A Trust Based Routing Scheme for Wireless Sensor Networks

Aveek Chakrabarti, Vishal Parekh, and Atin Ruia

Department of Computer Science and Engineering
Jadavpur University, India
{aveek.chakrabarti,vishal.jucse,atinruia.jucse}@gmail.com

Abstract. Wireless Sensor Networks are often deployed in unattended and hostile environments. These networks are susceptible to harsh physical conditions and attacks from adversaries. Sensor nodes have limited power, memory and computational ability and thus are vulnerable to capture. A few malicious adversaries can easily compromise sensor devices and inject false data to disrupt the integrity of the network. In this paper, we address this problem by proposing a three tiered architecture established upon a trust based framework which distinguishes illegal nodes from legal ones and filters out deceitful and forged data. Simulation results demonstrate that our trust based framework is an efficient approach to identify the trustworthiness of data.

Keywords: Wireless sensor network, Trust, Routing, Key management.

1 Introduction

Sensor nodes or motes are small devices with limited computing, communication and sensing capabilities. These nodes are typically deployed randomly over a specific area. They form an unattended wireless network, collect data, partially aggregate them and then sends this data to a base station for further processing. The deployment of sensor networks may contain tens to thousands of resource constrained nodes functioning collaboratively to perform a function [1]. Sensor nodes have applications in various areas such as – emergency response networks, energy management, logistics, medical, wildlife and climate monitoring, inventory support and battlefield management.

With the advent of new technology, sensor networks play a vital role in the age of pervasive computing, as personal mobile devices interact with sensor networks. However, security concerns constitute a potential stumbling block to the impending wide deployment of sensor networks. As sensor networks have mission-critical tasks, it is clear that security needs to be taken into account at design time. In an unattended and hostile environment, wireless sensor networks (WSNs) are vulnerable to various attacks such as physical node capture, eavesdropping and other sophisticated attacks [6]. As the main aim of WSNs is to gather sensory data an imminent threat from compromised nodes is the injection of false data. A major purpose of an attacker is to make the entire or partial network impractical or to gain control over individual

N. Meghanathan et al. (Eds.): CCSIT 2012, Part I, LNICST 84, pp. 159–169, 2012.

nodes. If an attacker gains control of a node it may send incorrect data, try to disrupt the transmission of aggregate data or not send any data at all.

In this paper we have proposed a systematic approach to identify the compromised nodes in a WSN and to circumvent these corrupted elements in order to ensure that the integrity of the network is not lost. This is done by calculating the trustworthiness or reputation of each element of the network which serves as a measure to gauge the credibility of that element. This trust value changes according to the data sent by each element. A three-tiered hierarchal architecture has been proposed and no assumptions have been made regarding which of the components can be compromised. The simulation results show that the proposed approach provides a constructive method for identifying corrupt nodes.

The rest of the paper has been organized as follows – Section 2 provides the related works. Section 3 describes the proposed network architecture with the trust based framework being explained in Section 4. Section 5 gives the experimental results and Section 6 concludes the article.

2 Related Work

There exists a large number of methods for securing aggregated information in literature. The basic approaches for security are to use Message Authentication Codes (MACs) and probabilistic key distribution schemes [7-8]. [10] and [11] proposes schemes to detect the compromised nodes by monitoring reported data. However in the schemes proposed in these papers the trust values of an entire network are stored by all the sensors of the network. These values are periodically circulated among themselves. This unnecessarily increases the network traffic and increases the workload on the sensors. There are centralized trust based systems for Internet such as [13]. These systems keep reputation values at a centralized trusted authority and therefore they are not feasible in wireless sensor network domain. Decentralized trust development systems are studied in mobile and ad-hoc networks [14]. These trust development systems are game theory based and try to counter selfish routing misbehavior of nodes by enforcing nodes to cooperate with each other. A trust based framework has been proposed in [12] which evaluates the trustworthiness of sensor nodes by extracting statistical characteristics from gathered information. However in this paper the sensor nodes have to take part in validation of aggregate nodes as well as send their sensed results. These nodes are typically low power nodes and the assignment of so much responsibility to these nodes is not feasible.

