A Super Peer-based Reputation Scheme for Mobile Computing Environments

Xu Wu
Department of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
Email: xrdz2006@163.com

Abstract—Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated. Many trust management mechanisms are proposed to provide effective security solution for wire and wireless networks, even some of them have become one of the most known in this field. However mobility, uncertainty and heterogeneity of mobile computing environments make trust management much more complicated, so they are inadequate in the mobile computing environments in which the clients are mobile, volatile and undetermined. In the paper, we presents a super peer-based reputation scheme (SPRS), where peers are classified into two groups, super peers and mobile peers and a super peer has zero or more mobile peers. We design two ways of selecting super peers, greedy method and maximal independent set method. The proposed scheme establishes a trusted mobile environment for mobile computing environments. It effectively avoids the communication overhead in global trust computation because each super peer maintains the appropriate reputation information of its mobile peers. The simulation results show that SPRS is highly robust and scalable in the dynamic environment of mobile networks.

Index Terms—Trust, mobile computing, peer to peer

I. INTRODUCTION

Mobile Computing Environments using wireless networks and Ethernet jacks have become popular in universities, companies, airports, hotels, cafes, on the streets, etc. With such communication mechanisms, a moving object receives information from its neighbors, or from remote objects by multi-hop transmission relayed by intermediate moving objects. All of these scenarios require secure communications and quality of service, but currently Mobile Computing Environments often have certain probabilities of failure due to security problems. Mobile Computing Environments are prone to different types of malicious attacks, such as denial of service, routing protocol attacks as well as replay attacks. These threats usually come from external attackers and internal compromised nodes. For example, the external attackers can successfully partition a network or introduce excessive traffic load into the network by inserting false routing information, replaying old routing information, and destroying useful routing information. Traditional cryptographic schemes, such as encryption and digital signature can defend against the external attacks. The internal attacks come from compromised nodes, which might send malicious routing information to other nodes. It is more severe because traditional cryptographic solutions are unable to identify the destructive threat by the authenticated nodes which have been compromised. In addition, cryptographic schemes are also unable to identify selfish and low competitive nodes, and motivate benevolent behaviors of nodes. Therefore, an efficient mechanism is urgently needed to deal with this problem efficiently, and enhance the security, reliability and impartiality of the system.

Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated. Trust is an important aspect in the design and analysis of secure distribution systems. It is also one of the most important concepts guiding decision-making. Trust is a critical part of the process by which relationships develop. It is a before-security issue in the ad hoc networks. By clarifying the trust relationship, it will be much easier to take proper security measures, and make correct decision on any security issues. Trust modeling is a technical approach to represent trust for digital processing. Recently, trust modeling is paid more and more attention in wire and wireless networks.

Indeed, wireless communications rely on open and public transmission media that raise further vulnerabilities in addition to the security threats found in wired networks. The highly decentralized and distributed nature of mobile computing environments makes classical, centralized security-managing mechanisms unusable. It does not suffice to provide user authentication because in a mobile computing environment, most users are unknown. Furthermore, the growing complexity of mobile terminals and the increased presence of interoperability software on them is making them vulnerable to viruses and hacking attacks. Users of these terminals need support to decide who to interact with in this plethora of self-interested peers. Therefore, trust is an important component of security. In a mobile computing environment, the communications depend highly on the trust among devices. Trust is tightly

Manuscript received February 1, 2014; revised June 25, 2014.
This work was supported by Natural Science Basis Research Plan in Shaanxi Province of China under Grant No. 2011JQ8006 and Shanxi Provincial Education Department under Grant No. 2013JK1132 and National Natural Science Foundation of China under Grant No.61373116 and special funding for key discipline construction of general institutions of higher learning from Shanxi province and special funding for course development from Xi'an University of Posts and Telecommunications.
Corresponding author email: xrdz2006@163.com.
doi:10.12720/jcm.9.6.475-482

connected to all aspects of authentication and authorization.

Trust has the following characteristics, for instances, temporality, dynamicity, applicability and intransitivity and subjectivity, etc, which means that trust in real sense is limited in a certain span of time, and aimed at a certain application environment and changed dynamically according to the mutual actions of the two sides. Trust establishment is mainly achieved in the following way [1]: the system collects the trust evidence of the clients, defines the trust polices, builds up the trust levels of the clients based on the trust evidence and policies. As more evidence becomes available, the system iteratively updates the trust information including trust evidence and polices. Applying current existing trust models or trust management systems on mobile computing environments require extracting user's trust standards in different contexts, user's experience or feedback dissemination and user's decision about trust or distrust. However mobility, uncertainty and heterogeneity of mobile computing environments make trust management much more complicated, so they are inadequate in the mobile computing environments in which the clients are mobile, volatile and undetermined.

