Computers and Electrical Engineering 000 (2017) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Multi-agent trust-based intrusion detection scheme for wireless sensor networks☆

Xianji Jin[a], Jianquan Liang[b,*], Weiming Tong[a], Lei Lu[a], Zhongwei Li[a]

[a] School of Electrical Engineering and Automation, Harbin Institute of Technology Harbin, 150001, China
[b] State Grid Heilongjiang Electric Power company Limited, Electric Power Research Institute, Harbin 150030, China

ARTICLE INFO

Article history:
Received 19 July 2015
Revised 13 April 2017
Accepted 14 April 2017
Available online xxx

Keywords:
Wireless sensor networks
Intrusion detection
Multi-agent
Node trust value

ABSTRACT

In order to achieve both a higher detection rate and a lower false positive rate of internal node intrusion detection in layer-cluster wireless sensor networks, an intrusion detection scheme based on the use of both a multi-agent system and a node trust value is proposed. In this scheme, the multi-agent model framework is established in both the cluster heads and the ordinary sensor nodes to perform intrusion detection. First, various, typical node trust attributes are defined and Mahalanobis distance theory is used to judge whether these attributes are normal. Second, the node trust value is calculated and updated based on the combination of the Beta distribution and a tolerance factor. Finally, node intrusion detection is realized. Simulation results demonstrate that the modified scheme has a higher detection rate and a lower false positive rate, even when several types of intrusions are present.

1. Introduction

The continuous development of wireless sensor networks (WSNs) has contributed to their extensive application in various industries, including in key areas such as the electrical, healthcare, and military industries. Each of these areas maintains strict security requirements because of its unique demands. Thus, the security of WSNs is crucial [1]. WSNs face both malicious external and malicious internal node attacks that are categorized based on the attack source. External node attacks can be prevented with authentication and encryption technologies; however, internal node attacks are difficult to eliminate with these approaches. Therefore, intrusion detection is considered a second line of defense for protecting the security of a WSN [2].

Agents are important concepts in the domains of both artificial intelligence and computing science, and they can be realized through either hardware or software programming. A multi-agent system is composed of a certain number and kind of agent that can perform specific tasks [3]. Agent technology features several characteristics, including autonomy, sociality, reactivity, and pro-activeness, that make it an ideal carrier for intrusion detection. When agent technology is used in intrusion detection, it can both improve the tolerance and increase the extensibility of the system. As a result, several studies related to intrusion detection for WSNs have been carried out by both domestic and foreign researchers. Thamilarasu and Ma proposed an autonomous mobile agent based intrusion detection architecture for addressing security in wireless body area networks [4]. In [5], Riecker et al. proposed a lightweight, energy-efficient intrusion detection scheme that made

☆ Reviews processed and approved for publication by Editor-in-Chief.

* Corresponding author.
E-mail addresses: mrking@hit.edu.cn (X. Jin), ljq_hit@163.com (J. Liang), dianqi@hit.edu.cn (W. Tong), lulei@hit.edu.cn (L. Lu), lzw@hit.edu.cn (Z. Li).

http://dx.doi.org/10.1016/j.compeleceng.2017.04.013
0045-7906/

use of mobile agents to detect intrusion based on the sensor node (SN) energy consumption. Wang et al. proposed a multi-agent mechanism in which the combination of a self-organizing map neural network and a K-means algorithm functioned to detect the abnormity of the nodes in the WSN, which made the system more flexible, more precise, and easier to implement [6]. Wang et al. discussed the use of a multi-agent intrusion detection system in a cluster-based WSN that both increased the extensibility and reduced the cost of the system [7]. The above-mentioned studies provide reference points for WSN intrusion detection research that highlights the unique advantages of agent technology in terms of both system scalability and flexibility [8].

On the other hand, the above-mentioned detection schemes are mainly aimed at detecting if nodes are experiencing a certain type of intrusion, which means that if there is are multiple types of intrusion occurring at the same time, the detection rate may decrease. Thus, an effective mechanism is needed to solve this problem. The prevailing method employed to accomplish this effectively is the use of a trust scheme. Trust schemes are typically applied to the following aspects of WSNs [9]: secure data aggregation, secure routing, secure localization, and intrusion detection.

Liu et al. [10], proposed an improved, reliable, trust-based, energy-efficient data-aggregation protocol for WSNs. The trust value used in [10] was calculated with the Beta reputation system. Gupta et al. also proposed a data-aggregation protocol for WSNs based on a trust scheme in [11]. Zahariadis et al. proposed a secure routing protocol that relied on a distributed trust model for the detection and avoidance of malicious neighbors [12]. The trust model proposed in [12] relied on both direct and indirect observation to derive the trust value of each neighboring node through the Beta distribution. A new security localization algorithm based on a trust mechanism was proposed by Zhang et al. in [13]. Both their initial trust value and trust update weight were set by a Beta distribution. Zhang et al. proposed a secure localization scheme based on trust evaluation for localization in WSNs [14]. The studies mentioned above demonstrate that the application of trust schemes to WSNs is both achievable and helps to solve security problems. However, to the best of our knowledge, research studies performed on intrusion-detection based trust schemes in WSNs are rare.

Ebinger and Bibmeyer proposed a cooperative intrusion detection method based on both reputation exchange and trust evaluation for mobile ad hoc networks [15]. They divided the network's reputation information into both trust and confidence and then merged these subcategories into the intrusion detection credibility. Gerrigagoitia et al. introduced a new intrusion detection design based on both the reputations and the trust values of the different nodes in a WSN for both decision-making and analysis of possible malicious attack sources [16]. In their design, each node had an intrusion detection system agent that monitored local activities, and the trust value was calculated with the Beta distribution. Bao et al. proposed a trust-based intrusion detection scheme in which both quality of service and social trust were considered as trust metrics for detecting malicious nodes in clustered WSNs [17]. Consequently, we now know that trust schemes can identify both malicious and non-collaborative nodes, resist cyber-attacks, and improve the security, confidentiality, and integrity of WSNs [18,19].