3 Network Architecture

Figure 1 depicts the network architecture in which we have implemented our scheme. Despite the popularity of flat wireless sensor networks, recent studies have revealed several limitations in these kinds of networks [2]. Flat networks have also been shown to have capacity limitations, and one approach to address this drawback is to employ a hierarchical architecture. In [3], it has been observed, when using the same amount of sensor nodes in a given coverage area for flat and hierarchical topologies, that the system throughput capacity increases, while system delay decreases. The main reason

for these improvements is the reduced number of hops since most sensor data are destined for the Internet, which is reachable in a few hops in the hierarchical approach. Thus, we have implemented our scheme based on a hierarchical structure.

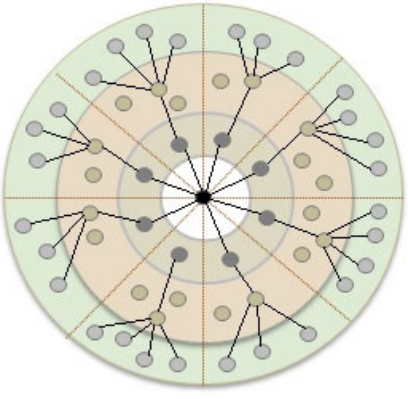

Fig. 1. Three tiered clustered architecture

In this paper we have used a three-tier clustered architecture. The sensor network is composed of densely deployed sensors which are organized into clusters. These clusters can be formed using an algorithm such as LEACH [4]. This architecture consists of three types of wireless devices: low power sensor nodes, aggregate nodes and cluster heads. The sensor nodes are responsible for sensing events and reporting these events to an aggregate node. As the name suggests, the aggregate node receives data from a certain number of sensors and aggregates this data into a single packet which is then forwarded to the cluster head. The cluster head receives data from all of the aggregate nodes within its cluster and forwards all of this data to the base station.

In Figure 1 the hierarchy of the WSN is shown. The entire network is partitioned into clusters. The node at the centre is the base station. The nodes situated one hop away from the base station are the cluster heads. Each of these nodes acts as a gateway to the base station for all the nodes in the cluster. The nodes present at the next hop are the aggregate nodes which relay the data sent by the sensor nodes to the cluster head. The nodes present at the last hop are the sensor nodes. These nodes report their sensed data periodically or by demand.

The three categories of nodes differ mainly in power, computation ability and communication. The sensor nodes are low power nodes with low computational power. The aggregate nodes are high power nodes. However as they are only responsible for forwarding data to their cluster heads, which are not located very far away, they do not require high computational ability. Cluster heads are nodes having the highest power capacity and also high computational power. The sensor nodes only communicate with the aggregate nodes. It is not required for them to be aware of the other sensor nodes or of the cluster head. The aggregate nodes communicate with both sensors and its cluster head. However, it is not aware of the base station. The cluster head can communicate with the aggregate nodes within its cluster and with the

base station. Each cluster head is associated with a forwarding node. This node is only responsible for relaying data from the cluster head to the base station.

Certain assumption have been made about the network –

- The Base Station is fixed and may be located far away from the sensor network. The distances between the sensors are much smaller as compared to the distance between the sensor nodes and the Base Station.
- The sensor nodes are static and energy constrained with a uniform initial energy allocation.
- Initially none of the nodes are corrupt.
- Each sensor node is assumed to be either in transmitting mode, receiving mode or in sleep mode. It has been assumed that energy spent by the node in sleep state is negligibly small as compared to the amount spent while being in transmitting or receiving mode.

4 Trust Based Framework

In this section we discuss the framework and the functions of each step of the framework. A large number of sensor nodes are deployed densely in an area to form a wireless sensor network. These nodes are then partitioned into clusters using algorithms such as [4]. A cluster head is selected for each cluster. There may be more than one cluster head within a single cluster but only one such node will be active at any point. The cluster head will randomly select the aggregate nodes that are to be powered on. Each sensor node must be able to send data to at least one active aggregate node at all times. There will be more aggregate nodes present within the cluster but these will remain passive until activated by the cluster head.

4.1 Key Establishment

In critical applications, using incorrect or maliciously corrupted data can have disastrous consequences. Security services are essential to ensure the authenticity, confidentiality, freshness, and integrity of the critical information collected and processed by such networks. The authentication of the data source as well as the data is critical since adversaries might attempt to capture sensors and tamper with sensor data. A popular method for ensuring that the data sent by a node cannot be corrupted is encryption. Encryption is the process of transforming data to using a secret key or cipher. This makes the data it unreadable to anyone except those possessing special knowledge i.e. the key. The result of this process is encrypted data. At the other end the message is decrypted using the shared key to obtain the original message.

