Hindawi
Journal of Sensors
Volume 2017, Article ID 7864671, 16 pages
https://doi.org/10.1155/2017/7864671

Research Article

An Efficient Dynamic Trust Evaluation Model for Wireless Sensor Networks

Zhengwang Ye,[1,2] Tao Wen,[1,3] Zhenyu Liu,[1,3] Xiaoying Song,[1] and Chongguo Fu[1,3]

[1]*School of Computer Science and Engineering, Northeastern University, Shenyang, China*
[2]*Department of Network Information Center, Tonghua Normal University, Tonghua, China*
[3]*School of Computer Science and Technology, Dalian Neusoft University of Information, Dalian, China*

Correspondence should be addressed to Zhengwang Ye; zhengwang119@126.com

Received 7 April 2017; Accepted 25 September 2017; Published 24 October 2017

Academic Editor: Jaime Lloret

Trust evaluation is an effective method to detect malicious nodes and ensure security in wireless sensor networks (WSNs). In this paper, an efficient dynamic trust evaluation model (DTEM) for WSNs is proposed, which implements accurate, efficient, and dynamic trust evaluation by dynamically adjusting the weights of direct trust and indirect trust and the parameters of the update mechanism. To achieve accurate trust evaluation, the direct trust is calculated considering multitrust including communication trust, data trust, and energy trust with the punishment factor and regulating function. The indirect trust is evaluated conditionally by the trusted recommendations from a third party. Moreover, the integrated trust is measured by assigning dynamic weights for direct trust and indirect trust and combining them. Finally, we propose an update mechanism by a sliding window based on induced ordered weighted averaging operator to enhance flexibility. We can dynamically adapt the parameters and the interactive history windows number according to the actual needs of the network to realize dynamic update of direct trust value. Simulation results indicate that the proposed dynamic trust model is an efficient dynamic and attack-resistant trust evaluation model. Compared with existing approaches, the proposed dynamic trust model performs better in defending multiple malicious attacks.

1. Introduction

Nowadays, technology development in the fields of microelectromechanical system (MEMS) and wireless communication has facilitated the extensive distribution of WSNs. WSNs are composed of a large number of sensor nodes. In general, sensor nodes are reliable, accurate, flexible, inexpensive, and easy to deploy. Some areas and industries that are subject to environmental constraints rely on WSNs for data collection and monitoring [1]. They are widely used in many applications such as emergency response [2], healthcare monitoring [3], military, agriculture [4], environmental monitoring, and smart power grid [5]. However, due to the characteristics of working environments (usually deployed in remote and unattended) and the way of wireless communication, WSNs are prone to sudden accidents failures and suffer from attacks of malicious nodes. Once a node is compromised, the availability and integrity of the network can be destroyed. In addition, it is difficult to predict the malicious attacks. Hence, network security is a vital issue, which needs to be addressed to guarantee correct operation of the whole network.

Recently, in the security field of wireless network, a great deal of research [6–8] has been carried out commonly using cryptography, authentication, and hash functions to improve the security of network. Undoubtedly, the present achievements have greatly promoted related research in improving security of network, especially the confidentially, integrity, authentication, availability, and no-repudiation of data in the network. But in the security field of WSNs, the above traditional security mechanisms such as cryptography and authentication are not mostly suitable for processing capability constrained and energy limited WSNs due to the complexity and huge computing memory [9]. Furthermore, the traditional security mechanisms are widely and availably used to deal with external attacks but cannot solve insider or node misbehavior attacks effectively which are caused by the

captured nodes [10]. In pursuit of the security of WSNs, trust and reputation mechanisms have proven to be more resilient against insider or node misbehavior attacks [10, 11].

Trust in the field of wireless communication networks may be defined as the degree of belief on the future behavior of other nodes, which is based on past experience and observations of the nodes' action [11]. So, we give the definition of trust in WSNs as follows: node A's trust in node B describes the belief or expectation or assurance of sincerity, competence, and integrity of node B's future action/behavior [12]. The basic idea of trust based scheme is to quantify trust to describe the trustworthiness, reliability, or competence of individual nodes [5]. Trust management system can be implemented in various applications for security management such as secure protocol [8], secure data aggregation [13], trusted routing [14], and intrusion detection system [15]. In recent years, lots of state-of-the-art models [5, 12–31] have been proposed in this field. Undoubtedly, the present achievements have greatly promoted related research in improving security of WSNs. Even so, trust evaluation in WSNs is still a challenging issue. Some limitations are exhibited which need more attention to be solved.

Considerable research has been done on modeling and managing trust and reputation in WSNs. Many current studies [18–20] have been done for trust establishment just only based on the communication interaction records between nodes without considering the data consistency, so they cannot be against attacks on data. While other studies [25–28] combine multifactors to calculate the trust value, the multitrust sums up in weighted manner to compute the integrated trust. But the weights are obtained by expert opinion method or average weight method. The results of the prediction are subjective, which affect the scientific and flexibility of the trust decision. In addition, trust evaluation is a dynamic phenomenon and changes with time and environment condition. In many current trust models [23, 24], the trust value is updated by a sliding time window using forgetting or aging mechanism. But the number of sliding windows is defined by expert opinion method. Once the number of the sliding time windows is confirmed, it is difficult to change. It makes the trust models unable to adapt to the dynamic changes of the network environment, which affects the accuracy of the result. To our knowledge, there is no literature that can dynamically adjust the number of the sliding time windows and the parameters to achieve a dynamic update mechanism. Moreover, some existing trust models [18, 23, 27] rarely consider the influence of the energy consumption. Due to these reasons, there is a growing demand for adequate provision of an efficient dynamic trust evaluation model for WSNs; it can achieve accurate trust evaluation dynamically according to the environment and requirements and can realize the identification and defense of various types of malicious attack.

In this paper, an efficient dynamic trust evaluation model (DTEM) for WSNs is proposed that aims to address the above problems. In the proposed trust model, the trust value is calculated considering multitrust factors; it can achieve accurate trust evaluation. Moreover, DTEM can dynamically adjust the weights of direct trust and indirect trust. It reflects the dynamic adaptability of the trust computing. It also can dynamically adjust the parameters of the update mechanism to update the trust value to meet the actual needs of the network environment. The DTEM can be against various types of malicious attack and can be configured and effectively applied to different environments with different requirements. The major contributions of this paper are listed as follows:

(1) To improve the accuracy of trust evaluation, against attacks on data, the trust value is calculated considering direct trust and indirect trust. The direct trust is calculated considering multitrust including communication trust, data trust, and energy trust with the punishment factor and regulating function to meet the following: character "trust is hard to acquire and easy to lose." The indirect trust is evaluated conditionally by the trusted recommendations from a third party.

(2) To ensure that the trust model makes a decision more scientifically, dynamically, and adaptively, we define a dynamic balance weight factor function which is changed dynamically with the number of communication interactions. The adaptive dynamic balance weight factor dynamically adjusts the weight of the direct trust and indirect trust.

(3) To make sure that the proposed trust model can be configured and effectively applied to different environments with different requirements and against on-off attack, we give an update mechanism by a sliding time window based on induced ordered weighted averaging operator (IOWA) to enhance flexibility. We can dynamically adapt the parameters and the interactive history windows number to change the weight sequence to update the trust value to adapt with different environments and requirements. Meanwhile, on-off attacks can be handled efficiently.

At last, compared to the existing trust models (RFSN [18] and BTMS [24]), simulation results show that the proposed trust model has remarkable enhancements in the accuracy of trust decision and has a better capability to capture dynamic malicious nodes behaviors.

The remainder of this paper is organized as follows. Section 2 gives an overview of related works. Network model and attack model are described in Section 3. Section 4 gives the overview and process of the DTEM. Section 5 discusses trust model and trust evaluation mechanism in DTEM. In Section 6, the experiment is made under simulative environments and the performance of the DTEM is evaluated. Section 7 concludes this paper.

