Can Friendship Be Counted on for Securing Wireless Ad Hoc Networks?

Lianggui Liu, Huiling Jia and Ting Shu

*School of Information Science and Technology,
Zhejiang Sci-Tech University, Hangzhou, China, 310018
lgliu@zstu.edu.cn, wannahealthy@126.com, shuting@zstu.edu.cn*

Abstract

Trust system plays a more and more important role in giving nodes incentives to cooperate in packet forwarding especially for wireless ad hoc networks. However, most existing works in this field either lack rigorous analysis of cost of their methods or have analysis in unrealistic models, which will clearly damage their effectiveness in real applications. In a previous work, Theodorakopoulos and Baras [1] develop a novel formulation of trust computation based on ordered semirings. In this paper, based on their work we proposed FROST (FRiendship and Ordered Semirings based Trust system) for wireless ad hoc networks. FROST introduce notion of friendship to reduce the trust table size and overhead while building and maintaining the trust system in large scale networks. Moreover, FROST use a more effective decaying model to enable the trust system to be more adaptive to the changing environment. Rigorous analysis and in-depth simulation show FROST has a good performance and can quantitatively measure reputation and defend trust system against malicious attacks.

Keywords: *friendship model, wireless ad hoc networks, malicious attack, trust, security*

1. Introduction

In wireless ad hoc networks, nodes depend on mutual cooperation to set up end-to-end connections and forward others' packets. Trust system is crucial to provide incentives for them to cooperate [2]. At the present time, it becomes the foundation for some other security approaches, such as key management [3] and secure routing [4, 5]. However, trust system itself is vulnerable to attack and the reputation of entities in networks can be manipulated intentionally by malicious ones. Till now, people from both academic and industry societies have conducted extensively research on the field of trust in networks for a wide range of applications [6]. However, their works are especially vulnerable to several kinds of attacks that have recently been regarded as critical problems, which include bad mouthing, on-off, conflicting behavior [2]. Due to the intrinsic characters of wireless ad hoc networks, traditional security methods are inadequate or too complicated to protect such autonomous networks from misbehaving nodes such as selfish nodes and malicious nodes [2]. How to incorporate trust into wireless ad hoc networks and wireless sensor networks has recently gained a large amount of research attention [7-14]. In order to perform trust systems in wireless ad hoc networks successfully, three requirements, that is, network nodes should have relatively long lifetime, trust values should be distributed and history record of interactions between nodes should have impact on present decision, should be met [15]. Here, we use *trust* to represent one estimated value about a node's actual quality in terms of its behavior in wireless ad hoc networks. Sometimes it is also referred to as *reputation* [15].

2. Related Works

Trust systems are important tools used in many fields such as sociology, economics and computer science. It shows that the trust systems are useful mechanisms to address the threat of malicious entities. They identify selfish or malicious nodes and exclude these nodes from the network. Trust systems have been extensively studied in various internet interactions [15-17].

Trust and reputation management systems in wireless networks have gained much attention of researchers recently and most works in this area can be classified into two major categories: individual-level [1, 8, 17-20] and system-level [5, 9, 21]. Most approaches have some drawbacks, which include but not limited to: Firstly, for existing trust systems there are still room for improvement to let the systems be more adaptive. Secondly, control load brought by reputation computation is relatively heavy. Thirdly, much memory space is needed to store trust values.

Recently, Xiaomei Dong, *et al.*, [22] proposed a monitoring based approach for secure data aggregation. A WSN architecture fit for monitoring was proposed, which divided the network into nonoverlapping virtual cells. The aggregation nodes were also organized as a grid tree to save energy. Therein a novel algorithm named FDSR was proposed to detect malicious nodes, which is effective for detecting on-off attacks. But with the network scale expanding, this scheme will suffer overload on trust table size and number of control messages. Moreover, insufficiently using of second-hand reputation information will lead to inaccuracy of the outcome of trust computation.

