Securing Distributed Networks Using Reliable Reputation System: Vulnerability and Attacks Analyses[1]

Lianggui Liu, Huiling Jia, Ting Shu

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

Abstract. Collaboration among distributed entities is urgently needed for distributed networks to guarantee desired performance due to their intrinsic characters. Reputation system plays important role in giving entities incentives to cooperate in packet forwarding. However, reputation system itself is vulnerable to attack and the reputation of entities in networks can be manipulated intentionally by malicious ones. Unlike prior work, in this paper, we present a reliable reputation system to quantitatively measure reputation and defend reputation system against malicious attacks. We introduce decaying model to enable the reputation system to be adaptive to the changing environment. Moreover, we use hypergraph and friendship model to decrease the overhead while maintaining the trust system. Particularly, the newly proposed reputations system is employed in fully distributed mobile ad hoc networks. We conduct an in-depth investigation on various attacks and evaluate the effectiveness of the proposed scheme.

Keywords: friendship model, distributed networks, malicious attack, trust, security

1 Introduction

In distributed networks there is no fixed network infrastructure and centralized approaches and network nodes can communicate with others out of their wireless transmission range through packet forwarding cooperation. Reputation system is crucial to give nodes incentives to cooperate in packet forwarding [1] [3]. Due to the intrinsic characters of distributed networks, conventional security methods are inadequate or too complicated to protect such autonomous networks from misbehaving nodes such as selfish nodes and malicious nodes. Here, we use *trust* to represent one estimated value about a node's actual quality in terms of its behavior in distributed networks. Sometimes it is also referred to as *reputation* [2].

[1] 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.

2 Core Design of Novel Reputation System

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

2.1 Semiring trust model

Semiring is a kind of algebraic structure $(S,\oplus,\otimes)$ [4].We use following semiring model to calculate group trust value:

$$(r_{ik},c_{ik})\otimes(r_{kj},c_{kj})\Rightarrow(r_{ik}r_{kj},c_{ik}c_{kj}) \tag{1}$$

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

where p_1 and p_2 are two different trust propagation paths, r is trust value and c is confidence value.

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

$$\mathscr{D}=\begin{cases}\mathscr{D}_1, & r\geq\mathscr{F}\\ \mathscr{D}_2, & r<\mathscr{F}\end{cases} \tag{3}$$

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

2.2 Decaying model

Here, we take decaying factor into account, that is, $\mathscr{D}=1-r$ or

$$\mathscr{D}=\begin{cases}\mathscr{D}_1, & r\geq\mathscr{F}\\ \mathscr{D}_2, & r<\mathscr{F}\end{cases} \tag{3}$$

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

2.3 Friendship model

In real social network, people **tend to** contact their friends to decrease the cost of transactions between them [5]. In completely distributed networks, the network is often too sparse to get trust values from non-familiar nodes, since in distributed networks, a node has experience with only a very small fraction of the other nodes. On the other hand, though every node within the network can infer trust values between itself and other nodes, the resource required is tremendous since every node 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 Fig. 1, node H has to store and maintain 4 relationships (corresponding to the size of its adjacency set). In hypergraph model (Fig. 2) the number of relationships is reduced to 2 – number of groups where H is member. Different from conventional cluster algorithms, here cluster heads and cluster members are equal in status.

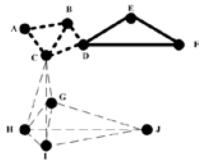

Fig. 1. Graph representation of a distributed network. Different trust levels between nodes are shown in different kinds of lines

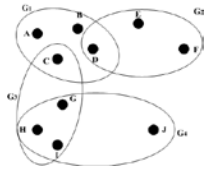

Fig. 2. Hypergraph representation of a distributed networks. Different trust levels are shown by ovals corresponding to the groups of nodes

Definition: $G_i = \{GH_i \mid \forall i, 1 \le i \le d_{gh}\} \cup \{GM_j \mid \forall j, 1 \le j \le d_{gm}\}$ 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.

3 Attacks and Analyses

Reputation system can effectively improve network performance and detect malicious entities. Thus, it is an attractive target for attackers. Our proposed approach can defense several representative attacks like bad mouthing attack, conflicting behavior attack and on-off attack.

4 Performance analysis

To compare with other reputation system using recommendation[3], a simulation was implemented using NS2 to evaluate the performance of new method. The MAC layer protocol is the IEEE 802.11 DCF [6]. 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. There are 60 traffic pairs randomly generated for each simulation. In this analysis, a metric *trust table size ratio* is used to describe the performance of the new reputation system.

$$trust\ table\ size\ ratio = \frac{total\ trust\ table\ size\ used\ in\ proposed\ method}{total\ trust\ table\ size\ used\ in\ reference\ method}$$

We also analyze the *additional control overhead* and the accuracy of the outcome of the proposed method. The former is brought through maintaining the group. Control overhead includes various control messages that is related to the trust computation. We define *control overhead ratio* as below:

$$control\ overhead\ ratio = \frac{total\ control\ overhead\ used\ in\ proposed\ method}{total\ control\ overhead\ used\ in\ reference\ method}$$

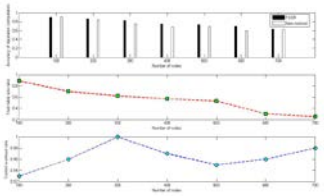

Fig. 4. Performance comparison between the new approach and reference method

5 Conclusion

A novel reliable reputation system is proposed in this paper to quantitatively measure reputation and cope with malicious attacks. We introduce decaying model to enable the reputation system to be adaptive to the changing environment. Hypergraph and friendship model are used to construct friendship groups to decrease the overhead brought by maintaining the reputation system. Semiring is adopted to calculate group trust more accurately. We perform the newly proposed reputation system in fully distributed mobile ad hoc networks and evaluate the performance of the proposed approach using extensive simulation.

References

1. Han Yu, Zhiqi Shen, Chunyan Miao, Cyril Leung and Dusit Niyato, “A survey of trust and reputation management systems in wireless communications,” Proceedings of the IEEE, vol. 98, no. 10, pp. 1755-1772, Oct 2010.
2. P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, “Reputation systems: Facilitating trust in internet interactions,” Communications of the ACM, vol 43, no. 12, pp. 45-48, 2000.
3 Xiaomei Dong; Shanshan Li, “A Secure Data Aggregation Approach Based on Monitoring in Wireless Sensor Networks” , Proc. 2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks (MSN), 2011 ,122 - 129.
4 G. Rote, “Path problems in graphs,” Computing Supplementum, vol.7, pp. 155–189, 1990.
5 Demir, M., Weitekamp. L.A, “I am So Happy Cause Today I Found My Friend: Friendship and Personality as Predictors of Happiness,” Journal of Happiness Studies, vol. 8, 2007, 181 – 211.
6 IEEE Computer Society LAN MAN Standards Committee, “Wireless lan medium access control (mac) and physical layer (phy) specifications,ieee std 802.11-1007,” The Institue of Electrical and Electrics Engineers.