Featuring Trust and Reputation Management Systems for Constrained Hardware Devices

Rodrigo Roman
Dpt. of Computer Science
University of Malaga
29071, Malaga, Spain
roman@lcc.uma.es

M. Carmen Fernandez-Gago
Dpt. of Computer Science
University of Malaga
29071, Malaga, Spain
mcgago@lcc.uma.es

Javier Lopez
Dpt. of Computer Science
University of Malaga
29071, Malaga, Spain
jlm@lcc.uma.es

ABSTRACT

Research on trust management systems for wireless sensor networks is still at a very early stage and few works have done so far. It seems that for those works which deal with the topic general features of how these systems should be are not clearly identified. In this paper we try to identify the main features that a trust management system should have and justify their importance for future developments.

Keywords

Trust Management, Sensor Networks

1. INTRODUCTION

Trust is an important factor in any network that deals with the uncertainty about the future behaviour of some participants on the network. Thus, trust becomes essential in the decision-making process.

In recent years wireless sensor networks has been widely used in many real-life scenarios due mainly to their autonomous capabilities or their potential to self configure. As in any network, trust is also crucial for wireless sensor networks (WSN in the following), for instance, for a node to determine whether another node in the network is the appropriate to perform a common goal. However, wireless sensor networks present some constraints such as energy-consuming or computational power that makes difficult for them to use some existing trust management systems specific for similar networks such as Ad-Hoc pr P2P networks.

In fact, the development of trust management systems for WSN is a very new area of research and not much work have been done so far [10, 26, 34, 33] (these are some examples of works devoted to the problem of trust for WSN). However, all of these works tend to design a suitable trust management system for a specific application and making some assumptions on the constraints about the network. Although the structure of a sensor network is largely influenced by its application, it is also necessary to review which could be the common features for any scenario.

In this paper, we try to identify which are the general features that a trust management system should possess in order to cover all the possible security problems that a trust management system for WSN could solve. The paper is organized as follows. Trust management systems for related areas is surveyed in Section 2. We give an overview of the concept of sensor networks and the importance of trust for them in Section 3. We identify the main features that a trust management system for WSN should have in Section 4. Section 5 concludes the paper.

AUTONOMICS 2007, 28-30 October 2007, Rome, Italy

DOI 10.4108/ICST.AUTONOMICS2007.2260

2. RELATED WORK

The term trust management was first coined by Blaze et al. [5] as an attempt to build a coherent framework for security policies, credentials and trust relationships.

Usually trust management systems are classified into two main categories: *credential and policy-based trust management systems* and *behaviour-based trust management systems*

The main goal of *credential and policy-based trust management systems* is to enable access control. Thus, peers in these systems verify credentials of other peers in order to establish trust decisions about other peers. These type of systems do not require the need of the requesting peer to establish trust on the resource owner. These systems are suitable for those applications which assume implicit trust in the resource owner. PolicyMaker [5], its successor KeyNote [4] and REFEREE [7] are credential-based trust management systems.

Behaviour-based trust management systems are mainly based ont he concept of *reputation*. Abdul-Rehman and Hailes [1] define reputation as an expectation about an individual's behaviour based on information about or observations of its past behaviour. Jøsang et al. [11] define reputation as a mean of building trust; one can trust another based on its good reputation. Reputation-based trust management systems provide mechanisms from which a requesting node can evaluate trust on another node based on global reputation of the peer or its perception on the evaluating peer. SPORAS, HISTOS [32] or REGRET [20] are examples of reputation-based trust management systems.