In this paper, we propose a novel solution named FROST to detect the malicious nodes and defend various attacks. The focus of our work is to testify whether the introduction of notion, friendship can result in reduction of the trust table size and overhead brought by building and maintaining the trust system in large scale wireless ad hoc networks while having no obvious passive effect on packet forwarding. In addition, we merge decaying model into FROST to enable the trust system to be more adaptive to the changing network environment.

The paper is organized as follows: In Part III, core design of novel trust system is given. Process of Merging Trust Semiring, Decaying Model and Friendship Model is reported in Part IV. Then attacks and analyses are described in Part V. We conduct in-depth performance evaluation using simulation in Part VI. Finally, conclusion is drawn in Part VII.

3. Design of Novel Trust System

The new proposed trust system runs at the middleware [23] of every mobile node in wireless ad hoc networks, which uses watchdog mechanism to monitor the actions of its neighbor nodes. Every mobile node maintains trust table about a subset. Here trustworthiness value should be represented and, be updated continuously based on new direct observations or group trust.

3.1. Reputation computation engines

Here we take two kinds of trust, direct trust and group trust, both of which are two important parts in trust table.

Direct trust: Direct trust is the sum of trust in trustee nodes about performing particular action such as routing.

Group trust: Group trust is a special type of direct trust showing to what degree a truster node will accept its neighbor nodes' recommendation about the good reputation of the third party node.

The direct trustworthiness value of one node can be represented by a tuple (*r*, *c*), where *r* is direct trust value and *c* is confidence value. Bayesian formulation uses Beta distribution $Beta(\alpha, \beta)$ where there are only two updating parameters that need to be maintained. Based on Bayesian's theorem, *r* and *c* can be calculated as follows, respectively:

$$r = \mu(s, f) = \frac{s}{s+f} \tag{1}$$

$$c = 1 - \sqrt{12}\sigma(s, f) = 1 - \sqrt{\frac{12sf}{(s+f)^2(s+f+1)}} \tag{2}$$

where $r, c \in [0,1]$ and s, f are the times of successful interaction and unsuccessful interaction between truster and trustee nodes. The trustworthiness space can be described as $T = [0,1] \times [0,1]$.

We use following semiring model [1] to calculate group trust value:

$$(r_{ik}, c_{ik}) \otimes (r_{kj}, c_{kj}) \Rightarrow (r_{ik}r_{kj}, c_{ik}c_{kj}) \tag{3}$$

$$(r_{ij}^{p1}, c_{ij}^{p1}) \oplus (r_{ij}^{p2} r_{ij}^{p2}) = \left(\frac{c_{ij}^{p1} + c_{ij}^{p2}}{\frac{c_{ij}^{p1}}{r_{ij}^{p1}} + \frac{c_{ij}^{p2}}{r_{ij}^{p2}}}, \frac{c_{ij}^{p1} + c_{ij}^{p2}}{2} \right) \tag{4}$$

where *p1* and *p2* are two different trust propagation paths.

3.2. Decaying model

Wireless ad hoc network is a kind of network with *dynamic* elements such as topology, channel, node location etc. On the other hand, trust is a *dynamic* event which will bring more challenge into securing wireless ad hoc network. In order to track these dynamic characteristics, an observation that has been made a long time ago will be less important than the one that is made recently while calculating trust values. Under this circumstance, the most commonly method is to introduce a decaying factor $\mathscr{D}$ [2]. There are many works on how to choose suitable value of this factor, but most of which are empirical methods. In the new method, we present a new way to choose the decaying factor, which is associated with positive outcomes and negative outcomes. If at time t_1 one truster node got Y times negative outcomes from one trustee node, it bespeaks that at time $t_2(t_2 > t_1)$ the trustee node has misbehaved $Y\mathscr{D}^{t_2 - t_1}$ times. If one trustee node changes its behavior more quickly, $\mathscr{D}$ should be set a larger value to show that the history behavior has less impact on present trust computing. Moreover, if it behaves normally or abnormally, $\mathscr{D}$ should also change according to these different behaviors because misbehaving one time will have more impact on trust computing than behaving normally one time. Moreover, behaving normally many times can compensate the impact brought by misbehaving one time. Thus, this value $\mathscr{D}$ is not a fixed number and it should vary based on the network environment.