There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. An infrastructure wireless network consists of an access point or a base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect or bridge the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity. In the paper, we only focus on the infrastructure wireless network consists of an access point or a base station.

Therefore, in the paper we propose a super peer-based reputation scheme for an infrastructure wireless network consists of an access point or a base station. The proposed scheme consists of three unique features: 1) peers are classified into two groups, super peers and mobile peers and a super peer has zero or more mobile peers. 2) When a peer wants to search the trust value of other peers, there is no need of multi-broadcasting because each super peer maintains the appropriate reputation information of its mobile peers, so the communication overload in global trust computation is avoided. 3) A protocol for trust management via polling is used. The polling processes can reduce the cost of trust evaluation than traditional global trust evaluation methods since the requesting node need only broadcast messages to all other member nodes.

The remainder of this paper is organized as following: Section 2 presents the related work. The Section 3 describes the proposed super peer-based reputation scheme in detail, and the trust computing adjusting is elaborated in Section 4. Theoretical analysis and simulation results to the performance of the new reputation scheme are given in Section 5. Finally, Section 6 concludes the paper.

II. Related Work

Trust-management approach for distributed systems security was first introduced in the context of Internet as an answer to the inadequacy of traditional cryptographic mechanisms. Some of the notable earlier works in this domain have been trust-management engines. Since then, reputation-based frameworks based on the approach of trust management have been extensively studied in many contexts and equally diverse domains such as human social networks, e-commerce, 802.11 networks, peer-to-peer networks etc. In this paper, we study the applicability of this approach in developing high integrity mobile peer to peer (P2P) networks.

The proposed mechanism does borrow some design features from several existing works in literature but as a complete system differs from all the existing reputation-based systems. Super node-based approach is used to reduce bandwidth consumption in many schemes, where the super node is in charge of using their observations, storing the trust values obtained by itself or other nodes and distributing the blacklisting. The approach usually uses a cluster-based architecture include cluster heads and numerous sensor nodes. In such schemes, some nodes referred to as super nodes are assumed have more computation power, storage, and power for communication. One example of such a scheme is called a group based trust management scheme (GTMS) proposed in [2] for clustered WSNs, which employs clustering. The GTMS assumes that BS is a central command authority. The downside of this centralized BS based approach is that it is a potential performance/reliability bottleneck introducing a single point of failure for model execution.

The other super node based trust management architecture (TMA) is proposed in [3]. A decaying trust function is employed in TMA, which can give more weight to the most recent trust value in the overall trust value computation. In addition, TMA also allows the nodes to move from one cluster to another by preserving their trust record, thereby making the scheme suitable for dynamic environments wherein the nodes move frequently. TMA has the same shortcomings with GTMS due to the similar architecture.

QDV [4] is an ant colony optimization approach for reputation and quality-of-service-based security in WSNs, where the more reputation a node has, the more reliable it is for communication purposes. The weighted sum of reputation and QoS is computed in order to select the

next node in the path, but the important limitations found in WSN such as bandwidth, power and memory of sensor nodes aren't taken into consideration in [4]. Therefore, Authors [5] apply a bio-inspired technique to develop a trust and reputation model (BTRM) for WSN. BTRM is based on the redefined bio-inspired algorithm of ant colony system. An ant is travelling along the WSN searching for the most trustworthy route leading to the most reputable server. QDV and BTRM have the same aim of helping a node requesting a certain service to the network to find the most trustworthy route leading to a node providing the right requested service.

A novel trust evaluation algorithm (NBBTE) is presented in [6]. NBBTE takes advantage of D-S evidence theory. A variety of trust factors include packet receive, send, strictness, delivery, consistency and availability in NBBTE are established to obtain direct and indirect trust values of neighbor nodes. Fuzzy set theory is used to decide the trustworthiness levels in accordance with the fuzzy subset grade of membership functions. Although the simulations show that the method can obtain nodes' trustworthiness efficiently, it is not well suited for sensor networks due to its higher consumption of resources in the process of trust evaluation.

A new trust model for WSNs is constructed in [7], and a novel power-aware and reliable scheme (PRS) for sensor selection is also proposed based on the trust model. The algorithm not only builds the multi-attribute value of the target node based on its interaction records among the nodes, but also integrates trust value from the third-party nodes.

