Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 363569, 14 pages
http://dx.doi.org/10.1155/2015/363569

Research Article

Trust-Based Anomaly Detection in Emerging Sensor Networks

Renyong Wu,[1] Xue Deng,[1] Rongxing Lu,[2] and Xuemin (Sherman) Shen[2]

[1]*College of Information Science and Engineering, Hunan University, Changsha 410082, China*
[2]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada N2L 3G1*

Correspondence should be addressed to Renyong Wu; wurenyong@hnu.edu.cn

Received 15 May 2015; Revised 30 September 2015; Accepted 5 October 2015

Academic Editor: Mauro Conti

Wireless sensor networks (WSNs) consist of a large number of small-size, energy-constrained nodes and generally are deployed to monitor surrounding situation or relay generated packets in other devices. However, due to the openness of wireless media and the inborn self-organization feature of WSNs, that is, frequent interoperations among neighbouring nodes, network security has been tightly related to data credibility and/or transmission reliability, thus trust evaluation of network nodes is becoming another interesting issue. Obviously, how to describe node's behaviors and how to integrate various characteristics to make the final decision are two major research aspects of trust model. In this paper, a new trust model is proposed to detect anomaly nodes based on fuzzy theory and revised evidence theory. By monitoring the behaviors of the evaluated nodes with multidimensional characteristics and integrating these pieces of information, the malicious nodes in a network can be identified and the normal operation of the whole network can be verified. In addition, to accelerate the detection process, a weighting judgment mechanism is adopted to deal with the uncertain states of evaluated nodes. Finally extensive simulations are conducted, and the results demonstrate that the proposed trust model can achieve higher detection ratio of malicious nodes in comparison with the previously reported results.

1. Introduction

In general, wireless sensor networks (WSNs) consist of a large number of small-size, energy-constrained nodes, which are responsible for data sensing, collecting, and relaying. Compared with the traditional networks, WSNs are more intelligent and flexible to organize network elements to support some predefined applications. Nowadays, with the rapid advances in information and communication technology (ICT), WSNs have been widely deployed in a variety of applications like environment monitoring, intrusion detection, and other civilian or military applications [1, 2]. Obviously, although the sensing objectives of these applications are not unique and highly application-dependent, for most WSN systems, the common performance criterion is to prolong network lifetime while satisfying coverage and connectivity in a certain deployment region.

However, due to the long-term exposure in natural environments and the inherent vulnerabilities of open spectrum, the reliability of data transmission between elements in WSNs becomes fragile. Thus security of WSNs has attracted wide attention from researchers and institutions. For instance, in military scenarios, the sensor nodes deployed in a war district have to keep on working for several months, which will undoubtedly increase the possibility of nodes being captured and turned into malicious nodes under intentional attacks. What is more, compared with the existing networks, the largest challenge of WSN is its limited resource capacities, including energy, memory, and computing power. As a result of this, some of the existing security technologies which work well in traditional wired networks, such as key management and host-based intrusion detection, cannot be directly extended to WSNs [3–5]. Therefore, to propose some energy efficient anomaly detection schemes for WSNs is an essential but a vital step on the way to practical application.

As the name suggests, anomaly detection is the identification of items, events, or observations which do not conform to the expected patterns. In a sensor network domain, the anomalous items are always referred to as intrusion or intrusion attempt to a network through tampering or intercepting data, altering data transmission direction or other ways of depleting nodes' energy. In other words, anomaly detection

is a technology used for assessing node behaviors that violate the normal operations of network, so its ultimate goal is to detect and report the unauthorized or abnormal nodes in communication networks. On the other hand, the idea trust assessment has attained much more consideration from academic institutions [6–8]. It was firstly proposed in the realm of e-commerce to select reliable transaction objects and now has been extended to other domains, including finance and navigation. Recall that trust is a common concept used in human society which facilitates the interactivity and communication between human beings, while anomalous always means doubtful and harmful.

For a communication network, according to where the attacks come from, generally the individual doubtful or illegal behaviors can be divided into two categories: one is by the internal nodes and the other is by external nodes. To combat external attacks, the existing identity authentication and data encryption theories have already been quite mature [9, 10], which can prevent most external nodes from intruding into a network so avoiding the eavesdropping from them. In contrast, to detect compromised members to eliminate internal attacks is a much more difficult task and still under study. Recently, some trust-based detection models have been proposed to fulfill this purpose; however some related issues remain open and challenging [11–13] for researchers.

Although these existing trust models play important roles in improving security in many aspects such as peer-to-peer networking and grid and cloud computing, trust evaluation is still a challengeable issue. Generally, trust evaluation is directly related to the past behaviors of a participant like transmission, control, and random access and then combined with the reputation from other recommenders, which means trust value of a node can be obtained from two ways: direct trust evaluation and indirect trust evaluation. Direct trust value is determined by periodically monitoring behaviors of an evaluated node and fusing all the information at each end of sampling period. However, how to calculate enough accurate trust value for a node in a realistic situation is under study [14], which is the major research motivation of this paper. On the other hand, indirect trust value is determined by collecting the recommended information from some neighboring nodes. However, to the best of our knowledge, the credibility of the recommended information has not yet been fully considered in existing literatures [15], which is another motivation of this paper. Finally, by integrating direct trust value and indirect trust value, a unique trust value is obtained to detect a malicious node from other normal nodes.

In this paper, aiming to address the above challenges, we propose a new trust model, shown in Figure 1, to detect malicious nodes in WSNs. First, the evaluation node collects multidimensional characteristics of the evaluated node's behaviors including energy consumption and packet processing, and then in accordance with the predefined fuzzy membership functions [16], it uses fuzzy set theory to deduce trustworthiness levels of every characteristics. Second, the evaluation node fuses all these pieces of level information to obtain a direct trust value by the evidence theory [17, 18]. Third, the evaluation node collects all credible recommended information from the evaluated node's one-hop neighbors

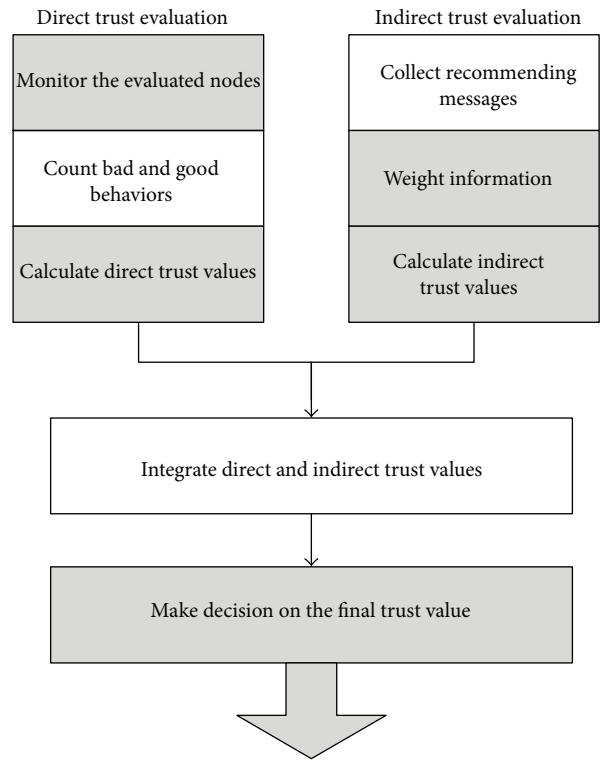

Figure 1: The framework for the proposed model.

and weights these pieces of information according to their credibility. Finally, the direct trust value and indirect trust value are integrated. It is noted that here the running state of the evaluated node is judged according to the decision rules and should be broadcasted to the evaluation node's surrounding nodes, which can be embedded in MAC or routing module. And, when the state of the evaluated node is uncertain for the evaluation node to decide, a weighting judgment algorithm is further introduced in this paper to accelerate the evaluation procedure. Finally simulation results show that the new trust model can achieve higher detection rate and lower false alarm rate compared with the group-based trust management model (GTMS) [19].

The remainder of this paper is organized as follows. Section 2 presents a review of related work. Section 3 presents a fundamental introduction of fuzzy theory and evidence theory, which will be applied in the trust model. Section 4 presents the proposed trust model in detail, including five process phases and some practical implement issues. Section 5 presents a weighting decision approach. An experimental evaluation of this proposed model is conducted in Section 6. Finally, in Section 7, we make some concluding remarks.

