An Efficient Distributed Trust Model for Wireless Sensor Networks

Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, *Member, IEEE*, and Mohsen Guizani, *Fellow, IEEE*

Abstract—Trust models have been recently suggested as an effective security mechanism for Wireless Sensor Networks (WSNs). Considerable research has been done on modeling trust. However, most current research work only takes communication behavior into account to calculate sensor nodes' trust value, which is not enough for trust evaluation due to the widespread malicious attacks. In this paper, we propose an Efficient Distributed Trust Model (EDTM) for WSNs. First, according to the number of packets received by sensor nodes, direct trust and recommendation trust are selectively calculated. Then, communication trust, energy trust and data trust are considered during the calculation of direct trust. Furthermore, trust reliability and familiarity are defined to improve the accuracy of recommendation trust. The proposed EDTM can evaluate trustworthiness of sensor nodes more precisely and prevent the security breaches more effectively. Simulation results show that EDTM outperforms other similar models, e.g., NBBTE trust model.

Index Terms—Wireless sensors networks, distributed trust model, energy efficient

1 Introduction

WSNs are emerging technologies that have been widely used in many applications such as emergency response [1], healthcare monitoring [2], battlefield surveillance, habitat monitoring, traffic management, smart power grid [3], etc. However, the wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs.

Various security mechanisms, e.g., cryptography, authentication, confidentiality, and message integrity, have been proposed to avoid security threats such as eavesdropping, message replay, and fabrication of messages. However, these approaches still suffer from many security vulnerabilities, such as node capture attacks and denial-of-service (DoS) attacks. The traditional security mechanisms can resist external attacks, but cannot solve internal attacks effectively which are caused by the captured nodes. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trustworthiness of another node.

Nowadays, many researchers have developed trust models to build up trust relationships among sensor nodes [4]. For example, in [5], a distributed Reputation-based Framework for Sensor Networks (RFSN) is first proposed for WSNs. Two key building blocks of RFSN are Watchdog and Reputation System. Watchdog is responsible for monitoring communication behaviors of neighbor nodes. Reputation System is responsible for maintaining the reputation of a sensor node. The trust value is calculated based on the reputation value. However, in RFSN, only the direct trust is calculated while the recommendation trust is ignored. A Parameterized and Localized trUst management Scheme (PLUS) is proposed in [6]. In PLUS, both personal reference and recommendation are used to build reasonable trust relationship among sensor nodes. Whenever a judge node (the node which performs trust evaluation) receives a packet from suspect node (the node which is in radio range of the judge node and will be evaluated), it always check the integrity of the packet. If the integrity check fails, the trust value of suspect node will be decreased irrespective of whether it was really involved in malicious behaviors or not. Therefore, suspect node may get unfair penalty. Another similar trust evaluation algorithm named as Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm (NBBTE) is proposed based on behavior strategy banding D-S belief theory [7]. NBBTE algorithm first establishes various trust factors depending on the communication behaviors between two neighbor nodes. Then, it applies the fuzzy set theory to measure the direct trust values of sensor nodes. Finally, considering the recommendation of neighbor nodes, D-S evidence theory method is adopted to obtain integrated trust value instead of simple weighted-average one. To the best of our knowledge, NBBTE is the first proposed algorithm which establishes various trust factors depending on the communication behaviors to evaluate the trustworthiness of sensor nodes. Therefore, NBBTE is chosen as the comparing algorithm in this paper.

From the literature on this topic, we can find that: 1) In the current research work, the assessment of trust values for sensor nodes is mainly based on the communication

- *J. Jiang, G. Han, and F. Wang are with the Department of Information & Communication Systems, Hohai University, Changzhou, China. E-mail: {jiangjinfang1989, hanguangjie}@gmail.com, wfeng@cczu.edu.cn.*
- *L. Shu is with Guangdong Petrochemical Equipment Fault Diagnosis Key Laboratory, Guangdong University of Petrochemical Technology, China. E-mail: lei.shu@ieee.org.*
- *M. Guizani is with Qatar University, Doha, Qatar. E-mail: mguizani@ieee.org.*

Manuscript received 28 Dec. 2013; revised 21 Feb. 2014; accepted 5 Apr. 2014. Date of publication 24 Apr. 2014; date of current version 8 Apr. 2015. Recommended for acceptance by N. Kato. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TPDS.2014.2320505

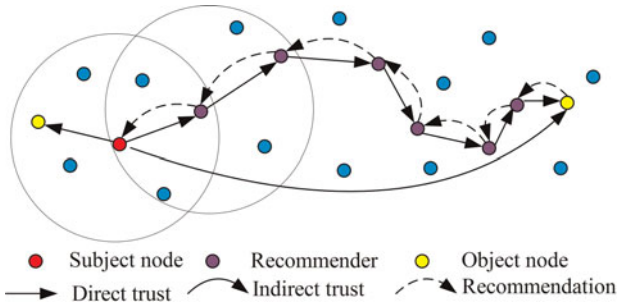


Fig. 1. The network structure.

(successful and unsuccessful communications) point of view. In fact, just considering the communication behavior, we cannot decide whether a sensor node can be trusted or not. Besides the communication behavior, other trust metrics such as the energy level should also be taken into account to calculate the trustworthiness of sensor nodes. In addition, an efficient trust model should deal with uncertainty caused by noisy communication channels and unstable sensor nodes' behaviors. 2) There are two common ways to establish trust in WSNs: calculating direct trust based on direct interactions and calculating indirect trust value based on recommendation from the third party. However, not all the third parties are trusty and not all the recommendations are reliable. Thus, a discriminate analysis about the third party and recommendation is essential. 3) Most existing studies only provide the trust assessment for neighbor nodes. However, in real applications, a sensor node sometimes needs to obtain the trust value of the non-neighbor nodes. For example, in some routing protocols (e.g., TPGFPlus [8]) or localization algorithms (e.g., improved LMAT algorithm [9]), sensor nodes need the information of the two-hop neighbor nodes to establish the routing or localize themselves. Therefore, providing the trust assessmentfor non-neighbor nodes becomes very important. 4) Because of the dynamic topology, the trust relationship between sensor nodes constantly changes in WSNs. Trust is a dynamic phenomenon and changes with time and environment conditions. However, most existing trust models do not solve the trust dynamic problem. The evolution of trust over time is another problem that needs further study. In order to solve the above-mentioned problems, we propose an efficient distributed trust model (EDTM). The proposed EDTM can evaluate the trust relationships between sensor nodes more precisely and can prevent security breaches more effectively.