Runfang Zhou and Kai Hwang [8] proposed a power-law distribution in user feedbacks and a computational model, i.e., PowerTrust, to leverage the power-law feedback characteristics. The paper used a trust overlay network (TON) to model the trust relationships among peers. PowerTrust can greatly improves global reputation accuracy and aggregation speed, but it can't avoid the communication overhead in global trust computation.

Some trust management schemes using multi-agent system [9], [10] are also proposed. The agent node relies on a watchdog mechanism to observe the behavior of the sensor nodes and computes the trust rating for them. These schemes few take into account the strong restrictions about processing, storage or communication capabilities, so they are difficult to implement.

A trust model based on recommendation evidence is proposed for P2P Networks by Tian Chun Qi etc [11]. The proposed model has advantages in modeling dynamic trust relationship and aggregating recommendation information. It filters out noisy recommendation information.

Authors [12] present a pre-standardization approach for trust and/or reputation models in distributed systems. A wide review of different trust models are carried out, and some common properties are extracted and some pre-standardization recommendations are provided. These trust models are compared against the common properties and recommendations. In addition, other protocols [13-15] address trust management methods in self-organization networks from different views.

III. Super Peer-based Reputation Scheme

Existing reputation methods assume that there exists always stable trust relationship between mobile peers, and a few considers the dynamic feature of mobile network environment. However, in mobile environments peers may move around and randomly leave, and connect the network again by changing their identities without any notices. Hence, the trust between mobile peers can not be set up simply on the traditional reputation scheme. In this section we propose new reputation scheme for mobile computing environments. We classify peers into two groups, super peers and mobile peers. The purpose of maintaining super peers is to manage their mobile peers that are connected to their super peer and allow the super peer to have their reputation information. A super peer has a reputation table in which each entry has a mobile peer's reputation information.

The trust establishment process runs as follows:

Step 1: When a mobile peer wants to find the trust value of other peer, it asks its super peer for the value.

Step 2: If the super peer finds it in its table entries, the super peer sends the trust value to the mobile peer. Otherwise, the super peer sends a message to other super peers to get the value.

Step 3: If any of super peers finds the value in its reputation table entries, it sends Response message to the super peer who sent message initially.

Since trust evidences of a peer are main collected in the super peers, the average length of trust computing chains is much shorter and more robust than other models, and avoids trust dilution. This scheme allows us to avoid multi-broadcasting in global trust computation., so SPRS reduce the bandwidth consumption. In the proposed scheme there are two ways of selecting super peers, greedy method and maximal independent set method.

A. Greedy Method

A greedy method is designed based on a greedy approximation algorithm [16]. Since peers themselves don't know which peer has the largest degree, we require a server to record the number of neighbors for each peer. The server then selects the peer whose degree is the maximum among others greedily as the first super peer and let its adjacent peers become its mobile peers. Ties are broken arbitrarily. After the selection the super peer and its mobile peers are removed virtually from the network. Then the method selects and removes repeatedly until there is no more peer in the network.

Fig. 1 shows a sample network constructed with the greedy method. Yellow peers are super peers and others are mobile peers. Note that although the rectangle peer has degree 4, it cannot be a super peer, because it is connected the super peer that were selected earlier by the

greedy method. As rectangle peer becomes a mobile peer, it is unnecessary to communicate with all connected mobile peers. So, the dotted lines will not be used. As soon as a super peer is selected, it collects appropriate reputation information from each mobile peer. Each mobile peer knows the id and address of its super peer by a server. In order to establish connections among super peers, when a peer is selected as a super peer, it asks its mobile peers to find other super peers in the near vicinity. Each mobile peer searches other peers that belong to different super peer, and it asks the information of their own super peers. Fig. 2 illustrates how to find the trust value in a sample network.