2. Related Works

In most current trust model researches focus on sensor radio communication behaviors. Sensor nodes build node trust model through wireless radio transaction with neighboring nodes. Ganeriwal and Srivastava [18] first proposed a reputation based framework for sensor networks (RFSN) where

nodes used reputation to evaluate other's trustworthiness. The framework uses watchdog mechanism to monitor communication behavior of neighboring nodes and represents node reputation distribution using Beta distribution. Then the trust value is figured out according to the statistical expectation of the probability reputation distribution. The trust framework is good robustness and very classic. But the recommendation trust is not considered; it cannot resist various internal attacks. In [19], an agent-based trust model was proposed in WSNs (ATSN); agent node was used to monitor behaviors of sensor nodes and classify the behaviors into good or bad ones. Agent nodes count all the number of good behaviors and malicious behaviors, respectively, and save the results into a three-tuple. ATSN scheme uses agent which can save the computational resources and energy consumption. However, in ATSN, only the direct trust value is calculated while the recommendation trust is ignored. In addition, the updating process of the trust value is not considered. Shaikh et al. [20] proposed a new lightweight group-based trust management scheme (GTMS) for clustered WSNs. The trust value is obtained through the communication behavior of neighboring nodes. It works on trust at three levels: the node level, the cluster head level, and the base station level. The model establishes trust mechanism from the above aspects to resist the attack of malicious nodes, respectively. GTMS can effectively resist the attacks of malicious nodes, and it does not require large data storage and complex computations. However, only observing the number of successful and unsuccessful interactions cannot reflect soundest trust value. Song et al. [21] proposed a dynamic trust evaluation method based on multifactor. The nodes' trustworthiness is measured by combining direct trust with indirect trust dynamically. Besides, both the involved classification standard and dynamic weight assignment are dependent on the interaction times between nodes, which are put forward under the background of Hoeffding's Inequality in Probability Theory. The simulation results show that this method is sensitive to multiple attacks. But the updating process of the trust value is not considered. Li et al. [22] proposed a lightweight and dependable trust system for the clustered WSNs. The trust decision-making scheme is proposed based on the nodes' roles in clustered WSNs. They improve system efficiency by canceling feedback between cluster members or between cluster heads. The trust scheme also defines a self-adaptive weighted method for trust aggregation at cluster head level. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. In [23], He et al. defined an attack-resistant and lightweight trust management scheme called ReTrust. This system is oriented to medical sensor network and based on hierarchical architecture, comprised of master nodes and sensor nodes. ReTrust uses sliding time window and aging factor to identify and eliminate the on-off attack. Bad-mouthing attack is avoided by eliminating outliers after collecting recommendations. It is resistant to bad-mouthing and on-off attacks. However, the drawback of this scheme is that master nodes must have abundant storage and energy. Feng et al. [24] proposed a credible Bayesian-based trust management scheme (BTMS). The trust management scheme takes the direct and indirect trust into account. The direct trust is calculated by a modified Bayesian equation with punishment factor and updated by a sliding window using an adaptive forgetting factor. Moreover, the indirect trust computation is invoked from a third party. BTMS performs better in resisting attacks.

While in above-mentioned trust models data security is neglected, in existing trust models many of them focus on the trust of data as the main work. In [25], Zhan et al. proposed a resilient trust model with a focus on data integrity and sensor node trust for hierarchical WSNs. The sensor node current trust level is evaluated through the past history and recent risk. And then it employs Gaussian model to rate data integrity in a fine-grained style. The model is proven to be resilient against faulty data and malicious data manipulation. But the energy consumption on node is not considered. In [26], a wireless sensor network based on multiangle trust of node was proposed. The method considers the sensing data and the node's energy in the factors of trust assessment; the integrated trust value is calculated through the average weight of the communication trust, energy trust, and data trust. It is more reliable and effective against Dos attack and data forgery attack. But the trust update mechanism is ignored. Jiang et al. [27] proposed an efficient distributed trust model (EDTM) for wireless sensor networks. In EDTM, the direct trust and recommendation trust are selectively calculated according to the number of packets received by sensor node. The direct trust value is calculated through the average weight of the communication trust, energy trust, and data trust. In addition, trust reliability and trust familiarity are defined to improve recommendation accuracy. EDTM can evaluate trustworthiness of sensor nodes more precisely and identify the malicious nodes more effectively. In [28], a consensus-aware sociopsychological trust model for WSNs was proposed. The trust model uses the concept of consensus and consistency in understanding the behavior of the sensor nodes for detecting fraudulent nodes in WSN. The factors of ability, benevolence, and integrity are used for the computation of trust. The approach can deal even in the presence of higher number of fraudulent nodes than benevolent nodes. It is more reliable and effective against attacks on data in WSNs. But, communication faults that delay the rate at which packets are sent are not considered.

Recently, several techniques are used in computing the trust of sensor nodes, such as the fuzzy logic approach, the Bayesian network approach, the game theoretic approach, swarm intelligence, and the cloud method. In [29], Feng et al. first established various trust factors depending on the communication behaviors to evaluate the trustworthiness of sensor nodes. The direct and indirect trust are obtained through calculating weighted average of trust factors. Meanwhile, the fuzzy set method is applied to measure how much the trust value of node belongs to each trust degree. And then the evidence difference is calculated between the direct and indirect trust, which links the revised D-S evidence combination rule to finally synthesize integrated trust value of nodes. Zhang et al. [30] proposed a trust evaluation method for clustered wireless sensor networks based on cloud model. The method considers multifactors including

communication factor, message factor, and energy factor to get factor trust cloud. And the trust cloud is calculated by assigning weights for each factor trust cloud and combining them. The final trust cloud is measured by synthesizing the recommendation trust cloud and immediate trust cloud and is converted to trust grade by trust cloud decision-making. The method can detect malicious nodes according to different secure requirements under different WSNs applications, which provides a safe running environment for different applications. Shen et al. [31] studied the trust decision and its dynamics that played a key role in stabilizing the whole network using evolutionary game theory. The evolutionary game theory is used for the area of trust evolution in WSNs. It sets up a WSNs trust game concerning the dynamics of trust evolution during sensor node's decision-making. When sensor nodes are making their decisions to select action trust or mistrust, a WSNs trust game is created to reflect their utilities. It can find out the conditions that will lead sensor nodes to choose action trust as their final behavior to ensure WSNs' security and stability.

Our work is partly motivated by those related works above; however, there are some distinctions compared with them. In our trust model, the trust value is calculated considering multitrust factors including communication trust, data trust, and energy trust. Not like the works in [18–20], the trust values are just only based on the communication interaction records, so they cannot be against attacks on data. While other studies [25–28] combine multifactors to calculate the trust value, they do not consider the following character: "trust is hard to acquire and easy to lose." In our proposed trust model, we add the punishment factor and regulating function to realize the punishment and adjustment of trust value against bad-mouth attack and collusion attack. Then, in most trust models such as in [18, 25–28], the direct trust and indirect trust sum up in weighted manner to compute the integrated trust. But the weights are obtained by expert opinion method or average weight method in [25–28]. In our proposed trust model, we define an adaptive dynamic balance weight function to dynamically adjust the weight of the direct trust and indirect trust. Although the works in [21, 22] have given various computation methods of the dynamic balance weight, the trust decision of our proposed trust model is more scientific and flexible. Furthermore, the most important thing is the dynamic of the trust evaluation model. In many current trust models [23, 24], the trust value is updated by a sliding time window using forgetting or aging mechanism against on-off attack and other malicious attacks, but the number of sliding time windows is predefined. Once the number of the sliding time windows is confirmed, it is difficult to adapt to the dynamic changes of the network. In our proposed trust model, we centrally focus on setting up a dynamic update mechanism. To our knowledge, there is no literature that can dynamically adjust the number of the sliding time windows and the parameters to achieve a dynamic update mechanism. In our proposed efficient dynamic trust model, an update mechanism is defined by a sliding time window based on induced ordered weighted averaging operator (IOWA) to enhance flexibility. We can dynamically adapt the parameters and the interactive history windows number to change the weight sequence to meet the actual needs of the network. Based on the above analysis, the proposed trust model can be dynamically adjusted according to the environment and requirements to achieve accurate trust evaluation and can realize the identification and defense of various types of malicious attack. It has a powerful capability of the trust estimation for WSNs.

3. Network Model and Attack Model

3.1. Network Model. In this paper, we consider a scenario in which all the sensor nodes are randomly deployed in a two-dimensional space. Nodes are neither added nor removed from network after deployment. It assumes that sensor nodes have the same capabilities of computing, communicating, and storing, initial energy level, and communication range, only when the two nodes enter the communication range of each other to start communication. Based on these assumptions, WSNs can be abstracted as a graph $G = (V, E)$, where V is the set of all nodes and E is the set of all edges. Each edge $e(i, j) \in E$ denotes that the two nodes are located within each other's transmission range. Each node keeps a list of neighboring nodes which stores their unique ID, communication information, and trust relationship. It assumes that neither the source nor the destination is malicious. Malicious nodes do not collude themselves and all communication links are bidirectional. And the communication channel is secure.

3.2. Attack Model for WSNs. With the open and remote deployment environment, WSNs are generally susceptible to various internal attacks, including black hole attack, wormhole attack, Sybil attack, and grey-hole attack. The attack behavior of those malicious nodes shows diversity [6], such as discarding routing packets, injecting large amounts of redundant information and error information, maliciously modifying data packets, and providing unreal recommendation trusted data information. According to the attack behavior and target of malicious attack, we divide the various attacks into three categories: attacks on routing protocols in WSNs [32, 33], attacks on communications data or messages, and attacks on trust models in WSNs [34]. The target of the first kind of malicious attack is the routing protocol. The malicious attack behavior of this type discards all the routing packets or drops part of the routing packets, which makes the data packets unable to be forwarded properly between nodes. This type of attack includes black hole attack, grey-hole attack, and wormhole attack. Due to the vulnerability of the wireless communication channel, the second type of malicious attack is that the malicious nodes can easily capture transmitting data information through a wireless link. The target of this type of malicious attack is communications data or messages. The transmitting data can be easily conducted with eavesdropping, forgery, and tamper. This type of attack includes Dos attack and message tampering attack. The third type of malicious attack is a special kind of attack, whose target is the trust management. This type of malicious attack can destroy the trust model by providing false information. This type of attack includes on-off attack, conflicting behavior, selfish attack, and bad-mouthing attack.