Here, we take two values into consideration, that is, $\mathscr{D} = 1 - r$ or

$$\mathscr{D} = \begin{cases} \mathscr{D}_1, & r \geq \mathscr{F} \\ \mathscr{D}_2, & r < \mathscr{F} \end{cases} \tag{5}$$

where $\mathscr{F}$ is a friendship factor which will be described in part 3.3 and $0 < \mathscr{D}_1 << \mathscr{D}_2 \leq 1$.

3.3. Friendship model

In social network, people **tend to** contact their friends to decrease the cost of transactions between them [24]. In wireless ad hoc networks, the web of trust is often too sparse to get trust values between non-familiar nodes, since in wireless ad hoc networks, a node has experience with only a very small fraction of the other community members. On the other hand, though every node within the network can infer the trust values between itself and other nodes, the resource required is tremendous since it should store and maintain many relationships(corresponds to the size of its adjacency set).

Here, we introduce one novel friendship factor according to which the network can be spitted into different groups. In Figure 1, user H has to store and maintain 4 relationships (corresponds to the size of its adjacency set). In hypergraph model (Figure 2) this is reduced to 2 – number of groups and user H is member. We will show that such models allow trust to be built between mutually unknown entities with less communication and computation load in Part V.

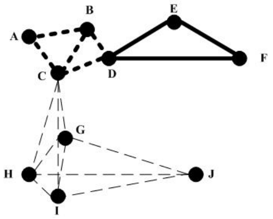

Figure 1. Graph representation of a wireless ad hoc networks. Different trust levels between nodes are shown in different kinds of lines

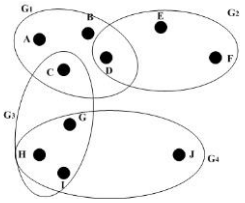

Figure 2. Hypergraph representation of a wireless ad hoc networks. Different trust levels are shown by ovals corresponding to the groups of nodes

Definition1: $G_i = \{GH_i \mid \forall i, 1 \leq i \leq d_{gh}\} \cup \{GM_j \mid \forall j, 1 \leq j \leq d_{gm}\}$ is the node set of *i*th group, where d_{gh} is the number of group head in the whole network and d_{gm} are the number of the group members.

Definition 2: the trust value in one group is shared by all the group members.

Let $R_{pq} = \{< r_{p,q}, c >| \forall p, q \in G_i, 1 \le p, q \le d_{gh} + d_{gm}\}$, then we get $R_j = \left\{ \left\langle N_q, r_{node\_jq} \right\rangle \middle| \forall N_q \in G_i, 1 \le q \le d_{gh} + d_{gm}, 1 \le j \le d_{gm} \right\} \ge \mathscr{T}$. Here, $r_{p,q}$ are the trust values between neighbors in the group, N represent the different group elements which include group header and group members, p,q represent arbitrary nodes who have trust relationship between each other in one group.

Normally, there may be two or more nodes in the same group which have their different direct trust values regarding one third party node. In this case, we use following scheme to merge these trust values.

Firstly, we assume that there is a binary hypothesis testing problem with two hypotheses: H_0: trust is absent; H_1: trust is present. The a priori probabilities of the two hypotheses can be described as $P(H_0) = P_0$ and $P(H_1) = P_1$. If there are n nodes with the trust values r_x (x=1,…,N)on the same third party node are statistically independent, then the conditional probability density function can be denoted as $p(r_x \left| H_{0,1} \right.), x = 1, ..., N$. Each node make a decision d_x based on the following rule:

$$d_x = \begin{cases} -1, & \text{if } H_0 \text{ is declared} \\ +1, & \text{if } H_1 \text{ is declared} \end{cases} \tag{5}$$