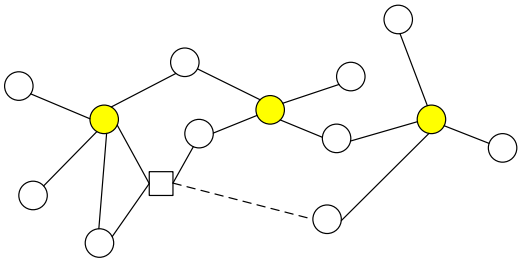


Fig. 1. Structure of a network constructed with the greedy method

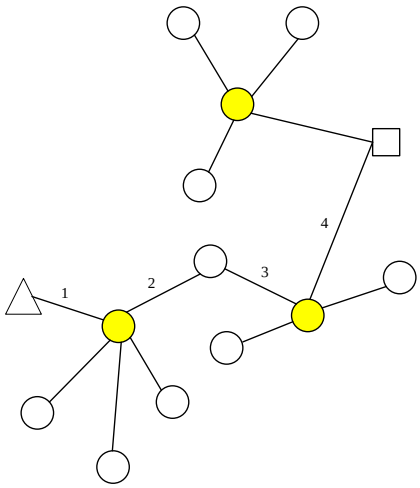


Fig. 2. The step of finding the trust value of the rectangle peer

The triangle peer wants to find the trust value of the rectangle peer. As in Fig. 2 yellow peers are super peers and others are mobile peers. The triangle peer first informs its super peer that it wants the trust value of the rectangle peer (Step 1). When the super peer gets the message from the mobile peer, it searches its reputation table entries. If it finds the trust value, then it sends the value to the triangle peer. Otherwise, the super peer sends messages to other super peers to find the value (Steps 2 and 3). As soon as other super peers receive the message from the super peer, they look into their reputation table entries for the value. One of super peers finds it (Step 4), it sends Response message to the super peer of the triangle peer.

B. Maximal Independent Set Method

As the greedy method needs a server to maintain super peers, it can't be implemented in a full distributed mobile P2P network. The maximal independent set method is designed to determine super peers in a distributed manner which is much natural to realistic mobile P2P environments. Luby's algorithm [17] is used in the method. In our method, each peer chooses a random number and then compares it with its adjacent peers. The random numbers are to be chosen between 1 and n^4, where n is the number of peers in the network. Choosing n random numbers in this range independently almost guarantees that the chosen numbers are unique. And a peer that has the largest number among its adjacent peers becomes a super peer. After removing super peers and their mobile peers, the method performs the same procedure repeatedly until all peers become either super peers or mobile peers. The expected number of iterations is at most O(logn).

Fig. 3 shows that four peers become super peers after the first iteration of the method. Yellow peer are super peers, and others are mobile peers. The number above each peer is a chosen random number. In the figure, the peer with random number 16 is left alone for the second iteration and becomes a super peer. In the last as shown in Fig. 3, super peers are selected in a full distributed manner based on the super peer selecting method.

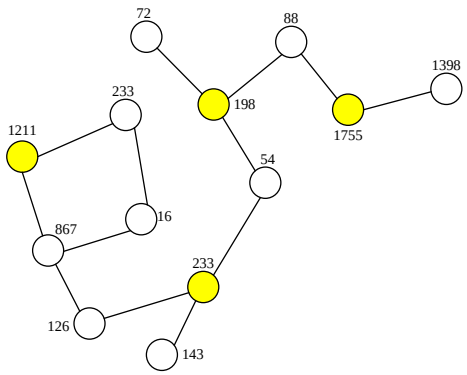


Fig. 3. Super peer selection after the first iteration with the maximal independent set method

IV. Trust Computing Adjustment

In the mechanism, the trust of a node is related to its reputation. We use mathematical method to represent the reputation of a node, and continuously update it based on new direct/indirect observations. A novel trust evaluation model [18] proposed by us is used to compute the trust value. Consider the situation where node *i* wants to interact with node *j* in order to accomplish a certain task. There are two ways in which to calculate trust value: direct and recommendation.

Direct trust is denoted as $D(T_i(j), S)$, where $T_i(j)$ is the direct trust value that node *i* calculates for node *j*. S expresses node *j*'s level of size of interaction which is granted by node *i*. The level of size of interaction satisfies the following rules.

1) The lowest level is given to a new node that doesn't have any interaction history.

2) A certain level is updated if the number of successful interactions reaches the predefined number in the level. The predefined number is decided by the node itself. The lower the current level is, the more the number of successful interactions it needs.

3) The predefined successful interaction number in a certain level is increased if interactions fail due to malicious activities.

Direct trust is used to evaluate trustworthiness when a peer has enough interacting experience with another peer. On the other hand, recommendation trust is used when a peer has little interacting experience with another one. Recommendation trust is calculated based on a polling protocol to be described below.

Let we assume that node *j* requests an interaction with node *i* and the size of the interaction is Q. First, node *i* computes node *j*'s direct trust denoted as $D(T_i(j), S)$.

1) If $Q \le S$ and $T_i(j)$ reaches a certain value (which is set by node *i*), node *i* considers node *j* to be trustworthy. It will then decide to interact with node *j*.