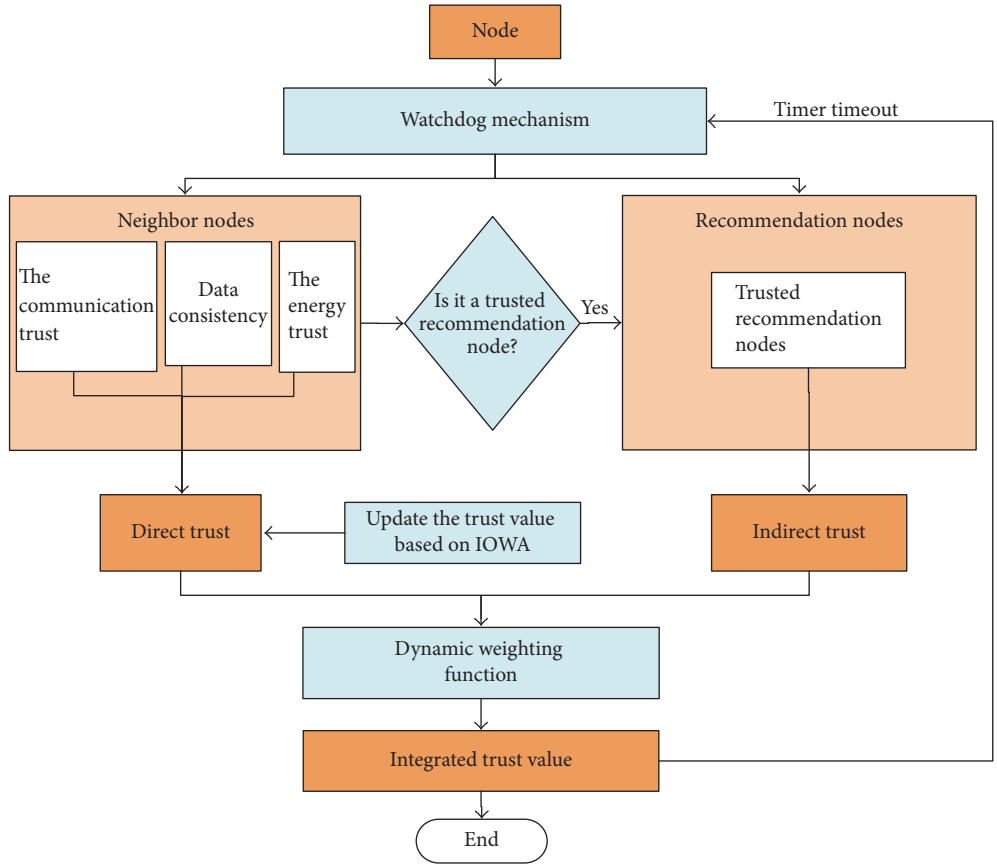

Figure 1: The process of the proposed trust model.

As we know, trust management system can deal with most of the existing attacks and improve the security of the network. However, it is difficult to detect these malicious nodes completely by conventional trust model. The proposed DTEM can evaluate trustworthiness of sensor nodes more precisely and identify the different malicious nodes more effectively.

4. Overview of the Efficient Dynamic Trust Evaluation Model

To efficiently compute the trust values on sensor nodes, we first need a clear understanding of the trust model process. The DTEM runs at the middleware of every sensor node. Every node maintains the trust value about other nodes; there is no central repository for storing trust values of every entity in the system. The process of DTEM is shown in Figure 1; the direction of the arrow represents the flow of information between them. And the specific process is as follows.

(1) Information gathering: we use watchdog mechanism to monitor neighboring nodes' activities periodically as RFSN [18] to collect evidence information. The available neighbor nodes' information is stored in the routing table of the node.

(2) Trust value calculation: in the proposed trust models, when a subject node wants to obtain the trust value of an object, it first checks its recorded list of neighbor nodes. The direct trust and recommendation are used to evaluate the trustworthiness of sensor nodes based on the recorded list. The direct trust is directly calculated based on the communication, data consistency, and energy. 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. Due to the dynamic behavior of WSNs and the impact of some special malicious attacks like on-off attack, the calculation of trust value should be based upon history interaction records and updated periodically.

(3) Trust value integration: to ensure that the trust model makes a decision more scientifically, dynamically, and adaptively, we define a dynamic balance weight factor to realize the integration trust value of direct trust and indirect trust.

Trust evaluation process is a complex process. The information on a sensor node's prior behavior is one of the most important aspects in trust model. Hence, every node maintains the trust value about other nodes in routing table;

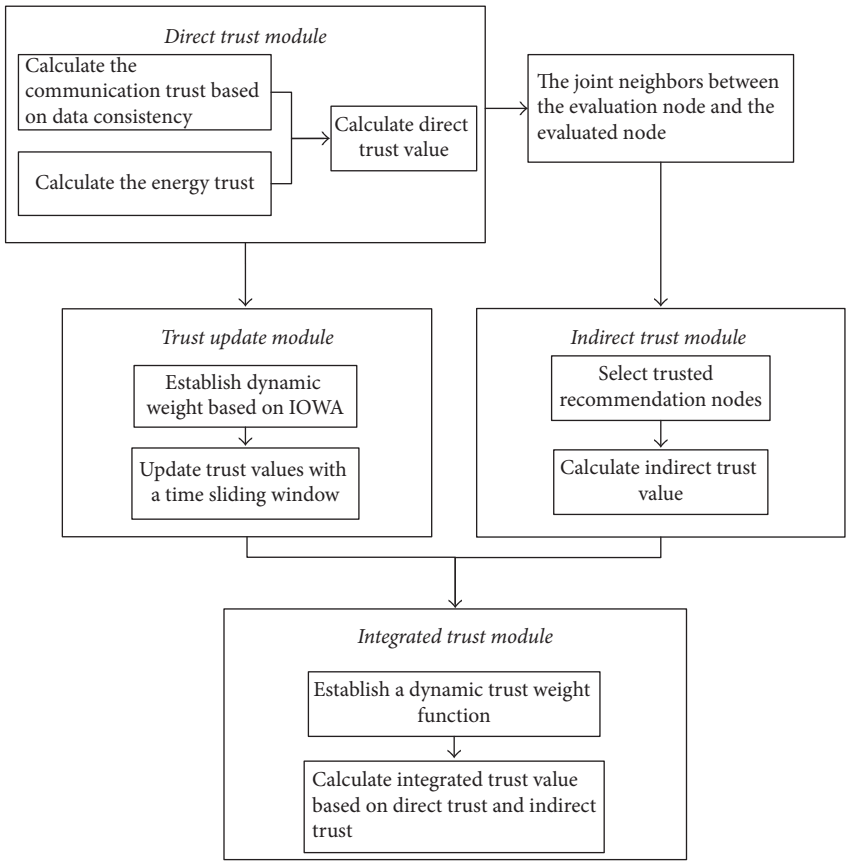

Figure 2: The relationship among the four modules.

the process of the trust model is periodic. The evaluation results of trust values depend on historical records of each node.

5. The Efficient Dynamic Trust Evaluation Model

In this section, we present the composition of the proposed efficient dynamic trust evaluation model and the calculation procedure of trust in detail.

5.1. The Composition of the Efficient Dynamic Trust Evaluation Model. The efficient dynamic trust model proposed in this paper consists of the following four modules: direct trust module, indirect trust module, integrated trust module, and trust update module. The direct trust is calculated based on the Beta trust model. The direct trust value of sensor node is calculated by taking communication trust, data trust, and energy trust into account. The indirect trust is evaluated based on the trusted recommendations from a third party. And then the integrated trust is calculated by assigning adaptive dynamic balance weights for direct trust and indirect trust and combining them. Finally, we give an update mechanism by a sliding time window based on IOWA to complete the updating of direct trust value according to historical interaction records. The relationship among the four modules is shown in Figure 2. And the specific implementation process is as follows.

5.2. The Calculation of Direct Trust. As we know, the evaluation of trust in WSNs is a complex process, which includes a lot of factors. In the proposed trust model, the direct trust value is calculated by taking communication trust, data trust, and energy trust into account. The communication trust measures whether sensor nodes can cooperatively perform the intended protocol. The data trust measures the trust of data created and manipulated by sensor node, which can assess the fault tolerance and consistency of data. The energy trust measures whether a node has enough residual energy to complete new communications and data processing tasks. We consider the communication behavior and data consistency to establish a trust environment against errors and attacks and combine the energy factor to prevent the low competitive nodes from participating in the network operation to ensure network security and reliable operation. Next, we give the detailed calculation procedure of direct trust.

5.2.1. The Communication Trust Based on Data Consistency. We assume that a node can monitor neighboring nodes' activities within its communication range using watchdog mechanism [18]. For example, a node can monitor its neighbors' transmissions, and in this way we can detect whether

the node is forwarding or dropping the packets. In most current trust models, they define trust as the probability that node i holds on node j to perform as expected [24]. Assume that Beta distribution is employed as the prior distribution of interactions among sensor nodes. They monitor the communication interaction record information based on watchdog mechanism to count the number of well behaviors or malicious behaviors between nodes to calculate the trust value. The trust model at every node uses Beta probability density function [35] to evaluate expected probability of well behavior of neighboring nodes because trust modeling problem is characterized by uncertainty. And the Beta probability density function can be represented as

$$f(x \mid \gamma, \beta) = \frac{1}{B(\gamma, \beta)} x^{\gamma-1} (1-x)^{\beta-1}, \quad (1)$$

where $0 \le x \le 1$, $\gamma > 0$, $\beta > 0$, and γ and β are two indexed parameters.