2. Related Work

It is well known that WSNs are valuable to various applications related to data collection and some security purposes; however, due to the inherent characteristics, there are also some risks to be faced. According to where the executors

come from, there are two categories of malicious attacks in WSNs: internal attacks and external attacks [20]. Most of the external attacks take advantage of powerful transceivers' ability to receive and transmit long distance signals to interfere with the network's normal operation, such as spoofing attack and sniffing attack. In comparison to these external attacks, the threat posed by internal attacks on a network is greater and more difficult to resist because the promise of its purpose is to detect these malicious ones from normal nodes while these malicious nodes always imitate themselves like normal ones. Thus in complex practical scenarios, it is so difficult to detect malicious nodes.

Recently, there have appeared some research works on internal attacks in WSNs [21, 22]. In [23], Tian and Georganas propose an acknowledgement (ACK) based anomaly detection model, which makes use of the idea that each next-hop node loopbacks ACK packet to the source node after it has received a data packet correctly. Thus the source node can make sure whether there is any unreliable transmission between itself and these intermediate nodes. Although this model is simple, the detection rate is not high enough and there are some difficulties existing in its implementation. In order to achieve a higher detection rate, Chatzigiannakis and Papavassiliou propose a data fusion-based anomaly detection method in [21], where they take advantage of the data association nature among adjacent nodes and adopt so-called principal component analysis (PCA) to check the completeness and accuracy of the collected data. However, this method needs to collect information as much as possible. In other words, it has a strict requirement on distribution density of nodes in a monitoring area and is not universally applicable. To relieve this limit, da Silva et al. introduce an efficient method in [24] to identify anomaly node based on statistical information. The characteristics of a behavior are gathered by monitoring the evaluated node and matching the characteristics with the behavior rules which are predefined according to experiences. Comparing to the malicious behavior patterns saved in the rule database, this method can detect anomaly nodes rapidly and correctly. However, this method strongly depends on the accuracy of rules and will become invalid when new types of attack appear in the network if they have not been described in the rule database. In fact, it is so difficult to accurately describe some behaviors' statistical information. To free the detection procedure from modeling behavior, Pissinou et al. propose a classical probability model based on statistical analysis to find anomaly nodes in networks [14]. However, this scheme does not take into consideration any recommended information from other nodes. As a result, it may lead to a high false alarm rate. In view of this situation, Zhang and Lee try to improve the performance by combining the direct observed characteristics with the indirect information to obtain an integrated trust value [15]. However, there are some inadequacies existing in their model because it only simply takes the attitude of full trust to the recommended information and does not take into consideration the credibility of the information. Thus, how to introduce credibility in the schemes has become a focus of this type of approaches. In [25], moving average technique is used to balance between direct and indirect trust value based on recommendation credibility, and in [26] fuzzy logic is applied to quantify the trust recommendation relationships.

It is well known that a model selected to describe behavior has to deal with multiple input parameters, so how to fuse these pieces of information with different properties is a more important problem. By applying fuzzy theory, Moon and Cho [22] propose an intrusion detection scheme for discovering and combating sinkhole attack in directed diffusion based sensor networks. In the scheme, some nodes act as master nodes and periodically send out packets, that is, a type of path reinforcement message, in their respective coverage areas, and then a detection value is derived from the received messages for each area using fuzzy logic. However, this scheme is mainly designed to handle sinkhole attack and does not consider other attack types fully. To fuse multidimensional characteristics, in [27] Chang and Liu introduce evidence theory in their anomaly detection model where D-S evidence theory is used to fuse current state information with the historical information to obtain a comprehensive assessment value, which can improve detection rate. However, because hard threshold is adopted in the scheme to determine a node's state, high false alarm rate will frequently appears especially under some complex situations.

In this paper, we proposed a new trust model, which combines fuzzy theory with evidence theory to detect anomaly nodes in WSNs. Although fuzzy theory has been applied in [22], only reinforcement and radius information are fuzzed up there and our model handles five different behavior characteristics to obtain node's trust value. Based on nodes' behaviors and modified evidence theory, Feng et al. have proposed a trust evaluation algorithm for wireless sensor networks in [28]. In the scheme, fuzzy set is employed to generate a basic input vector for evidence calculation, and weighted fusion is used to calculate a direct trust value. Meanwhile, the evidence difference among the indirect and direct trust values is noticed, which leads to the revised D-S evidence combination rules to finally synthesize the integrated trust values. All these aspects are similar in some degree to this paper. However, it does not fully take into consideration the uncertain states when waiting for the next-ring trust assessment. In this paper, a weighting mechanism is proposed to speed up the convergence procedure in determining nodes' states. Thus after observing the behaviors of the evaluated nodes, we are able to identify malicious nodes in a network and guarantee the normal operations of a network.

3. Preliminary

In this section, the fundamental concepts of Dempster-Shafer (D-S) evidence theory, fuzzy set theory, and weighting algorithm are introduced briefly, which will be involved in the other sections.

3.1. D-S Evidence Theory. D-S evidence theory is a method of uncertainty reasoning which was first proposed by Dempster [17] in 1967 and then further promoted by Shafer [18] in 1976. The theory can be regarded as a generalized broaden of

the classical probabilistic inference theory in finite fields and has been widely applied in probabilistic inference, probabilistic diagnosis, risk analysis, and decision support. Furthermore, evidence theory can clearly express uncertainty and effectively deal with uncertain information in case of no prior information, so it has been widely applied in expert systems, medical diagnostics, and so forth.

3.1.1. Reliability Functions and Distributions. If all obtained possible outcomes for an issue of jurisdiction are regarded as members of a set, this complete set is called a frame of discernment (Θ) and consists of all possibilities of the problem. An evidence can provide support to one or more propositions, which can be shown by some basic probability assignment functions.

Definition 1. If there is a mapping m: $2^{\Theta} \rightarrow [0,1]$ (2^{Θ} is the power set of Θ) which satisfies the following requirements, $m(\Theta)$ is called a basic probability assignment (BPA) function of the frame of discernment Θ or a mass function:

$$\begin{aligned} m(\Phi) &= 0, \\ \sum_{i=1}^{n} m(A_i) &= 1, \quad A_i \subseteq \Theta. \end{aligned} \tag{1}$$

It is said that $m(A)$ represents the precise level of trust to proposition A. In this paper, empty set is denoted as Φ.

Definition 2. If a subset A of Θ satisfies $A \subseteq \Theta$, $A \neq \Phi$, and $m(A) > 0$, A is named a focal element of m.

It is noted that, in D-S evidence theory, two basic functions, belief (Bel) and plausibility (Pls), are defined to characterize the uncertainty and to support certain hypotheses. Bel measures the minimum or necessary support to the hypothesis, whereas Pls measures the maximum or potential support.

Definition 3. Belief and plausibility functions are two measures, derived from mass values, and are defined as a mapping from a set of hypotheses to interval $[0,1]$ which is shown as follows:

$$\begin{aligned} \mathrm{Pls}(A) &= \sum_{B \cap A \neq \Phi} m(B), \\ \mathrm{Bel}(A) &= \sum_{B \subseteq A} m(B). \end{aligned} \tag{2}$$

Belief function is also regarded as the bottom limit of the BPA function, while plausibility function is the top limit.

3.1.2. Dempster Combination Rules. The synthesis rules in evidence theory represent a method that is used for information combination of multiple independent information sources.

Denote m_1, m_2 are two BPA functions based on two independent evidences and come from the same frame of discernment, and their focal elements are, respectively, denoted as $A_1, A_2, \ldots, A_k$ and $B_1, B_2, \ldots, B_l$. If they satisfy

$$K = \sum_{A_i \cap B_j = \varnothing} m_1(A_i)\, m_2(B_j) < 1, \tag{3}$$

where $A_i, B_j \subseteq \Theta$ and K is the measure of confliction between two different independent evidences, using Dempster combination rules, we can turn two BPA functions into synthesis.

Definition 4. Dempster combination rules are

$$m(A) = \begin{cases} 0, & A = \Phi, \\ \dfrac{\sum_{A_i \cap B_j = A} m_1(A_i)\, m_2(B_j)}{1 - K}, & A \neq \Phi,\ A_i, B_j \subseteq \Theta, \end{cases} \tag{4}$$

where A is a subset of Θ and coefficient $1/(1-K)$ is used as a normalization factor to prevent a nonzero value being assigned to an empty set. The closer the value of K being to 1, the greater the confliction between two evidences, and vice versa.