The false alarm and detection probabilities of the kth node in one group will be P_{fk} and P_{dk}, respectively. Each d_x is then transmitted through a fading channel and the output of the channel for the kth node is $y_k = d_k h_k + n_k$, where h_k is a real valued fading envelope of Rayleigh fading channel and n_k is zero mean Gaussian noise with variance σ^2. Here we assume that the variances of all channels are same and the distance (number of hops) between group member and group header is 1. The group header will make system decision based on y_k. Then we can derive the optimal likelihood ratio at the group header as:

$$\begin{aligned} \Lambda_{LR} &= \log \frac{p(\mathbf{y} \mid H_1)}{p(\mathbf{y} \mid H_0)} \\ &= \log \prod_{k=1}^{N} \frac{P_{dk} e^{\frac{(y_k - h_k)^2}{2\sigma^2}} + (1 - P_{dk}) e^{\frac{(y_k + h_k)^2}{2\sigma^2}}}{P_{fk} e^{\frac{(y_k - h_k)^2}{2\sigma^2}} + (1 - P_{fk}) e^{\frac{(y_k + h_k)^2}{2\sigma^2}}} \end{aligned} \tag{6}$$

where $\mathbf{y} = [y_1, ..., y_N]^T$ is a vector containing the output of the channel for all the N nodes.

4. Process of Merging Trust Semiring, Decaying Model and Friendship Model

During the bootstrapping phase, in our trust system, it is necessary that all nodes in wireless ad hoc networks should be grouped based on their own identities or object (many networks such as wireless sensor networks, military ad hoc networks can meet these requirements easily). Based on formula (1) and (2), the direct trustworthiness value of one node, tuple (r, c) can be inferred from the times of normal behavior and abnormal behavior. According to the decaying model in Part 3.2, the adoption of decaying factor $\mathscr{D}$ will have impact on the computation of times of positive outcomes and negative outcomes. If at time t_1 one truster node get X times positive outcomes and Y times negative outcomes from one trustee node, it bespeaks that at time $t_2 (t_2 > t_1)$ the trustee node has behaved normally $X\mathscr{D}^{t_2 - t_1}$ times and misbehaved $Y \mathscr{D}^{t_2 - t_1}$ times. If during the period of time between t_1 and t_2 $(t_2 > t_1)$, the trustee node has behaved X_1 times and misbehaved Y_1 times, then at time t_2, s will be updated to $s\mathscr{D}^{t_2 - t_1} + X_1$ and f will be updated to $f\mathscr{D}^{t_2 - t_1} + Y_1$. Then we can calculate the current value of tuple (r, c) based on the updated s and f. Based on formula (3) and (4), tuple (r, c) between any truster and trustee node also can be calculated and the process of merging trust semiring, decaying model will be finished. Once this work is done, the trustworthiness value in one group is shared by all the group members.

5. Attacks and Analyses

Trust system can effectively improve network performance and detect malicious entities. Thus, it is an attractive target for attackers. In this section, we will show that FROST can defense several representative attacks.

5.1. Black/Gray hole attack

Black hole attack and gray hole attack are two types of routing attacks which conduct packet forwarding misbehavior. In a black hole attack, malicious node replies to every route request with message that it has route to the destination. Then all the packets will be routed to the malicious node and it will discard them. Different from the black hole attack, in a gray hole attack the malicious node perform as an good node during route discovery process, then it drops some of the data packets other nodes want it to forward even when there is no network congestion. Based on decaying model, our approach can detect this kind of misbehavior in time. Then friendship model can exclude the malicious nodes from network once their trust values fall below the given $\mathscr{T}$

5.2. Conflicting Behavior Attack

Another kind of dangerous attack in trust system is conflicting behavior attack. Malicious node can undermine good trustees' trust by performing differently to different nodes. For example, a malicious node *i* can always behave well to node *j* and behave badly to another node *k*. Thus, these two nodes have developed different conflicting opinions about the malicious node *i*. Some existed contexts [8, 25] do not mention this kind of attack, but it exists in their system for they take recommendation into consideration. But in our approach, the node use trustable second hand information from their friend neighbors. Moreover, once the trust value of one node is less than $\mathscr{T}$, every node in one group will stop cooperating with it, and it will be excluded outside. Thus, this approach can defense the conflicting behavior attack.