The rest of the paper is organized as follows: In Section 2, the assumptions and network model are introduced. In Section 3, the overview of EDTM is presented. In Section 4, the EDTM is specifically depicted, including its design idea and practical implementation approach. In Section 5, the performance of the EDTM is evaluated. Finally, conclusions are made in Section 6.

2 Assumptions and Network Model

Scenario. In this paper, we consider a scenario in which all the sensor nodes are randomly deployed without mobility. As shown in Fig. 1, there are three kinds of nodes in the network: subject nodes, recommender and object nodes. If a sensor node A wants to obtain the trust value of another sensor node B, the evaluating sensor node A is named as subject node and the evaluated node B is the object node. This paper is a multi-hop network which means that the sensor nodes can only directly communication with the neighbor nodes within their communication range. The packets exchanged between any two non-neighbor nodes are forwarded by other nodes. The forwarding node not only can just "pass" the packets from source nodes to destination nodes but also can process the information based on their own judgments. Generally, the trust value is calculated based on a subject's observation on the object and recommendations from a third party. The third party which provides recommendations is a recommender.

Node capability. It assumes that sensor nodes have the same capability of computing, communicating and storing. Their communication ability is limited by specific wireless techniques. Only when two nodes move into each other's communication range could they detect each other and start communication. A homogeneous WSN is considered, that is all the sensor nodes have the same initial energy level and communication range. Additionally, in order to secure data transmission over the wireless network, each node is assigned a unique ID and a pair of public/private keys for encrypting and decrypting data, as well as with a public key certificate issued by some trustable Public Key Infrastructure (PKI). Each node keeps a list of neighbor nodes which stores their IDs and their communication information.

Attack model. There exist many malicious attacks in WSNs, such as DoS attack, node replication, Sybil attack, wormhole attack, attacks on Information, etc. Moreover, it should be noticed that similar to most security schemes, a trust model is also vulnerable to many malicious attacks, such as bad/good-mouthing attack and on-off attack. In a bad-mouthing attack, malicious nodes intentionally give dishonest recommendation to neighbor nodes. For example, they maliciously provide lower recommendation for normal ones during trust evaluation. Thus, recommendations under bad-mouthing attack cannot reflect the real opinions of the recommender. On the contrary, the sensor nodes conducting good-mouthing attack intentionally provide higher trust value for malicious nodes. In an on-off attack, malicious nodes can behave good or bad alternatively. When the trust values of malicious nodes are significantly reduced, they can act well for a period to improve their trust values. Therefore, it is difficult to detect these malicious nodes by conventional trust models.

3 Overview of EDTM

To efficiently compute the trust values on sensor nodes, we first need a clear understanding of the trust definition and the various trust properties that are adopted in a trust model.

3.1 Definition and Properties of Trust

Trust. There are several definitions given to trust in the literature [10]. Trust is always defined by reliability, utility, availability, risk, quality of services and other concepts.

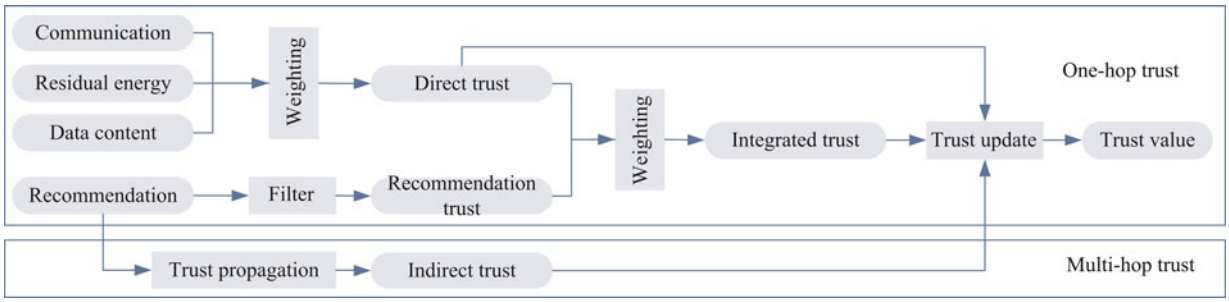


Fig. 2. The EDTM structure.

Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviors. That is, the trust value is used to reflect whether a sensor node is willing and able to act normally in WSNs. In this paper, a trust value ranges from 0 to 1. A value of 1 means completely trustworthy and 0 means the opposite.

Direct trust. Direct trust is a kind of trust calculated based on the direct communication behaviors. It reflects the trust relationship between two neighbor nodes.

Recommendation trust. As mentioned above, since the recommendations from third parties are not always reliable, we need an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust.

Indirect trust. When a subject node cannot directly observe an object nodes' communication behaviors, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes.

Based on [11] and [12], we can conclude that there are three main properties of trust: asymmetry, transitivity and composability. Asymmetry implies that if node A trusts node B, it does not necessarily mean that node B trusts node A. Transitivity means the trust value can be passed along a path of trusted nodes. If node A trusts node B and node B trusts node C, it can be inferred that node A trusts node C at a certain level. The transitivity is a very important property in trust calculation between two non-neighbor nodes. Composability implies that trust values received from multiple available paths can be composed together to obtain an integrated value.

3.2 The Structure of EDTM

In this section, we describe the overall architecture of EDTM. When we say node B is trustworthy or untrustworthy for node A, there is a trust model between node A and node B. As shown in Fig. 2, EDTM consists of two main components: one-hop trust model and multi-hop trust model which includes the following six components: direct trust module, recommendation trust module, indirect trust module, integrated trust module, trust propagation module and trust update module. When a subject node wants to obtain the trust value of an object, it first checks its recorded list of neighbor nodes. If the ID of the object node is in the list of neighbor nodes, the one-hop trust model is triggered. Otherwise, the multi-hop trust model is started. In the one-hop trust model, if the trust is calculated based on node B's direct experiences with node A completely, this model is called direct trust model. Otherwise, the recommendation trust module is built. In the multi-hop trust model, once the subject node A receives recommendations from other nodes about the object node B, indirect trust model can be established.

In current trust models, the direct trust and recommendation are always used to evaluate the trustworthiness of sensor nodes. The direct trust is directly calculated based on the communication behaviors between two neighbor nodes. However, due to malicious attacks, using only direct trust to evaluate sensor nodes is not accurate. Thus, the recommendation from other sensor nodes is needed to improve the trust evaluation. In addition, if the number of communication packets between two neighbor nodes is too small, it is difficult to decide whether an object node is good or bad based on only few interactions. Therefore, in the one-hop trust model, we define a threshold of communication packets Th_{num}. If the communication packets between the subject and object nodes are higher than the threshold Th_{num}, only the direct trust is calculated. Otherwise, the recommendations from the recommenders are needed for the object's trust evaluation.