If the number of successful (well behavior) outcomes is represented by a and b represents the number of unsuccessful (malicious behavior) outcomes between nodes, the probability for outcomes can be obtained by setting the values for γ and β as follows:

$$\begin{aligned} \gamma &= a + 1, \\ \beta &= b + 1. \end{aligned} \quad (2)$$

The probability expectation value for Beta probability density function is defined as

$$E(x) = \frac{\gamma}{\gamma + \beta} = \frac{a+1}{a+b+2}. \quad (3)$$

Equation (3) can be used for the computation of the probability expectation of successful outcomes between nodes. The probability expectation value is defined as the trust value.

Based on the above discussion, we assume that the way of future interaction is the same as that of the previous one; the probability expectation function can be represented by the mathematical expectation of Beta distribution as the communication trust. In our proposed model, the communication trust, denoted by $TC_{ij}(t)$, is derived from the direct observations of node i on node j at time t, which is defined as

$$TC_{ij}(t) = \frac{S+1}{S+F+2} \left(1 - \frac{F}{W}\right) \left(1 - \frac{1}{S+\delta}\right), \quad (4)$$

where S and F denote the total amount of successful and unsuccessful interactions between nodes i and j during t, respectively. But they are different from the above discussion that just considered whether the node is forwarding or dropping the packets. In (4), the node's successful or unsuccessful interaction is accessed by communication behavior and data consistency together. The expression $(1 - F/W)$ [24] is called punishment factor, where W is the total number of effect interaction records. The punishment factor punishes trust value by the dynamic change of the number of malicious behaviors between nodes. The expression $(1 - 1/(S + \delta))$ is called regulating function, which approaches 1 rapidly with the increasing of the number of successful interactions, where δ is a positive constant that can be tuned to control the speed of reaching 1. It would take longer time for a node to increase its trust value for another node. The detailed realization of each part is as follows.

In (4), successful or unsuccessful communication between nodes is judged by the communication behaviors and data consistency together. The successful communication means that a node not only forwards the packets to its next hop neighbor but also requires forwarding the packets reliably in its true form. Otherwise, it will be considered as unsuccessful communication. The evaluated node forwards the packets to its next hop successfully based on the watchdog monitored [18]. The data consistency based on the detection algorithm is as follows.

Following the idea introduced in [36], the data trust affects the trust of the sensor nodes that created and manipulated the data. The data packets have spatial correlation in WSNs; that is, the packets sent among neighboring nodes are always similar in the same area. And the difference among nodes is reduced to zero. In our proposed paper, we use the detection algorithms [37] to assort abnormal and honest data in the network. The detection algorithm compares a localized threshold $\lambda_i(t)$ to the difference produced by each node data and its neighbors. The node i makes a measurement independently and transfers the measurement data value $x_i(t)$ to its neighboring node j. Then, node i compares the data value $x_i(t)$ to its neighbor's node j's value $x_j(t)$. It is denoted as normal if $|x_j(t) - x_i(t)| < \lambda_i(t)$ is satisfied, and else if $|x_j(t) - x_i(t)| \ge \lambda_i(t)$ is satisfied, it is denoted as abnormal. According to commutation behavior and data consistency, we can get S and F, which denote the total amount of successful and unsuccessful interactions between nodes during t, respectively.

Considering that the malicious node injection false data has a large deviation from the sensing data of authentic nodes, we can detect the attacker by comparing the threshold with the difference between the neighbors and the node i. The equation of the threshold $\lambda_i(t)$ of each node i as follows:

$$\lambda_i(t) = \frac{1}{|N_i|} \sum_{j \in N_i} \left| x_j(t) - \frac{x_i(t) + \sum_{j \in N_i} x_j(t)}{|N_i| + 1} \right|, \quad (5)$$

where N_i represents the neighbor set of node i. The number of element in N_i is denoted by $|N_i|$.

In (4), the punishment function shows strict punishment to trust value according to the number of malicious behaviors. Once the number of misbehavior behaviors increases, the trust value drops rapidly. It reflects the following trust character: "trust is easy to lose." It can quickly and accurately identify the malicious behavior.

We choose the regulating function in (4) instead of a linear function since such a function would approach very slowly to 1 with the increasing of successful interactions which is similar to literature [20]. According to the regulating function, it would take longer time for a node to increase one's trust value. This design can effectively restrain the trust value rapidly increasing with the sudden increasing

number of successful communication interactions. It reflects the following trust character: "trust is hard to acquire." It can restrain the collusion or on-off attack.

5.2.2. The Energy Trust. The energy trust is introduced mainly to complete the assessment on the performance of a node itself. By introducing the energy factor, we can effectively avoid the low competitiveness of nodes participating in network operation. When the energy consumption of a node is lower than a certain energy threshold E_{th}, the node can only complete simple basic operation to prolong the network lifetime and balance energy consumption between nodes. The energy trust is defined as

$$TE_j(t) = \begin{cases} 0, & \text{if } E_{\text{res}} < E_{\text{th}}, \\ 1, & \text{else}, \end{cases} \tag{6}$$

where E_{res} represents the residual energy of a node. E_{th} represents the energy threshold.

5.2.3. The Direct Trust. Based on the communication trust $TC_{ij}(t)$ and the energy trust $TE_j(t)$, we can obtain the direct trust between two neighbor nodes as

$$TD_{ij}(t) = \begin{cases} TC_{ij}(t), & \text{if } TE_j(t) = 1, \\ 0.5 * TC_{ij}(t), & \text{else } TE_j(t) = 0. \end{cases} \tag{7}$$

5.3. The Calculation of Indirect Trust. Similar to most existing related works, we also consider the indirect trust to evaluate the trust value in the proposed trust model. The indirect trust value is evaluated by the recommendations from a third party. The recommendations are composed of the common neighboring node k of node i and node j, symbolized as N_k. As we know, trust has the property of transitivity. In the most existing trust models, the trust value T_{ij}^{v} from node i to node j is calculated by the recommendation N_v ($N_v \in N_k$) and is notated as

$$T_{ij}^{v} = T_{iv} \times T_{vj}, \tag{8}$$

where T_{ij}^{v} is the trust value of node i to node v to node j. T_{iv} is the direct trust value of node i to the common neighbor node N_v; T_{vj} is the direct trust value of the common neighbor node N_v to j. But not all the recommendations are reliable. How to detect and get rid of malicious recommendations is important since it has great impact on the calculation of trust. In order to judge the credibility of recommendations to calculate indirect trust more accurately, it needs to detect dishonest recommendations and exclude them before recommendation aggregation. In our proposed model, we only choose the recommendation whose trustworthiness is higher than the specified trust threshold θ ($0 \le \theta \le 1$). Suppose there are k recommendations and their direct trust values held by node i are notated as $T_{i1}, T_{i2}, \ldots, T_{in}, \ldots, T_{i(k-1)}, T_{ik}$. If $T_{in} \ge \theta$ ($n = 1, 2, \ldots, k$), the recommendation from N_n is accepted. Otherwise, it will be totally neglected.

Due to the above discussion, we can get the trusted recommendations. In our trust model, we assign different weights to the selected recommendations by their direct trust. Intuitively, we should give more weight to the selected recommendation from recommenders with high reputation. Hence, we allocate weights based on the trust degree of the recommenders to avoid individual preference. The following approach is taken to calculate the weight ϖ_n of the selected recommendation N_n:

$$\varpi_n = \frac{T_{in}}{\sum_{n=1}^{q} T_{in}}, \quad n = 1, 2, \ldots, q, \tag{9}$$

where T_{in} is the direct trust value of node i to the common neighbor node N_n, and q is the number of the selected recommendations. And $0 \le \varpi_n \le 1$ and $\sum_{n=1}^{q} \varpi_n = 1$.

Finally, the indirect trust value, denoted by $TI_{ij}(t)$, is obtained:

$$TI_{ij}(t) = \sum_{n=1}^{q} \varpi_n * T_{ij}^{n}, \quad n = 1, 2, \ldots, q, \tag{10}$$

where ϖ_n is the weight of T_{ij}^{n}. T_{ij}^{n} is obtained using (8), which represents the trust value from node i to node j calculated by the recommendation N_n.