Research in the area of trust management and reputation systems for WSN is at an early stage. However, more efforts have been made in related areas such as Ad-Hoc and P2P networks. The routing process in Ad-Hoc networks is consid-

ered in [14] and [30]. In both cases trust values are assigned to the nodes and then by calculations such as averages or a linear function a global trust value is given to a node. Reputation is used in [17]. In this system each node monitors the activities of its neighbours and sends the information to a reputation handling module which is part of a bigger mechanism called the *trust manager* that is in charge of building trust. Concerning P2P networks the mechanisms used in order to derive trust can be several. Thus, Bayesian networks are used in [3, 28]. Other statistics methods such as standard deviation and mean are used in [25]. The approach followed by [2] uses reputation for deriving trust as well as PET [31] that also evaluates risk. Other systems worth to be mentioned are TrustMe [23] that provides anonymity for both the requesting and the hosting peer; EigenTrust [12] and PeerTrust [29]; or NICE [22] where transactions are made by secure exchange of certificates.

The trust management and reputation systems described above are not in general suitable for WSN due mainly to energy-consuming constraints and lack of computational power. A complete analysis of this suitability can be found in [9].

3. SENSOR NETWORKS AND THE IMPORTANCE OF TRUST

3.1 Wireless Sensor Networks: Description and Security Issues

The main purpose of a Wireless Sensor Network (or Sensor Network) is to serve as an interface to the real world, providing physical information such as temperature, light, radiation, and others, to a computer system. Its main elements are the Sensor Nodes and the Base Station. There is a high number of sensor nodes, usually densely deployed, that can sense their surroundings. They also have limited computational capabilities (e.g , include a wireless transceiver, and are powered by batteries. These nodes can can perceive the physical events as they occur, and process and forward this information to the base station. The base station (or sink), a powerful device that controls the entire network, use that information to offer a number of services to an external system. We can abstract a sensor network as a "living being", since its "cells" (sensor nodes) fully cooperate on providing the information that the "brain" (base station) will use.

A sensor node is totally autonomous; no human user controls it, and the only way to access to its information is through the base station. As a result, the node needs to self-configure and maintain itself during the lifetime of the network. A sensor network can function for long periods of time, ranging from several days to one or two years. Regarding the functionality of the node, and due to its inherent constraints, it can only implement a simple and predefined set of protocols. Such protocols implement the basic functionality of the network (e.g. routing, aggregation, and time synchronization), and may also implement some additional capabilities (e.g. over-the-air programming, node location).

Since sensor networks is a young technology there are many interesting research problems, like development of models and tools for the design of better WSN architectures, elaboration of standard protocols adapted to work robustly on certain scenarios, etc. However, one of the most important issues that remains mostly open is *security* [27]. Sensor nodes are highly constrained in terms of computational capabilities, memory, communication bandwidth and battery power. Additionally, it is easy to physically access the nodes because they must be located near the physical source of the events, and they usually are not tamper-resistant due to cost constraints. Furthermore, any device can access the information exchange because the communication channel is public.

As a result, any malicious adversary can manipulate the sensor nodes, the environment, or the communication channel for its own benefit. For these reasons, it is necessary to provide the sensor network with basic security mechanisms and protocols that can guarantee a minimal protection to the services and the information flow, while assuring that the network is capable of being self-sufficient. This means to provide protection on the hardware layer, the communication stack, and the core protocols. In other words, (i) it is necessary to protect the hardware of the nodes against attacks, (ii) the communication channels must meet certain security goals (like confidentiality, integrity and authentication), and (iii) the core protocols of the network must be robust against any possible interferences. Other mechanism that can help the network to manage itself autonomously and securely are the trust management systems.

3.2 Trust and Sensor Networks

Trust is a very important factor in the decision-making processes of any network. Also, one of the main reasons for the existence of trust management systems is uncertainty, that is, when the outcome of a certain situation cannot be clearly established or assured. Uncertainty originates basically from two sources [24]: information asymmetry (a partner does not have all the information it needs about others), and opportunism (transacting partners have different goals). On the context of sensor network, opportunism is not a problem. All the elements of the network work towards the same goal, and they have neither reason nor the will to behave egoistically. On the other hand, a sensor node does not have information regarding others that will allow it to know in advance how a transacting partner is going to behave. Therefore, there is some information asymmetry that the node must deal with.