In existing schemes, such as those proposed in [10–13], and [16], trust values are calculated using the Beta distribution. However, with respect to the statistics of successful/failed interactions, specific methods for judging interaction results were not presented. Moreover, there was no regard for abnormal physical states of the SNs in the trust metrics utilized. An abnormal physical state can refer to either an abnormal measured value or abnormal energy consumption of a node.

As a result, in this paper, we propose a multi-agent intrusion detection scheme based on a node trust value for layer-cluster WSNs. The scheme is realized based on a multi-agent model in which the agents collaborate with one another to manage the trust value. We adopt the Mahalanobis distance to discriminate between the successful/failed interactions of each node, which helps to improve the accuracy of the trust value. In addition, the trust value is calculated based on both beta distribution theory and a tolerance factor. The tolerance factor increases both the veracity and the flexibility of the trust value computation.

The remainder of this paper is organized as follows. In Section 2, we establish an intrusion detection framework and discuss a multi-agent model for both the cluster heads (CHs) and the SNs. Later, in Section 3, we present an implementation of this intrusion detection scheme that includes the trust value calculation and the intrusion detection for both CHs and SNs. Section 4 describes the performance analyses of the proposed scheme, with simulation results provided to characterize the scheme. In Section 5, we set up an experimental platform to verify the feasibility of the proposed intrusion detection scheme. Finally, we draw conclusions in Section 6.

2. Intrusion detection framework modeling

2.1. Network topology

The implementation of a layer-cluster topology achieves an improved scalability while, at the same time, effectively reducing both the management complexity and communication cost of a network. Hence, for most practical applications, the topology of WSNs is cluster-based. As shown in Fig. 1, the layer-cluster network considered in this paper is composed of ordinary SNs, CHs, and a base station (BS). The power supply, computing, storage, communication, and other capabilities of the SNs are constrained. The communications between the SNs and the CHs can be accomplished with single hops, while the communications between the SNs and the BS can be performed through the CHs. The communications between the CHs and the BS can be accomplished in either a single-hop or a multi-hop manner. The CHs are responsible for the management

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

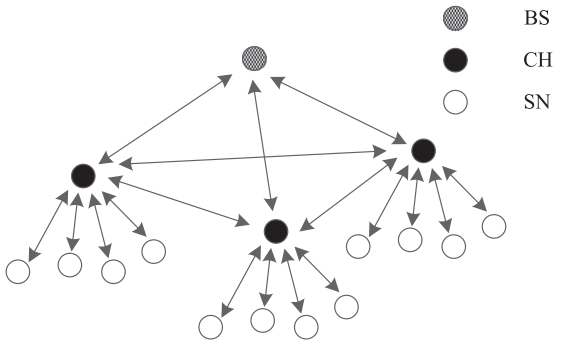

Fig. 1. Network topology structure.

Table 1
Common network attacks in WSNs.

Attack type	Attack behavior
Selective forwarding attack	Subjectives refuse to forward specific packets and discarded packets.
Black hole attack	Neighboring nodes send all packets to malicious nodes, which are then discarded by these nodes.
Spoofing and tampering attack	Subjectives forge and modify message content.
Sinkhole attack	Similar to the black hole attack but with malicious nodes located closer to the sink node.
Denial of Service (DoS) attack	A malicious node forces the node that provides services to produce an error or deplete resources via either deception or camouflage.
Wormhole attack	A malicious node has a strong transceiver ability, causing the physical nodes on multi-hop neighboring nodes to be mistaken for one another.
Flooding attack	Malicious nodes communicate with and query other nodes for replies constantly, exhausting these nodes' energies.
Sibyl attack	Malicious nodes disguise a node using multiple identities.

of the nodes in each cluster, and because they are required to accomplish more tasks, they need more energy, memory, and computing resources than the SNs do.

2.2. Trust feature definition

WSNs employ a wireless channel that has limited resources and is unable to adopt complex communication node technologies, which makes it more likely for them to encounter various kinds of attack. The main characteristics of typical network attacks are shown in Table 1.

Based on the analysis of typical attacks on WSNs, we can conclude that most attacks are characterized by discarding or rejecting messages, forwarding packets, or draining node energies. Therefore, in order to calculate the trust value of each node easily and accurately, we refer to the feature modeling utilized in [20] and combine the characteristics of different types of network attacks. The trust feature (TF) is then defined as follows:

Definition 1. Packet loss rate

With respect to the communication between node A and the other nodes, the ratio of A's lost packets to its total transmitted packets is defined as the packet loss rate of node A, and its value can be obtained by

$$TF_1 = \frac{P_1}{P_a} \tag{1}$$

where TF_1 is the packet loss rate, P_1 is the number of A's packets lost, and P_a is the number of packets sent out of node A. Packet loss rate can reflect the quality of a node's data transmission. If the value of TF_1 is always large, this indicates that the node is likely to experience an invasion such as a selective forwarding attack, black hole attack, or sinkhole attack.

Definition 2. Packet transmission frequency

Packet transmission frequency describes the number of messages transmitted over a certain period of time. It is represented by

$$TF_2 = \frac{P_b}{\Delta t} \tag{2}$$

where TF_2 is the packet transmission frequency andP_b is the number of packets transmitted successfully in time period Δt. If the value of TF_2 is always large, this indicates that the node is likely to experience an invasion such as a DoS attack, wormhole attack, or flooding attack.

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

Definition 3. Packet receiver frequency

Packet receiver frequency is the number of packets received successfully in a certain period of time, which can be obtained by

$$TF_3 = \frac{N_r}{\Delta t} \tag{3}$$

where TF_3 is the packet receiver frequency and N_r is the number of packets received successfully in time period Δt. If the value of TF_3 is always large, this indicates that the node is likely to experience an invasion such as a black hole attack, sinkhole attack, wormhole attack, or sibyl attack.