For two nodes to set up a secret and authenticated link, they need to establish a shared secret key. The key establishment problem studies how to set up secret keys between a pair of nodes in the network. A class of random key pre-distribution techniques that address the problem of key establishment has been discussed in [7-9]. Each sensor node shares a secret key with the base station. Whenever a sensor node sends data to an aggregate node it uses this key to encrypt the message it sends. This prevents eavesdropping and ensures that the aggregate node or the cluster head cannot

tamper with the data and send incorrect readings. The sensor node forms a message with its id and its sensed reading. It then encrypts this message and sends it to an aggregate node which in turn forwards this message to the cluster head. Neither of these two nodes has the secret key and so they cannot decrypt this message. Thus they cannot intentionally change the data sent by the sensor node. If either the aggregate node or the cluster head try to alter the data, it can be easily recognised by the base station, as the changed data will produce gibberish or meaningless data on being decrypted.

4.1.1 Routing

The sensor nodes send data to the aggregate nodes at specific intervals of time. The sensors of a cluster encrypt their sensed data and send the encrypted message to one of the aggregate nodes in its cluster along with its id. An aggregate node accumulates all the data it receives from all of the sensors reporting to it and forwards it to the cluster head. The cluster head receives this message from all the aggregate nodes within its cluster and then forwards it to the base station. This operation within a cluster has been illustrated in Figure 2. An attacker may compromise a node at any level. Each attack must be detected and dealt with before the integrity of the data of the entire cluster is lost.

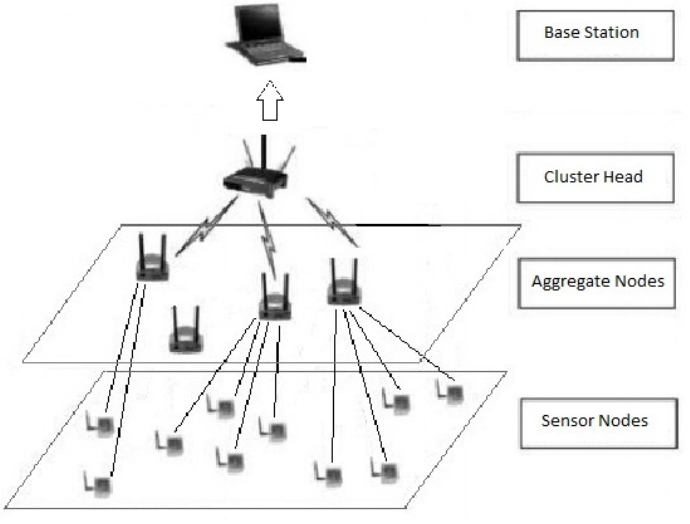

Fig. 2. Routing within a cluster

Sensor Node – If an aggregate node does not receive any data from a sensor node it sends all 1s in the corresponding field for that sensor in its message to signify an error. The base station maintains a trust index for all nodes in the sensor network. The trust value for a particular node gives the reputation of that node to the base station. The base station gives weightage to the data it has received from that node according to this value and changes its trust according to the data it receives. If the base station

detects incorrect data sent by a node the trust value for that node is decreased. In the same way receiving correct data from a node increases its trust value. The decrease in the trust value of a node on receiving incorrect data is more than the increase in case of receiving correct data. Thus the reputation of a node decreases rapidly when it sends incorrect data but increases slowly for correct data. The method for calculating the change in trust values has been explained in the next section.

Aggregate node – If an aggregate node is compromised it could change the values of one or more of the fields of the message it sends. However as the aggregate node does not know any of the secret keys shared by the base station and the sensor nodes it cannot meaningfully change the values sent by the individual sensors. It can at most change some random bits of the message which it has received. This would transform the message into gibberish making it meaningless. On decrypting this message the base station could detect the change as the message will not make any sense. Thus the base station will be able to determine that the aggregate node has been compromised. The base station also keeps a trust value for all the aggregate nodes in the WSN. On receiving an incorrect message from any aggregate node it will decrease the trust value of that node. Once the trust value of a particular aggregate node is lowered beyond a threshold value then that aggregate node is deemed to be corrupt. When this occurs, the base station informs the cluster head. The cluster head switches off the compromised aggregate node and switches on one of the remaining passive aggregate nodes present within that cluster. For this purpose there are multiple aggregate nodes in the cluster of which some are kept passive. The base station updates the trust value of the new aggregate node and the cluster head broadcasts the id of the new node to all the sensors which were reporting to the previous one.

