Research on Light-weight Trust Management Approach in 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—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. In this paper, we propose a distributed trust model in a mobile computing environment based on a set of useful observations about a user behavior. The proposed trust model is particularly appealing to mobile computing environments as it is extremely light-weight, both in terms of memory requirements and computational load. The kind of way greatly avoids heavy interactions that may be required by some existing trust management solutions. The simulation experiments verify the effectiveness and benefits of our proposed model.

Index Terms—trust, mobile computing, P2P

I. Introduction

Rapid advances in wireless networking and increased popularity of portable devices are turning mobile computing into a reality. Today's mobile computing environments bring the users access to any information at any time, from any place, in any form. 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. Three essential properties of mobile computing are wireless communication, mobility, and portability. The mobile computing community is experiencing new technical challenges, as important and vital information is often placed on a mobile device that is vulnerable to theft and loss. Consider a mobile peer-to-peer (P2P) file-sharing application that lets peers share files without a centralized index.

A mobile peer locates nearby peers and queries them directly for desired content. These mobile peers can forward the queries to other nearby peers. The original mobile peer eventually receives the result locations and can choose a specific peer from which to download the content directly. Such mobile P2P systems don't rely on a central authority to manage and coordinate peers, and it is difficult for administrators to locate, track, and identify users in mobile computing environments. Therefore attacks on file-sharing applications by malicious peers are common. Malicious peers might offer corrupted files, or even worse, files that carry viruses or trojans. Downloading and opening these files poses a significant risk to users. With no centralized infrastructure, each peer must adopt suitable countermeasures against such attacks. These attacks also threaten other domains, such as decentralized auctioning and emergency response. Without a set of guiding principles to address the threats, deployment of mobile computing will be limited.

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 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

Manuscript received August 10, 2013; revised October 19, 2013.
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.8.12.877-882

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 [12]-[14] 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.

In this paper, we propose a distributed trust model in a mobile computing environment. Based on a set of useful observations about a user behavior, a distributed trust model is derived and used to foresee the behaviors of peers in mobile computing environments. The observations are got through auto-monitoring users' behaviors via user-device interactions, and these useful information is extracted to evaluate and manage trust in the mobile computing environments. The kind of way greatly avoids heavy interactions that may be required by some existing trust management solutions. New observations are fed in by means of a set of recursive mathematical equations that can be efficiently computed in order to increase the accuracy of the prediction. Developing such a distributed trust model is significant for a mobile device, as we cannot assume the existence of a trusted third party that can be contacted on demand to acquire trust information about an entity.

The rest of the paper is organized as follows. Section 2 presents some related work. Section 3 gives the details of the proposed model. Section 4 contains experimental study. Finally, Section 5 discusses the conclusions and ideas for future work.

II. Related Work

Trust-management approach is emerging as a promising technology to facilitate collaboration among entities in an environment where traditional security paradigms cannot be enforced due to lack of centralized control and incomplete knowledge of the environment. In this paper, we study the applicability of this approach in enhancing the security of mobile computing environments. The proposed model does borrow some design features from several existing works in literature but as a complete system differs from all the existing reputation-based systems.

Most of existing work follows the research steps that, what is trust referent, what are factors or aspects related to trust, and evaluate or assess trust based on those factors and aspects and try to manage trust accordingly [2]. But it is actually hard to computationally model some influencing factors, such as usability and a user's subjective factors. Since trust is a subjective concept, assessing trust need to understand the trustor's trust criteria regarding each factor or aspect, even for different contexts. This may raise a lot of interaction requirements in order to get the trustor's criteria in various situations or contexts. In most digital information systems, the trustor is a user and the trustee is a device or a device application. This will increase interactions between the user and device, and thus cause a usability issue that requires more efforts to overcome.

A reputation based trust model [3] proposed by Xiong and Liu is developed for P2P e-commerce communities. It relies on a user to provide feedback. Sometimes, it may not be appropriate or convenient to require user to provide feedback because it could cause many usability problems. This introduces a requirement for experiential feedbacks to be largely automated. English and Terzis presented an interaction monitor that enables automated collection of detailed interaction evidence based on interaction modeling [4]. The monitor is a prototype implementation of a generic interaction monitoring architecture that applied a well-understood rule engine and an event management technology. Our trust evidence collection in the proposed model takes on a similar approach as the one in [4].

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 it 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 [6] 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.

