasures.

In future work, we plan to conduct an in-depth study of trust-based strategies, taking into account the requirements for deployment area issues, network applications and security levels. Moreover, trust computations and management can be an attractive target for attackers, since major decisions can be taken based on these trust computations. A malicious node may behave well towards one group of nodes and badly towards another group; this is known as a conflicting behaviour attack. Hence, defence mechanisms are required that can ensure trusted information, confidentiality and integrity in order to enable and support the most secure routing decisions.

Acknowledgment. This work is sponsored by the Natural Science Foundation of China (NSFC) under Grant No. 61402245, the Project funded by China Postdoctoral Science Foundation under Grand No. 2015T80696 and 2014M551870, the Shandong Provincial Natural Science Foundation No. ZR2014FQ010, the Project of Shandong Province Higher Educational Science and Technology Program No. J16LN06, the Qingdao Postdoctoral Application Research Funded Project.

References

1. Sicari, S., Rizzardi, A., Grieco, L.A., et al.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
2. Liu, Y.X., Dong, M.X., Ota, K.: ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **11**(9), 2013–2027 (2016)
3. Yao, J.P., Feng, S.L., Zhou, X.Y.: Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying. IEEE Trans. Commun. **64**(2), 753–764 (2016)
4. Govindan, K., Mohapatra, P.: Trust computations and trust dynamics in mobile adhoc networks: a survey. IEEE Commun. Surv. Tutor. **14**(2), 279–298 (2012)
5. Movahedi, Z., Hosseini, Z., Bayan, F., Pujolle, G.: Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey. IEEE Commun. Surv. Tutor. **18**(2), 1287–1309 (2016)
6. Shen, H.Y., Li, Z.: A hierarchical account-aided reputation management system for MANETs. IEEE-ACM Trans. Netw. **23**(1), 70–84 (2015)
7. Chen, X., Sun, L., Ma, J.F., Ma, Z.: A trust management scheme based on behavior feedback for opportunistic networks. China Commun. **12**(4), 117–129 (2015)
8. Shabut, A.M., Dahal, K.P., Bista, S.K., Awan, I.U.: Recommendation based trust model with an effective defence scheme for MANETs. IEEE Trans. Mob. Comput. **14**(10), 2101–2115 (2015)
9. Cho, J., Chen, I.: On the tradeoff between altruism and selfishness in MANET trust management. Ad Hoc Netw. **11**(8), 2217–2234 (2013)

10. Barnwal, R.P., Ghosh, S.K.: KITE: an efficient scheme for trust estimation and detection of errant nodes in vehicular cyber-physical systems. Secur. Commun. Netw. **9**(16), 3271–3281 (2016)
11. Li, W.J., Song, H.B.: ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **17**(4), 960–969 (2016)
12. Tan, S.S., Li, X.P., Dong, Q.K.: A trust management system for securing data plane of ad-hoc networks. IEEE Trans. Veh. Technol. **65**(9), 7579–7592 (2016)
13. Chen, X., Wang, L.M.: A cloud-based trust management framework for vehicular social networks. IEEE Access **5**, 2967–2980 (2017)
14. Yao, L., Man, Y.M., Huang, Z., Deng, J., Wang, X.: Secure routing based on social similarity in opportunistic networks. IEEE Trans. Wirel. Commun. **15**(1), 594–605 (2016)
15. Yan, Z., Wang, M.J.: Protect pervasive social networking based on two-dimensional trust levels. IEEE Syst. J. **11**(1), 207–218 (2017)
16. Wilensky, U.: NetLogo (1999). http://ccl.northwestern.edu/netlogo/