Since all nodes belong to the same "living being", it is possible to think that the existence of information asymmetry is not a real problem. When a sensor node chooses a partner to collaborate with, such partner is supposed to be honest and fully collaborative. However, this is not entirely true. As well as living beings are affected by illnesses, sensor networks can suffer the attack of malicious nodes or the existence of faulty nodes. As a result, uncertainty in sensor networks is a problem that must be dealt with. Trust Management becomes an important tool for securing a long-lived sensor network, allowing its autonomous nodes to avoid "dubious nodes" that can affect the overall functionality and to choose the "best partner" for a certain operation.

The current solutions available for trust management systems for sensor networks sometimes deal with the problem of uncertainty and consider it as an important part of the process of measuring trust. In [21] the authors propose a group-based trust management system called GTMS where the nodes of a sensor network falls into trusted, untrusted or uncertain nodes group depending on the value assigned by the base station. Certainty is considered in [6] in order to derive first, a reputation space and after this a trust

space. The watch dog mechanism is used to obtain the reputation values from observations or first-hand information. This works uses of a watchdog mechanism, like many other works such as [10]. The reputation management system developed by Ganeriwal et al is based on bayesian formulation.

The idea of organizing the nodes of a sensor network into clusters is also used in order to develop a reputation or trust management systems. Zhang et. al [33] use this method for the aggregation problem. In this case they consider the problem of nodes acting as 'aggregators' responsible for aggregating data and reporting information to the cluster head. This information is gathered in the form of reputation values. Setting a threshold for the reputation values the aggregator is able to determine whether the other nodes are compromised. The problem of selecting a malicious or compromised node is addressed in [8]. This work introduces a mechanism for electing the cluster head in a wireless sensor networks. A specific application of trust a management framework for sensor networks can be found in [19] where the system detects fault or malicious sensors in industrial facilities. Also in order to locate malicious or misbehaving nodes Tanachaiwiwat *et al* [26] propose a location-centric architecture for isolating misbehaviour and establishing trust routing in sensor networks. Trust values are calculated as a function of cryptography, availability and packet forwarding. If a value is below a specific threshold the node is considered insecure and it is isolated. In this work the traffic flow is from/to the base station. One of the latest approaches of trust management for wireless sensor networks is introduced in [34]. They propose a framework similar to existing approaches for Ad-hoc networks where trust values are assigned to each node.

4. FEATURES OF TRUST MANAGEMENT SYSTEMS FOR WSN

As explained in the previous section, there have been many solutions that try to solve the problem of applying trust values to decision-making processes in wireless sensor networks. Although their underlying architecture is similar, there are some important features and problems that are taken into account in some solutions, but partially or completely ignored in others. Even more, some specific issues like the initialization of reputation and trust are, in most cases, neglected. For the development of a specialized trust management system, adequate for sensor network environments, it is necessary to review and point out the features such system should have, alongside with the open problems that need further research. This is the task of this section.

4.1 Architecture and Components

The overall architecture of a trust management system that infers reputation and trust through observation is shown on Figure 1. In this architecture, the trust entity is the component that is in charge of managing the reputation and trust. The first task of any trust entity is to obtain information about the behaviour of the members of its neighbourhood, either through observation and experience (i.e. "first-hand information") or by sharing the observed events with other entities (i.e. "second-hand information"). After this process, the "reputation manager" can use this list of events to infer and store the reputation of the members of its neighbourhood. Such reputation will be later used by the "trust manager" to obtain the trust values. They can be used to decide which is the best partner for a certain operation, or discover if one entity is behaving maliciously. Both, reputation and trust, need to be maintained and updated during the lifetime of the network.