QDV [7] 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 [7]. Therefore, Authors [8] 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 [9].

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 [10], 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. However, the proposal doesn't consider the requirements changes of trust management in WSNs.

Some trust management schemes using multi-agent system [11], [12] 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.

Authors [13] 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. Authors [14] list the best practices that are essential for developing a good trust management system for WSN and make an analysis of the state of the art related to these practices. These two references make an excellent summary, propose many profound viewpoints and show an additional insight on the trust evaluation field. In addition, other protocols [15]-[17] address trust management methods in self-organization networks from different views.

III. Distributed Trust Model

In the section we firstly present the overview of the proposed trust model. We then present the details about how to predict the trustworthiness of mobile devices by the model.

A. An Overview of Tthe Proposed Trust Model

We proposed a distributed trust model in the paper. In our model, there are two types of observations related to a trusting decision: direct observation and indirect observations obtained from neighbors' recommendations. The trust model designed for mobile computing should be as simple as possible to avoid unnecessary overhead, as mobile devices are powered by batteries and also have limited computational ability. Our trust model is comprised of three key phases which are shown in Fig. 1.

1) Collection of observations: An interaction monitor [4] is used to collect the detailed interact evidence through auto-monitoring users' behaviors, then these useful information is inputted to the filter of observations.
2) Filter of Observations: Filter of Observations is designed based on Kalman filter theory [5]. It is essentially a set of recursive mathematical equations that provide an optimal way to estimate the current state of a dynamic system, starting from observations that contain random errors. After each observation, the filter updates its inner state, so to make a more accurate estimate the next time.
3) Prediction of Trust: The trustworthiness of a mobile device is predicted based on the filter of observations. Because of the high dynamicity of mobile computing environments, it is not feasible to train a filter so to predict the actual values of the attributes advertised by a mobile device. What we can do instead is to predict the discrepancy between the attribute values advertised by a mobile device and what the other device's measurements. Our model then can define mobile device A's trust in mobile device B in terms of these discrepancies, in a way that trust decreases as a result of high discrepancies.

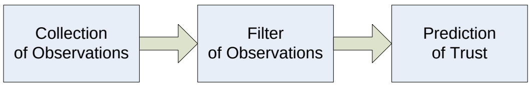


Fig. 1. The proposed trust model

Our model has three main advantages. Firstly compared with some existing trust models, it automatically collects the detailed interacting evidence through auto-monitoring users' behaviors. Sometimes, it may not be appropriate or convenient to require user to provide feedback because it could cause many usability problems. The proposed trust model effectively solves the problem of trust evidences collection. Secondly as the introduction of filter, it provides a light-weight trust prediction method. Even in the simplest formulation, the filter is able to make a prediction based on an arbitrary long history of interactions; it implicitly represents the concept of confidence in the trust prediction, as the more frequently device A interacts with device B, the more quickly the filter stabilizes and reduces the distance between prediction and actual state; finally, it enables simple yet effective modeling of the subjective nature of trust by means of the measurement and system errors. Thirdly it is designed as simple as possible, and only collects a set of useful observations about a user behavior.

However current trust models and management schemes require extracting user's trust standards in different contexts, user's experience or feedback dissemination and user's decision about trust or distrust, which are inadequate in the mobile computing environments in which the clients are mobile, volatile and undetermined.

B. *Trust Prediction*

In the section, we detailed illustrate how to use the basic Kalman filter to derive an autonomic, light-weight, and yet accurate trust predictor. Firstly, an introduction to the Kalman filter theory is provided. The Kalman filter provides an optimal prediction algorithm in that it minimizes the estimation error. Even though these assumptions (which are necessary for optimality) rarely holds, yet the filter works well for many applications.

The basic Kalman filter takes the following form1:

$$s_i = s_{i-1} + \varphi_{i-1} \tag{1}$$

A certain quality of service at time i depends on the quality of service at time i-1 and a random noise φ_{i-1}. The noise φ_{i-1} is a white gaussian noise with covariance ϑ_{i-1}. Intuitively, the higher the noise φ_{i-1}, the higher the importance of the latest observation. The Kalman equations thus project the current state forward (prediction) and incorporate noise to improve the estimate (correction).