In the multi-hop trust model, the subject node first needs to select a set of recommenders. Then, the indirect trust is calculated based on recommendations and trust propagation. Next, we describe the detail calculation of direct, recommendation, and indirect trust.

4 Trust Calculation in EDTM

In this section, we present the trust calculation procedure of trust in details.

4.1 The Calculation of Direct Trust

Unlike prior work, we compose our direct trust by considering communication trust, energy trust and data trust. The sensor nodes in WSNs usually collaborate and communicate with neighbor nodes to perform their tasks. Therefore, the communication behaviors are always checked to evaluate whether the sensor node is normal or not. However, due to the nature of wireless communication, there are many reasons resulting in the packets loss and the communications between sensor nodes are unstable. The unsuccessful communication maybe caused by malicious nodes or unstable communication channel. Therefore, just evaluating the communication behaviors is not enough for trust evaluation. In addition, it is generally known that all communications in WSNs will consume a certain amount of energy to

transmit some data packets or any information. If there are malicious nodes in WSNs, the abnormal energy will be consumed or the transmitted data packets will be falsified to conduct malicious attacks. Therefore, communication trust, energy trust and data trust are defined in EDTM. The communication trust reflects if a sensor node can cooperatively execute the intended protocol. The energy trust is used to measure if a sensor node is competent in performing its intended functions or not. The data trust is the trust assessment of the fault tolerance and consistency of data, which affects the trust of the sensor nodes that create and manipulate the data.

4.1.1 Calculation of the Communication Trust

The information on a sensor node's prior behavior is one of the most important aspects of the communication trust. However, communication channels between two sensor nodes are unstable and noisy, thus monitoring sensor node's behaviors in WSNs based on previous communication behaviors involves considerable uncertainty. To deal with this uncertainty, we adopt a Subjective Logic framework [13]. The trust value in SL framework is a triplet $T = \{b, d, u\}$, where b, d and u correspond to belief, disbelief and uncertainty respectively, $b, d, u \in [0, 1], b + d + u = 1$. Following the trust model based on Subjective Logic framework [14], the communication trust T_{com} is calculated based on successful (s) and unsuccessful (f) communication packets:

$$T_{com} = \frac{2b + u}{2}, \tag{1}$$

where $b = \frac{s}{s+f+1}$, $u = \frac{1}{s+f+1}$.

4.1.2 Calculation of the Energy Trust

Energy is an important metric in WSNs since sensor nodes are extremely dependent on the amount of energy they have. Malicious nodes always consume abnormal energy to launch malicious attacks. For example, malicious nodes which conduct DoS attack consume much more energy than normal nodes while selfish nodes consume less energy. Therefore, we use energy as a QoS trust metric to measure if a sensor node is selfish or maliciously exhaust additional energy. Using an energy prediction model, sensor nodes' energy consumption in different periods can be obtained. If the environment conditions do not change much, the energy consumption rate of normal nodes can maintain a stable value.

First, an energy threshold θ is defined. When the residual energy E_{res} of one sensor node falls below the threshold value, the sensor node is not competent enough (do not have adequate energy) to perform its intended function. Thus, the energy trust of the sensor node is considered to be 0. Otherwise, The energy trust is calculated based on the energy consumption rate p_{ene}, $p_{ene} \in [0, 1]$. The higher the energy consumption rate p_{ene} is, the less residual energy remains, which ultimately leads to a smaller ability of sensor nodes to complete the task. Thus, the trust values of the sensor nodes are considered to be smaller. The energy trust is calculated by:

$$T_{ene} = \begin{cases} 1 - p_{ene}, & if\ E_{res} \geq \theta, \\ 0, & else, \end{cases} \tag{2}$$

where p_{ene} is calculated based on the Ray Projection method [15].

For a object node, if the energy consumption rate in n previous time slots is $P_{ene} = (p_{ene}(1), p_{ene}(2), \ldots, p_{ene}(n))$ and the energy consumption rate in current time slot is $p_{ene}(n+1)$, according to the Ray Projection method, the change of energy consumption rate in each time slot is first calculated by $k_i = p_{ene}(i) - p_{ene}(i-1)$, where $i = 2, 3, \ldots, n$. Then, the subject node chooses k_i with the same plus or minus number as k_n and calculate $|k_n - k_i|$. Place the results of $|k_n - k_i|$ in an arrangement according to the order from small to large and label as (d_i, l), where $d_i = |k_n - k_i|$ and l is the labeled position of d_i in the arrangement. Finally, we obtain $\hat{p}_{ene}(l) = p_{ene}(n) + k_{i+1}$. The minimum value of $\hat{p}_{ene}(l)$ is chosen as the predicted energy consumption rate $p_{ene}(n+1) = \min(\hat{p}_{ene}(l))$.

4.1.3 Calculation of the Data Trust

Following the idea introduced in [16]: the trust of the data affects the trust of the network nodes that created and manipulated the data, and vice-versa, we introduce the evaluation of data trust in this section. The data packets have spatial correlation, that is, the packets sent among neighbor nodes are always similar in the same area. The data value of these packets in general follows some certain distribution, such as a normal distribution [17], [18]. For the sake of simplicity, in this paper, we also model the distribution of the data as a normal distribution. For a set of data, the probability density function is $f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, where x is the attribute value v_d of a data item, and μ and σ are mean and variance of the data, respectively.

Since the mean μ of a set of data is the most representative value that reflects the value similarity of the data, the mean is supposed to have the highest trust value [18]. If the value of a data item is close to the mean, the trust value of this data is relatively high, and vice-versa. Therefore, the trust value of the data item is defined as:

$$T_{data} = 2\left(0.5 - \int_{\mu}^{v_d} f(x)\, dx\right) = 2\int_{v_d}^{\infty} f(x)\, dx. \tag{3}$$

Based on the communication trust T_{com}, the energy trust T_{ene} and the data trust T_{data}, we can obtain the direct trust between two neighbor nodes as:

$$T_{n-direct} = w_{com} T_{com} + w_{ene} T_{ene} + w_{data} T_{data}, \tag{4}$$

where w_{com}, w_{ene} and w_{data} are the weight values of the communication trust, energy trust and data trust respectively, $w_{com} \in [0, 1]$, $w_{ene} \in [0, 1]$, $w_{data} \in [0, 1]$ and $w_{com} + w_{ene} + w_{data} = 1$.