5.3. Selective misbehavior

Selective misbehavior attack is similar to conflicting behavior attack. But in this kind of attack, the malicious node aims to exclude victim nodes who it wants to attack from the network while performing normal behaviors with nodes that play important roles in routing or packet forwarding in networks [26]. In our approach, because of the introduction of friendship model, node in one group will get second hand information from their trusted friend neighbors, which will guarantee the accuracy of recommendation. Moreover, similar scheme used in defending conflicting behavior attack can also be adopted to exclude the malicious node outside.

5.4. Bad Mouthing Attack

As long as recommendations are introduced into trust computing, malicious parties can provide dishonest recommendations to frame good parties and/or increase trust values of malicious nodes. Bad mouthing attack [7] is a kind of straightforward attack. Here we treat group trust separately from direct trust and can only be established based on previous recommendation behaviors. Friendship factor is also taken into consideration to add a necessary condition to trust propagation. That is, trust value can propagate along path A-B-C only if the trust between A and B is greater than the value of the friendship factor. Moreover, the introduction of decaying model can also restrain the possibility of this kind of attack.

5.5. On-off Attack

On-off attack uses the dynamic properties of trust through time-domain with inconsistent behaviors. In On-off attack, malicious nodes behave well and badly alternatively, tending to be able to remain undetected by other nodes when they conduct damage in networks. The trust computation is a dynamic process. A good node may be compromised or hardware fault and turned into a malicious node, while an incompetent or hardware fault node may become competent due to environmental changes. In order to track this dynamics, the observation result got long time ago should not carry the same weight as that had recently. Due to the introduction of decaying factor $\mathscr{D}$ that we have descried in section 3.2, our approach can cope with this kind of attack. Moreover, we will take on-off attack for example in Part V to conduct profound performance analysis.

6. Performance Analysis

To compare with other trust system using recommendation, a simulation was implemented using NS2 to evaluate the performance of new method. The MAC layer protocol is the IEEE 802.11 DCF [27]. DSR is used as the routing algorithm. The dimension of space is size 1000m by 1000m. The maximum radio range is 250m. Each network node moves randomly according to the random waypoint model with a speed uniformally distributed between 0 m/sec and 10m/sec. There are 60 traffic pairs randomly generated for each simulation. For the performance analysis, we compare the behavior of new method to other trust system using recommendation.

6.1. Performance comparison between the new approach and reference methods

In this part, the main objective is to determine the impact of the introduction of friendship model on some key metrics like packet delivery ratio, normalized trust table size and normalized trust load described as below, in wireless ad hoc networks where some of the nodes conduct attacks. For these two metrics, the performance investigation will be carried out in terms of percentage of malicious nodes, number of nodes and node mobility.

Packet delivery ratio: This metric reflect the degree of successful packet forwarding in wireless ad hoc networks. We express it as:

$$P = \frac{\sum_{i=1}^{n} Packets_{received}}{\sum_{i=1}^{n} Packets_{sent}} \qquad (7)$$

where *n* is the number of network nodes.

Normalized trust table size: This metric reflect the usage of physical resource while building and maintaining trust system. We define this metric according to following formula:

$$S = \frac{\sum_{i=1}^{n} S_{occupied}}{\sum_{i=1}^{n} S_{assigned}} \qquad (8)$$

Normalized trust load: Normalized trust load is the number of control packets transmitted and related to building and maintaining trust system per data packet delivered at the destination. This metric is used to show the trust establishing control penalty involved in forwarding packet in wireless ad hoc networks.

The packet delivery ratio versus percentage of malicious nodes in the network is depicted in Figure 3. For CONFIDANT and FROST, The packet delivery ratio although decrease with the increasing of percentage of malicious nodes, it sustains about 0.8. But for the defenseless DSR, it falls grammatically when the percentage grows. This is because trust system in both CONFIDANT and FROST help the network to identify and isolate the malicious nodes. Compared with CONFIDANT, FROST has lower packet delivery ratio because it narrow the trust exchanging field using group trust which leads to mild performance deterioration of FROST, that is, different from exchanging recommendations with any possible nodes to get a more comprehensive acquaintance with the third party node, members in one group only accept the recommendations on the third party node from their neighbors in the same group.