Cluster head – Each aggregate node also evaluates the honesty of its cluster head. The aggregate nodes can overhear the message sent from the cluster head to the base station. It in turn compares the fields of this message which it has sent, with the data which it had itself sent to the cluster head. If the corresponding fields do not match then the aggregate node deems the message sent by the cluster head to be dishonest. Each aggregate node stores a trust value for the cluster head. When this value is lowered below a threshold value then that aggregate node makes a vote to change the cluster head. When the majority of the aggregate nodes within a cluster vote for a change, the cluster head is deemed to be compromised. The aggregate nodes have the ability to switch off a cluster head and switch on one of the passive cluster heads present in the cluster. There are multiple cluster heads present in each cluster for this purpose. However, only one cluster head will be active at any particular time. The new cluster head informs the base station of the change and each aggregate node updates its trust value for the cluster head.

4.1.2 Trust Evaluation

The trust value denotes the confidence or reputation of one node with respect to another. In the proposed scheme the base station keeps track of the trust values or reputation of all the sensor nodes and aggregate nodes in the network while the aggregate nodes of a cluster keep track of trust values of its cluster head. The trust values change according to certain factors –

a. **Battery** – The battery factor represents the remaining lifetime of a node. We have chosen the discrete radio model [5] for estimating the power consumption of each node during the transmission and reception of data. This model is used for calculating power consumption and determining which links between sensor motes are available for transmission.

We have assumed that when a node is compromised, its battery usage is greater than an incorrupt node. This is because a compromised node will be executing extra lines of code and tries to interfere with the data sent by other nodes. Thus if the remaining battery of any node is much lower than the average remaining battery of the other sensors then that node has been compromised. Thus the battery factor of any sensor node in the WSN is given by:

$$\mathbf{b}_f = \left\{ b - \left(\frac{\sum_{i=1}^{n} bi}{\mathrm{n}} \right) \right\} / b \tag{1}$$

where, b_f is battery factor of the sensor node, b is the remaining battery of that node and n is the number of nodes. The value of b_f can range from 1 to -1. A negative value for this node indicates that the node has been using excessive power and hence is corrupt.

b. **Sensing Communication** – A node has a limited sensing range. Any event is said to be detectable if at least one node lies within its observable range. Now, the sensing models of sensor nodes can be broadly classified into two subcategories, the Boolean sensing model and the Probabilistic sensing model. The Boolean sensing model assumes the detection of an event if it occurs within the sensing radius of the node with equal probability (equal to one). However, it is not the case with the probabilistic sensing models, where the probability of detection of an event is a decreasing function of distance of the event from the sensor node.

Each sensor must send a data packet after a certain time interval. A node is deemed to be corrupt if it fails to send a packet within this interval. Thus the failure of a node, to send data, results in the decrease in its trust value. The sensing communication factor of any node in the sensor network is given by:

$$\mathbf{S}c = \frac{\mathbf{S}\mathrm{true} - \mathbf{S}\mathrm{false}}{\mathbf{S}\mathrm{true} + \mathbf{S}\mathrm{false}} \tag{2}$$

where, S_c is the sensing communication factor for a sensor. S_{true} and S_{false} are values which give the number of times an event has been successfully sensed or not by that node. If the sensor node does not send data within the time period S_{false} is incremented by 1 and if it does send information S_{true} is decremented by 1.

c. **Variation** – This factor is used to determine the correctness of the data sent. A sensor node may report numerical values or boolean values. The validity of this data is determined by comparing this data with the data sent by four of its nearest neighbours within its cluster. The co-ordinates of each node in the WSN are stored by the base station. Thus on receiving the data of a sensor node, the base station can compare it with the data of its four nearest neighbours to determine the correctness of the data. The optimum result of any sensor node based upon the values sent by its four nearest neighbours is given by:

$$\text{optimum result of sensor s} = \frac{\sum_{i=1}^{4}(\mathbf{TV}i * \mathbf{distance}i * \mathbf{result}i)}{\mathbf{TV}i * \mathbf{distance}i} \quad (3)$$

where, TV_i is the trust value of sensor node i, $distance_i$ is the distance between sensor i and sensor s and $result_i$ is the result sent by sensor i.