This architecture is clearly applicable to wireless sensor networks, because a sensor node can obtain information about its surroundings either directly or indirectly. In addition, the sensors have limited computational capabilities. Consequently, by using lightweight algorithms, they can be able to infer the reputation of its neighbours and decide if they trust them for certain operations. In fact, the architecture had been applied by most of the existing research on trust management system, although only a few of those works take reputation explicitly into account [6, 10, 33]. Still, having both reputation and trust in the same system is important. By not calculating the trust directly from the behaviour of a node, it is possible to better handle aspects such as the evolution of the node, aging, etc.

Once the architecture has been introduced, it is time to define where the trust entities should be located. That is: Which nodes need the trust values? In a wireless sensor network, all the sensor nodes do. All sensor nodes participate on the protocols that support the network, such as routing. The decisions regarding the execution of the protocols (e.g. who could be the next node in the routing path when transporting an "Out-of-Band" message) are usually made by the nodes on their own, and in exceptional situations with the help of its direct neighbourhood (e.g. when clustering a flat network, or when aggregating some data). Finally, faulty and/or malicious nodes may appear on any part of the network. Therefore, nodes need to know whether they can trust their neighbourhood in order to deal with uncertainty. Note that even in the case of a clustered network, the nodes need also to ensure that their cluster head can be trusted.

Sensor nodes are not the only members of the network that can take advantage of trust, as pointed out by Tanachaiwiwat [26]. Due to its role as a network manager and data repository, the base station receives information from all the nodes in the network. As a result, its information asymmetry is reduced: it has a global point of view of the state of the network, whereas sensor nodes can only manage to observe their immediate surroundings. The base station can take advantage of this wealth of information to observe and analyze the behaviour of its nodes, storing their reputation and making global trust decisions. Although it cannot directly influence over the behaviour of the nodes, it can issue orders that those nodes must fulfill.

4.2 Initialization and Information Gathering

Before the entities in the nodes and the base station can start measuring the trust of their neighbourhood, it is necessary to initialize adequately the trust and reputation values. This, which could be seen as a problem, is not that important. Before deployment, sensor nodes are programmed in a controlled environment by the network manager, with similar tasks and services. Thus, at the beginning or their life they can be completely trusted: Their hardware is supposed to be tested for failures before deployment, and also at this stage any malicious adversary had neither the time nor the chance to influence or subvert a node. Reputation is built over time, using the behaviour of the nodes as a feedback. Initial reputation should not affect negatively both

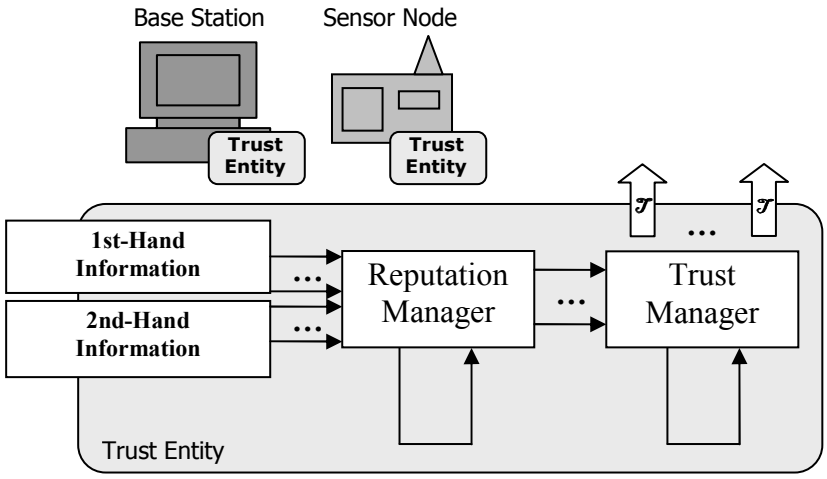

Figure 1: Overall Architecture of a Trust Management System for Sensor Networks

trust and the decisions taken by the nodes. Note that other systems tend to link initial reputation and trust values with authenticating the nodes. However, in a realistic sensor network setting, any node with no credentials should be expelled from the network, since the communication channel needs to be protected with cryptographic primitives due to its public nature.