Let us now re-phrase the whole problem in terms of trust for a mobile peer-to-peer file-sharing system. Mobile peer A is willing to assess the trust of mobile peer B before deciding whether to interact with B or not. It does so by means of a basic Kalman filter that predicts B's trust at time i based on i-1 previous observations of B's behavior (direct experiences). After each observation, the filter updates its inner state, so to make a more accurate estimate the next time. The Kalman filter is particularly appealing to mobile computing environments as it is extremely light-weight. Moreover, it captures many facets of peer trust. It also makes a prediction based on the last interactional experiences; it implicitly represents the concept of confidence in the trust prediction, as the more frequently A interacts with B, the more quickly the filter stabilizes and reduces the distance between prediction and actual state.

Now, we deal with the problem of our trust prediction. The first step captures a wide spectrum of peer trust facets. As shown in formulae 1, the corrective-predictive behavior of the filter depends on parameter φ_{i-1}. By tuning the value of parameter, we can assign a different weight to the direct experience, with respect to the last history of interactions. For example, if a peer selects a profile that describes itself as a risk averse one, parameter φ_{i-1} will be set to a high value, so that higher relevance is given to the history with respect to the latest experience. Even better, this value may be set to vary with the number of interactions, so to fine tune the prediction during the system lifetime; for example, we may assign lower values of φ_{i-1} at bootstrap (when no historical information is present), and then gradually increase them. Note that, by varying the values of φ_{i-1} over time, we are able to capture the level of confidence in a trust prediction, which depends on both the number of interactions occurred, and their frequency. Let us assume that A interacts with every i time units; as long as A and B interact with this frequency, we increase the value of φ_{i-1} every n time units. If the frequency of interaction falls well below i, we start decreasing φ_{i-1} again, so to give higher importance to freshly available information. Simulation can be used to study how to set the parameters. The peer trust can then be denoted as the following form2:

$$T_i = 1 - s_i, T_i \in [0,1] \tag{2}$$

The basic Kalman filter, illustrated in equations 1 and 2, can now be used to make an accurate prediction of how much the peer's experience of a P2P service will deviate from what the P2P service provider has promised s_i and, consequently, of how much the provider can be considered trustworthy T_i.

IV. Distributed Trust Model

The objective of our experiments is to verify the effectiveness and benefits of our proposed model. We study the behavior of the predictor for different values of φ_{i-1}. 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 $500m \times 500m$. 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 1. 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.

Fig. 2 illustrates the behavior of the discrepancy predictor s_i (top) and of the associated trust predictor $T_i = 1 - s_i$ (bottom). It shows examples of static profiles, with peers' risk attitude that do not change in 150 interactions. The initial guess of the Kalman filter s_0 has been set to 0.6. We have set the φ_{i-1} to 0.1. More advanced profiles can be obtained by autonomically changing the values of φ_{i-1} with peer' risk attitude. We have built three trust predictors with varying values of φ_{i-1} and compared their estimations. The results are plotted in Fig. 3. As shown, the higher the value of φ_{i-1} (the higher noise in the interaction), the more importance is given to past interactions.

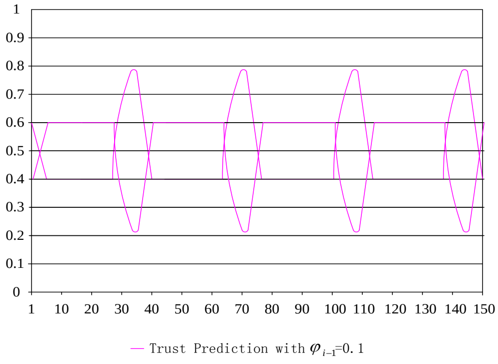


Fig. 2. Trust prediction example of static profile. Top: prediction of discrepancies. Bottom: prediction of trust.

In the second experiment, the comparisons are done between our proposed LTME with the previously proposed schemes include GTMS and BTRM in terms of energy consumption. We implement a peer recommendation scenario, and assume that all nodes have a same amount of battery power. The simulation software used is SENSE version 3.0, which is written in C++, and is simulation software for wireless sensor network. Fig. 4 shows that our model consumes less energy as compared to the GTMS and BTRM scheme.