4.2 Calculation of the Recommendation Trust

The recommendation trust is a special type of direct trust. When there are no direct communication behaviors between

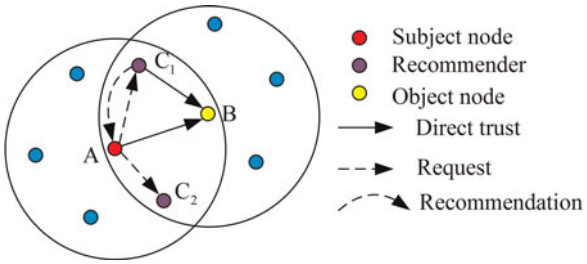


Fig. 3. Calculation of the recommendation trust.

subject and object nodes, the recommendations from recommender are always taken into account for trust calculation. However, in most existing related works, the true and false recommendations are not distinguished. How to detect and get rid of false recommendations is important since it has great impact on the trust calculation.

As shown in Fig. 3, when a subject node A wants to obtain the recommendations of an object node B. The subject node A first checks its trust records and then selects a set of common neighbor nodes of node A and node B as the recommenders $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n$, which have the trust value larger than the threshold 0.5. Subsequently, subject node A transmits a recommendation request message to the selected recommenders through multi-casting. Obviously, the identity of node B should be added into the recommendation request. Upon receiving a request message, the qualified nodes will reply if they have recommendation of node B. Based on the recommendations, the subject node A filters the false recommendation and compute the recommendation trust of node B.

4.2.1 Calculation of the Recommendation Reliability

During the calculation of the recommendation trust, the recommendations from malicious neighbor nodes are first isolated by choosing the trust recommenders. However, not all the recommendations from the recommenders are reliable. Therefore, when the subject node receives several recommendations from neighbor nodes, it will first check whether the recommendations are true or false. This judgment can be done by outlier detection schemes (e.g., checking consistency among multiple recommendations [18]). We consider a simple checking method among multiple recommendations by defining the recommendation reliability T_{rel}. T_{rel} is calculated as follows:

$$T_{rel} = 1 - \left|T_{\mathrm{C}_i}^{\mathrm{B}} - T_{ave}^{\mathrm{B}}\right|, \tag{5}$$

where $T_{\mathrm{C}_i}^{\mathrm{B}}$ is the recommendation value of object node B reported by recommender C_i, and T_{ave}^{B} is the average value of all the recommendations.

4.2.2 Calculation of the Recommendation Familiarity

Generally, the higher trust value of the recommender, the more important recommendation is. Intuitively, it seems to be reasonable. However, it is questionable that nodes with higher trust values give more honest recommendations. Therefore, we introduce the concept of relationship familiarity, which is based on the age of the relationship between two nodes. The concept of familiarity allows sensor nodes to give more importance to recommendations sent by long-term neighbor nodes rather than short-term neighbor nodes. The familiarity is defined as:

$$T_{fam} = \frac{num_{\mathrm{C}_i}^{\mathrm{B}}}{num_{\mathrm{C}_i}} \times \alpha^{\frac{1}{num_{\mathrm{C}_i}^{\mathrm{B}}}}, \tag{6}$$

where $num_{\mathrm{C}_i}^{\mathrm{B}}$ is the successful communication times between recommender C_i and object node B, num_{C_i} is the total successful communication times of the recommender, and α is the regulatory factor of the communication times, $\alpha \in (0, 1)$.

Based on the trust value of the recommended node T_{C_i}, the recommendation value $T_{\mathrm{C}_i}^{\mathrm{B}}$, the reliability of recommendation T_{rel} and the familiarity T_{fam} of recommended nodes about the object node, the recommendation trust is calculated as follows:

$$T_{n-recom} = \frac{\sum_{i=1}^{n} 0.5 + \left(T_{\mathrm{C}_i}^{\mathrm{B}} - 0.5\right) \times T_{rel} \times T_{fam}}{n}, \tag{7}$$

where n is the number of the recommender.

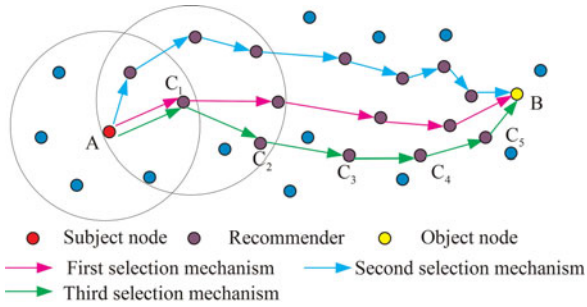


Fig. 4. Calculation of the indirect trust.

4.3 Calculation of the Indirect Trust

WSNs are multi-hop networks, when there are no direct communications between subject and object nodes, indirect trust can be established since trust is transitive. In this paper, the calculation of indirect trust includes two steps: 1) the first step is to find multi-hop recommenders between subject and object nodes, and 2) the second step is the trust propagation which aims at computing the direct trust. The path from the subject node to the object node established by the recommenders is named as Trust Chain.

As shown in Fig. 4, based on the location information of sensor nodes, we observe three different kinds of mechanisms for choosing the recommender in this paper: 1) finding a recommender which is closest to the object node to save energy consumption, 2) finding a recommender which has the highest trust value to guarantee the reliability of Trust Chain and 3) finding an optimal Trust Chain by both considering the distance information and the trust value. The first selection mechanism can find the shortest Trust Chain, thus the communication overhead for indirect trust calculation can be minimized. However, in this case, the indirect trust evaluation is not accurate because malicious nodes maybe chosen as recommenders. While the second selection mechanism can

choose the most believable Trust Chain but this Trust Chain is not energy efficient. Relatively speaking, the third selection mechanism is the best one.

After establishing the Trust Chain, all the recommenders should participate in the trust propagation step. The subject node A first broadcasts a recommendation request message to its next-hop recommender and waits for replies. Upon receiving a request message, the recommender will check if they have information needed by node A and whether the object node is a neighbor node. If the object node B is not a neighbor node of the current recommender, it continually forwards the request message to its next-hop recommender; otherwise, it will reply the request message with the recommendation value to its previous-hop node until the reply is received by the subject. Based on the recommendation value $T^{\mathrm{B}}_{\mathrm{C}_i}$ and the trust value of the recommender T_{C_i}, the indirect trust is calculated by:

$$T_{n-indirect}(^{\mathrm{B}}_{\mathrm{C}_1}) = \begin{cases} T_{\mathrm{C}_1} \times T^{\mathrm{B}}_{\mathrm{C}_1}, & if\ T^{\mathrm{B}}_{\mathrm{C}_1} < 0.5 \\ 0.5 + (T_{\mathrm{C}_1} - 0.5) \times T^{\mathrm{B}}_{\mathrm{C}_1}, & else, \end{cases} \tag{8}$$

$$T_{n-indirect}(^{\mathrm{B}}_{\mathrm{C}_{i+1}}) = \begin{cases} T_{\mathrm{C}_{i+1}} \times T_{n-indirect}(^{\mathrm{B}}_{\mathrm{C}_i}), \\ if\ T_{n-indirect}(^{\mathrm{B}}_{\mathrm{C}_i}) < 0.5 \\ 0.5 + (T_{\mathrm{C}_{i+1}} - 0.5) \\ \times T_{n-indirect}(^{\mathrm{B}}_{\mathrm{C}_i}), else, \end{cases} \tag{9}$$

$i = 1, \ldots, n$, where n is the number of recommender on the Trust Chain.