3.2. Fuzzy Set Theory. As an extension of classical set theory, fuzzy set theory was first proposed by Zadeh [29] to map linguistic variables within decision-made process in 1965 and then was extended to other various fields, such as natural science, social science, and engineering fields [16]. The difference between classical set theory and fuzzy set theory is that, in fuzzy set theory, the concept of membership degree is used to indicate a degree with which an element belongs to a fuzzy set. The way of this method to recognize a target is similar to the thinking mode of human being. Each element in a fuzzy set has an exclusive corresponding membership function, so all these membership functions determine an exclusive fuzzy set. The outputs of these membership functions define the degrees with which the specified concentration belongs to a fuzzy set, which assign each element multiple grades within the interval $[0,1]$. Membership function and membership degree of a fuzzy set are defined as follows.

Definition 5. The collection of all objects is called the domain of a fuzzy set, denoted by U. The domain of a fuzzy set can be continuous or discrete.

Definition 6. Let $X = \{x_1, x_2, \ldots, x_n\}$ be the domain of a fuzzy set; a fuzzy subset A of X is defined as follows: for any $x \in X$, there exists a value $\mu_A(x) \in [0,1]$. The mapping is denoted as

$$\mu_A : X \longrightarrow [0,1] \tag{5}$$

or

$$x \longrightarrow \mu_A(x) \in [0,1]. \tag{6}$$

Map each $x_i \in X$ to a certain value $\mu_A(x) \in [0,1]$, which is called the membership degree with which x belongs to set

A. The mapping μ_A is called a membership function of fuzzy set A.

Generally, for n fuzzy subsets $A_1, A_2, \ldots, A_n$ with the same domain U, if there are m evidences $\mu_1, \mu_2, \ldots, \mu_m$ existing with an identical object: $\forall x \in U$, all possible membership degrees can be written down as follows:

$$\begin{gathered}\mu_{1,A_1}(x), \mu_{1,A_2}(x), \ldots, \mu_{1,A_n}(x)\\ \mu_{2,A_1}(x), \mu_{2,A_2}(x), \ldots, \mu_{2,A_n}(x)\\ \vdots\\ \mu_{m,A_1}(x), \mu_{m,A_2}(x), \ldots, \mu_{m,A_n}(x).\end{gathered} \tag{7}$$

3.3. The Weighting Algorithm. Weighting algorithm is vital to combination and decision process of multidimensional information because its output will directly reflect each factor's importance and position in the final results [30]. In the process of fusion, assume there are n attributes in system and the ith attribute's weight is denoted as ω_i; these n weights are subject to

$$\omega_1 + \omega_2 + \cdots + \omega_n = 1. \tag{8}$$

The core ideas behind the weighting algorithm are expert evaluation method, fuzzy statistics, and duality contrast sorted method. However, if the weight values are simply determined from expert experience, which is subjected to the primary characteristic, they cannot objectively reflect the actual circumstance and sometimes even result in false decision-made process. Therefore in this paper, evidences' weights are obtained according to their distances from the mean value and their historical contribution. Considering actual application environment, the attribute's importance is fully taken into account to assure the evidence importance by combining the objective weights and subjective weights from experience knowledge. As a result, it will lead to a more accurate final output than under the situation that weight values only depend on the experience knowledge.

4. Anomaly Detection Model

The trust-based anomaly detection model consists of five phases: the monitoring phase, the fuzzy phase, the trust fusion phase, the collection phase of recommended information, and the decision phase. Note that, in the proposed algorithm, the related participants will be classified into three roles: evaluation node, evaluated node, and neighboring node. As shown in Figure 2, node A assesses node B, so nodes A and B are, respectively, named evaluation node and evaluated node. And, nodes C and D are called neighboring nodes when they can provide some recommending information of B to A, which means that both nodes C and D may have done some interactions with node B. Note that, in fact, here connections exist between A and B, C, and D.

4.1. The Monitoring Phase. In most of previous models, a node is assessed according to only one factor, such as packet loss rate and data flow. However, it is well known that different attack types have different impacts on nodes' different characteristics, so only considering a single factor is not enough to detect various attacks. In this paper, we present a multidimensional feature extraction model, which monitors a node from five aspects specifically: energy consumption rate, packet receiving rate, packet sending rate, packet forwarding rate, and data consistency. For instance, if node i needs to assess node j, it has to monitor the following five measures of node j. Note that, in this paper, Δ indicates the update period of trust assessment and t represents the tth update period.

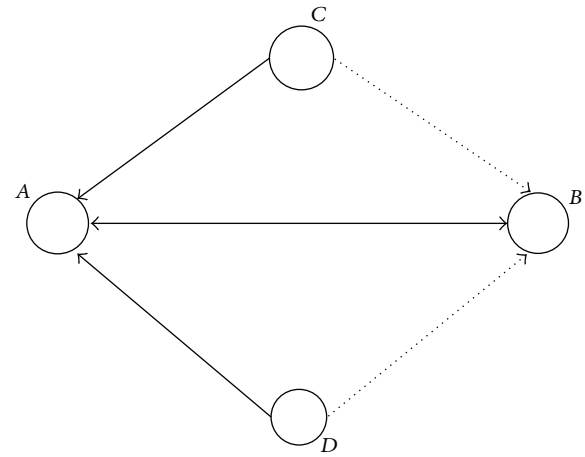

Figure 2: A topology example of trust assessment.

4.1.1. Energy Consumption Rate (ECR). Recall that sensor nodes may have limited energy and any behavior of a node needs to consume its stored energy, which means that a malicious node will consume energy more quickly due to more stimulated actions than normal nodes, including transmitting, processing, and receiving. Thus we can know the energy consumption information of a node by comparing its energy consumption rate with the normal level. If node i makes assessment of node j, the calculation formula is defined as

$$\mathrm{ECR}(t) = \frac{|\Delta E(t) - \Delta E|}{\Delta E}, \tag{9}$$

where $\Delta E(t) = E_j(t) - E_j(t-1)$ represents the energy consumption difference of node j in the $(t-1)$th and tth sampling period and ΔE represents the normal consumption level in update period Δ.

4.1.2. Packet Receiving Ratio (PRR). The ACK-mechanism is also taken into consideration to calculate the number of packets received by the evaluated node during a sampling period. By this way, we can determine whether there is heavy packet loss happening on the evaluated node:

$$\mathrm{PRR}(t) = \frac{R_j(t)}{S_i(t)}, \tag{10}$$

where $R_j(t)$ indicates the number of data packets received in node j that are sent by node i during the tth period, which is equal to the number of ACK-messages that node i can receive from node j (here assume that all ACK-messages can be received successfully), and $S_i(t)$ is the total number of packets sent by node i to node j during the tth period.

4.1.3. Packet Sending Ratio (PSR). After an evaluated node has been compromised, it may fabricate some packets and send to its neighboring nodes. This behavior will result in unnecessary energy loss in the neighboring nodes and network congestion. The difference of two successive periods is more accurate to describe the evaluated node's state and is defined as

$$\mathrm{PSR}(t) = \frac{\left|S_j(t) - S_j(t-1)\right|}{S_j(t) + S_j(t-1)}, \tag{11}$$

where $S_j(t)$ indicates the total number of packets sent by the evaluated node j during the tth period and the denominator is used to normalize the output value.

4.1.4. Packet Forwarding Ratio (PFR). If a node has received some packets while it is not the destination node, it is needed to forward the packets according to the routing table stored in memory. However, after the node has been compromised, it may intercept these packets and may not forward them sequentially:

$$\mathrm{PFR}(t) = \frac{S_{i,j}(t)}{S_{(i,j)}(t)}, \tag{12}$$

where $S_{i,j}(t)$ indicates the number of packets node j has received from node i and forwarded to next-hop node according to the routing table and $S_{(i,j)}(t)$ is the total number of packets node i wants to send to their destinations with the help of node j.

4.1.5. Data Consistency (DC). The current research has shown that the sensed data from adjacent nodes is closely correlative in space domain. It is said that, comparing the data generated by the evaluation node and evaluated node or by the evaluated node and its neighbors can determine whether the evaluated node has modified data packets. So DC is defined as

$$\mathrm{DC}(t) = \frac{TS_{i,j}(t)}{TS_{i,j}(t) + NTS_{i,j}(t)}, \tag{13}$$

where $TS_{i,j}(t)$ and $NTS_{i,j}(t)$ are, respectively, the total number of accordant packets and discordant packets during the tth period. Here the update rule is rather simple: if the difference is in the range of 10% ~20%, the value of $TS_{i,j}(t)$ is increased by 1; otherwise the value of $NTS_{i,j}(t)$ is increased by 1.