Definition 4. Energy consumption rate

Energy consumption rate is the amount of energy consumed by a node energy in a certain period of time. This value can be obtained by

$$TF_4 = \frac{|E_{t+\Delta t} - E_t|}{\Delta t} \tag{4}$$

where TF_4 is the energy consumption rate, $E_{t+\Delta t}$ is the residual energy at time $(t + \Delta t)$, and E_t is the residual energy at time t. If the value of TF_4 is always large, this indicates that the node is likely to experience an invasion such as a DoS attack or Flooding attack.

Definition 5. Sensor measurement value

Some kinds of malicious intrusion tamper with or forge sensor data in such a way that the network transmission does not show any abnormalities. This kind attack seriously affects the execution of normal functions in the physical system. Under normal circumstances, TF_5 is a stationary series, but it deviates significantly from its usual state when attacks such as spoofing or tampering occur.

2.3. Multi-agent modeling

In this paper, an intrusion detection scheme is proposed based on a multi-agent model established for CHs and SNs. Functions such as *TF* collection, trust value calculation, intrusion judgment, and intrusion response are achieved via the cooperation of multiple agents. For this reason, agent settings are implemented with respect to CH and SN intrusion detection.

2.3.1. Multi-agent model of CH

The multi-agent model of the CH consists of the following types of agent, shown in Fig. 2.

Cluster trust collection agent (CTCA): The function of this agent is to calculate the *TF* of the CH according to both the communication status and the definition of *TF*. However, there is no TF_5 in the CH. Then, the CTCA sends the calculated *TF* to the CCA.

Cluster communication agent (CCA): The functions of this agent are as follows: receiving the *TF* from its adjacent CHs and SNs in its cluster, sending its own *TF* to its adjacent CHs, and uploading the security statuses of the SNs in its cluster and of the adjacent CHs to the BS.

Trust calculation agent (TCaA): This agent uses corresponding rules to calculate the trust value of its adjacent CHs and SNs in its cluster according to the trust properties received from the CCA.

Intrusion judgment agent (IJA): This agent makes the intrusion judgment according to the TCaA calculation value of the SNs in its cluster.

Intrusion response agent (IRA): This agent takes actions on the nodes corresponding to the judgment of the IJA, such as cutting off their communications, updating their communication keys, and performing new authentications.

Cluster management agent (CMA): This agent monitors and coordinates the other agents.

2.3.2. Multi-agent model of SN

In order to reduce the network overhead, in this paper, the multi-agent model of SN performs the functions of trust collection and communication. The structure of the SNs, which consists of the trust collecting, communication, and management agents, is shown in Fig. 3.

SN trust collection agent (STCA): The function of this agent is to collect the *TF* of the SN itself.

SN communication agent (SCA): This agent is responsible for sending the *TF* from the STCA to the CHs.

SN management agent (SMA): This agent mainly performs management and coordination with both the STCA and the SCA.

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

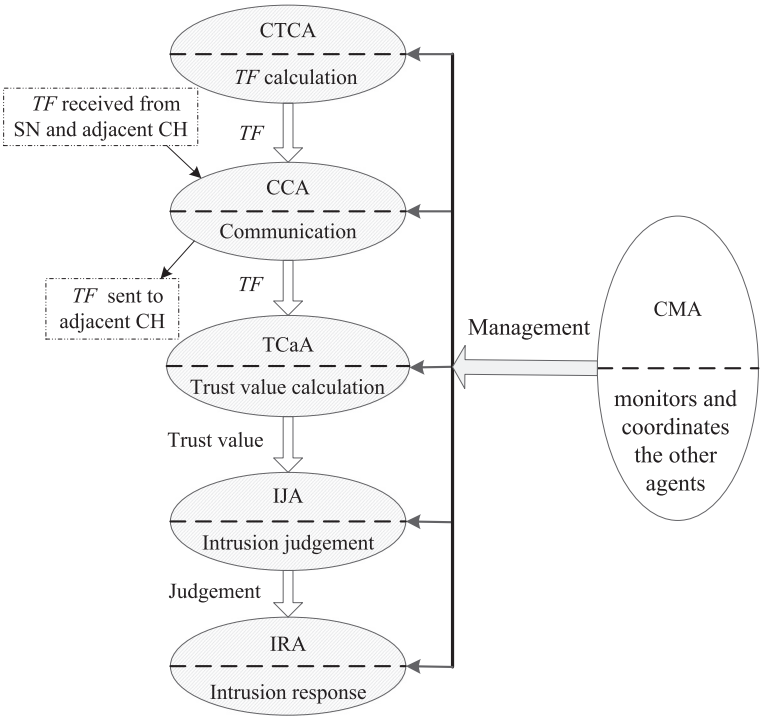

Fig. 2. Multi-agent model of cluster header.

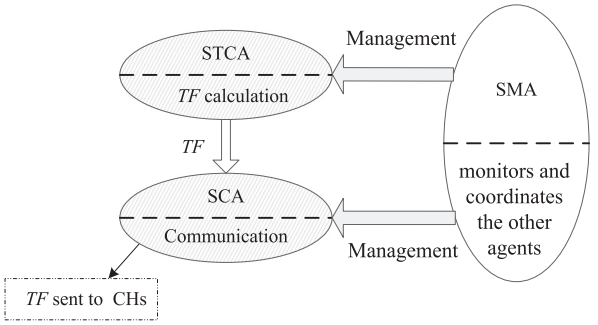

Fig. 3. Multi-agent model of SN.