2) If $Q \le S$ but $T_i(j)$ fails to reach a certain value, node *i* chooses to join a group based on its interest. Then it checks its own group and location with GPS and floods a HELLO message which containing a packet <GroupID, Position> to announce itself to other nodes by using Echo protocol [19], then requests all other members of the group to cast a vote for node *j* from the perspective of trust in the level of Q. For any new node without any interaction history, its trust value would be 0 and would be granted the lowest level of the size of interaction. Without requesting, it will be permitted to interact at the lowest level.

3) If $Q \ge S$ but $T_i(j)$ fails to reach a certain value, peer *i* immediately refuses to interact with peer *j*.

4) If $Q \ge S$ and $T_i(j)$ reaches a very high value, peer *i* chooses to join a group based on its interest and then requests all other members of the group to cast a vote for peer *j* from the perspective of trust in the level of Q.

Lastly, peer *i* gathers up all poll information of peer *j* from the repliers and gets peer *j*'s recommendation trust by this equation:

$$T = \frac{\sum_{i=1}^{N(w)} R(w) \times p}{N(w)} \quad (1)$$

where $N(w)$ denotes the total number of votes and $R(w)$ denotes peer w's vote accuracy factor which is in the range of (0, 1). p is related to $DT_w(j)$ such that if $DT_w(j) > 0$, $p = 1$, else $p = 0$. Peer *i* has trust table RT_i. It is related to every peer *j* for which peer *i* maintains a trust.

At the end of interaction, peer *i*(*j*) updates the *j*(*i*)'s trust value in its trust table according to the following trust evaluation principle.

1) The trust of a peer should be increased as the probability of its normal action, in order to avoid that newcomers take very long time to cumulate enough trust values to take part in the interaction in the network.

2) When the peer behaves well, its trust should be increased with small span in order to prevent that the malicious peer can reenter the network system by changing its network identities to get good trust values.

3) When the peer behaves badly, its trust should be decreased in large span in order to prevent the networks from the attacks of malicious peers.

The principle can efficiently encourage participators to take part in the systems actively and friendly.

V. Experimental Study

The simulation environment is set up as follows: we create 300 peers that will perform interacting in a mobile P2P resource sharing system. 300 mobile peers are uniformly distributed at the area whose size is 500 m ×500 m. Communicating range of a mobile device is 70m. We made the assumption that all state variables are independent.

TABLE I: DEFAULT SIMULATIONS PARAMETERS IN THE THIRD EXPERIMENT

Number of Peers	300
Communicating Range (m)	70
Simulation Area (m^2)	500x500
Number of Malicious Peers	0%-70% of all peers
Risk Attitude	Averse, Neutral, Seeking
Communication Protocol	802.11
Life Time (s)	[50, 100]
Maximum Speed (m/s)	20

The simulated experiments were run on a dual-processor Dell server and the operation system installed on this machine is Linux with kernel 2.6.9. To make our simulation as close to the real mobile P2P systems where peers often go offline, we simulate the offline peers by assigning every peer a random lifetime (or Time-To-Live) within the step range [50, 100]. After reaching the lifetime, the peer will not respond to any service request, and won't be counted in the statistics either. After one more step, the peer comes alive again with a new life time randomly chosen from the range [50, 100]. In this analysis, we assume that all mobile peers have a same amount of battery power and participate in communication positively regardless of their roles. In the first experiment and second one, all peers participate 1000 rounds of interacting. In each round, each peer acts as both client and server to share its resources with other peers, and communicates with each other via IEEE 802.11. The default parameters in simulation experiments are showed in the Table I. Moreover in each experiment peers must follow the decision model through the whole interacting process. After completing the interaction, the involved parties update their trustworthiness of the other

peers. Our results for some interesting cases are reported below.

The comparisons are done between SPRS with the previously proposed schemes include GTMS and BTRM in terms of the rate of inauthentic downloads of nodes, message overhead. Greedy method is used to select super peers in the first group of experiments. The first group of experiments we carried out had the following structure. We launch the three solutions over the system composed of 100 peers separately. On the network, the percentage of sensors acting as clients is always a 15%. The 85% left were, therefore, sensors acting as servers. Each client applies for file download service 50 times. The scheme's performance is demonstrated under two attack models: independent cheat and group cheat. Under independent cheat, the malicious nodes firstly accumulate trust values through small interactions, gaining a relatively high trust. After trusted by most adjacent nodes, the node takes advantage of its high trust value to attack another node, which means to always provide an inauthentic file to another node when selected as download source. Group cheat is that there is a group in which the node of the group provides an authentic file to each other and provides an inauthentic file to the node outside the group.