4.2. The Fuzzy Phase. As a matter of fact, most behavior characteristics of nodes even cannot be simply imagined as definitive, which implies that the trust values may be subjective and uncertain. Fuzzy theory is a good choice for this type of problem. In this paper, without loss of generality, the trust status can be divided into three grades: trust, distrust, and uncertain, respectively, labeled as T_1, T_2, and T_3. Note that after collecting the values of behavior characteristics, the evaluation node normalizes each characteristic into a value $\in [0, 1]$ to simplify the subsequent processing. Their fuzzy membership functions $\mu_{T_1}(x)$, $\mu_{T_2}(x)$, and $\mu_{T_3}(x)$ are defined as in the following formula:

$$\begin{aligned} \mu_{T_1}(x) &= \mathrm{sigmf}\left(kx, [a \;\; b]\right), \\ \mu_{T_2}(x) &= 1 - \mathrm{sigmf}\left(kx, [c \;\; d]\right), \\ \mu_{T_3}(x) &= 1 - \mu_{T_1}(x) - \mu_{T_2}(x), \end{aligned} \tag{14}$$

where s-shaped membership function $\mathrm{sigmf}(kx, [a \;\; b]) = 1/(1 + e^{-a(kx-b)})$ and k, a, b, c, d are five predefined system parameters.

The larger the membership degree is, the more normal the evaluated node is. An example of the fuzzy membership functions is shown in Figure 3, where $k = 13$ and a, b, c, d are set as 13, 0.65, 9, 0.55, and 5, respectively.

4.3. The Trust Fusion Phase. The evidence theory is suitable for processing uncertain information to obtain a reasonable output. In this paper, the synthesis rules of the revised evidence theory are used to determine whether the system is threatened by invasion. Note that, to apply the revised evidence theory to fusion evidences, it is needed to define the mass functions for every focal elements.

The outputs of the fuzzy phase are membership values of the three status. In this phase, each membership value is assigned to the corresponding focal element's BPA function so as to produce five group evidences, and then the revised evidence theory is utilized to fuse these group evidences and obtain a direct trust value (DTV). The formula is shown as

$$\begin{aligned} m_n\left(T_j\right) &= \mu_{n,T_j}(t), \\ \mathrm{DTV}_{i,j}(T_i) &= \sum_{\cap T_j = T_i} \prod_{n=1}^{5} m_n\left(T_j\right) + k \cdot f(T_i), \\ &\qquad \forall T_i \neq \Phi, \end{aligned} \tag{15}$$

where parameter $k = \sum_{\cap T_j = \Phi} \prod_{n=1}^{5} m_n(T_j)$ and function $f(T_i) = (1/5) \sum_{n=1}^{5} m_n(T_i)$ refers to geometric mean.

4.4. The Recommended Information Collection Phase. In this phase, the evaluation node further gathers recommended information from the evaluated node's neighbors to calculate an indirect trust value, so the key problem is how to integrate these pieces of information. For instance, to combat bad-mouthing attack, the scheme has to weight the recommended information from different neighbors.

It is well known that there may be some relatives between these pieces of recommended information, so we can calculate and compare the distance between every recommended

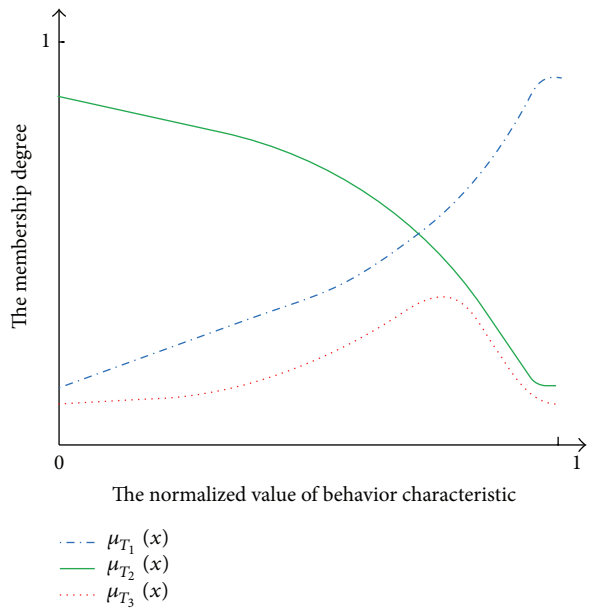

Figure 3: The fuzzy membership functions.

information and their mean value to determine the weights. Obviously, the fundamental principle behind this idea is the information with smaller distance implies better reliability and should be assigned a larger weight. Assume that the evaluated node j has n neighboring nodes to provide recommended information and their distance are denoted as $d_{R_k,E}$ (index k refers to the kth neighboring node), then the largest distance $d_{\max} = \max(d_{R_1,E}, d_{R_2,E}, \ldots, d_{R_n,E})$ and its relative distance is denoted as $d_{\max}/d_{R_i,E}$ $(i = 1, 2, \ldots, n)$. Thus node k's weight ω_{R_k} can be determined

$$\omega_{R_k} = \frac{d_{\max}}{d_{R_k,E}} \frac{1}{\sum_{i=1}^{n} \left(d_{\max}/d_{R_i,E}\right)} = \frac{1}{\sum_{i=1}^{n} \left(d_{R_k,E}/d_{R_i,E}\right)}, \quad (16)$$

where

$$d_{R_k,E} = \sqrt{\sum_{i=1}^{5} \left[X_{k,i} - E\left(X_i\right)\right]^2}, \quad (17)$$

where $X_{k,i}$ indicates the ith behavior characteristic of node k, $E(X_i)$ represents the expected value of the characteristic of all neighbors.

After obtaining the weight values of all recommended information, the indirect trust value can be calculated as

$$\mathrm{ITV}_{i,j}\left(T_i\right) = \sum_{k=1}^{n} w_{R_k} \cdot \mathrm{DTV}_{k,j}\left(T_i\right), \quad (18)$$

where $\mathrm{DTV}_{k,j}(T_i)$ is the direct trust value of node k to j, while $\mathrm{ITV}_{i,j}(T_i)$ is the indirect trust value of node i to j.

4.5. The Decision Phase. After obtaining the direct trust value and indirect trust value, the evaluation node is needed to integrate them and outputs the final trust value $\mathrm{TV}_{i,j}(T_i)$

$$\mathrm{TV}_{i,j}\left(T_i\right) = w_1 \cdot \mathrm{DTV}_{i,j}\left(T_i\right) + w_2 \cdot \mathrm{ITV}_{i,j}\left(T_i\right), \quad (19)$$

where w_1 and w_2 are two empirical coefficients and subject to $w_1 + w_2 = 1$, depending on the environment and expert experience.

Finally, the evaluation node will make a decision according to the rules

$$\begin{aligned} &\mathrm{Bel}_{i,j}\left(T_2\right) > \mathrm{Bel}_{i,j}\left(T_1\right) + \mathrm{Bel}_{i,j}\left(T_3\right), \\ &\mathrm{Bel}_{i,j}\left(T_1\right) < \alpha, \\ &\mathrm{Pls}_{i,j}\left(T_2\right) - \mathrm{Bel}_{i,j}\left(T_2\right) < \beta, \end{aligned} \quad (20)$$

where $\mathrm{Bel}_{i,j}(\cdot)$ is belief function and $\mathrm{Pls}_{i,j}(\cdot)$ is plausibility function and parameters α and β are dynamically adjusted according to the predefined security acquirements.

If an evaluated node satisfies the above conditions, it will be judged as malicious and its ID information will be broadcasted to all neighbors, till it finally reaches the base station. Thus the base station can isolate this malicious node and ignore all packets relayed by it. Otherwise, if Formula (21) is satisfied, the evaluated node will be regarded as a trust member and continue its normal operations with the whole network:

$$\begin{aligned} &\mathrm{Bel}\left(T_1\right) + \left(\mathrm{Pls}\left(T_1\right) - \mathrm{Bel}\left(T_1\right)\right) \\ &\quad \cdot \left(1 - \left(\mathrm{Pls}\left(T_1\right) - \mathrm{Bel}\left(T_1\right)\right)\right) > \gamma, \end{aligned} \quad (21)$$

where γ is a threshold and is adjusted according to the predefined security acquirements, which will be shown in Figure 10. Its value must guarantee that Formulas (20) and (21) are mutually exclusive, which is proved in the Appendix.