3. Implementation of intrusion detection scheme

3.1. Basic theory

3.1.1. Trust value calculation based Beta distribution

Trust management distributions such as binomial distributions and the Beta, Poisson, and Gaussian distributions can be used to describe the reputation distribution of a node. The Beta distribution is characterized by its simplicity, flexibility, and strong theoretical statistical basis [21]. Thus, it is suitable for building a trust system for resource-constrained WSNs. This distribution can be expressed by beta(α, β), and the probability density function of the Beta distribution is as follows:

$$f(x|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}(1-x)^{\beta-1} \tag{5}$$

where α and β represent the ratings of the cooperation and non-cooperation of an event, respectively. The Beta distribution satisfies $0 \le x \le 1$, $0 \le \alpha$, and $0 \le \beta$, and states that if $\alpha < 1$, then $x \ne 0$, and if $\beta < 1$, then$x \ne 1$.

The expected value of the Beta distribution can be obtained by

$$E(beta(\alpha,\beta)) = \frac{\alpha}{\alpha+\beta}. \tag{6}$$

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

The BRSN model proposed in [22] performed a fitting analysis on the Beta and reputation distributions. The researchers concluded that the Beta distribution can easily describe the reputation distribution, and that the trust value of a node is the statistical expectation of its reputation distribution. Therefore, from (6), we can obtain

$$TR = E(beta(S+1, L+1)) = \frac{S+1}{S+L+2} \tag{7}$$

where S is the number of normal behaviors and L is the number of abnormal behaviors of the node.

In this paper, the calculation of the trust value is based on concept of calculating the statistical expectation of the Beta distribution.

3.1.2. Judgment of abnormal node behaviors based on Mahalanobis distance

The Mahalanobis distance, which considers the relationships among various features, is an important tool for judging the similarities present in the multi-sample. Therefore, it is reasonable use this distance to judge the anomalies of the trust feature, and it is defined as follows [23].

$\boldsymbol{G}$ is an m-dimensional set (with m being the index) with a sample mean vector of $\boldsymbol{\mu}= (\mu_1,\mu_2,...,\mu_m)^T$ and a covariance matrix of $\boldsymbol{\Sigma}= (\sigma_{ij})$, and the Mahalanobis distance between the sample $\boldsymbol{X}= (x_1,x_2,..., x_m)^T$and the set $\boldsymbol{G}$ is

$$d(\boldsymbol{X}, \boldsymbol{G})=\sqrt{(\boldsymbol{X}-\boldsymbol{\mu})^T\sum^{-1}(\boldsymbol{X}-\boldsymbol{\mu})}. \tag{8}$$

In this scheme, we first sample every type of TF_j (with $j=1, 2, 3, 4, 5$) n_1 times on the premises of both the security network and the normal TF at the network's entrance. The set of samples denoted by $\boldsymbol{G}$ is given as follows:

$$\begin{cases} \boldsymbol{G} = \left(\boldsymbol{G}_j\right)^T & j = 1, 2, ..., 5 \\ \boldsymbol{G}_j = \left\{TF_j'(1), TF_j'(2), ..., TF_j'(n_1)\right\} \end{cases} \tag{9}$$

where TF_j' is the sample value of TF_j and j represents the type of TF. Here, $j \in [1, 5]$, while i is the sample number for each type of TF, where $i \in [1, n_1]$.

The sample average vector $\boldsymbol{\mu}$ can be calculated by

$$\begin{cases} \boldsymbol{\mu}=\left(\mu_j\right)^T & j = 1, 2, ..., 5 \\ \mu_j=\frac{1}{n_1}\sum_{i=1}^{n_1} TF_j'(i) \end{cases} . \tag{10}$$

The covariance matrix $\boldsymbol{\Sigma}$ can be calculated by combining the sample average vector $\boldsymbol{\mu}$with the TF sample. Therefore, the Mahalanobis distance between $TF_j'(i)$ and $\boldsymbol{G}$ is calculated by

$$\left(d_j^i\right)^2=d^2\left(\boldsymbol{TF}_j'(i), \boldsymbol{G}\right)=\left(\boldsymbol{TF}_j'(i)-\boldsymbol{\mu}\right)^T\boldsymbol{\Sigma}^{-1}\left(\boldsymbol{TF}_j'(i)-\boldsymbol{\mu}\right) \tag{11}$$

where d_j^i is the Mahalanobis distance between $\boldsymbol{TF}_j'(i)$ and $\boldsymbol{G}$.

As a result, we can calculate all of the Mahalanobis distances for each TF by executing Eq. (11), and the maximum Mahalanobis distance can be denoted as $d^M= \max\{d_j^i | j = 1, 2, ..., 5; i = 1, 2, ..., n_1\}$.

The calculation above is performed offline with the aid of auxiliary equipment because of the limited computing resources available in WSNs. In addition, the parameters used for calculating the Mahalanobis distances are saved in the CHs to be used under normal WSN operation. Under normal WSN operation, the CHs acquire the $\boldsymbol{TF}_j$ of the SNs in their clusters as well as from adjacent CHs during every time period Δt. If the Mahalanobis distance between $\boldsymbol{TF}_j$ and $\boldsymbol{G}$ is less than d^M, then the node's number of normal behaviors increases by one while its number of abnormal behaviors decreases by one.

However, under normal WSN operation, the variations in the value of $\boldsymbol{TF}_j$ **c**an be affected by many unpredictable factors, including both invasive and non-invasive factors (i.e., environmental factors). As a result, if no measurements are taken, the false positive rate increases and affects the performance of the system. Hence, it is of great significance to learn how to reduce the occurrence of such situations. This paper introduces a tolerance factor, q, and utilizes it in the trust value calculation. Specifically, the number of abnormal behaviors used in the trust calculations is obtained by dividing the actual number of abnormal behaviors by the tolerance factor q, and this actual number is obtained via the Mahalanobis distance judgment. However, when the value of q is too large, it decreases the intrusion detection rate. Thus, in practical implementation, dynamic adjustment is performed according to the actual security situation of the network.