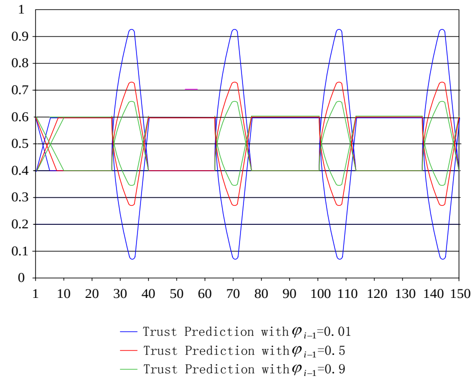
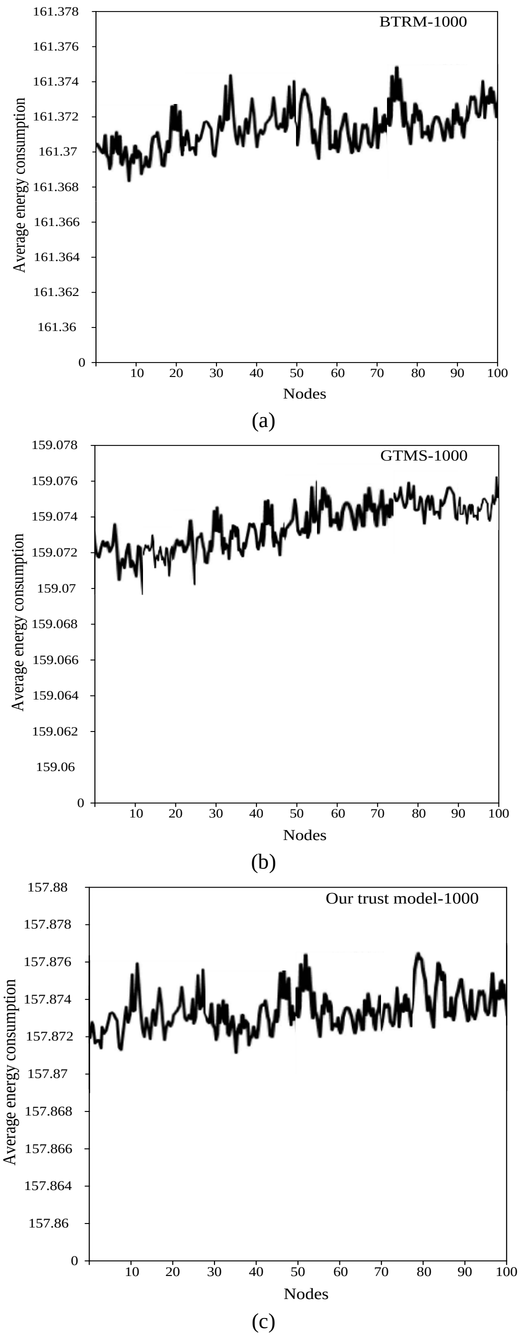


Fig. 3. Trust prediction example of dynamic profile. Top: prediction of discrepancies. Bottom: prediction of trust.



(a)

(b)

(c)

Fig. 4. Average energy consumption at each node: (a) BTRM (b) GTMS (c) Our trust model.

V. Conclusions and Future

In this paper, we have described a distributed trust model in a mobile computing environment based on a set of useful observations about a user behavior. The proposed trust model is particularly appealing to mobile computing environments as it is extremely light-weight, both in terms of memory requirements and computational load. The kind of way greatly avoids heavy interactions that may be required by some existing trust management solutions. New observations are fed in by means of a set of recursive mathematical equations that can be efficiently computed in order to increase the accuracy of the prediction. Developing such a distributed trust model is significant for a mobile device, as we cannot assume the existence of a trusted third party that can be contacted on demand to acquire trust information about an entity. In future, we will refine our trust predictor to improve both its accuracy and its human-facet.

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 Helen Lowe, "Dynamic trust models for ubiquitous computing environments," in *Proc. UBICOMP2002-Workshop on Security in Ubiquitous Computing, Göteborg*, Sweden, September 2002.

[2] Z. Yan and S. Holtmanns, "Trust modeling and management: from social trust to digital trust," *Book chapter of Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions, IGI Global*, 2007.

[3] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer ecommerce communities," in *Proc. IEEE International Conference on E-Commerce*, San Diego, CA, July 2003, pp. 228-229.

[4] C. English and S. Terzis, "Gathering experience in trust-based interactions," in *Proc. 4th International Conference on Trust Management*, 2006.

[5] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Transactions of the ASME - Journal of Basic Engineering*, vol. 82, pp. 35–45, 1960.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] H. Chen, H. Wu, X. Zhou, and C. Gao, "Agent-based trust model in wireless sensor networks," in *Proc. 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007, pp. 119-124.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

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 a 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.