5.4. The Integration of Trust Value. The integrated trust value $T_{ij}(t)$, which node i holds about node j at time t, is established via the following formula:

$$T_{ij}(t) = \varphi TD_{ij}(t) + (1 - \varphi) TI_{ij}(t), \tag{11}$$

where φ is the balance weight factor, which is referred to as self-confidence factor and $\varphi \in [0, 1]$. The value of φ is the degree of recognition of the direct trust and indirect trust of i to j. φ is defined using a dynamic function; the function introduced in the literature [38] is given as

$$\varphi = f(k) = \frac{1}{2} + \frac{1}{\pi} \arctan\left(10 \times \frac{k - \text{COM}_{\text{th}}}{N}\right), \tag{12}$$

where the balance weight factor φ is changed dynamically with the number of communication interactions k to defect caused by allotting weights subjectively. N is the maximum interaction between i and j. The specific value is determined according to the network environment and the specific requirement. COM_{th} is the threshold of communication interactions. When the communication interactions between evaluation node and evaluated node are higher than the threshold COM_{th}, the weight factor becomes much more and the integrated trust value is more dependent on the direct trust value. Otherwise, the communication interactions between neighbor nodes are too small; it is difficult to decide whether the evaluated node is good or bad, and the integrated trust value is more dependent on the indirect trust value. We can dynamically adjust the importance of direct trust and indirect trust according to the dynamic weight factor function.

In the process of the integrated trust quantitative calculation, we introduce a dynamic balance weight factor to

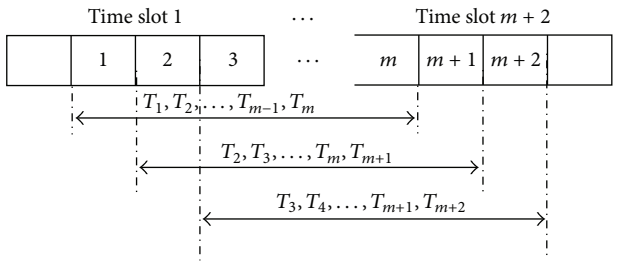

Figure 3: The sliding time window.

solve the weight problem of direct trust and indirect trust. The balance weight is changed dynamically with the number of communication interactions, which reflects the dynamic adaptability of the trust computing.

5.5. The Update of the Direct Trust. In our proposed model, we use a sliding time window to update the trust value [20], which can reflect the extent of variation of the trust value in a particular time interval.

The sliding time window is used to update the direct trust value. It consists of several time slots; each slot is a cycle time. Only interactive records within the sliding time windows are valid. We define the length of sliding window as m, which reflects evaluator's emphasis on historical records. As Figure 3 shows, each sliding time window is divided into m slots from left to right. The update process of the trust value can be shown as $T_1, T_2, \ldots, T_{m-1}, T_m$; $T_2, T_3, \ldots, T_m, T_{m+1}$; $T_3, T_4, \ldots, T_{m+1}, T_{m+2}$. However, it is intuitive that old historical record has less contribution and new historical record has more influence on trust decision. We give an update mechanism using a sliding time window based on induced ordered weighted averaging operator (IOWA) [39] to solve the problem of trust update. We use the IOWA operator to obtain the weight of each time window, which can give more accurate evaluation of the direct trust in DTEM.

IOWA is defined as follows: assume $\langle v_1, a_1\rangle, \langle v_2, a_2\rangle, \ldots, \langle v_m, a_m\rangle$ is two-dimensional array for m, and

$$f_W\left(\langle v_1, a_1\rangle, \langle v_2, a_2\rangle, \ldots, \langle v_m, a_m\rangle\right) = \sum_{i=1}^{m} w_i^* a_{v\text{-index}(i)}. \tag{13}$$

The function f_W is called the m-dimensional induced ordered weighted averaging operator generated by $v_1, v_2, \ldots, v_m$, abbreviated as IOWA operator, and v-index(i) is the index of the $v_1, v_2, \ldots, v_i, \ldots, v_m$ in the order from large to small ones. $W = (w_1^*, w_2^*, \ldots, w_m^*)^T$ is the ordered weighted vector of IOWA and satisfies $\sum_{i=1}^{m} w_i^* = 1$, $0 \le w_i^* \le 1$, $i = 1, 2, \ldots, m$.

From (13), we can know that the value of $a_1, a_2, \ldots, a_m$ corresponds to the order in which the induced values of $v_1, v_2, \ldots, v_m$ in descending sorting are ordered weighted averages; the weight coefficient w_i^* has nothing to do with the size and position of a_i but is related to the location of the induced value v_i. Hence, the model can be used to sort the historical trust value according to the time of occurrence, and the sliding time window is used as the induced value of the IOWA operator, and the IOWA operator is completely used to update the trust value.

In accordance with the occurrence time, the trust evaluation sequence of nodes i on the node j is expressed as follows: $T = \{T_1, T_1, \ldots, T_t, \ldots, T_m\}$, $0 \le T_t \le 1$, $1 \le t \le m$, in which T is the trust evaluation sequence based on the sliding time window. Each value corresponds to a child window, and the time parameter is added to each of the T elements: $\langle t_1, T_1\rangle, \langle t_2, T_2\rangle, \ldots, \langle t_m, T_m\rangle$, and the two-dimensional trust sequence is defined as the induced value based on the time sliding window. The trust update depends on both real-time and historical windows to complete the updating operation. It means that we know $\langle t_1, T_1\rangle, \langle t_2, T_2\rangle, \ldots, \langle t_m, T_m\rangle$, obtaining $\langle t_{m+1}, T_{m+1}\rangle$, and this is what IOWA can solve. The definition can be expressed as

$$T_{m+1} = f_W\left(\langle t_1, T_1\rangle, \langle t_2, T_2\rangle, \ldots, \langle t_m, T_m\rangle\right) = \sum_{i=1}^{m} w_i^* T_{v\text{-index}(i)}, \tag{14}$$

where w_i^* represents the importance of the trust value of the ith child window, and $\sum_{i=1}^{m} w_i^* = 1$, $0 \le w_i^* \le 1$, $i = 1, 2, \ldots, m$. So the ordered weighted vector $W^* = (w_1^*, w_2^*, \ldots, w_m^*)^T$ is T's weight; the key problem of the updating mechanism of trust model is how to find the classification weight of each window.

Let $W^* = (w_1^*, w_2^*, \ldots, w_m^*)^T$ be the ordered weighted vector of any IOWA operator. The perfect method of the weighted vector is based on the maximum degree of dispersion [35], which can make full use of all the data information under given and/or degree [40]. We can get the weight vector as follows:

$$\alpha = Orness\left(W^*\right) = \frac{1}{m-1}\sum_{i=1}^{m}(m-i)\, w_i^*, \tag{15}$$

$$w_j^* = \sqrt[m-1]{w_1^{*m-j} w_m^{*j-1}}, \quad 2 \le j \le m, \tag{16}$$

$$w_1^*\left[(m-1)\alpha + 1 - m w_1^*\right]^m = \left[(m-1)\alpha\right]^{m-1}\left[\left((m-1)\alpha - m\right) w_1^* + 1\right], \tag{17}$$

$$w_m^* = \frac{\left((m-1)\alpha - m\right) w_1^* + 1}{(m-1)\alpha + 1 - m w_1^*}. \tag{18}$$

In addition, the relationship of trust has time decay. In the trust sequence of $\langle t_1, T_1\rangle, \langle t_2, T_2\rangle, \ldots, \langle t_m, T_m\rangle$, the element of $\langle t_m, T_m\rangle$ has the greatest influence on $\langle t_{m+1}, T_{m+1}\rangle$, and the longer the time, the smaller the influence on trust decision. In (18), we can know that the calculation of the weight coefficient vector is mainly determined by two parameters: the parameters α and the number of interactive history windows m. According to the literature [41], we know that when $\alpha \in [0.5, 1]$, the distribution of the weight coefficients satisfies the characteristic of time decay. The corresponding weight sequences in different m and α are shown in Table 1.

Table 1: The weight sequence in different m and α.

	$\alpha = 0.5$	$\alpha = 0.6$	$\alpha = 0.7$	$\alpha = 0.8$	$\alpha = 0.9$	$\alpha = 1$
$m = 3$	{0.3333, 0.3333, 0.3333}	{0.2384, 0.3233, 0.4384}	{0.1540, 0.2921, 0.5540}	{0.0819, 0.2363, 0.5540}	{0.0263, 0.1474, 0.8263}	{0.0, 0.0, 1.0}
$m = 4$	{0.25, 0.25, 0.25, 0.25}	{0.1671, 0.2133, 0.2722, 0.3474}	{0.0984, 0.1647, 0.2756, 0.4614}	{0.0450, 0.1065, 0.2520, 0.5965}	{0.0103, 0.0434, 0.1821, 0.7641}	{0.0, 0.0, 0.0, 1.0}
$m = 5$	{0.2, 0.2, 0.2, 0.2, 0.2}	{0.1278, 0.1566, 0.1920, 0.2353, 0.2884}	{0.0706, 0.1086, 0.1672, 0.2574, 0.3962}	{0.0290, 0.0599, 0.1240, 0.2565, 0.5307}	{0.0051, 0.0175, 0.0602, 0.2068, 0.7105}	{0.0, 0.0, 0.0, 0.0, 1.0}

Table 2: Simulation parameters.

Parameter	Value
Initial energy/J	0.5
Initial trust value	0.5
Packet length/bit	2000
d/m	37
Number of behaviors in each time unit	10
Trust estimation period/s	10
Simulation time/s	1000
θ	0.5
m	4
α	0.7

It can be seen from Table 1 that the value of the parameter α reflects the forgetting degree of the history interactive experience in trust model. When α is larger, the historical experience is easier to forget. And if $\alpha = 1$, the previous history is completely forgotten. So, we can dynamically adjust α to meet the different needs of the trust model. The value of parameter m responds to the number of windows of historical experience. When m is larger, the trust value is obtained more accurately. But it requires more energy consumption and storage space. So, the determined parameter m requires a combination of the actual demand and considers the restriction of WSNs in accordance with the requirements definition.