When the evaluated node does not meet one of both judgment mechanisms mentioned above, its state is regarded as uncertain. Most of existing trust models do not provide any solution to deal with this critical state but to wait till the next round of collection. What is worse, the balance between the frequency of behavior characteristic collection and effective judgment is a big problem. Due to information exchange among nodes, too frequent collection of behavior characteristic will accelerate energy consumption rate of nodes, while too long interval will give enough opportunities to malicious node to disrupt the normal operation of network. In order to solve this problem effectively, a dynamic weighting algorithm is introduced in this paper. More details are described in the next section.

5. Fusion of Weighted Evidences

In general, the trust status of an evaluated node is just denoted as either trustful or distrustful (or represented as 1 or 0). However, in practice the fused result appears uncertain so frequently. One important reason is that some normal evidences weaken the appearance of an abnormal behavior and confuse the fusion process. It is said, the final judgment result cannot be simply determined as trust or distrust. On the other hand, it is noted that taking the measure of equal treatment to all evidences during evidence confusion is obviously inadequate because various attacks have different impacts on different behavior characteristics. When a node is

Table 1: Decision table.

Fuzzed evidences	T_1	T_2	T_3	Judgment result
m_1	0.65	0.3	0.05	T_1
m_2	0.2	0.7	0.1	T_2
m_3	0.8	0.1	0.1	T_1
m_4	0.6	0.25	0.15	T_1
m_5	0.20	0.25	0.55	T_3

captured, some of its characteristics will change rapidly, while some may still maintain in normal levels.

In evidence theory, if the importance of each evidence can be known accurately, the fusion precision can be guaranteed and the convergence speed can be accelerated at the same time. When an evaluated node is in an uncertain state, we first select a behavior characteristic as main parameter which should make the greatest contribution to recent judgment, and all the others are auxiliary parameters. This treatment has two advantages: on one hand, selecting main parameter can avoid covering the part of exception involved by other normal values; on the other hand, auxiliary parameters can play correction roles in the judging process comparing to the main parameter. Table 1 shows an example of decision table on how to select the main parameter.

As shown in Table 1, because the third behavior characteristic is the most apparent support of such a judgment, the contribution value of the third characteristic is added to 1. Similarly, using sliding window, the behavior characteristic with the most largest contribution in the latest rounds can be found and set as main parameter, which is illustrated in Figure 4.

The number of behavior characteristics with the largest contribution in each round is recorded and the window slides one unit from left to right, which means the first unit in right side is dropped. As shown in Figure 4, the sliding window consists of six units, which means every round, the window records the newest knowledge but discards the oldest knowledge. Due to three times of appearance in recent judgment, the behavior characteristic 1 will be selected as the main parameter.

After having selected main parameter and auxiliary parameters, their weights are, respectively, set as $\omega_1^{\text{his}}, \omega_2^{\text{his}}, \ldots, \omega_5^{\text{his}}$, where identification his implies that these values are related to their historic values. This weight is determined based on historical judgment; it reflects the relative contribution of historical decisions of each behavioral characteristic; the higher the contribution of the behavioral characteristics the greater the weight value obtained. However, in the actual work environment, there are still a lot of uncertainty factors on sensor node; in order to avoid state misjudgment by an abnormal value, we need to calculate the real-time reliability of each behavior characteristic. Then, the final weight of behavior characteristic is achieved by comprehensive historical contribution and real-time reliability. The value of real-time behavioral characteristics reliability is calculated by the distance between evidences [31].

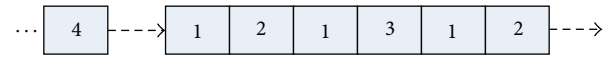

Figure 4: An example of sliding window.

For evidence of m_i and m_j, the distance between them is

$$d_{\text{BPA}}\left(m_i, m_j\right) = \sqrt{\frac{1}{2}\left(M_i - M_j\right) D \left(M_i - M_j\right)^T}, \tag{22}$$

where $M_i = [m_i(T_1), m_i(T_2), m_i(T_3)]$ and D is a 3×3 matrix whose elements are

$$D\left(T_i, T_j\right) = \frac{\left|T_i \cap T_j\right|}{\left|T_i \cup T_j\right|}, \quad i, j = 1, 2, 3, \tag{23}$$

where $T_i \cap T_j$ is used to measure conflict and similarity between focal elements T_i and T_j. When $T_i \cap T_j = 0$, the similarity between T_i and T_j is zero, which means the largest conflict appears here. Therefore, the above equation can be used to measure the degree of similarity between the focal elements.

Combining Formulas (22) and (23), we can obtain another way to calculate d_{BPA}:

$$\begin{aligned} &d_{\text{BPA}}\left(m_i, m_j\right) \\ &= \sqrt{\frac{1}{2}\left(\left\|M_i\right\|^2 + \left\|M_j\right\|^2 - 2\left\langle M_i, M_j\right\rangle\right)}, \end{aligned} \tag{24}$$

where $\langle M_i, M_j \rangle$ is the scalar product defined by

$$\begin{aligned} \left\langle M_i, M_j\right\rangle &= \sum_{m=1}^{3}\sum_{n=1}^{3} m_i\left(T_m\right) m_j\left(T_n\right) \frac{\left|T_m \cap T_n\right|}{\left|T_m \cup T_n\right|}, \\ \left\|M_i\right\|^2 &= \left\langle M_i, M_i\right\rangle. \end{aligned} \tag{25}$$

According to Formula (24), we obtain the distance between m_i and m_j:

$$D = \begin{bmatrix} 0 & d_{12} & \cdots & d_{15} \\ d_{21} & 0 & \cdots & d_{25} \\ \vdots & \vdots & \vdots & \vdots \\ d_{51} & d_{52} & \cdots & 0 \end{bmatrix}. \tag{26}$$

A similarity coefficient between m_i and m_j can be defined as

$$s_{ij} = 1 - d_{ij}. \tag{27}$$

It can be expressed by the form of similarity matrix

$$S = \begin{bmatrix} 1 & s_{12} & \cdots & s_{15} \\ s_{21} & 1 & \cdots & s_{25} \\ \vdots & \vdots & \vdots & \vdots \\ s_{51} & s_{52} & \cdots & 1 \end{bmatrix}. \tag{28}$$

Through adding each row of the similarity matrix, the support degree to m_i of all evidences is

$$\mathrm{Sup}\left(m_i\right) = \sum_{j=1}^{5} s_{ij}. \tag{29}$$

Then by normalizing, we can obtain the real-time reliability of each behavior property:

$$\omega_i^{\mathrm{cur}} = \frac{\mathrm{Sup}\left(m_i\right)}{\sum_{j=1}^{5} \mathrm{Sup}\left(m_j\right)}, \quad i = 1, 2, 3, 4, 5. \tag{30}$$

The above formula reflects the real-time reliability of the behavioral characteristics, and it satisfies the condition $\sum_{i=1}^{5} \omega_i^{\mathrm{cur}} = 1$. If the value of a behavior characteristic is similar to others, we think it has higher degree of mutual support, so its real-time reliability is greater. Conversely, the behavior characteristic will be regarded as being less reliable.

Integrating historical contribution and real-time reliability of each behavioral characteristic, the composite weight value of behavioral characteristic can be obtained:

$$\omega_i^{\mathrm{com}} = \sqrt{\omega_i^{\mathrm{cur}} \cdot \omega_i^{\mathrm{his}}}. \tag{31}$$

So the final weight value of each behavior characteristic can be obtained:

$$\omega_i = \frac{\omega_i^{\mathrm{com}}}{\sum_{j=1}^{5} \omega_j^{\mathrm{com}}}, \quad i = 1, 2, 3, 4, 5. \tag{32}$$

Having obtained the weight value of each behavior, now we will focus on the fusion process again. First, use the weight value as discount factor to revise the basic probability assignment

$$\begin{aligned} m_i^*\left(T_k\right) &= \omega_i m_i\left(T_k\right), \quad (k = 1, 2), \\ m_i^*\left(T_3\right) &= 1 - \sum_{k=1}^{2} m_i^*\left(T_k\right). \end{aligned} \tag{33}$$

Then according to Formula (15), fuse all evidences and judge again. Here the physical significance of Formula (33) can be understood like this. The evidence's information is discounted according to discount factor, and then the discount part is added to focal element of uncertain. Increasing the value of uncertain information can reduce the conflict between the evidences. For some evidences which have big relative weights and high reliabilities, the discounts are small, so these evidences can maintain the confidence allocation as before. For the evidences which have small relative weights and low reliabilities, the discounts parts are large. Then, the value of the uncertain states will increase and the impact on the fusion results will decrease. When $\omega_i = 0$, the BPA of evidence i is $m_i^*(T_3) = 1$, and the other BPA of focal elements is 0. Evidence like this is called identify element, and no matter which evidence is selected to combine with it, BPA will be maintained unchanged.