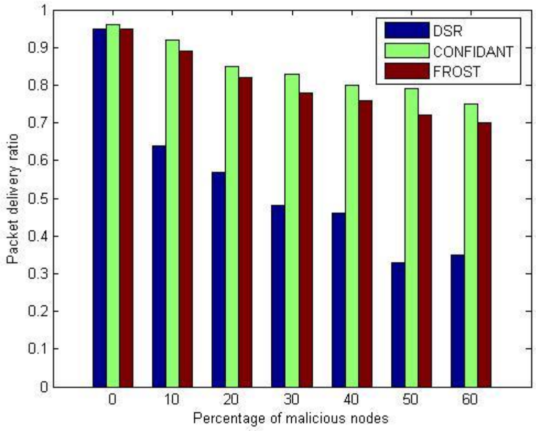

Figure 3. Packet delivery ratio versus percentage of malicious nodes

Figure 4 shows normalized trust table size as a function of number of nodes in the network. FROST manages a trust table consisting of entries for nodes and their trust values. We assign a same initial size for both CONFIDANT and FROST in the beginning. Referring to part 3.3, the introduction of friendship model can reduce the trust table size dramatically especially for large scale wireless ad hoc networks which can be seen as one important advantage of FROST. Figure 4 illustrates that when the number of nodes is relative small, the difference between two sizes is trivial, but when network size grows large, if no corresponding scheme can be adopted the trust table size will grow exponentially while table size in FROST increases much slower than CONFIDANT. Concise trust table will result in a lower cost brought by maintaining the table.

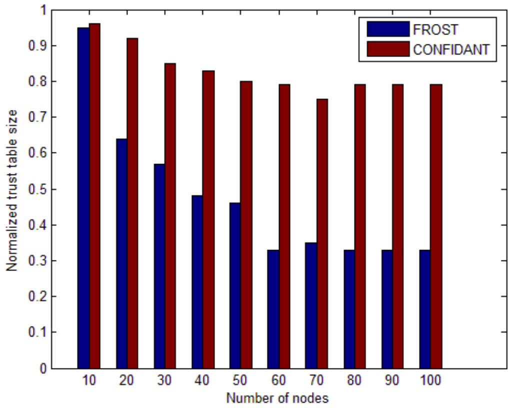

Figure 4. Normalized trust table size versus number of nodes

Figure 5 reports normalized trust load as a function of node mobility. From Figure 5, we can see the other advantage of the new method. Because the friendship model is introduced, the frequency of information exchanging between neighbors in the same group is relative low, leading to fewer control messages. In a word, because of the introduction of friendship model, the trust level is a common value for a group of users rather than individuals. As the groups can differ in purpose, one entity can be a member of more groups. Trust between two entities is then inferred based on their group memberships. Such model allows trust to be built between mutually unknown entities with less communication and computation load and can save memory space.

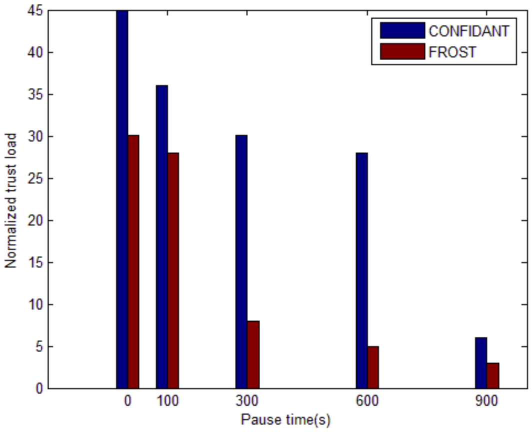

Figure 5. normalized trust load node mobility(percentage of malicious nodes is 30%)