3.2. SN intrusion detection

We denote a particular CH as c, and node n is the SN in the same cluster as c, so the intrusion detection of node n can be realized by c as follows.

Step 1: The STCA of node n collects its own TF_j as TF_j^n, which is sent to c through the SCA of node n.

Step 2: The CCA of c receives TF_j^n, and the TCaA of c is activated by the CMA of c to calculate the trust value of node n.

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

Step 3: The TCaA of c calculates the trust value of node n as follows:

$$TR_{cn}(t) = \frac{S_n(t) + 1}{S_n(t) + L_n(t)/q + 2} \tag{12}$$

where $S_n(t)$ is the number of normal behaviors of node n at time t, $L_n(t)$ is the number of abnormal behavior of node n at time t, and q is the tolerance factor. $S_n(t)$ and $L_n(t)$ can be calculated by accumulating the numbers of normal and abnormal behaviors of node n, respectively, using the Mahalanobis distance in the abovementioned way.

Step 4: The IJA of c judges whether or not node n has been intruded on according to the trust value of node n as calculated in Step 3. If $TR_{cn} < TR_{th1}$, node n was intruded on. Otherwise, node n is credible. TR_{th1} is the threshold trust value selected according to both its practical application as well as the trust value of all of the SNs.

Step 5: If node n is judged a malicious node in Step 4, then the IRA of c adopts security measures, such as updating the communication key, performing re-authentication, and cutting off communications with node n.

Step 6: The CMA of c broadcasts the identity of node n to other nodes in the cluster and reports c's handle information to the BS through c's CCA.

3.3. CH intrusion detection

In the scheme introduced in this paper, CH intrusion detection is implemented by the BS. We denote the BS as b, the CH to be detected as c, and the CH adjacent to c as k. Thus, the intrusion detection of c can be realized by b as follows:

Step 1: The CTCA of c collects its own TF as TF_j^c, which is sent to k by the CCA of c.

Step 2: The CCA of k receives TF_j^c, and the TCaA of k is activated by the CMA of k to calculate the trust value of c.

Step 3: The TCaA of k calculates the trust value of c with an equation similar to (12), and this value is denoted as TR_{kc}. Consequently, b calculates the trust value of c by:

$$TR_{bc}(t) = avg\{TR_{kc}(t)\} \tag{13}$$

where $TR_{bc}(t)$ is the trust value of c calculated by b at time t, which is an average value, and $TR_{kc}(t)$ is the trust value of c calculated by k (only when k is credible) at time t.

Step 4: The intrusion judgment evidence b provides to c is mainly composed of two aspects. On the one hand, the trust value $TR_{bc}(t)$ is compared with the threshold trust value, which is the minimal trust value of all of the CHs. On the other hand, the proportion of SNs judged malicious by c to the total number of SNs in its cluster is compared with another threshold value related to the proportion of malicious SNs. Therefore, the intrusion judgment of c can be realized by the following logical expression:

$$\Pi = (TR_{bc}(t) < TR_{th2}) \left| \left(N_c^{mali} > N_{th}\right)\right. \tag{14}$$

where TR_{th2} is the threshold trust value, which is the minimal trust value of all of the CHs, N_c^{mali} is the proportion SNs judged malicious by c to the total number of SNs in its cluster, and N_{th} is the maximum proportion of malicious nodes within a cluster. If Π is 1, then c is abnormal. Otherwise, c is normal.

Step 5: If c was judged abnormal in Step 4, then b cuts off communications with c, recovers the SNs that were judged malicious by c, and broadcasts the identity of c to all of the other nodes.

4. Simulation and analysis

4.1. Analysis of trust value calculation algorithm realization

Trust value calculation is the fundamental concept of the scheme, and whether it can be realized reliably or not is crucial to the successful functioning of the algorithm. A node's physical and MAC layer features can easily be locally obtained. In this paper, TF_1–TF_4 could be calculated with the results of the two layers. TF_5 was easily obtained through sensor measurement and, hence, the trust feature values were attained easily. Furthermore, all of the trust information was obtained directly from both the SNs and the nearby CHs. Therefore, no Bad-mouth attack existed, resulting in a more reliable trust value calculation.

The Mahalanobis distance was used to judge whether the trust features were normal or not, which also resulted in more reliable trust value calculation. As for the trust value calculation for resource-constrained WSNs, the Beta distribution was deemed suitable for the task due to its simplicity as well as its advanced and reliable implementation.

4.2. Reliability and scalability analysis

Our scheme adopted multiple trust features to calculate the trust value and, more significantly, introduced the physical state of the trust feature. The intrusion behavior features covered a comprehensive range, enabling both more intrusion to be detected and a higher reliability of detection.

The framework of the intrusion detection scheme was designed based on multi-agent functioning, and all of the agents' configurations were determined by the intrusion detection functions of each node. Each agent was an autonomously running program entity, which made the system easy to configure dynamically, improving its scalability.

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

Table 2
Simulation parameter settings.

Parameter	Default value
Network deployment area	300 m × 300 m
Number of nodes	100
Communication speed (Kbps)	250
MAC layer protocol	IEEE 802.15.4
Routing protocol	LEACH
Detection time interval ($\Delta t/s$)	60
Data packet length (B)	128
Transmission power (mW)	1
Tolerance factor q	3

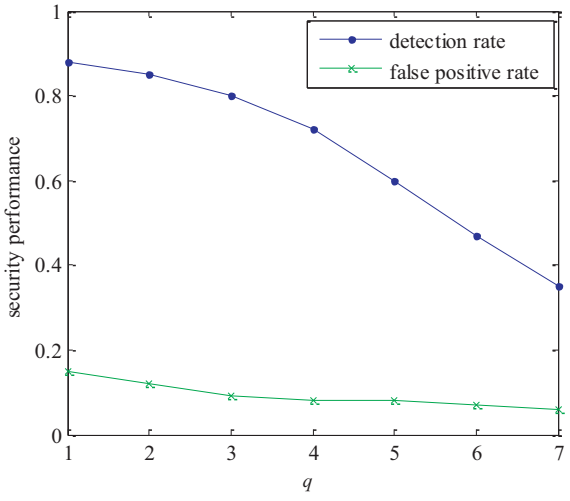

Fig. 4. Simulation of effects of tolerance factor q on security performance.