4.4 Update of Trust Value

Due to the dynamic behavior of WSNs such as leaving or joining the network, the trust values of sensor nodes should be updated periodically. First, the trust value should not be updated too often. Because frequently updating the trust value will waste a lot of energy, and the trust evaluation will be easily affected by the network traffic conditions (e.g., congestion and delay). In addition, the update cycle time cannot be too long. A node's historical trust values should be taken into account to measure its current trustworthiness. If the cycle time is too long, it cannot efficiently reflect the current behaviors of the object node. To solve these issues, we use a sliding time window concept to update the trust value.

The time window consists of several time slots for the trust update. Each time slot is a cycle time. In each cycle time, the subject evaluates the trust of the subject as $T(i), i = 1, \ldots, m$, where m is the number of time slots. In the next cycle time, the trust value is updated as: $T(i+1)_{new} = w_i T(i) + w_{i+1} T(i+1), i = 1, \ldots, m,\ \ w_i + w_{i+1} = 1$. w_i and w_{i+1} are the weight values of the historical trust and the current trust level, respectively. However, a historical trust value computed a long time ago should carry less importance than the trust value made more recently. Therefore, we define an aging factor β for trust value attenuation: $\beta = e^{t_i - t_{i+1}}$, where t_i and t_{i+1} are the trust calculation time of $T(i)$ and $T(i+1)$, respectively. Therefore, the weight value is $w_i = \beta, w_{i+1} = 1 - \beta$.

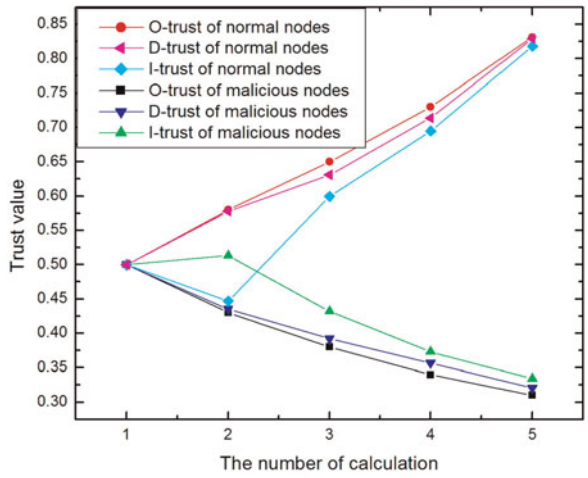


Fig. 5. Communication packets are higher than the threshold.

5 Simulation Results and Analysis

Our experiments are performed using Matlab. We implemented two different sets of simulations. First, we evaluate the performance of EDTM based on different simulation parameters, e.g., the threshold of packets and the different weight values. Then, we compare the detection rate of malicious node and the energy consumption of EDTM and NBBTE. The deployment area is set to be 100*100 m. There are 100 sensor nodes randomly deployed in the sensing area. The malicious nodes are simulated by the following five kinds of malicious attacks: selective forwarding attack, data forgery attack, DoS attack, on/off attack, bad and good mouthing attack. In order to compare the subjective trust value calculated by a sensor node, the objective trust is also derived. The objective trust is calculated based on the actual information of each node without considering any network dynamics such as node mobility, trust decay over time, and any malicious attacks. Therefore, the subjective trust values are mostly lower than the objective trust values.

5.1 Performance of EDTM

5.1.1 *The Selection of Threshold* Th_{num}

In EDTM, a threshold of communication packets Th_{num} is defined to save energy consumption. When the communication packets between the subject and object nodes are higher than the threshold Th_{num}, only the direct trust is calculated. Therefore, the energy consumption, communication overhead and memory space for recommendation calculation are saved. In this section, we simulate the trust model between two neighbor nodes. The rate of malicious nodes is set as 30 percent. As shown in Figs. 5 and 6, we observe that the trust value of a normal node is close to 1 and that of a malicious node is close to 0.

Fig. 5 shows the results of the object trust value (O-trust), direct trust value (D-trust) and integrated trust value (I-trust) of normal nodes and malicious nodes, respectively. We observe that when the communication packets between the subject and object nodes are higher than the threshold Th_{num}, the direct trust values are closer to the object trust values compared with the integrated trust values since the integrated trust values are more or less influenced by the

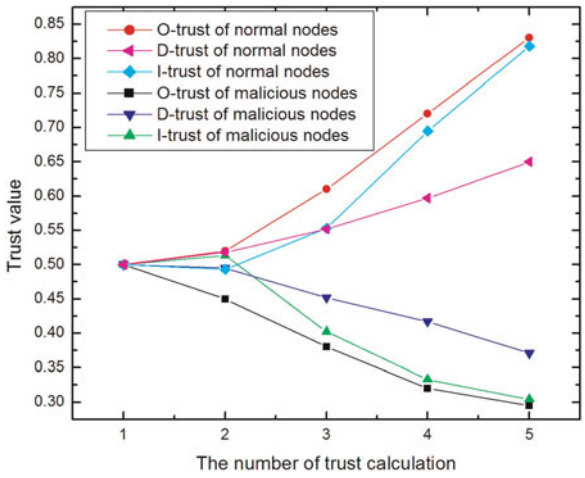


Fig. 6. Communication packets are lower than the threshold.

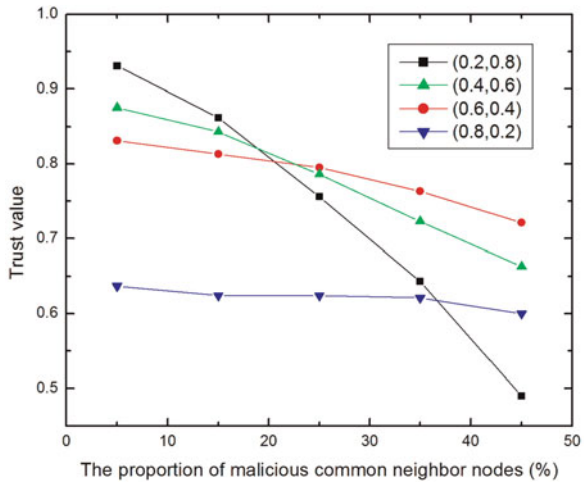


Fig. 8. Influence of the weight value.

malicious recommendations. Therefore, in this case, only calculating the direct trust is much more accurate and energy efficient.