6.2. Trust value computations after D is introduced

In this analysis, we focus on the robustness of the proposed method against attacks trigged by malicious nodes in networks. Due to the intrinsic character of wireless ad hoc networks, some nodes may drop packets due to network traffic congestion or bad quality of wireless channel. This kind of node can be defined as normal node. On the other side, we call node malicious node, which can attack other nodes deliberately. Thus, in this section, we divide the whole network nodes into two categories: normal (good) nodes and malicious (bad) nodes. More precisely, here nodes that will perform on-off attack are malicious nodes. Based on the above platform, we set the numbers of them 32 and 30, respectively. Then, initial trust vale are set within the range of (0.45, 0.55), initial confidence value (0.05, 0.15), that is, moderate trust value and relatively low confidence value.

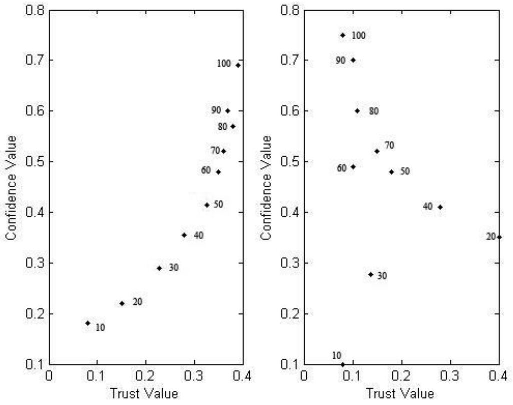

Figure 6. trustworthiness truster node have on on-off node in trustworthiness space (number beside the point means the order number of simulation cycle)

In Figure 6, left subfigure, when the decaying model is not introduced, though the on-off nodes have conducted attack, the truster node can not detect this kind of attack and the trustworthiness value still approach (1,1). In right subfigure, the situation has been changed after the decaying model is introduced because this scheme will punish the behavior of the on-off nodes and the trustworthiness value will approach (0,1).

7. Conclusions

A novel reliable trust system, called FROST is proposed in this paper to quantitatively measure reputation and cope with malicious attacks in wireless ad hoc networks. Friendship model is used to construct friendship groups and conduct trust computation to decrease the trust table size and control overhead brought by building and maintaining the trust system. In addition, we merge decaying model into FROST to enable the trust system to be more adaptive to the changing network environment. We perform the newly proposed trust system in wireless ad hoc networks and evaluate the performance of the proposed approach using rigorous analysis and extensive simulation.

Acknowledgements

This work is supported by National Natural Science Foundation of China (NSFC) under grant No. 61002016, 61101111 and Science Foundation of Zhejiang Sci-Tech University under Grant No.1004839-Y.These should be brief and placed at the end of the text before the references.

References

[1] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks", Selected Areas in Communications, IEEE Journal on.vol. 24, no. 2, **(2006)**.

[2] Y. Han, S. Zhiqi, M. Chunyan, C. Leung and D. Niyato, "A Survey of Trust and Reputation Management Systems in Wireless Communications". Proceedings of the IEEE, vol. 98, no. 10, **(2010)**.

[3] R. Li, J. Li, P. Liu and H. H. Chen, "On- demand public- key management for mobile ad hoc networks", Wireless Communications and Mobile Computing, vol. 6, no. 3, **(2006)**.

[4] Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Wireless Networks, vol. 11, pp. 1-2, **(2005)**.

[5] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the CONFIDANT protocol. Proceedings of Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, **(2002)**.

[6] A. Jsang and R. Ismail, "The beta reputation system", Proceedings of Proceedings of the 15th bled electronic commerce conference, **(2002).**

[7] S. Buchegger, "Coping with false accusations in misbehavior reputation systems for mobile ad-hoc networks", **(2003)**.

[8] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks", ACM Transactions on Sensor Networks (TOSN), vol. 4, no. 3, **(2008)**.

[9] R. Molva and P. Michiardi, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Institute EurecomResearch Report RR-02-062, **(2001)**.

[10] Y. Sun, Z. Han, W. Yu and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks", Proceedings of IEEE INFOCOM, **(2006)**.