4.3. Simulation

This paper adopted OMNeT++ 4.3.1 as simulation software. The MAC layer protocol used was IEEE802.15.4, and the routing protocol used was LEACH [24]. For this simulation, the threshold trust value TR_{th1} was 0.8, TR_{th2} was 0.6, and $N_{th}$was 0.5. The other simulation parameters are shown in Table 2.

The performance of the scheme was analyzed via two indicators: the detection and false positive rates obtained from the simulation results. The detection rate is the number of nodes detected as malicious nodes compared to the total number of malicious nodes in a network. The false positive rate is the proportion of the number of nodes that are mistakenly identified as malicious nodes to the total number of nodes detected.

4.3.1. Tolerance factor selection

In this simulation, 20 nodes were selected randomly, and the tolerance factor q was selected from the set {1, 3, 5, 7}. Each q value ran 10 times in independent simulations, and the average detection and false positive rates were extracted. The simulation results are shown in Fig. 4.

As shown in Fig. 4, as q increases, the detection and false positive rates decrease. However, the detection rate decreases faster than the false positive rate does. An excellent detection performance produces both a high detection rate and a low false positive rate. The simulation results indicate that the best performance is achieved when q is 3, because the detection rate is high and the false positive rate is low.

4.3.2. Security performance analysis

The simulation included two situations: (a) the presence of a single flooding attack, and (b) the presence of three different kinds of attack: a selective forwarding attack, a DoS attack, and a flooding attack. A certain type of attack node was randomly chosen during each simulation, and the number of nodes for each simulation was selected from the set {1, 3, 6, 10, 15, 20}. Each number of nodes ran 10 times in independent simulations, and the average value of detection and false positive rates was extracted. The simulation results were compared with the scheme used in [5] that was based on a single network feature: energy consumption. The simulation results are shown in Figs. 5 and 6.

Fig. 5 compares the false positive rate of our scheme with that of the single feature scheme based on two situations. The simulation results indicate that the false positive rates of the two schemes increased as the numbers of attack nodes

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

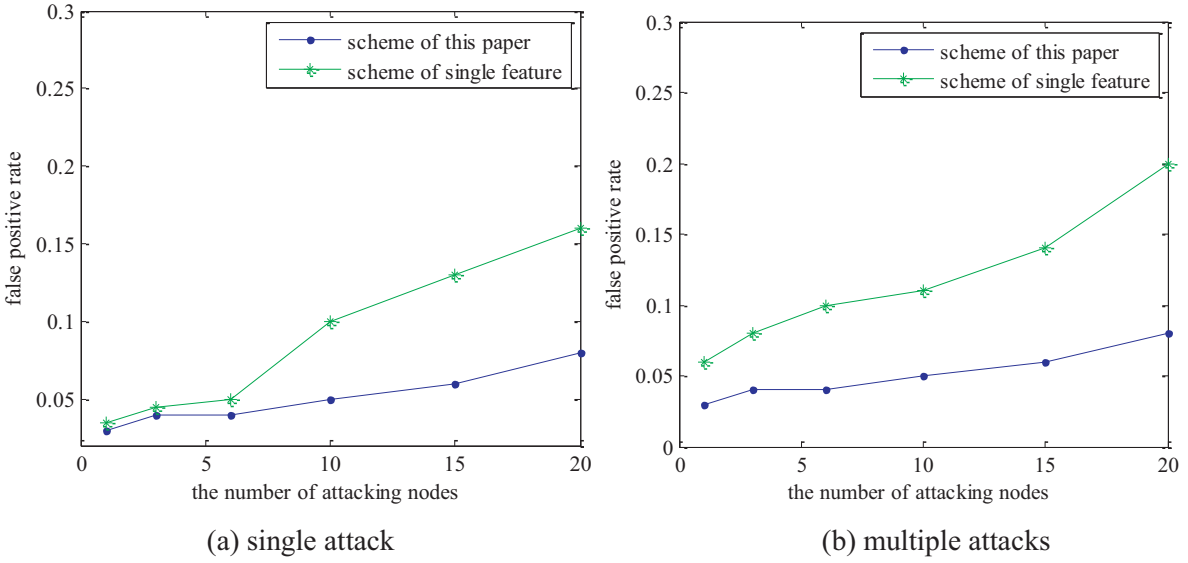

Fig. 5. Comparison of simulated false positive rates.