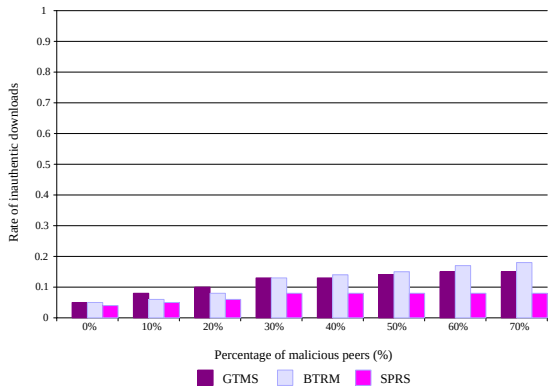


Fig. 4. Simulation results of peers under independent cheat

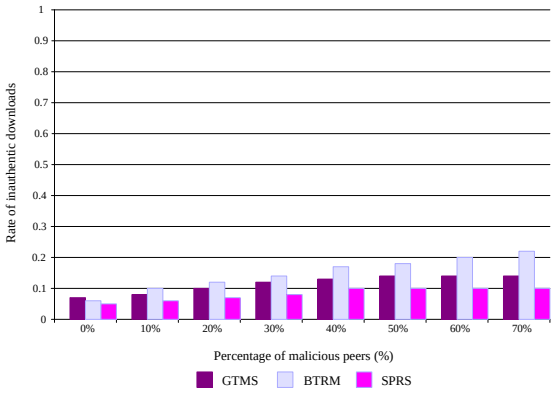
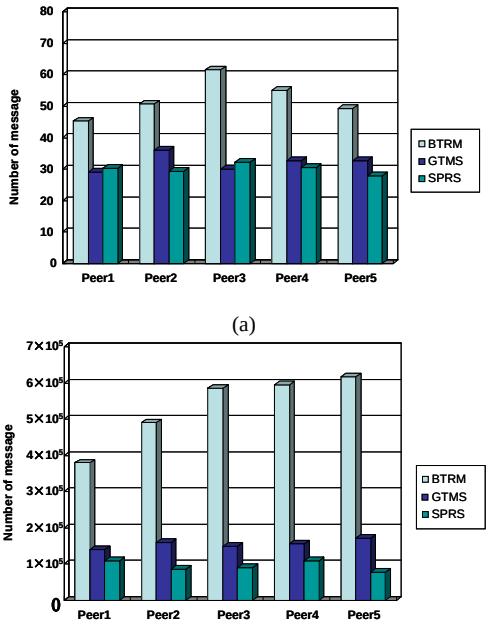


Fig. 5. Simulation results of peers under group cheat

The rate of inauthentic downloads of nodes is evaluated in the first group of experiments. We add a number of malicious servers to the network such that malicious nodes make up between 0% and 70% of all servers in the network. For each fraction in steps of 10% we run experiments under two attack models separately and depict the results in Fig. 4 and Fig. 5.

We observed a 10% fraction of inauthentic downloads of SPRS at most in Fig. 4 and Fig. 5. For independent cheat and group cheat, SPRS performs well even if a majority of malicious nodes is present in the network at a prominent place. Even if no malicious nodes are present in the system, downloads are evaluated as inauthentic in 3%-5% of all cases – this accounts for mistakes users make when creating and sharing a file, e.g., by providing the wrong meta-data or creating and sharing an unreadable file. As Fig. 4 and Fig. 5 shows, comparing with GTMS and BTRM, our proposed scheme gets more efficient. The main reason is that SPRS can adjust the node trust value according to its behavior based on a flexible trust evaluation principle expressed in Section 4. After one malicious behavior, a node needs to successfully conduct many more honest interactions to make up for the loss of trust value.

Maximal independent set method is used to select the power peer in the second group of experiments. We separately compute trust value of 5 different sensor peers with SPRS, GTMS and BTRM in the second group of experiments. During GTMS simulation, random numbers of source nodes are selected in each cluster, which perform node recommendation with the other nodes. Also, each cluster head will perform node recommendation with neighboring cluster heads only. During BTRM simulation, a number of iterations is defined as N_S^{Niter}, (similar to the number of ants definition) where *Ns* is the number of sensors belonging to the WSN and $Niter \in [0, 1]$. During our reputation simulation, we assume a node has little interacting experience with another one, so recommendation trust is calculated based on a polling protocol to be described in Section 4.