As mentioned above, the fusion result which combines multidimensional behavioral characteristics is determined by high relative weights of behavior attributes. What is more, considering false detection and other reasons which will lead to high conflict information assigned low weight, and its influence on the fusion results will also reduce. This will be conductive to quickly arrive at a correct judgment and decision-making based on the fusion results. The flow chart of the proposed anomaly detection scheme is shown in Figure 5.

Table 2: Parameters in simulations.

w_1, w_2	0.6, 0.4
α, β	0.5, 0.2
γ	0.6
District	1000 m × 1000 m
Node number	600
Transmission radius	100 m
Initial trust value	1
Initial energy	1000 J
Node location	Random
MAC protocol	IEEE 802.11
Routing protocol	DSDV
Packet size	512 bytes
Transmission power	0.5 w
Receiving power	0.2 w
Idle power	0.15 w

6. Simulation Results

Assume that there are 600 nodes randomly deployed over a square area of 1000 × 1000 meters, and each node's transmission range is fixed and equal to 100 m. All of these nodes are fixed and cannot move. 10% of nodes are malicious and randomly distributed within the network. The malicious behavior patterns include flooding attack, select forwarding attack, and bad-mouthing attack, which is unknown to normal nodes. Assume that all nodes are healthy (uncompromised) and cooperative at the beginning, so all nodes' initial trust values are set as 1. During the simulation, each malicious node can randomly select a malicious behavior and activate attack. More initial parameters of the simulation are listed in Table 2. In this section, we use C++ language to simulate the trust model.

The trust model works as follows. The evaluation node monitors an evaluated node's behaviors and state, including ACK packets, sending packets, receiving packets, forwarding packets, and energy consumption rate. In order to make balance between energy consumption and security level, here we set the monitor interval $\Delta = 50$ seconds, which means a node reads its remaining energy value at the end of each interval and broadcasts to its neighbors. Assume that, in this paper, each node generates one sensing packet per second. It is well known that direct trust value is more accurate and reliable than indirect trust value, so the weight of direct trust value is larger than the weight of indirect trust value. As soon as a distrustful node has been determined, the evaluation node broadcasts its node ID to all one-hop neighbors and

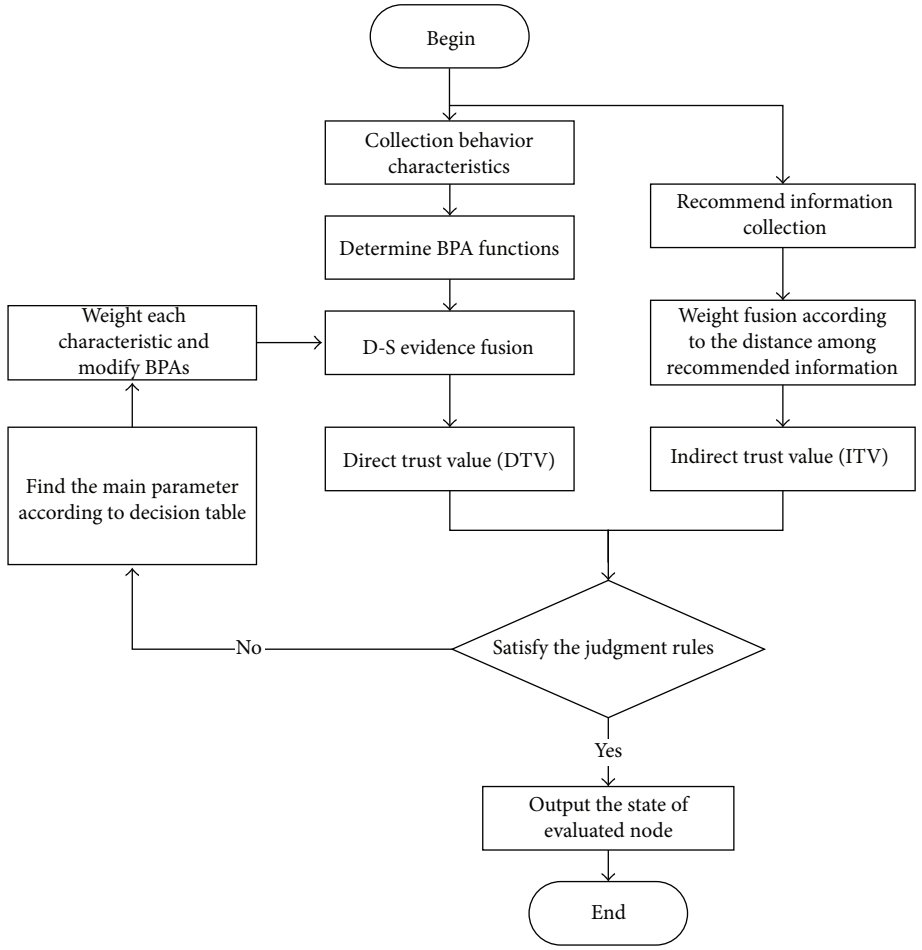

Figure 5: Flow chart of the proposed model.

tries to find a trust node to replace its place to forward packets.

Considering the accuracy and reliability of recommended information, assume that the evaluation node only accepts the packets from one-hop neighbors in this paper. For instance, as shown in Figure 6, node i can evaluate node j because node j lies in its communication range and there are interoperations between them. On the other hand, node i only accepts recommended information on node j from node R_1, R_2, or R_3, as common neighboring nodes.

In order to effectively illustrate the performance indexes, a comparison is made between our scheme and GTMS (group-based trust management model) [19], where the trust values are obtained by counting the number of successful and unsuccessful interactions on node level. Besides average trust value, four performance indexes are further defined here: detection ratio, false alarm ratio, true positive ratio, and false negative ratio. The detection ratio is defined as the percentage of nodes that are successfully detected out of all malicious nodes, while the false alarm ratio is claimed as the percentage of normal nodes that are incorrectly determined as anomalous. The true positive ratio is the percentage of malicious nodes that are successfully determined out of all normal nodes while the false negative ratio is the percentage of negative nodes that were incorrectly reported as normal nodes. Obviously, the average trust value of malicious nodes indicates the capability or possibility that malicious nodes can be detected by the algorithm.

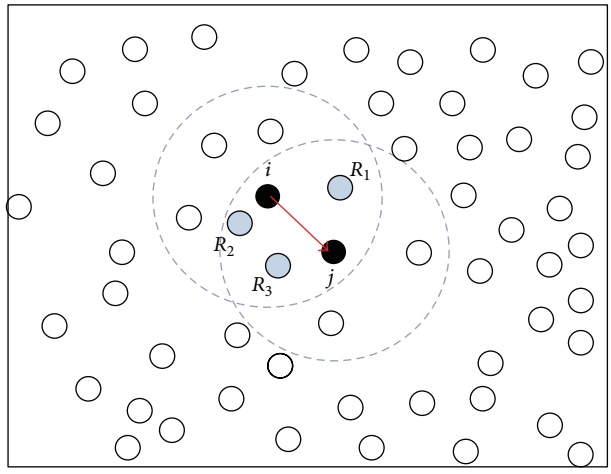

Figure 6: Simulation scenario.

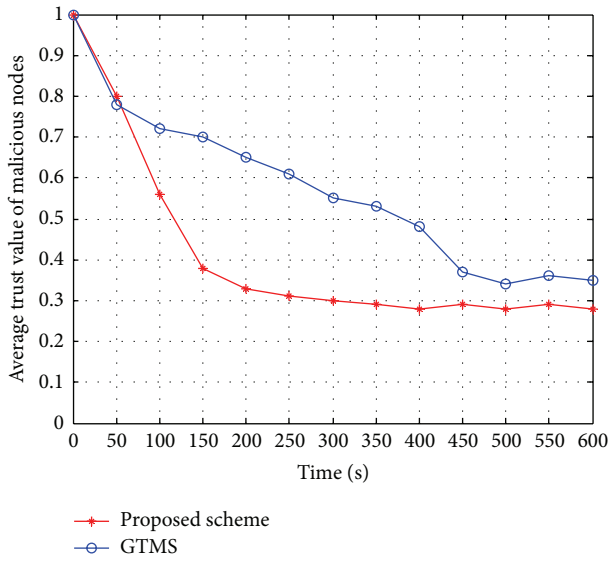

Figure 7: Average trust value versus time.