From Fig. 6, we can see that when the communication packets between the subject and object nodes are lower than the threshold Th_{num}, the integrated trust values are closer to the object trust values compared with the direct trust values, since in this case the communication packets are not enough to accurately react the sensor nodes' real behaviors. When the communication times is small, it is hard to distinguish normal nodes and malicious nodes due to the selective forwarding attack. Therefore, recommendation is essential for the trust evaluation.

Fig. 7 shows the relationship between the trust value and communication packets threshold Th_{num}. The x–axis represents the average communication packets in each trust calculation period. We experiment with a varying number of packets ranging from 0 to 1,000 with an increment of 10 to examine the impact on the trust evaluation. First, we recognize that the trust value increases as the number of packets increases. In addition, the trust evaluations of the same node under different communication packets threshold Th_{num} are different. It is noticeable that when the number of packets is below 400, the trust value under $Th_{num} = 40\%$ is the most closet one to the object trust. While the number of packets exceeds 400, choosing the threshold as $Th_{num} = 60\%$ performs better. However, when the number of packets is large enough, the trust model under $Th_{num} = 20\%$ performs as well as the trust model under $Th_{num} = 60\%$. This implies that a subject node can select a certain threshold value Th_{num} to obtain a much more real trust value for an object node according to the number of communication packets.

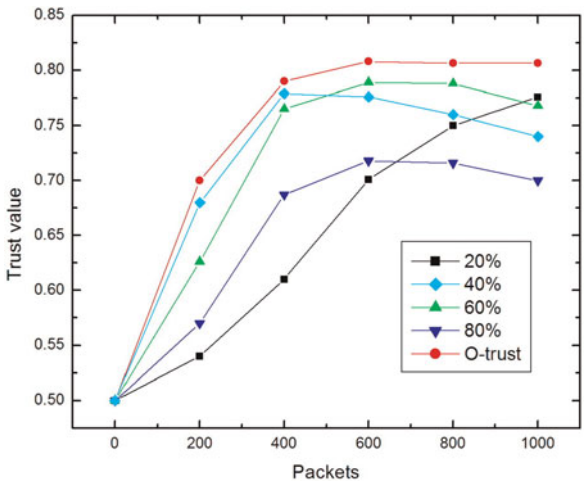


Fig. 7. Relationship between trust value and communication packets threshold.

5.1.2 Selection of the Weight Value

From Figs. 6 and 7, we can conclude that combining the direct trust and recommendation trust is very important when there are not enough interaction information for sensor nodes' trust evaluation. The proper weight values for the direct trust and recommendation trust depends on the conditions of the environment. In EDTM, the subject node uses the recommendations from the common neighbor nodes of the object node and itself. Therefore, we vary the percentage of malicious common neighbor nodes from 5 to 45 percent with a 5 percent increment.

In general, when there are more malicious neighbor nodes, the lower trust value is obtained because the malicious attack such as the bad mouthing attack can directly disturb the regular trust evaluation. We assume there are enough packets interactions and set the average packets between two neighbor nodes as 600 during each period. The evaluated object node is a normal node. The weight values for the direct trust and recommendation trust are labeled as (w_{direct}, w_{recom}).

As shown in Fig. 8, when the percent of malicious nodes does not exceed 20 percent, the trust evaluation under (0.2, 0.8) works best, since only calculating direct trust is enough for trust evaluation without the influence of malicious nodes. However, the trust value decreases rapidly as the percent of malicious neighbor nodes continually grows. With the increase number of malicious neighbor nodes, the higher weight value of recommendation trust is, the lower obtained trust value, since more use of recommendation trust leads to more malicious nodes participating in trust computing. Therefore, we draw a conclusion that more

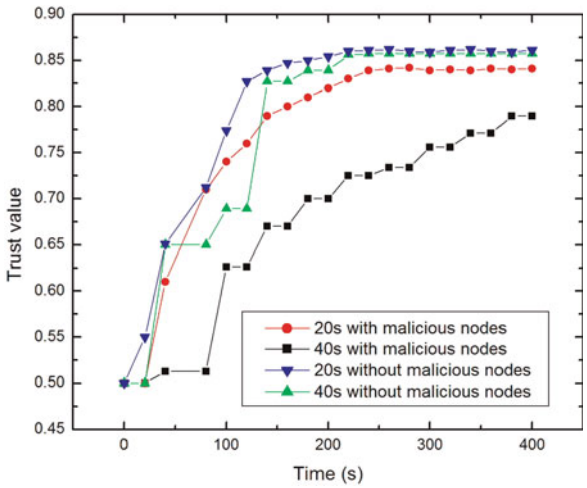


Fig. 9. Influence of the update cycle time.

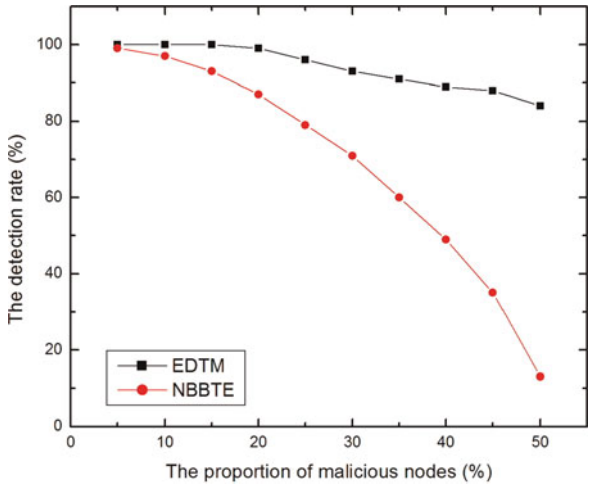


Fig. 11. Comparison of the detection rate.

malicious neighbor nodes leads to a lower trust evaluation and the weight values for the direct trust and recommendation trust should be dynamically adjusted based on the proportion of malicious nodes in their neighbor nodes. However, in real applications, the percent of malicious nodes is not known in advance, thus how to select the proper weight values under different environment conditions needs further research and will not be addressed in this paper.