If this optimum result differs by the result sent by sensor s then var_{false} is incremented by 1 or else var_{true} is incremented by 1. The variation factor for sensor s is given by:

$$\mathbf{V}c = \frac{\mathbf{var}true - \mathbf{var}false}{\mathbf{var}true + \mathbf{var}false} \quad (4)$$

Based on all these factors the trust value of a node is changed. The formula for this is given by:

$$\mathbf{TV}new = (\mathbf{TV}old * 0.9) + \left(0.1 * \frac{(\mathbf{b}f * k1 + \mathbf{S}c * k2 + \mathbf{V}c * k3)}{k1 + k2 + k3}\right) \quad (5)$$

Thus using this formula we get the new trust value for a sensor node depending on its old trust value and the three factor factors. The values of the constants k1, k2 and k3 have been taken to be 0.2, 0.3 and 0.4 respectively. The battery of all the sensor nodes decreases with time and thus this factor has the least weightage. If a sensor sends incorrect data the value of the aggregate result could change drastically. As this sensor is trying to manipulate the end result it needs to be identified at the earliest possible moment. Thus the constant associated with variation of data, k3 is assigned the highest value. The sensing constant is assigned a value in between as a failure to report an event will not change the end result considerably. However if a node consistently fails to send data it could be faulty. In that case any data which it does send may not be accurate.

5 Results

In this section a set of simulations are presented to evaluate the performance of our framework against attacks. We have considered a network of twenty sensor nodes in our simulations. Of these twenty nodes four nodes are compromised. A compromised node may send correct or incorrect data. At times it may also send no data. Figure 3 shows the variation of the remaining battery of an uncompromised node and a compromised node with time. Initially the battery of both nodes are at 100 and as the number of iterations increase the battery consumption of the compromised node is observed to be much more than that of the uncompromised one.

Figure 4 shows the variation of the trust values of all the nodes in the network with time. Initially the trust values of all the nodes are 50. With the increase in time, the trust values of the nodes change according to the data it sends. As can be seen from Figure 4 the trust values for nodes numbered 8, 12, 16 and 19 decrease.

The plots for most of the uncompromised nodes overlap each other as they always send correct data and their trust values increase in the same way. As it can be seen from the graph in Figure 4 the trust values of all of the compromised nodes decrease