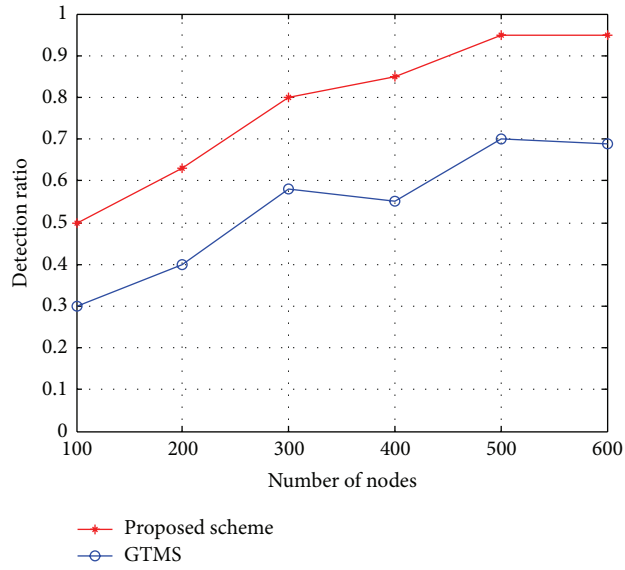

Figure 8: Detection ratio versus node number.

As shown in Figure 7, the average trust value of our scheme descends faster than GTMS in the beginning. Recall that various types of attacks are introduced simultaneously in this paper, while GTMS mainly counts the number of successful transmission packets. It is said that GTMS does not take into account multiple attack types and can detect only one type of attack like selective forwarding. As a result of this, when a network meets multiple types of attacks besides packet loss, GTMS cannot decrease the average trust value of malicious node as quickly as possible, which is wholly different from the proposed scheme where more aspects of various attacks are considered.

On the other hand, it is also shown in Figure 7 that both average trust values gradually become stable, and our model invariably maintains better performance than GTMS during the whole running period. The stable average trust value in our model finally lies between 0.3 and 0.4 while the one in GTMS is between 0.5 and 0.6.

As shown in Figure 8, both detection ratios arise as the whole node number increases from 100 to 600. The reasonable explanation is that, with the increasing of node number, the recommended information that can be utilized by the model also increases, so there are more malicious nodes detected correctly. It is also noted that the detection ratio of the proposed model is higher because, by using fuzzy theory, trust value can reflect the practical situation more accurately.

To show how the parameters influence system performance, a few additional experiments are carried out in this paper. Recall that, in the decision phase, parameters α, β, and γ play vital roles to the performance of trust model and are determined on the basis of experience and practical environment. The detection ratio, false alarm ratio, true positive ratio, and false negative ratio of our trust model are shown in Figures 9 and 10, respectively. Note that each time only one parameter is changed while the other two parameters are maintained unchangeable.

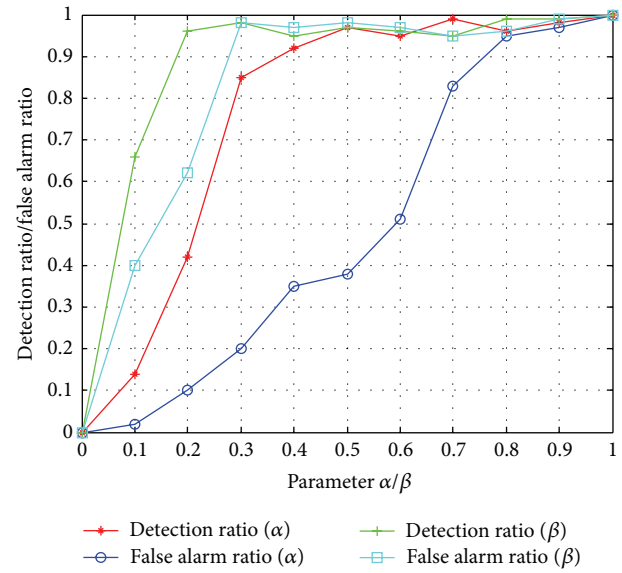

Figure 9: Detection and false detection ratio versus parameter α or β.

As shown in Figure 9, both detection ratio and false alarm ratio arise with the increasing of parameters α and β. It is worth noting that when $\alpha = 0$ or $\beta = 0$, all nodes in the network cannot satisfy Formula (20); that is, $\text{Bel}_{i,j}(T_1) < \alpha$ and $\text{Pls}_{i,j}(T_2) - \text{Bel}_{i,j}(T_2) < \beta$ cannot be satisfied, so both ratios are equal to 0. On the contrary, when $\alpha = 1$ or $\beta = 1$, all nodes satisfy the conditions $\text{Bel}_{i,j}(T_1) < \alpha$ and $\text{Pls}_{i,j}(T_2) - \text{Bel}_{i,j}(T_2) < \beta$, so the detection ratio and false alarm ratio are 1. Obviously, the values of parameters α and β ought to be set up to make the final detection ratio as high as possible and false alarm ratio as low as possible. However, as shown in Figure 9, high detection ratio requires large α while low false alarm ratio needs small α, which is a paradox. The situation is similar for parameter β. In order to improve the system

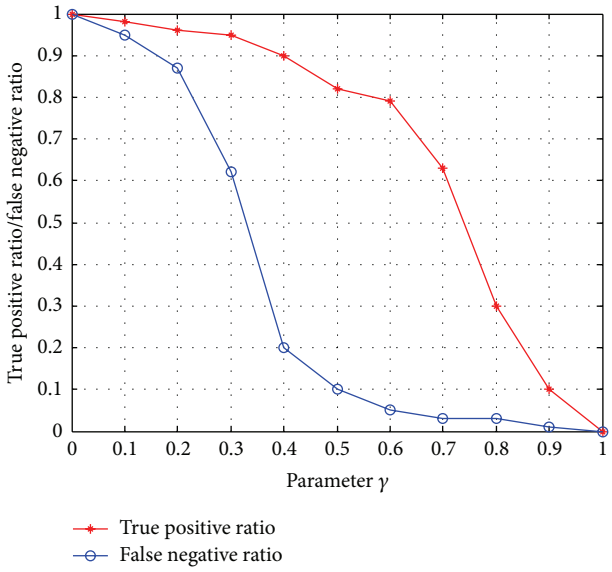

Figure 10: True positive ratio and false negative ratio versus parameter γ.

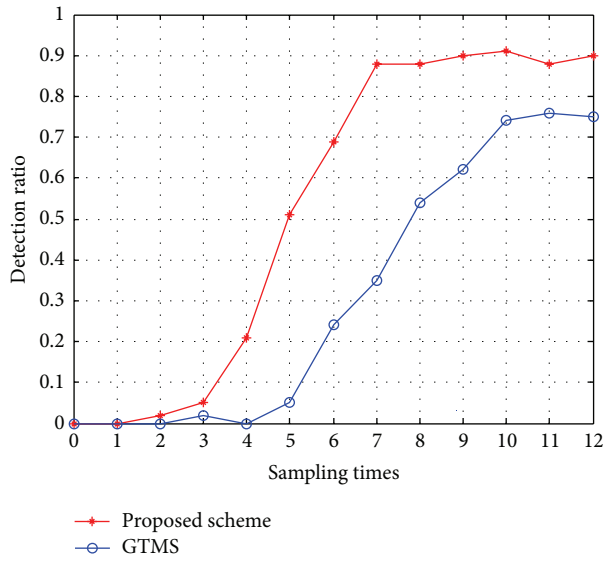

Figure 11: Ratio of detected malicious node versus collection times.

performance in this paper, the feasible values for parameters α and β are, respectively, set as 0.5 and 0.2 where the gaps between detection ratio and false alarm ratio are the largest.