5.1.3 Selection of the Trust Update Time Cycle

The trust value needs to be updated dynamically. It is generally known that frequent trust update wastes a lot of energy. On the contrary, if the trust update interval is too long, it cannot efficiently reflect the current behaviors of the object node. As shown in Fig. 9, two groups of experimental results are compared: trust values evaluation with and without malicious nodes under different update cycle time. At the beginning of the simulation when the system is without malicious nodes, the trust value with longer update period grows slowly. However, after 150s, the trust values with the cycle time 20 and 40 s are almost the same. Therefore, in order to save energy consumption, a longer update time period can be used for trust evaluation in this case. However, the trust values calculated with malicious nodes under different time cycles are very different, thus shorter update time periods should be used.

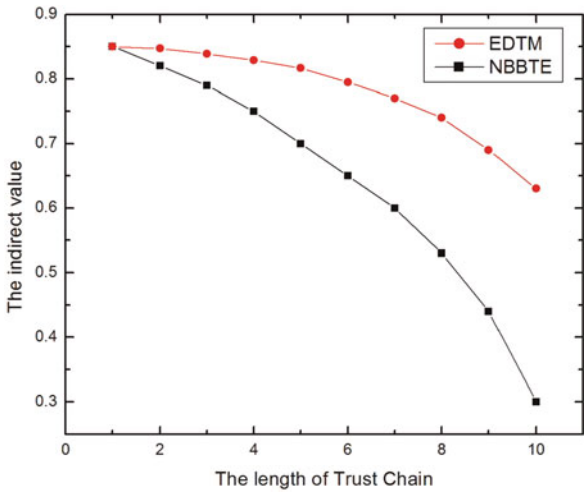


Fig. 10. Comparison of the Indirect trust value.

5.2 Comparison of EDTM and NBBTE

5.2.1 Comparison of the Indirect Trust Value

In NBBTE, the indirect trust value is calculated by $T_{n-indirect}(NBBTE) = T_{C_i} \times T_{C_i}^{B}$. In this section, we simulate the trust calculation of a normal node under the different method in EDTM and NBBTE. Fig. 10 shows that the indirect trust calculation method in NBBTE cannot reasonably reflect the sensor nodes' real trust level. For example, if one subject wants to obtain the trust value of an object node which has its objective trust value as 0.6. There are two recommenders on the Trust Chain with the trust value of 0.8 and 0.6. The recommendation value provided by the closet recommender is 0.8. By EDTM and NBBTE, we can get the indirect value as: $0.6 + (0.6 - 0.5) \times [0.5 + (0.8 - 0.5) \times 0.8] = 0.574$ and $0.6 \times (0.8 \times 0.8) = 0.384$. It is obvious that the trust value calculated by EDTM is much more closer to its objective trust values ($0.384 < 0.574 < 0.6$). The subject node can evaluate the object node as a normal node by EDTM ($0.5 < 0.574$), but consider the object as a malicious node by NBBTE ($0.384 < 0.5$). Therefore, EDTM outperforms NBBTE in terms of indirect trust value calculation.

5.2.2 Comparison of the Detection Rate

In this section, the simulated malicious attacks are selective forwarding attack, data forgery attack, DoS attack, on-off attack, bad/good mouthing attack. We vary the percentage of malicious nodes from 5 to 50 percent with a 5 percent increment. As shown in Fig. 11, it is obvious that the performance of the EDTM is better than that of NBBTE. NBBTE only takes the selective forwarding attack and the attack on information into account and is vulnerable against other attacks, e.g., DoS attack, on-off attack, bad/good mouthing attack. So, with the increase number of malicious nodes, the detection rate decreases rapidly, while EDTM is robust to the five kinds of malicious attacks. Next, we will compare

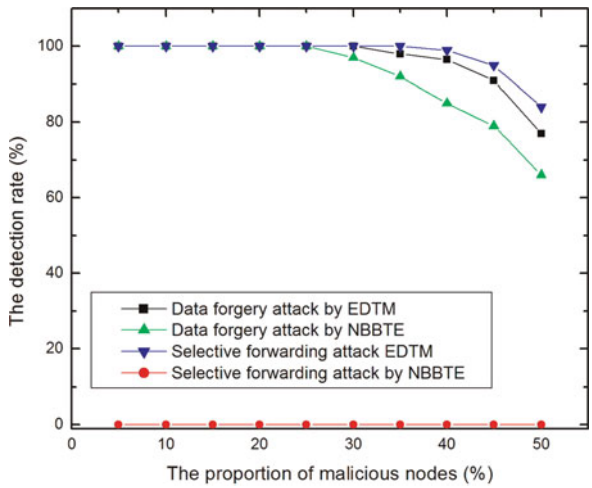


Fig. 12. Comparison of the robustness against certain malicious attacks.

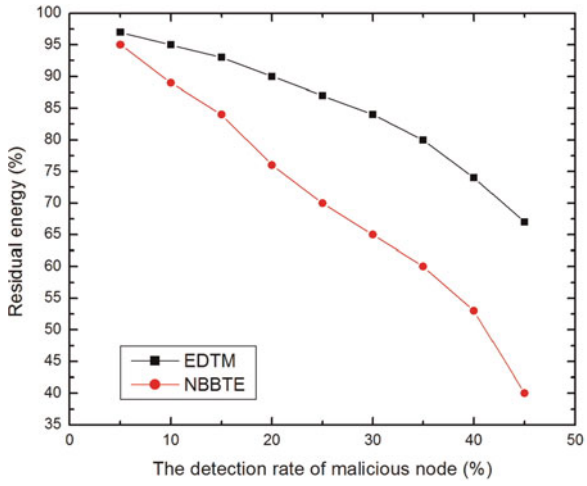


Fig. 13. Comparison of the energy consumption.

the performance of EDTM and NBBTE against the selective forwarding attack and the data forgery attack. As shown in Fig. 12, both EDTM and NBBTE are robust against the data forgery attack, but EDTM works better. NBBTE cannot detect malicious nodes with selective forwarding attack because in this simulation, the packet loss rate is set to a constant value. The rate of data forwarding in NBBTE is calculated based on the change of the number of transmission packets in different periods.

5.2.3 Comparison of the Energy Consumption

Finally, we compare energy consumption of EDTM and NBBTE for obtaining the same malicious nodes detect rate. We vary the percentage of malicious nodes from 5 to 45 percent with a 5 percent increment. The communication packets threshold is set to 60 percent, the weight values for direct trust and recommendation trust is set to (0.6, 0.4) and the trust update cycle time is 40 s. As shown in Fig. 13, EDTM is much more energy efficient, because in EDTM sensor nodes interact only with their neighbor nodes. As a result, nodes do not keep trust information about every node in the network. Only keeping neighborhood information implies significant lower energy consumption, less processing for trust level calculation, and less memory space. While in NBBTE, each node needs to store the information for all the sensor nodes in the network.