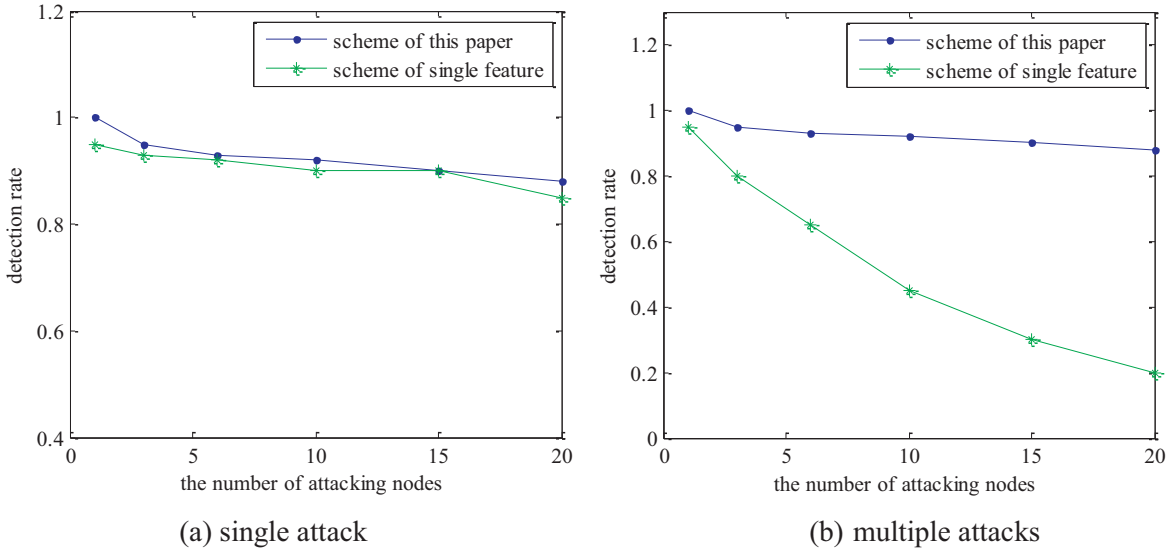

Fig. 6. Comparison of simulated detection rates.

increased. The false positive rates of both schemes were low. However, our scheme employed a tolerance factor, q, and some of the abnormal trust features produced by non-invasive factors were excluded, greatly reducing the false positive rate. As shown in Fig. 5, the false positive rate of our scheme increased more slowly than that of the single feature scheme, and our scheme produced a better performance.

In Fig. 6, the detection rate of our scheme is compared with that of the single feature scheme. The detection rates of both schemes decreased as the numbers of attacks nodes increased. The difference between the detection rates of the two schemes was low in situation (a) but high in situation (b). This was because the intrusion detection mechanism utilized by the scheme in [5] was based on a single network feature. The detection mechanism failed to detect some attacks, which caused the detection rate to decline more rapidly in situation (b).

Figs. 5 and 6 indicate that the detection rate is influenced by detection failures and that the false positive rate can be greatly reduced by the scheme proposed in this paper. The scheme can achieve both a high detection rate and a low false positive rate with adjustments of its q value.

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

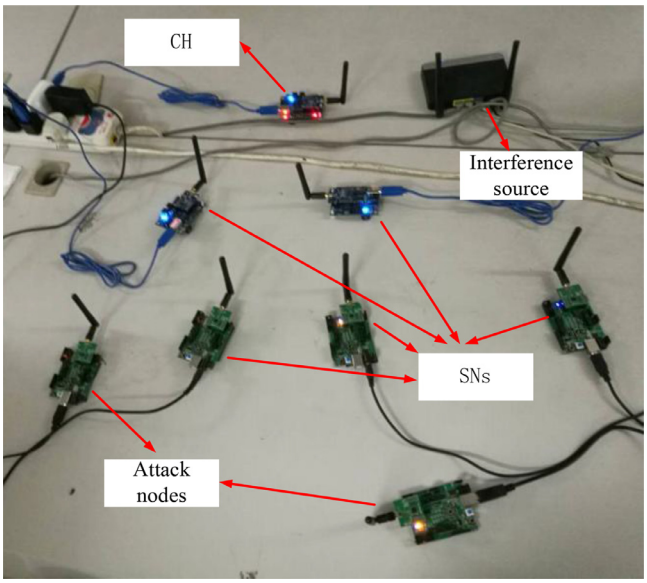

Fig. 7. Experimental platform.

Table 3
The detection rate and false positive rate according to experiment.

	Interference absent	Interference present
Detection rate (%)	98.6	97.5
False positive rate (%)	3.13	5.04

5. Experiment

In order to verify the feasibility of implementing the proposed intrusion detection scheme in both embedded platforms and real environments, we constructed the experimental platform shown in Fig. 7. The network consisted of eight ZigBee nodes, including: (1) one CH, (2) five SNs, (3) two attack nodes (one simulating DoS attacks and one simulating sinkhole attacks), and (4) one wireless router (used as an interference source).

The SNs periodically transmitted data for 5 seconds. The CH stored the received data and calculated the node trust values. One of the two attack nodes acted as a DoS attack node, and the other acted as a sinkhole attack node. The DoS attack node performed uninterrupted transmission, and of the sinkhole attack node enticed other nodes to send it data, which it discarded.

The experiment was performed for two cases: the presence of interference and the absence of interference. The interference source was 2.4-GHz wireless router. The two cases were simulated 100 times each, the results of each simulation were recorded, and the average detection and false positive rates were obtained for each case, as shown in Table 3.

Table 3 shows that the detection and false positive rates are similar to those in the simulation results, which confirms that the proposed intrusion detection scheme is practically achievable and has a high detection performance.

6. Conclusion

In this paper, we proposed an intrusion detection scheme based on both multi-agent functioning and trust values for layer-cluster WSNs. The characteristics of the scheme are as follows:

(1) The node trust feature abnormalities are judged by the Mahalanobis distance, which makes the judgment more accurate and improves the accuracy of the trust value.
(2) A tolerance factor q that reduces the false positive rate of the scheme was introduced in the trust value calculation. The dynamic adjustment of q corresponding to the environment's security situation can improve the system's flexibility.
(3) The scheme was implemented based on a multi-agent framework that enhances the system's scalability and improves its fault tolerance.

The simulation results showed that the modified scheme demonstrated both a higher detection rate and a lower false positive rate for both a single attack and a variety of attacks occurring at the same time. This confirms that it can detect common intrusions accurately. In future studies, the scheme will be improved through the implementation of an evaluation

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013

strategy for the tolerance factor q, an assessment of the trust threshold value's boundary behavior, and further reduction of detection failure.

Acknowledgments

This research study was funded by Fundamental Research Funds for the Central Universities of China (HIT.NSRIF.2015017) and the National Natural Science Foundation of China (51077015, 50907014).