6. Simulation Results and Analysis

Our experiments are performed using Matlab to analyze the performance of the proposed algorithm similar to the literature [25, 29]. The concrete simulation scene is set to be 100 m × 100 m, with 50 randomly deployed nodes. Some parameters vary with the scenes and the purposes of experiment and will be explained in detail. The other default simulation parameters that we have chosen are summarized in Table 2.

In this section, the simulations can be divided into two parts. First, we analyze the performance of the DTEM, which includes the effect of dynamic weight value on integrated trust value and the direct trust value update mechanism. Then, we compare DTEM with the existing trust models, typical RFSN [18], and BTMS [24]. The results demonstrate that the DTEM has a powerful capability of the trust estimation.

6.1. The Performance of the DTEM. In this section, we analyze the dynamic performance of the DTEM.

6.1.1. The Effect of Dynamic Weights on Integrated Trust Value. The value of φ is the degree of recognition of the direct trust and indirect trust of i to j. The relationship between the dynamic weight of φ and the number of interaction times is shown in Figure 4. As shown in Figure 4, in the early stage of trust measurement, when the number of interactions is less

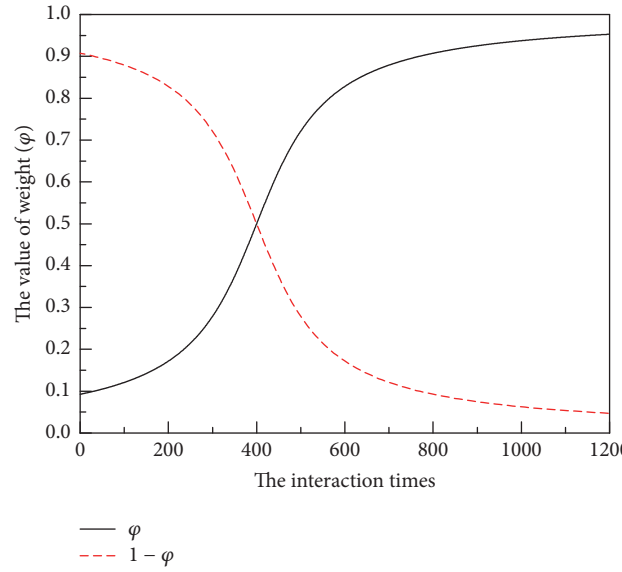

Figure 4: The dynamic weights of the direct values φ and $1 - \varphi$.

than COM_{th}, the trust calculation is much more dependent on the indirect trust value. With the increasing of the number of interactions, when the number of interactions is greater than COM_{th}, the node i is more willing to believe their direct interactive experience, and the weight φ of direct trust will become much larger. Hence, the weight factor φ is dynamically changed with the interaction times. And the value of COM_{th} can be adjusted according to the actual demand of the network to achieve a more reasonable distribution of the weights between direct trust and indirect trust. In this paper, we give $N = 1200$, and $\text{COM}_{\text{th}} = N/3$. And giving $\varphi = 0.1, 0.5, 0.9$ and the dynamic value, the effect of φ on the integrated trust value is shown in Figure 5, respectively. As shown in Figure 5, at the beginning, the interactions between nodes are very few; the effect of dynamic weight φ on integrated trust value is relatively close to $\varphi = 0.1$. That notes when the number of interactions between nodes is less, the trust value is more dependent on the indirect trust, and with the increasing of interaction times, the effect of dynamic weight φ on integrated trust value slowly trends towards $\varphi = 0.9$. That means with the increasing of the number of interactions between nodes, the integrated trust value metric measure is more dependent on direct trust. The results obtained are in agreement with the previous theoretical analysis. The weight factor φ can be dynamically adjusted according to the number of the interactions between nodes, which can better ensure the accuracy of trust measurement.

6.1.2. The Effect of Update Mechanism on Direct Trust Value. From the analysis in Table 1, we can see that the IOWA operator is determined by m and α. In this section, the effect of different m and α on the direct trust value is realized. Figure 6 shows the effect of the different α on the update trust value when $m = 4$. As shown in Figure 6, with the increasing of α, the update trust values are much closer to the trust value without update, which shows that the greater α is, the less

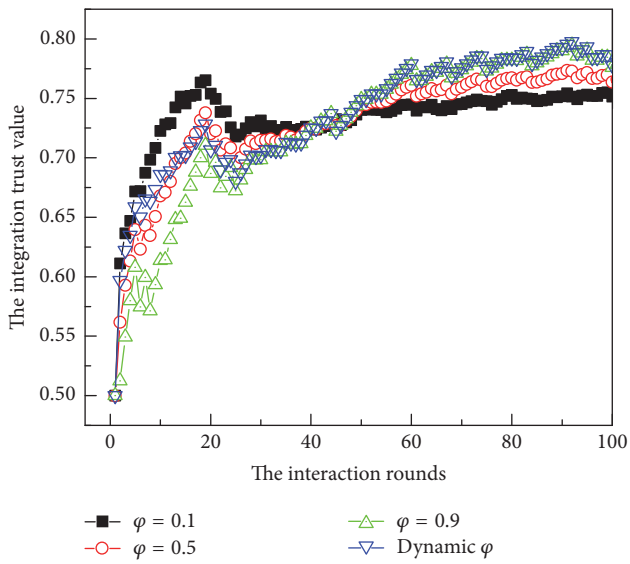

Figure 5: The effect of dynamic weights on integrated trust value.

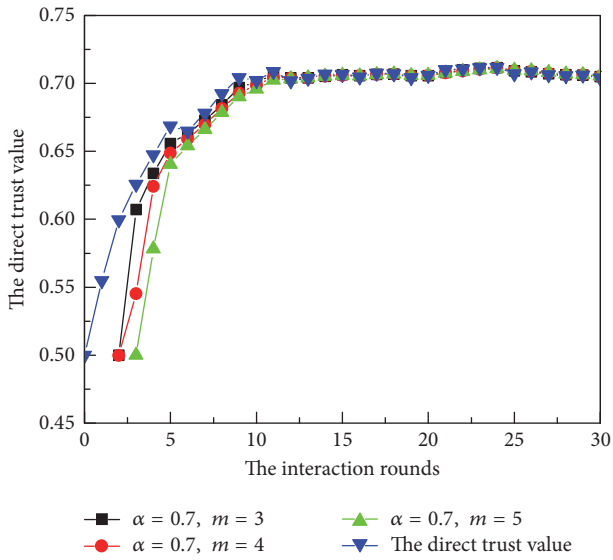

Figure 7: The effect of the parameter m under $\alpha = 0.7$.

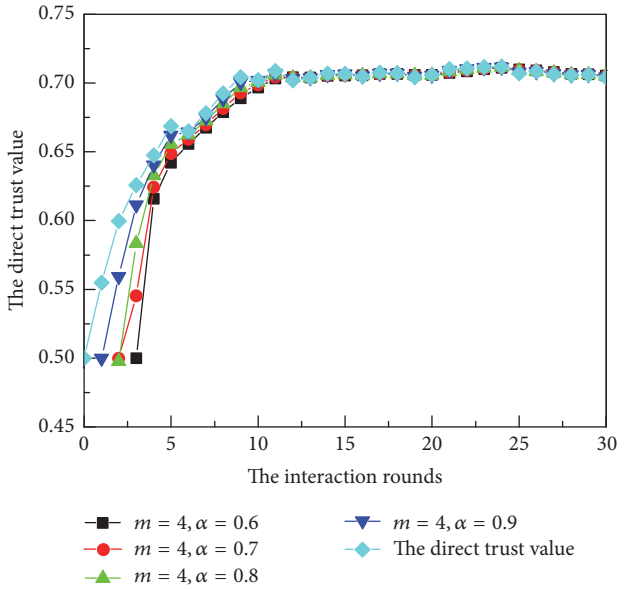

Figure 6: The effect of the parameter α under $m = 4$.

dependent the update trust value is on historical experience. Figure 7 shows the effect of the different m on the update trust value when $\alpha = 0.7$. As shown in Figure 7, with the increasing of m, the updated trust value is more accurate, which shows that the update trust value is more dependent on the historical experience. According to dynamic adjusting of m and α, we can effectively control the impact of historical interactions on trust value and enhance the accuracy of trust value.

6.2. Comparison of DTEM, RFSN, and BTMS. In this section, we compare DTEM with the existing trust models RFSN and BTMS. The former is one of the earliest classical trust schemes for WSNs; the latter is one of the representative classical trust schemes.