(a)

(b)

Fig. 6. Simulation results of peers under independent cheat

Firstly, the simulation is done in a system of 1,000 nodes. Fig. 6 (a) shows the number of messages to aggregate all trust scores in SPRS, GTMS and BTRM. The average number of messages made by BTRM is 52.01, the GTMS method showed 31.06, while our method has the best result, 30.05. The experiment expresses SPRS and GTMS outperform BTRM. For a system of 1,000 nodes, the GTMS and BTRM method show similar results. Secondly, we repeat the same simulation in a system of 10,000 nodes, Fig. 6 (b) shows our system averagely needs 90,870.08 messages to aggregate all trust scores, whereas the GTMS and BTRM averagely need 168,500.03, 532,000.06 messages to perform the same task separately. Using SPRS, the nodes do experience a noticeably lower messaging overhead. In other words, SPRS can better alleviate the message overhead problem, whereas the GTMS and BTRM cannot. Therefore, SPRS is scalable in handling an even larger number of services.

Greedy method is used to select super peers in the third experiment. The third experiment shows that our proposed reputation mechanism is slightly affected by the dynamic joining and departing of peers. Table II shows the experimental results after we removed m=500, 1000, 1500, 2000, 2500 peers randomly. We see that the network still have a good performance even after 25% peers leaving. Table III shows similar results for peers' joining. In our model, peers joining does not have significant influence on network performance. Secondly, a dynamical joining/leaving process is simulated.. The probability of joining and leaving of a node equals to 0.5. This means that nodes' leaving and joining are of the same chance. We examined the network performance at each 250 interval and get the results as shown in Fig. 7. The whole process ended when network has experienced 3000 times joining/leaving actions. The simulation is conducted on a network with size n=10,000 and n=6,000. Compared with the network of size 6000, the performance is basically the same. We can see that the network performance actually has little change. Fig. 7 represents the experiment result which clearly shows that SPRS is very robust in a dynamic environment.

TABLE II: THE NETWORK PERFORMANCE AFTER PEERS LEAVING

M	BEFORE LEAVING	AFTER LEAVING
500	3.10	3.12
1000	3.20	3.26
1500	3.01	3.05
2000	2.80	2.81
2500	3.51	3.60

TABLE III: THE NETWORK PERFORMANCE AFTER PEERS JOINING

M	BEFORE JOINING	AFTER JOINING
500	2.20	2.26
1000	2.40	3.43
1500	3.10	3.13
2000	2.60	2.63
2500	2.81	3.84

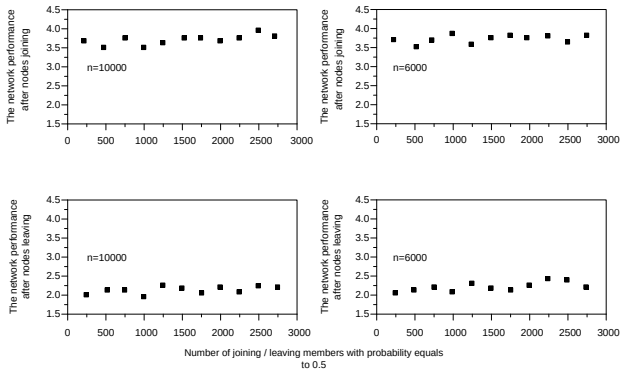


Fig. 7. The network performance after nodes joining or leaving

VI. CONCLUSIONS AND FUTURE

The realization of reputation mechanism in mobile computing environments is quite different due to some characteristics of mobile environment such as high mobility of the peers, limited-range as well as unreliability of wireless links, which indicates the trust between participants can not be set up simply on the traditional reputation mechanism. Therefore, in the paper we present a super peer-based reputation mechanism and give two super peer selecting method for mobile computing environments. In the proposed scheme, peers are classified into two groups, super peers and mobile peers and a super peer has zero or more mobile peers. We design two ways of selecting super peers, greedy method and maximal independent set method. When a peer wants to search the trust value of other peers, there is no need of multi-broadcasting because each super peer maintains the appropriate reputation information of its mobile peers, so the communication overload in global trust computation is avoided. The simulation results show that SPRS is highly robust and scalable in the dynamic environment of mobile networks. SPRS deals with the fundamental reputation management problem, it can serve as the building block for higher level security solutions such as key management schemes or secure routing protocols. In the near future, we would like to test SPRS into mobile computing environments and analyze the system performances.