References

[1] Sedjelmaci H, Senouci SM. Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks. In: *Proc. of IEEE conf. on global information infrastructure symposium, october 28–31*; 2013. p. 1–6.
[2] Bao F, Chen R, Chang MJ, Cho JH. Trust-based intrusion detection in wireless sensor networks. In: Proc. of IEEE conf. on communications june 5–9; 2011. p. 1–6.
[3] Jennings NR. Commitments and conventions: the foundation of coordination in multi-agent systems. Knowl Eng Rev 1993;8(3):223–50.
[4] Thamilarasu G, Ma Z. Autonomous mobile agent based intrusion detection framework in wireless body area networks. In: Proc. of 16th international symposium on world of wireless, mobile and multimedia networks, june 14–17; 2015. p. 1–3.
[5] Riecker M, Biedermann S, Hollick M. Lightweight energy consumption-based intrusion detection system for wireless sensor networks. Int J Inf Secur 2015;14(2):155–67.
[6] Wang H, Yuan Z, Wang C. Intrusion detection for wireless sensor networks based on multi-agent and refined clustering. In: Proc. of WRI international conference on communications and mobile computing, january 6–8; 2009. p. 450–4.
[7] Wang P, Zhou XW, Qin BP, Zhao P, Zheng LC. Multi-agent based intrusion detection system for wireless sensor networks. Chin J Sensors Actuators 2007;20(3):677–81.
[8] Vinyals M, Rodriguez-Aguilar JA, Cerquides J. A survey on sensor networks from a multi-agent perspective. Comput J 2010;1:455–70.
[9] Han GJ, Jiang JF, Shu L, Niu JW, Chao HC. Management and applications of trust in wireless sensor networks: a survey. J Compu Syst Sci 2014;80(3):602–17.
[10] Liu C, Liu Y, Zhang Z. Improved reliable trust-based and energy-efficient data aggregation for wireless sensor networks. Int J Distrib Sensor Netw 2013;2013:1–11.
[11] Gupta GP, Misra M, Garg K. Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks. J Netw Comput Appl 2014;41:300–11.
[12] Zahariadis T, Trakadas P, Leligou HC, Maniatis S, Karkazis P. A novel trust-aware geographical routing scheme for wireless sensor networks. Wireless Pers Commun 2013;69(2):805–26.
[13] Zhang Y, Jin Z, Luo Y, Xiujuan DU. Node secure localization algorithm in underwater sensor network based on trust mechanism. J Comput Appl 2013;33(5):1208–11.
[14] Zhang T, He J, Zhang Y. Trust based secure localization in wireless sensor networks. In: Proc. of 2nd international symposium on intelligence information processing and trusted computing, oct. 22–23; 2011. p. 55–8.
[15] Ebinger P, Bibmeyer N. TEREC: trust evaluation and reputation exchange for cooperative intrusion detection in MANETs. In: *Proc. of 7th annual comm. networks and services research, may 11–13*; 2009. p. 378–85.
[16] Gerrigagoitia K, Uribeetxeberria R, Zurutuza U, Arenaza I. Reputation-based intrusion detection system for wireless sensor networks. In: *Proc. of IEEE Conf. on Complexity in Engineering,* june 11–13; 2012. p. 1–5.
[17] Bao F, Chen R, Chang MJ, Cho JH. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans Netw Serv Manage 2012;9(2):169–83.
[18] Chang KD, Chen JL. A survey of trust management in WSNs, internet of things and future internet. KSII Trans Internet Inf Syst 2012;5(1):5–23.
[19] Lopez J, Roman R, Agudo I, Fernandez-Gago C. Trust management system for wireless sensor networks: best practices. Comput Commun 2010;33(9):1086–93.
[20] Huabo L, Jianming C, Hongjun D. Multivariate classification-based malicious node detection for wireless sensor network. Chin J Sensors Actuators 2011;24(5):771–7.
[21] Jsang A, Ismail R. The beta reputation system. In: Proc. of the 15th bled electronic commerce conference, june; 2002. p. 41–55.
[22] Ganeriwal S, Balzano LK, Srivastava MB. Reputation-based framework for high integrity sensor networks. ACM Trans Sensor Netw 2008;4(3):66–77.
[23] De Maesschalck R, Jouan-Rimbaud D, Massart DL. The Mahalanobis distance. Chemom Intell Lab Syst 2000;50(1):1–18.
[24] Heinzelman WB, Chandrakasan AP, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks. IEEE Trans Wireless Commun 2002;1(2):660–70.

Xianji Jin is currently working as an assistant professor at the Harbin Institute of Technology, China. He received his Ph.D. in Electrical Engineering from the Harbin Institute of Technology in 2013. His research interests include power system information and communications technology, wireless network security, and intrusion detection.

Jianquan Liang is currently working as a research fellow at Heilongjiang Electric Power Research Institute. He received his Ph.D. in Electrical Engineering from the Harbin Institute of Technology in 2016. His research interests include wireless sensor network security, key management, and intrusion detection.

Weiming Tong is currently a professor at the Harbin Institute of Technology. He got his PhD. title from the Harbin Institute of Technology, China, in 1999. His research interests include electrical intelligent technology, distribution and substation automation, and wireless network security. He has published more than 200 peer reviewed research papers.

Lei Lu is currently a Ph.D. candidate at the Harbin Institute of Technology in China. He obtained his M.S. in electrical engineering at the same university in 2009. His main research interest is power system information security.

Li Zhongwei is currently working as an associate professor at the Harbin Institute of Technology, China. He received his Ph.D. in Electrical Engineering from the Harbin Institute of Technology in 2006. His research interests include smart grid communications, information security, and intelligent power management.

Please cite this article as: X. Jin et al., Multi-agent trust-based intrusion detection scheme for wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.013