6.2.1. The Trust Evaluation. In this section, we assess the integrated trust of normal node and malicious node, respectively. It is assumed that a normal node always chooses to cooperate, and a malicious node always chooses not to cooperate. The target of this kind of attack is the routing protocol. As depicted in Figure 8, the integrated trust increases with the increasing of successful interactions among normal nodes and decreases with the increasing of unsuccessful interactions among malicious nodes in RFSN, BTMS, and DTEM. On the one hand, we can see intuitively that, for the integrated trust between normal nodes, the trust value increases faster than the other two algorithms in RFSN. In BTMS, the trust value increases more slowly than the other two algorithms because of the effect of the punishing factor at the beginning. In our proposed model in DTEM, the trust value changes with the increasing number of the interaction rounds. At the beginning, the trust value increases faster than BTMS and more slowly than the RFSN. After a few rounds, the increasing of the trust value becomes the slowest. On the other hand, for the integrated trust between malicious nodes in DTEM, the integrated trust value decreases fastest in all the algorithms. From the above analysis, we can get that the DTEM reflects the following character: "trust is hard to acquire and easy to lose." Having compared RFSN, BTMS, and DTEM, DTEM evaluates the trust more accurately among normal nodes. It reflects nodes' commutation behavior changing acutely and has more sensitive changing of the malicious actions, which can effectively identify routing attacks.

6.2.2. The Data Attack. We analyze the efficacy of DTEM against faulty data and malicious data manipulation. The target of this type of malicious attack is communications data or messages. We generate a few common types of faults and

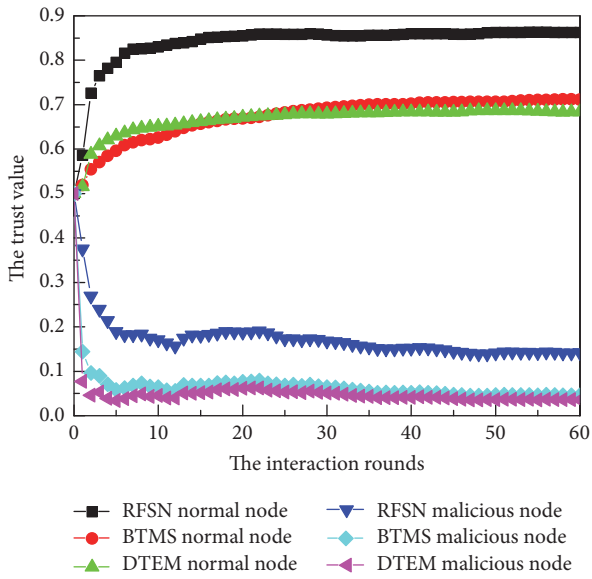

Figure 8: Comparison of the trust value of the normal node and malicious node.

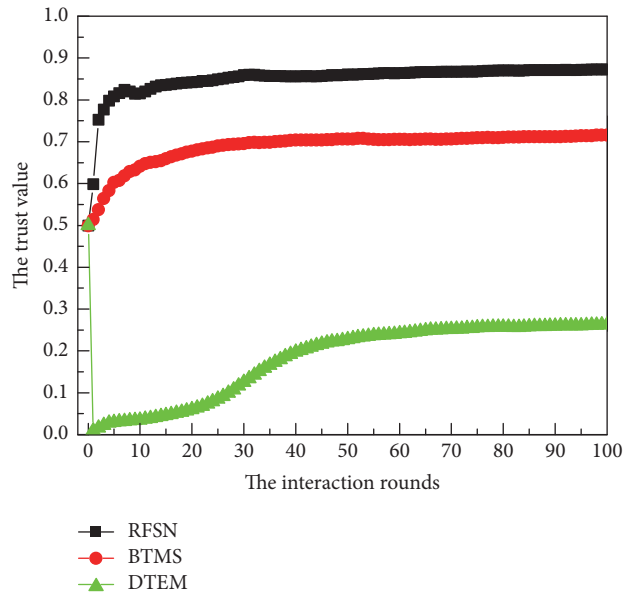

Figure 9: Comparison of the trust value under data attack.

fake data attacks together against the normal data. Firstly, we generate random data at randomly selected sensor nodes, but it does not affect the data communication. This means that although the sensor node sends false data, it can be considered as successful communication. Running RFSN, BTMS, and DTEM in this scene, the result is shown in Figure 9. As shown in Figure 9, in BTMS and RFSN, the trust value does not make any change. It is shown that these two algorithms do not consider the consistency of the data; they just only consider communication behaviors between nodes to calculate the trust value. In DTEM, the trust value decreases sharply, and then with the increasing of the number of interaction rounds, the trust value increases, but the trust value is always lower than 0.5. The result indicates that the resilience of DTEM is very good, which can fast and accurately identify the faulty data manipulation of malicious node. It is more sensitive in order to identify data information attacks compared with RFSN and BTMS.

6.2.3. The On-Off Attack. In this section, we analyze the efficacy of DTEM against the on-off attack. This type of malicious attack is a special kind of attack, whose target is the trust management. The on-off attack malicious node alternates its behavior from malicious to normal and from normal to malicious so it remains undetected while causing damage [42]. In this paper, we suppose that an on-off attacker behaves well in the first 30 interaction rounds to build up good reputation but behaves badly in the next 30 rounds. After that, it behaves well continuously. The result is shown in Figure 10. It is not difficult to see that the trust value increases in the first 30 interaction rounds, and the malicious node does nothing or only performs well. But in the next 30 rounds the trust value drops when the malicious node launches attacks. Having compared RFSN, BTMS, and DTEM, the DTEM can acutely reflect nodes' changing and sensitively detect

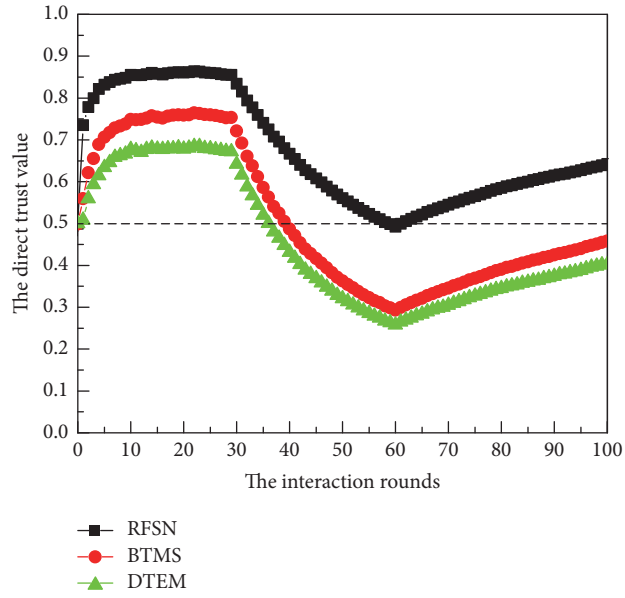

Figure 10: Comparison of the direct trust value under on-off attack.

on-off malicious attack. And more importantly, an on-off malicious node recovers its trust value more slowly and much longer. We can come to a conclusion that DTEM outperforms RFSN and BTMS against on-off attack. Meanwhile, the simulation result again verifies the character "trust is hard to acquire and easy to lose" in DTEM. This is because the trusted recommendation node selection mechanism and dynamic update mechanism are added to the process of trust evaluation, which makes the evaluation of trust between nodes more objective and accurate. It can effectively identify trust model attacks such as on-off attack and bad-mouth attack.

Table 3: Comparison of state-of-the-art trust model.

Trust model	RFSN [18]	GTMS [20]	NBBTE [29]	BTMS [24]	DTEM (ours)
Estimation method	Probabilistic	Weight	Fuzzy logic	Probabilistic	Probabilistic
Direct trust module	Transmission factors; data factors	Transmission factors	Received packets rate; successfully sending packets rate and so on	Transmission factors	Transmission factors; data factors; energy factors
Indirect trust module	Recommendation nodes	Recommendation nodes	Recommendation nodes	Trusted recommendation nodes	Trusted recommendation nodes
Integrated trust module	Probability	Weighted	D-S evidence	Self-confidence factor	Dynamic weighting function
Trust update module	Aging	×	×	Sliding window	Adjustable sliding window
Black hole attack	√	√	√	√	√
Attack on information	×	√	×	×	√
On-off attack	×	×	√	√	√

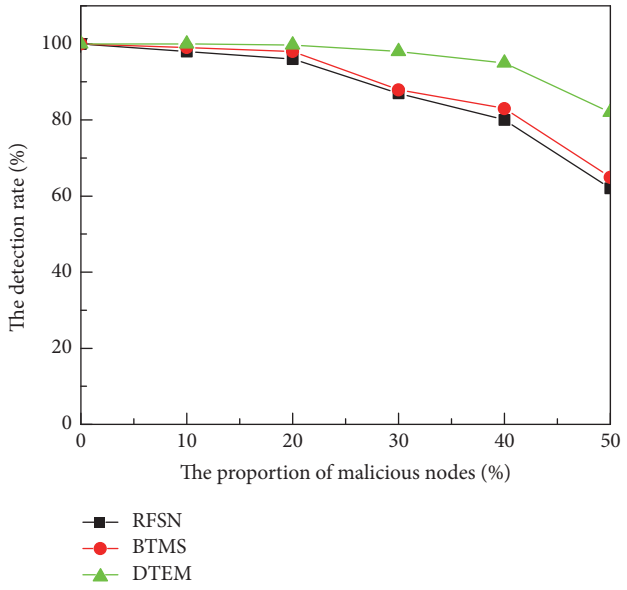

Figure 11: Comparison of the detection rate.