After the network starts functioning, the nodes will provide its services, and the trust management system will be able to start gathering "first-hand" and "second-hand" information from its direct neighbourhood. The monitoring process that gathers "first-hand information" must obtain general information from the behaviour of the nodes, but also specific information related to the particular instances of the protocols used in the network. The sources of general information have been discussed in previous research [9], and some studies specify how to handle particular protocol information (cf. aggregation by Zhang et.al. [33]). Still, there is the need for more research on this matter.

Regarding "second-hand information", distributing the reputation information about other nodes is a extremely important property of trust management systems [18]. However, mainly due to the possible existence of subverted nodes, a trust entity for sensor networks also faces the problem of integrating honest reports. The inherent redundancy of sensor networks can help to develop a robust sharing algorithm, since the existence of a malicious report (e.g. a bad-mouthing attack) that is not coherent with the state of the neighbourhood is a clear indicative of a malicious presence.

On this information gathering process, it is important to note that a source of second-hand information can be a sensor node accusing itself of being malicious. Following the simile of the "living being", this entire process is similar to the concept of *apoptosis*, when a cell suicides due to malfunctioning, virus infection, or other reasons [13]. Due to the embedded intelligence of a sensor node, it can detect whether its batteries are low, its readings are inconsistent with its neighbourhood, or its transceiver seems to not work. On discovering these issues, the sensor node can try to alert its neighbourhood about its state. This situation can also be reported to the base station: A malfunctioning sensor node can be recovered and subsequently repaired by a human operator.

As with all second-hand information, it is possible for a malicious adversary to try to take advantage of this apoptosis process. It can fake the message with the purpose of alerting that a healthy, trusted node, has an internal problem. However, if all these messages are sent using an authenticated channel (e.g. using techniques such as μTESLA [16] or public key cryptography [15]), the only option left to the adversary is to use its subverted nodes to accuse themselves of being malicious. Even if such case occurs, this is counterproductive for the adversary: it will alert the network and the base station about its existence.

4.3 Information Modeling

Once the information, either "first-hand" or "second-hand", has been gathered, the trust entity can calculate and update the existing reputation values. Due to its memory constraints, a sensor node cannot store all the events that its neighbours produce during its lifetime. Therefore, it is necessary to create a lightweight reputation manager that could capture and efficiently store the behaviour of other entities in the previous interactions, while being able to update it with new information if possible. Moreover, such policy has to take into account that some events can have more influence on the reputation of a node. For example, selective forwarding is a clear indicative of malicious activity.

The dimension of a sensor network as a balanced "living being", that should have none or little deviation from its behavioral patterns, must be taken into account while updating the reputation values. This dimension also affects the aging of reputation. A node that acts maliciously in the context of a sensor network will most surely keep such evil behaviour in further interactions. Therefore, "bad" reputation should not be forgotten easily. The evolution of the reputation is also an important factor that a node cannot ignore, and a trust entity should remember if a node achieved high "bad" reputation ratings on the past.

An issue that surfaces at this point, and that has been usually neglected by other existing works, is the granularity of the trust management system. As aforementioned, the reputation of a certain node is built according to its behaviour and the events it triggers. Most systems simplify the rep-

utation into one single set of values. However, the actions of the nodes are not reduced to the execution of one task. For example, a node can read the physical measurements of its environment using the sensors, and route information to the base station, amongst others. A node needs to maintain separate opinions about the existing actions of their peers, thus it needs a different set of reputation values. A consequence of this fact is the need of linking the existing events with the different reputation values they influence.

The existence of different reputation values also implies the existence of different trust values. A specific trust value (e.g. sensing) will help the node to decide about the possible outcome of a specific interaction with another peer. On the other hand, that value cannot be used in most cases to deduce what the peer could do in a different task (e.g. routing). For example, a node that reports inconsistent values or has flagged itself using apoptosis with "broken sensors" cannot be trusted as a source of data, but it can be trusted as a message forwarder during the routing process.