[11] Y. L. Sun, W. Yu, Z. Han and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", Selected Areas in Communications, IEEE Journal on vol. 24, no. 2, **(2006)**.

[12] S. K. S. Shio Kumar Singh, M. S. MP Singh and D. S. DK Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks", International Journal of Advanced Science and Technology, vol. 30, **(2011)**.

[13] M. S. Islam and S. AshiqurRahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", International Journal of Advanced Science and Technology, vol. 36, **(2011)**.

[14] K. Sharma, M. Ghose, D. Kumar, R. P. K. Singh and V. K. Pande, "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology, vol. 17, **(2010)**.

[15] P. Resnick, K. Kuwabara, R. Zeckhauser and E. Friedman, "Reputation systems", Communications of the ACM, vol. 43, no. 12, **(2000)**.

[16] S. Ahmad, B. Ahmad, S. M. Saqib and R. M. Khattak, "Trust Model: Cloud's Provider and Cloud's User", Journal of Advanced Science and Technology, vol. 44.

[17] A. Srinivasan, J. Teitelbaum and J. Wu, "DRBTS: distributed reputation-based beacon trust system", Proceedings of Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on, **(2006).**

[18] F. Almenarez, A. Marin, D. Díaz and J. Sanchez, "Developing a model for trust management in pervasive devices", Proceedings of Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on, **(2006)**.

[19] H. Chen, H. Wu, X. Zhou and C. Gao, "Agent-based trust model in wireless sensor networks", Proceedings of Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, **(2007)**.

[20] T. Qin, H. Yu, C. Leung, Z. Shen and C. Miao, "Towards a trust aware cognitive radio architecture", ACM SIGMOBILE Mobile Computing and Communications Review, vol. 13, no. 2, **(2009)**.

[21] Q. He, D. Wu and P. Khosla, "SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks", Proceedings of Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, **(2004)**.

[22] X. Dong and S. Li, "A Secure Data Aggregation Approach Based on Monitoring in Wireless Sensor Networks", Proceedings of Mobile Ad-hoc and Sensor Networks (MSN), 2011 Seventh International Conference on, **(2011)**.

[23] L. J. Liu JingYong, Z. L. Zhang LiChen, Z. Y. Zhong Yong and C. Y. Chen Yong, "Middleware-based Distributed Systems Software Process", International Journal of Advanced Science and Technology, vol. 13, **(2009)**.

[24] M. Demır and L. A. Weitekamp, "I am so happy'cause today I found my friend: Friendship and personality as predictors of happiness", Journal of Happiness Studies, vol. 8, no. 2, **(2007)**.

[25] C. Dellarocas, "Mechanisms for coping with unfair ratings and discriminatory behavior in online reputation reporting systems", Proceedings of Proceedings of the twenty first international conference on Information systems, **(2000)**.

[26] J. Li, R. Li and J. Kato, "Future trust management framework for mobile ad hoc networks", Communications Magazine, IEEE, vol. 46, no. 4, **(2008)**.

[27] I. C. S. L. M. S. Committee, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, ed: IEEE Std, **(1997)**.

Authors

Lianggui Liu received the PhD degrees in Communications and information system from Nanjing University of Posts & Telecommunications, Nanjing, China. He is now an associate professor with School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China. He was a Visiting Associate Professor (2011) with Cornell University, Ithaca, NY, USA. His current research interests focus on network communications, network security, natural computation. Dr. Liu is the author of one monograph, *Effective QoS Routing in Ad Hoc networks based on Natural Computation*, published by Zhejiang University Press and first author of more than 20 academic papers on resource optimization and information security and assurance in wireless networks.

Jia Huiling received the PhD degrees in Communication and Information System from Zhejiang University. She is now a lecturer with School of Information, Zhejiang Sci-Tech University, Hangzhou, China. Her current research interests include wireless sensor networks, heterogeneous wireless networks, radio resource management.

Shu Ting received the PhD degrees in Computer Science and Technology from Zhejiang University. He is now an associate professor with School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China. His current research interests include network protocol test, Ad Hoc networks, wireless sensor networks.