It is shown in Figure 10 that both true positive ratio and false negative ratio decrease with the increasing of parameter γ. It is also worth noting that when $\gamma = 0$, all nodes satisfy Formula (21), so all of them are judged as normal nodes disregarding whether they are normal nodes or malicious nodes. Under this situation, both true positive rate and false negative rate are equal to 1. On the contrary, when $\gamma = 1$, both true positive ratio and false negative ratio are 0. Similarly, parameter γ can be determined according to the performance gap between true positive ratio and false negative ratio, which is shown in Figure 10. In this paper, γ is set as 0.6.

One other point worth mentioning is weight. In our trust model, we take a weighting method to indicate the importance of each evidence of an uncertain status node and adapt the weights according to the new trust value. Compared to the previous trust models, here for a node with uncertain state, we win a new opportunity to deduce its state, so the detection process is accelerated.

As shown in Figure 11, both detection ratios increase with the continuing of simulation, and our scheme is better than GTMS. It is noted that the scheme is able to detect more than 50% malicious nodes after 250 seconds ($= 5\Delta$) while the detection ratio of GTMS is about 5%.

7. Conclusions

As an emerging technology, wireless sensor networks have been widely studied and applied. At the same time, its security problem has received widespread attention. Anomaly detection has become one of current research hotspots on wireless sensor network security because of its characteristic of active defense. In this paper, a trust-based anomaly detection model is proposed, where the evaluation node monitors the behaviors of evaluated nodes from five aspects and uses the trust model which employs fuzzy theory and revised evidence theory to calculate the nodes' state. What is more, when the state of an evaluated node is uncertain, weighting algorithm is used to make decision feasible before next round of detection. The simulation results show that when an evaluated node activates various attacks, the average trust value will decrease more rapidly in our trust model so that it will outperform GTMS in detection ratio index. Furthermore, because weighting algorithm is taken, convergence rate is accelerated. In our future work, we will extend the idea to different fields like secure routing, data aggregation, and so forth and improve their efficiency.

Appendix

According to fuzzy theory, we know that $\mathrm{Bel}(T_1) + \mathrm{Bel}(T_2) + \mathrm{Bel}(T_3) = 1$. If T_3 represents an uncertain status and $T_3 = U - \{T_1, T_2\}$, then from Definition 3, we have $\mathrm{Pls}(T_2) = \mathrm{Bel}(T_2) + \mathrm{Bel}(T_3)$ and $\mathrm{Pls}(T_1) = \mathrm{Bel}(T_1) + \mathrm{Bel}(T_3)$. Thus Formula (20) can be rewritten as

$$\begin{aligned} \mathrm{Bel}(T_1) + \mathrm{Bel}(T_3) &< 0.5, \\ \mathrm{Bel}(T_1) &< \alpha, \\ \mathrm{Pls}(T_2) - \mathrm{Bel}(T_2) &< \beta \end{aligned} \tag{A.1}$$

and Formula (21) can be rewritten as

$$\mathrm{Bel}(T_1) + \mathrm{Bel}(T_3) * (1 - \mathrm{Bel}(T_3)) > \gamma. \tag{A.2}$$

According to Formula (A.1), the max value of $\mathrm{Bel}(T_1) + \mathrm{Bel}(T_3)$ is not larger than 0.5. If we denote $\mathrm{Bel}(T_1) = x$, $\mathrm{Bel}(T_3) = 0.5 - x$ and substitute them into the left part of Formula (A.2), we will obtain a quadratic function with parameter x:

$$f(x) = x + (0.5 - x) * (0.5 + x) = -x^2 + x + 0.25. \tag{A.3}$$

Obviously, the maximum value of $f(x)$ is 0.5. Because $\text{Bel}(T_1) + \text{Bel}(T_3) < 0.5$, the maximum value of $f(x)$ is less than 0.5. So, if we set $\gamma > 0.5$, the values of $\text{Bel}(T_1)$ and $\text{Bel}(T_3)$ will not satisfy Formula (21) at the same time. It is said, if the value of γ lies in the range of (0.5~1), Formula (20) and Formula (21) are mutually exclusive.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] I. F. Akyildiz, T. Melodia, and K. R. Y. Chowdury, "Wireless multimedia sensor networks: a survey," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 32–39, 2007.

[2] B. Mukherjee, J. Yick, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] H.-W. Lee, A.-S. K. Pathan, and C. S. Hong, "Security in wireless sensor networks: issues and challenges," in *Proceedings of the 8th International Conference Advanced Communication Technology (ICACT '06)*, pp. 1043–1048, Phoenix Park, Ireland, February 2006.

[4] X. Du and H.-H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60–66, 2008.

[5] L. Qin, Y. X. Li, and Q. Liang, "Research on wireless sensor network security," in *Proceedings of the International Conference on Computational Intelligence & Security*, pp. 493–496, Nanning, China, December 2010.

[6] C. Y. Miao, C. Leung, H. Yu, Z. Q. Shen, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[7] X. Wang, L. Ding, and S. Wang, "Trust evaluation sensing for wireless sensor networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 6, pp. 2088–2095, 2011.

[8] J. Ma and M. A. Orgun, "Trust management and trust theory revision," *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*, vol. 36, no. 3, pp. 451–460, 2006.

[9] R. X. Lu, X. D. Lin, H. J. Zhu, X. H. Liang, and X. Shen, "BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 1, pp. 32–43, 2012.

[10] P. Wang, C. Li, and J. Zheng, "Combined data aggregation and encryption using clustered slepian-wolf coding for wireless sensor networks," in *Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07)*, pp. 920–925, IEEE, Washington, DC, USA, November 2007.

[11] T. A. Zia, "Reputation-based trust management in wireless sensor networks," in *Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '08)*, pp. 163–166, Sydney, Australia, December 2008.

[12] S. S. Zheng and J. S. Baras, "Trust-assisted anomaly detection and localization in wireless sensor networks," in *Proceedings of the 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 386–394, IEEE, Salt Lake City, Utah, USA, June 2011.

[13] X. Z. Cheng, F. Liu, and D. C. Chen, "Insider attacker detection in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications*, pp. 1937–1945, Anchorage, Alaska, USA, May 2007.

[14] N. Pissinou, G. V. Crosby, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06)*, pp. 13–22, Columbia, Md, USA, April 2006.

[15] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 257–283, ACM, Boston, Mass, USA, August 2000.

[16] M. Ganesh, *Introduction to Fuzzy Set and Fuzzy Logic*, Prentice Hall, 2006.

[17] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *Annals of Mathematical Statistics*, vol. 38, no. 2, pp. 325–339, 1967.

[18] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, 1976.

[19] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. 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.

[20] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," *Journal of Network & Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[21] V. Chatzigiannakis and S. Papavassiliou, "Diagnosing anomalies and identifying faulty nodes in sensor networks," *IEEE Sensors Journal*, vol. 7, no. 5, pp. 637–645, 2007.

[22] S. Y. Moon and T. H. Cho, "Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks," *International Journal of Computer Science and Network Security*, vol. 9, no. 7, pp. 118–122, 2009.

[23] D. Tian and N. D. Georganas, "Energy efficient routing with guaranteed delivery in wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '03)*, vol. 3, pp. 1923–1929, IEEE, New Orleans, La, USA, March 2003.

[24] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks (Q2SWinet '05)*, vol. 7, pp. 16–23, ACM, Montreal, Canada, October 2005.

[25] H. X. Xia, W. Meng, and H. Z. Song, "A dynamic trust model based on recommendation credibility in grid domain," in *Proceedings of the International Conference on Computational Intelligence and Software Engineering (CiSE '09)*, pp. 1–4, Wuhan, China, December 2009.

[26] X. Liu, J. H. Luo, and M. Y. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks," *Computer Networks*, vol. 53, no. 14, pp. 2396–2407, 2009.

[27] Y. H. Chang and F. Liu, "Wireless sensor intrusion detection system based on the theory of evidence," in *Proceedings of the International Conference on Computer Science and Network Technology (ICCSNT '11)*, vol. 4, pp. 2811–2814, IEEE, Harbin, China, December 2011.

[28] 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.

[29] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.

[30] W. K. Shi, L. Z. Chen, and F. Du, "Weighting factors assignment of evidence theory based on evidence distance," *Journal of Systems Engineering and Electronics*, vol. 16, no. 2, pp. 273–278, 2005.

[31] D. Grenier, A.-L. Jousselme, and É. Bossé, "A new distance between two bodies of evidence," *Information Fusion*, vol. 2, no. 2, pp. 91–101, 2001.