6 Conclusion

The trust model has become important for malicious nodes detection in WSNs. It can assist in many applications such as secure routing, secure data aggregation, and trusted key exchange. Due to the wireless features of WSNs, it needs a distributed trust model without any central node, where neighbor nodes can monitor each other. In addition, an efficient trust model is required to handle trust related information in a secure and reliable way. In this paper, a distributed and efficient trust model named EDTM was proposed. During the EDTM, the calculation of direct trust, recommendation trust and indirect trust are discussed. Furthermore, the trust propagation and update are studied. Simulation results show that EDTM is an efficient and attack-resistant trust model. However, how to select the proper value of the weight and the defined threshold is still a challenging problem, which we plan to address in our future research endeavors.

Acknowledgments

The work was supported by "Natural Science Foundation of JiangSu Province of China, No. BK20131137", "Science & Technology Pillar Program (Social development) of Changzhou Science and Technology Bureau, No. CE20135052", "the Guangdong University of Petrochemical Technology's Internal Project, No. 2012RC0106" and "Jiangsu Province Ordinary University Graduate Innovation Project, No. CXZZ13_02". Guangjie Han is the corresponding author.

References

[1] H. Chan and A Perrig, "Security and privacy in sensor networks," *Comput.*, vol. 36, no. 10, pp. 103–105, Oct. 2003.

[2] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical-based healthcare monitoring architecture in wireless heterogeneous sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 7, pp. 400–411, May 2009.

[3] V. C. Gungor, L. Bin, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[4] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Managements and applications of trust in wireless sensor networks: A Survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, 2014.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw.*, 2004, pp. 66–77.

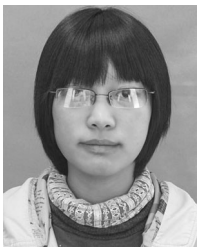
[6] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst.*, 2008, pp. 437–446.

[7] 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, pp. 1345–1360, 2011.

[8] G. Han, Y. Dong, H. Guo, L. Shu, and D. Wu, "Cross-layer optimized routing in WSN with duty-cycle and energy harvesting," *Wireless Commun. Mobile Comput.*, 3 Feb. 2014, DOI: 10.1002/wcm.2468.

[9] G. Han, X. Xu, J. Jiang, L. Shu, and N. Chilamkurti, "The insights of localization through mobile anchor nodes in wireless sensor networks with irregular radio," *KSII Trans. Internet Inf. Syst.*, vol. 6, pp. 2992–3007, 2012.

[10] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, 2nd Quarter 2012.
[11] K. Nordheimer, T. Schulze, and D. Veit, "Trustworthiness in networks: A simulation approach for approximating local trust and distrust values," *IEEE Commun. Surveys Tuts.*, vol. 321, pp. 157–171, 2010.
[12] A. Josang, "An algebra for assessing trust in certification chains," in *Proc. Netw. Distrib. Syst. Security Symp.*, 1999, pp. 1–10.
[13] W. Gao, G. Zhang, W. Chen, and Y. Li, "A trust model based on subjective logic," in *Proc. 4th Int. Conf. Internet Comput. Sci. Eng.*, 2009, pp. 272–276.
[14] M. Chen, Y. Zhou, and L, Tang, "Ray projection method and its applications based on Grey Prediction," *Chinese J. Statist. Decision*, vol. 1, p. 13, 2007.
[15] H. S. Lim, Y. S. Moon, and E. Bertino, "Provenance based trustworthiness assessment in sensor networks," in *Proc. 7th Int. Workshop Data Manage. Sens. Netw.*, 2010, pp. 2–7.
[16] E. Elnahrawy and B. Nath, "Cleaning and querying noisy sensors," in *Proc. 2nd ACM Int. Conf. Wireless Sens. Netw. Appl.*, 2003, pp. 78–87.
[17] M. Rabbat and R. Nowak, "Distributed optimization in sensor network," in *Proc. 3rd Int. Symp. Inf. Process. Sens. Netw.*, 2004, pp. 20–27.
[18] K. Shao, F. Luo, N. Mei, and Z. Liu, "Normal distribution based dynamical recommendation trust model," *J. Softw.*, vol. 23, no. 12, pp. 3130–3148, 2012.



Jinfang Jiang received the BS degree in information & communication engineering from Hohai University, China, in 2009. She is currently working toward the PhD degree from the Department of Information & Communication System at Hohai University, China. Her current research interests are security and localization for sensor networks.

Guangjie Han received the PhD degree from the Department of Computer Science from Northeastern University, Shenyang, China, in 2004. He is currently a professor of Department of Information & Communication System at Hohai University, China. He is also a visiting research scholar of Osaka University from 2010 to 2011. He finished the work as a post doctor of Department of Computer Science at Chonnam National University, Korea, in 2008. He has served as an editor of KSII and JIT. His current research interests are security and trust management, localization and tracking, routing for sensor networks.

Feng Wang is currently working toward the PhD degree from the Department of Information & Communication Engineering at the Hohai University, China. He is also a lecturer in the School of Information Science & Engineering at the Changzhou University. His current research interests are task allocation for wireless sensor networks.

Lei Shu (M07) received the PhD degree from the National University of Ireland, Galway, Ireland, in 2010. Until March 2012, he was a specially assigned researcher in the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is a member of the IEEE, IEEE ComSoc, EAI, and ACM. Since October 2012, he joined Guangdong University of Petrochemical Technology, China as a full professor. Meanwhile, he is also working as the vice-director of the Guangdong Provincial Key Laboratory of Petrochemical Equipment Fault Diagnosis, China. He is the founder of Industrial Security and Wireless Sensor Networks Lab. His research interests include: wireless sensor networks, multimedia communication, middleware, security, and fault diagnosis. He has published more than 200 papers in related conferences, journals, and books. He had been awarded the Globecom 2010 and ICC 2013 Best Paper Award. He is serving as an editor in chief for EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, and associate editors for a number of famous international journals. He served as more than 50 various co-chair for the international conferences/workshops; TPC members of more than 150 conferences. He is a member of the IEEE.

Mohsen Guizani [S85, M89, SM99, F09] is currently a professor and the associate vice president for Graduate Studies at Qatar University, Doha, Qatar. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial boards of six technical Journals and the founder and EIC of *Wireless Communications and Mobile Computing Journal* published by John Wiley. He served as the chair of IEEE Communications Society Wireless Technical Committee (WTC) and chair of TAOS Technical Committee. He was an IEEE Computer Society Distinguished Lecturer from 2003 to 2005. He is a senior member of the ACM and a fellow of the IEEE.