ACKNOWLEDGMENT

The work in this paper has been supported by Scientific Research Program Funded by Natural Science Basis Research Plan in Shaanxi Province of China (Program No.2011JQ8006) and Shanxi Provincial Education Department (Program No.11JK1060 and 2013JK1132) and National Natural Science Foundation of China (Program No. 61373116) and special funding for key discipline construction of general institutions of higher learning from Shanxi province and special funding for course development from Xi'an University of Posts and Telecommunications.

REFERENCES

[1] C. English, P. Nixon, S. Terzis, A. McGettrick, and H. Lowe, Dynamic Trust Models for Ubiquitous Computing Environments, UBICOMP2002-Workshop on Security in Ubiquitous Computing, Göteborg, Sweden, September 2002.

[2] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. L. and Y. Jae Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, 2009, pp.1698–1712.

[3] J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan, and A. Sattar, "A trust management architecture for hierarchical wireless sensor networks," in *Proc. 35th Annual IEEE Conference on Local Computer Networks*, IEEE Computer Society Press, Denver, Colorado, USA, 2010, pp. 264-267.

[4] S. K. Dhurandher, S. Misra, M. S. Obaidat, and N. Gupta, "An ant colony optimization approach for reputation and quality of-service-based security in wireless sensor networks," *Security and Communication Networks*, vol. 2, no. 2, pp.15–224, 2009.

[5] G. M. Felix and M. P. Gregorio, "Providing trust in wireless sensor networks using a bio-inspired technique," *Telecommunication Systems*, vol. 46, no. 2, pp. 163-180, 2010.

[6] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345-136, 2011.

[7] G. Han, L. Shu, J. Ma, J. H. Park, and J. Ni, "Power-aware and reliable sensor selection based on trust for wireless sensor networks," *Journal of Communications*, vol. 5, no. 1, pp. 23–30, 2010.

[8] R. Zhou and K. Hwang, "Power trust: A robust and scalable reputation system for trusted P2P computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 5, 2007.

[9] H. G. Chen, H. F. Wu, J. C. Hu, and C. S. Gao, "Agent-based trust management model for wireless sensor networks," in *Proc. International Conference on Multimedia and Ubiquitous Engineering*, 2008, pp. 150-154.

[10] F. G. Marmol and G. M. Perez, "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems," *Computer Standard and Interfaces*, vol. 32, no. 4, pp. 185-196, 2010.

[11] C. Q. Tian, S. H. Zou, W. D. Wang, and S. D. Cheng, "A new trust model based on recommendation evidence for P2P networks," *Chinese Journal of Computers*, vol. 31, no. 2, pp. 271-281, 2008.

[12] J. Lopez, R. Roman, I. Agudo, and C. G. Fernandez, "Trust management systems for wireless sensor networks: Best practices," *Computer Communications*, vol. 33, pp. 1086-1093, 2010.

[13] J. L. Li, L. Z. Gu, and Y. X. Yang, "A new trust management model for P2P networks," *Journal of Beijing University of Posts and Telecommunications*, vol. 32, no. 2, pp. 71-74, 2009.

[14] B. Ma and X. X. Zhong, "Cloud trust model for wireless sensor networks," *Computer Science*, vol. 37, no. 3, pp. 128-132, 2010.

[15] S. Y. Guan, W. G. Wu, X. D. Dong, and Y. D. Mei, "Survey of trust management in open distributed environments," *Computer Science*, vol. 37, no. 3, pp. 22-35, 2010.

[16] V. Chvatal, "A greedy heuristic for the set-covering problem," *Math. of Oper. Res.*, vol.4, no. 3, pp, 233-235, 1979.

[17] L. Michael, "A simple parallel algorithm for the maximal independent set problem," *SIAM Journal of Computing*, vol. 15, no. 4, pp. 1036-1053, 1986.

[18] X. Wu, "A novel trust evaluation model for mobile P2P networks," in *Proc. 7th IFIP International Conference on Network and Parallel Computing, Lecture Notes in Computer Science*, vol. 6289, 2010, pp. 210-219.

[19] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of locotion cloims," in *Proc. 2nd ACM Workshop on Wireless Security*, New York, 2003, pp. 1-10.

Xu Wu received his Ph.D. degree in Computer Science, from the Beijing University of Technology, in 2010. Her research interests include trusted computing, pervasive computing, mobile computing, and software engineering. She has published more than 30 technical papers and books/chapters in the above areas. She is currently an associate professor of Xi'an University of Posts and Telecommunications. Her research is supported by Scientific Research Program Funded by Natural Science Basis Research Plan in Shaanxi Province of China and Shanxi Provincial Education Department.