The last part of the trust entity that needs to be covered is the trust manager. This module is in charge of calculating a certain trust measurement of a node using as an input its existing reputation, and providing the trustor with a measurement that can help it to take a decision over a certain trustee. For a single node, the different reputation values should be weighted and combined according to the risk of the interaction between the trustor and the trustee, and according to the importance of the reputation value and that specific interaction. Risk and importance influence when calculating the trust, but they also influence when selecting the threshold. That is, when a certain trust value labels a trustee as "trusted" or "untrusted" for a certain operation. There are other, non-exclusive ways to use the trust values, such as when one trustor have to choose over a group of trustees.

5. CONCLUSIONS

The development of trust management systems for WSN is a new area of research. As such, most of the important features that such a system should possess have not been identified or dealt with in the current literature. In this paper, we have identify some of these important features. We believe the main problems to be considered in order to tackle uncertainty is opportunism and information asymmetry. As opportunism is not a problem on WSN, we believe that the information gathered, first or second-hand information is crucial as the assigning or calculating of reputation or trust values depend on them. On this information gathering process we have highlighted how these should be carried out in order to provide meaningful outputs of reputation and trust. We have also point out the importance of how this information is updated as well as the granularity of the information gathered.

6. ACKNOWLEDGMENTS

This work has been partially supported by the project SMEPP (EU-FP6-IST 0333563), funded by the European Commission, and CRISIS (TIN2006-09242), funded by the Spanish Ministry of Education. Also, the first author has been funded by the Spanish Ministry of Education under the "Programa Nacional de Formacion de Profesorado Universitario".

7. REFERENCES

[1] A. Abdul-Rahman and S. Hailes. Supporting Trust in Virtual Communities. In *Proceedings of the 33rd Hawaii International Conference on System Sciences*, 2000.

[2] K. Aberer and Z. Despotovic. Managing trust in a peer-2-peer information system. In H. Paques, L. Liu, and D. Grossman, editors, *Proceedings of the Tenth International Conference on Information and Knowledge Management (CIKM01)*, pages 310–317. ACM Press, 2001.

[3] T. Bearly and V. Kumar. Expanding Trust Beyond Reputation in Peer to Peer Systems. In *15th International workshop on Database and Expert Systems Applications (DEXA'04), IEEE Computer Society*, 2004.

[4] M. Blaze, J. Feigenbaum, and A. D. Keromytis. KeyNote: Trust Management for Public-Key Infrastructures (position paper). *Lecture Notes in Computer Science*, 1550:59–63, 1999.

[5] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *IEEE Symposium on Security and Privacy*, 1996.

[6] H. Chen, H. Wu, X. Zhou, and C. Gao. Reputation-based Trust in Wireless Sensor Netwoks. In *In Proceedings of the 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*, 2007.

[7] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust Management for Web Applications. *Computer Networks and ISDN Systems*, 29:953–964, 1997.

[8] G. V. Crosby, N. Pissinou, and J. Gadze. A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks. In *In Proceedings of the Second IEEE Workshop on Dependability in Sensor Networks and Systems (DSSNS'06)*. IEEE Computer Society, 2006.

[9] M. C. Fernandez-Gago, R. Roman, and J. Lopez. A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks. In *In Proceedings of the 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)*, Istanbul (Turkey), July 2007.

[10] S. Ganeriwal and M. B. Srivastava. Reputation-Based Framework for High Integrity Sensor Networks. In *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks.*, pages 66–77, Washington, DC, USA, 2004.

[11] A. Josang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 2006.

[12] S. D. Kamwar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International Conference on World Wide Web (WWW'03)*, ACM Press, pages 640–651, Budepest, Hungary, 2003.

[13] A. Lawen. Apoptosis – An Introduction. *BioEssays*, 25:888–896, 2000.