6.2.4. The Detection Rate. In this section, the simulated malicious attacks are selective forwarding attack, on-off attack, conflicting behavior attack, data forgery attack, and data tampering attack. We vary the percentage of malicious nodes from 10 to 50 percent with a 10 percent increment. As shown in Figure 11, which gives the detection rate in different trust model, we can see that the performance of the DTEM is better than RFSN and BTMS. RFSN and BTMS are vulnerable against data forgery attack and data tampering attack. So, with the increasing of the number of malicious nodes, the detection rate decreases rapidly, but the DTEM keeps high detection rate. Hence, the DTEM is an efficient trust evaluation model which can identify different kinds of malicious nodes and can be dynamically adjusted according to the specific requirements of the network.

In order to better illustrate the operation mechanism and performance of DTEM, Table 3 shows the comparison of state of the art in terms of trust estimation method, direct trust factors, indirect trust module, integrated trust module, trust update module, and considered attacks. Through the above proof and analysis of the experiment, we can know that DTEM is an efficient dynamic trust evaluation model for WSNs. It can effectively identify various malicious attacks.

7. Conclusion

In this paper, we propose an efficient dynamic trust evaluation model for WSNs. It includes the direct trust module with multiple trust factors, the trusted recommendation trust module, the dynamic trust integration module, and the adjustable trust update module. In the course of the calculation of direct trust, we take the communication trust, data consistency, and energy trust into account; it can achieve accurate trust evaluation against routing attacks and data information attacks. The punishment factor and regulating function are introduced based on the character "trust is hard to acquire and easy to lose." The calculation of indirect trust is invoked conditionally in order to enhance the accuracy of trust value, which can be against the trust model attacks such as bad-mouth attack. Moreover, in the process of the integrated trust quantitative calculation, we define a dynamic balance weight factor function to overcome the defect caused by allotting weights subjectively. Afterwards, we give the update mechanism based on IOWA to enhance flexibility. During this process, we can dynamically adapt the parameters to change the weight sequence to meet the actual needs of the network. The proposed dynamic trust model enables dynamic, accurate, and objective evaluation of trust between nodes based on the behavior of nodes.

We have performed several tests to validate the proposed trust model. Simulation results indicate that DTEM is an efficient dynamic and attack-resistant trust evaluation model. It can dynamically evaluate the reputation among nodes

based on the communication behavior, data consistency, and energy consumption of nodes. And having compared RFSN, BTMS, and DTEM, DTEM is of great help in defending against routing attacks, data information attacks, and trust model attacks. It can effectively identify various malicious attacks.

The traditional security mechanisms (cryptography, authentication, etc.) are widely used to deal with external attacks. Trust model is a useful complement to the traditional security mechanism, which can solve insider or node misbehavior attacks. Hence, trust model is important to providing security service for upper layer network application in WSNs, such as secure routing and secure data fusion. In our future work, we would like to focus on the application of trust model in routing and data fusion for WSNs.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research is supported by the National Natural Science Foundation of China (61772101, 61170169, 61170168, and 61602075).

References

[1] R. D. Gomes, M. O. Adissi, T. A. da Silva, A. C. Filho, M. A. Spohn, and F. A. Belo, "Application of wireless sensor networks technology for induction motor monitoring in industrial environments," in *Intelligent Environmental Sensing*, vol. 13 of *Smart Sensors, Measurement and Instrumentation*, pp. 227–277, Springer International Publishing, Cham, 2015.

[2] M. M. Alam, D. Ben Arbia, and E. Ben Hamida, "Wearable wireless sensor networks for emergency response in public safety networks," *Wireless Public Safety Networks*, pp. 63–94, 2016.

[3] M. Bhuiyan, G. Wang, J. Wu et al., "Dependable structural health monitoring using wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–47, 2015.

[4] T. Ojha, S. Misra, and N. S. Raghuwanshi, "Wireless sensor networks for agriculture: the state-of-the-art in practice and future challenges," *Computers and Electronics in Agriculture*, vol. 118, pp. 66–84, 2015.

[5] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: a survey," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 602–617, 2014.

[6] H. Modares, A. Moravejosharieh, R. Salleh, and J. Lloret, "Security overview of wireless sensor network," *Life Science Journal*, vol. 10, no. 2, pp. 1627–1632, 2013.

[7] R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, "Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 492–505, 2011.

[8] R. Lacuesta, J. Lloret, M. Garcia, and L. Peñalver, "A secure protocol for spontaneous wireless Ad Hoc networks creation," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 629–641, 2013.

[9] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 131–140, 2008.

[10] M. Momani and S. Challa, "Survey of trust models in different network domains," *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, vol. 1, no. 3, pp. 1–19, 2010.

[11] A. Boukerch, L. Xu, and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2413–2427, 2007.

[12] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.

[13] Y. Liu, C.-X. Liu, and Q.-A. Zeng, "Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks," *Telecommunication Systems*, vol. 62, no. 2, pp. 319–325, 2016.

[14] X. Anita, M. A. Bhagyaveni, and J. M. L. Manickam, "Collaborative lightweight trust management scheme for wireless sensor networks," *Wireless Personal Communications*, vol. 80, no. 1, pp. 117–140, 2015.

[15] G. Rajeshkumar and K. R. Valluvan, "An Energy Aware Trust Based Intrusion Detection System with Adaptive Acknowledgement for Wireless Sensor Network," *Wireless Personal Communications*, vol. 94, no. 4, pp. 1993–2007, 2016.

[16] Y. L. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 112–119, 2008.

[17] F. Ishmanov, S. W. Kim, and S. Y. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 7040–7061, 2015.

[18] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 66–77, October 2004.

[19] H. Chen, H. Wu, X. Zhou, and C. Gao, "Agent-based trust model in wireless sensor networks," in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD '07)*, pp. 119–124, IEEE, Qingdao, China, August 2007.

[20] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, 2009.

[21] J. Song, X. Li, J. Hu, G. Xu, and Z. Feng, "Dynamic trust evaluation of wireless sensor networks based on multi-factor," in *Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, pp. 33–40, fin, August 2015.

[22] X. Li, F. Zhou, and J. Du, "LDTS: a lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.

[23] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, 2012.

[24] R. Feng, X. Han, Q. Liu, and N. Yu, "A credible bayesian-based trust management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 678926, 2015.

[25] G. Zhan, W. Shi, and J. Deng, "SensorTrust: a resilient trust model for wireless sensing systems," *Pervasive and Mobile Computing*, vol. 7, no. 4, pp. 509–522, 2011.

[26] H.-H. Dong, Y.-J. Guo, Z.-Q. Yu, and C. Hao, "A wireless sensor networks based on multi-angle trust of node," in *Proceedings of the International Forum on Information Technology and Applications (IFITA '09)*, vol. 1, pp. 28–31, May 2009.

[27] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, 2014.

[28] H. Rathore, V. Badarla, and S. Shit, "Consensus-aware sociopsychological trust model for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 12, no. 3, article no. 21, 2016.

[29] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.

[30] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Networks*, pp. 1–21, 2016.

[31] S. Shen, L. Huang, E. Fan, K. Hu, J. Liu, and Q. Cao, "Trust dynamics in WSNs: an evolutionary game-theoretic approach," *Journal of Sensors*, vol. 2016, Article ID 4254701, 10 pages, 2016.

[32] J.-W. Ho, M. Wright, and S. K. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 512–523, 2012.

[33] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113–127, May 2003.

[34] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *Proceedings of the INFOCOM 2006: 25th IEEE International Conference on Computer Communications*, esp, April 2006.

[35] A. Jøsang and R. Ismail, "The Beta Reputation System," in *Proceedings of the 15th Bled Electronic Commerce Conference (Bled EC)*, pp. 324–337, Slovenia, 2002.

[36] E. Elnahrawy and B. Nath, "Cleaning and querying noisy sensors," in *Proceedings of the the 2nd ACM international conference*, p. 78, San Diego, CA, USA, September 2003.

[37] S. Mi, H. Han, C. Chen, J. Yan, and X. Guan, "A secure scheme for distributed consensus estimation against data falsification in heterogeneouswireless sensor networks," *Sensors*, vol. 16, no. 2, 2016.

[38] B. Zhao, H. Jing-Sha E, Y. Zhang X et al., "Analysis of multi-factor in trust evaluation of open network," *Journal of Shandong University*, vol. 49, no. 9, pp. 103–108, 2014.

[39] R. R. Yager, "Induced aggregation operators," *Fuzzy Sets and Systems*, vol. 137, no. 1, pp. 59–69, 2003.

[40] R. Fullér and P. Majlender, "An analytic approach for obtaining maximal entropy OWA operator weights," *Fuzzy Sets and Systems*, vol. 124, no. 1, pp. 53–57, 2001.

[41] X.-Y. Li and X.-L. Gui, "Cognitive model of dynamic trust forecasting," *Ruan Jian Xue Bao/Journal of Software*, vol. 21, no. 1, pp. 163–176, 2010.

[42] L. F. Perrone and S. C. Nelson, "A study of on-off attack models for wireless ad hoc networks," in *Proceedings of the 2006 1st Workshop on Operator-Assisted (Wireless-Mesh) Community Networks, OpComm 2006*, deu, September 2006.