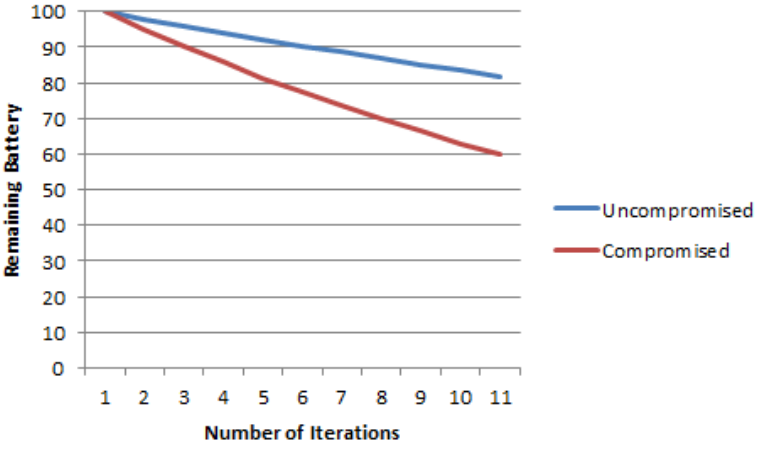

Fig. 3. Trust value of nodes vs. number of iterations

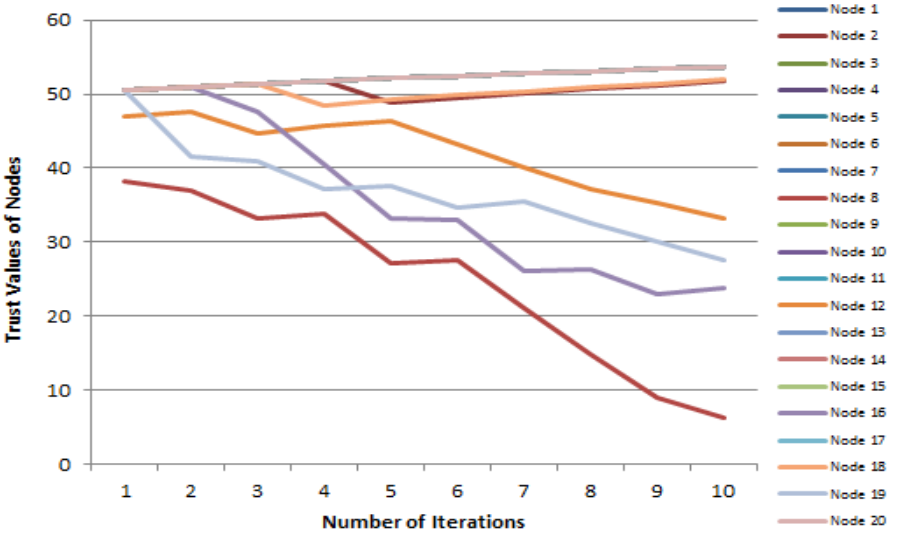

Fig. 4. Trust value of nodes vs. number of iterations

with time. However at some iteration the values also increase. This is because these nodes at times send correct data to delay their detection as much as possible.The trust values of some uncompromised nodes can also decrease at certain iterations. This is due to transmission errors or failure of a sensor to sense an event due to some fault. These changes are more noticeable as the decrease in the trust value of a node is much more than an increase in the trust value. This is to ensure that a compromised node can be detected as soon as possible. Thus in our framework with the reputation of compromised nodes decreasing, such corrupted nodes can be effectively identified and blocked to ensure that the true aggregation results are consistent.

6 Conclusions

In wireless sensor networks, compromised sensors can disrupt the integrity of data by intentionally sending incorrect data reports, by injecting fake data during data aggregation, and also by impeding the transmission of aggregated data. Since cryptographic solutions are not sufficient to prevent these attacks, general reputation based trust systems are proposed in the literature. This paper has presented a novel reliable data aggregation and transmission framework to provide a context-aware trust based security system for wireless sensor networks. A combination of context awareness and trust reasoning allows our system to calculate a trust value of a node based on the previous interactions with that node. As can be observed from the obtained simulation results, the framework proposed in this paper will provide a sound and complete security solution. It can be implemented to combat the inherent security weaknesses of a wireless sensor network.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: a survey. Computer Networks Journal 38, 393–422 (2002)
2. Gupta, P., Kumar, P.: The capacity of wireless networks. IEEE Transactions on Information Theory IT-46(2), 388–404 (2000)
3. Johnson, D., Maltz, D., Broch, J.: DSR: The dynamic source routing protocol for multihop wireless ad hoc networks. In: Perkins, C.E. (ed.) Ad Hoc Networking, pp. 139–172. Addison-Wesley (2001)
4. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy efficient Communication Protocol for Wireless Micro sensor Networks. In: Proceedings of Hawaii International Conference on System Science (HICSS), Maui, Hawaii, pp. 3005–3014 (2000)
5. Hussain, S., Mallinson, M., Drane, P.: Discrete radio power level consumption model in wireless sensor networks. In: Workshop Proceedings of the Fourth IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS (2007)
6. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
7. Chan, H., Perrig, A., Song, D.: Random Key Pre-distribution Schemes for Sensor Networks. In: IEEE Symp. Security and Privacy (May 2003)
8. Du, W., et al.: A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In: Proc. 10th ACM Conf. Comp. and Commun. Security, pp. 42–51 (October 2003)
9. Eschenauer, L., Gligor, V.D.: A Key-Management Scheme for Distributed Sensor Networks. In: Proc. 9th ACM Conf. Comp. and Commun. Security, pp. 41–47 (November 2002)
10. Atakli, I., Hu, H., Chen, Y., Ku, W., Su, Z.: Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation. In: The Symposium on Simulation of Systems Security (January 2008)
11. Hur, J., Lee, Y., Yoon, H., Choi, D., Jin, S.: The 7th International Conference on Advanced Communication Technology, ICAT 2005, pp. 491–496 (July 2005)

12. Zhang, W., Das, S., Liu, Y.: A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks. In: IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON (2006)
13. Resnick, P., Zeckhauser, R.: Trust among strangers in Internet transactions: empirical analysis of eBays reputation system. In: Baye, M.R. (ed.) Advances in Applied Microeconomics, vol. 11. Elsevier Science (2003)
14. Xiong, L., Liu, L.: A reputation-based trust model for peer-to-peer ecommerce communities. In: Proc. of IEEE Conference on Ecommerce 2003, p. 275 (2003)