[14] Z. Liu, A. W. Joy, and R. A. Thompson. A Dynamic Trust Model for Mobile Ad-hoc Networks. In *10th*

IEEE International Workshop on Future Trends of Distributed Computing Systems, pages 80–85, Suzhou, China, May 2004.

[15] J. Lopez. Unleashing public-key cryptography in wireless sensor networks. *Journal of Computer Security*, 14(5):469–482, 2006.

[16] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. Spins: Security protocols for sensor networks. In *Proceedings of Mobile Computing and Networking (MOBICOM'01)*, 2001.

[17] Y. Rebahi, V. E. Mujica-V, and D. Sisalem. A Reputation-Based Trust Mechanism for Ad-hoc Networks. In *10th IEEE Symposium on Computers and Communications (ISCC 2005)*, 2005.

[18] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation Systems. *Communications of the ACM*, 43(12), 2000.

[19] T. Ryutov and C. Neuman. Trust-based Approach for Improving Data Reliability in Industrial Sensor Networks. In M.-S. B. S. Etalle, S., editor, *In IFIP International Federation for Information Processing, Trust Management*, volume 238, pages 349–365, 2007.

[20] J. Sabater and C. Sierra. REGRET: A Reputation Model for Gregarious Societies. In *Fourth Workshop on Deception Fraud and Trust in Agent Societies*, ACM Press, 2001.

[21] R. A. Shaik, H. Jameel, S. Lee, S. Rajput, and Y. J. Song. Trust Management Problem in Distributed Wireless Sensor Networks. In *12th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06)*, IEEE Computer Society, 2006.

[22] R. Sherwood, L. Seungjoon, and B. Bhattacharjee. Cooperative peer groups in nice. *Computer Networks*, 50(4):523–544, 2006.

[23] A. Singh and L. Liu. TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems. In *Third International Conference on Peer-to-Peer Computing (P2P'03)*. IEEE, 2003.

[24] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei. Reputation and Trust-based Systems for Ad Hoc and Sensor Networks. In A. Boukerche, editor, *On Trust Establishment in Mobile Ad-Hoc Networks*. Wiley & Sons, 2007.

[25] N. Stakhanove, S. Basu, J. Wong, and O. Stakhanov. Trust Framework for P2P Networks using Peer-Profile based Anomaly Technique. In *25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'05)*. IEEE, 2005.

[26] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy. Location-centric Isolation of Misbehavior and Trust Routing in Energy-Constrained Sensor Networks. In *IEEE COnference on Performance, Computing and Communications*, pages 463–469, 2003.

[27] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. Wireless sensor network security - a survey. In Y. Xiao, editor, *Security in Distributed, Grid, Mobile, and Pervasive Computing*. Auerbach Publications, CRC Press, 2007.

[28] Y. Wang and J. Vassileva. Trust and Reputation Model in Peer-to- Peer Networks. In *Third International Conference on Peer-to-Peer Computing (P2P'03)*, 2003.

[29] L. Xiong and L. Liu. Peertrust: Supporting reputation-based trust for peer-to peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):843–857, 2004.

[30] Z. Yan, P. Zhang, and T. Virtanen. Trust Evaluation Based Security Solutions in Ad-hoc Networks. In *NordSec 2003, Proceedings of the Seventh Nordic Workshop on Security IT Systems*, 2003.

[31] W. S. Z. Liang, and. PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing. In *38th Hawaii International Conference on System Sciences*, 2005.

[32] G. Zacharia and P. Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(9):881–907, 2000.

[33] W. Zhang, S. Das, and Y. Liu. A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks. In *In Proceedings of the IEEE SECON 2006*, Reston, VA, September 2006.

[34] Z.Yao, D. Kim, I. Lee, K. Kim, and J. Jang. A Security Framework with Trust Management for Sensor Networks. In *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pages 190–198, 2005.