TIDS: Trust Intrusion Detection System Based on Double Cluster Heads for WSNs

Na Dang[1], Xiaowu Liu[1(✉)], Jiguo Yu[2], and Xiaowei Zhang[1]

[1] School of Information Science and Engineering, Qufu Normal University, Rizhao, China
ycmlxw@l26.com
[2] Shandong Computer Science Center (National Supercomputer Center), Jinan, China

Abstract. The efficiency and reliability are crucial indexes when a trust system is applied into Wireless Sensor Networks (WSNs). In this paper, an efficient and reliable Trusted Intrusion Detection System (TIDS) with double cluster heads for WSNs is proposed. Firstly, an intrusion detection scheme based on trust is discussed. The monitoring nodes are responsible for evaluating the credibility of Cluster Member (CM) instead of depending on the feedback between CMs, which is suitable for decreasing the energy consumption of WSNs and reducing the influence of malicious nodes. Secondly, a new trust evaluation method is defined in TIDS and it takes the data forwarding and communication tasks into consideration which may enhance the reliability of Cluster Head (CH). The theoretical and simulation results show that our solution can effectively reduce the system overhead and improve the robustness of WSNs.

Keywords: Wireless Sensor Network · Trust system · Data Aggregation

1 Introduction

The development of micro-chip and short distance communication technique makes WSNs develop in an amazing manner. WSNs are widely deployed in the fields of environmental monitoring, health care and space exploration. Due to the limitation of resource and unattended deploying manner, WSNs are faced with more serious security challenges than the cable networks. Traditional security techniques such as encryption and authentication can protect WSNs from being eavesdropped or tampered. However, these techniques are difficult to be implemented in each node because of the performance limitation of sensors. Therefore, it is necessary to exploit new attack detection and defense techniques for WSNs.

As an active defense technique, intrusion detection can not only identify potential attacks, but also take corresponding protection measures for monitored network [1]. Meanwhile, it provides relevant data records which may be used as the data source to trace the behavior of malicious activity. Because of the limited transmission range of the sensor node, it is almost impossible to directly transmit each sensing data of each node to the Base Station (BS) in a large-scale WSN. Generally speaking, there may be data redundancy between neighbor nodes which cause the unnecessary communication

E. S. Biagioni et al. (Eds.): WASA 2019, LNCS 11604, pp. 67–83, 2019.
https://doi.org/10.1007/978-3-030-23597-0_6

overhead. To solve this problem, the Data Aggregation (DA) is a favorable choice [2]. Although there are a several studies which combined DA with the intrusion detection, the energy efficiency and data precision are important issues in large-scale WSNs. In this paper, we propose a Trusted Intrusion Detection System (TIDS) used in cluster-based WSNs in order to evaluate the reliability of the node and isolate the malicious node from the network.

The remainder of this paper is organized as follows: Sect. 2 describes an overview of related work. Section 3 discusses our network model and some assumptions. The efficient and reliable trust system is analyzed in Sect. 4. Section 5 provides the theoretical and simulation evaluation of TIDS. Section 6 concludes this paper.

2 Related Work

2.1 Clustering Algorithms for WSNs

The sensor node can directly communicate with the BS or interact with each other through relay nodes. The larger the sensor network is, the greater the energy consumes. Therefore, nodes far away from the BS will exhaust their energy at a faster speed than the nearer ones. Faced with this problem, the clustering mechanisms such as LCA [3], LEACH [4], GS^3 [5] and EC [6] were proposed to improve the network scalability and throughput. The nodes in a WSN are divided into different groups and the node with more energy is elected as a CH in a cluster and all CHs of different clusters form a higher-level backbone network. Clustering is an important management strategy which has the ability to facilitate DA technique in a WSN. A double CH model is different from the traditional model, where two cluster heads are selected. Each CH performs DA and its results are sent to BS individually [7]. The BS computes the similarity of two results. If the similarity coefficient does not exceed the pre-defined threshold, the two CHs are added to the blacklist. Meanwhile, the feedback is transmitted from the BS to the trust system which can be used to identify and isolate the compromised sensor nodes in time.

The cluster topology is convenient for creating a trust system locally and carries out DA in a WSN. Furthermore, it simplifies the communication and effectively prolongs the lifetime of network. In addition, a trust system can be applied into the cluster topology easier than other topologies such as tree and ring.

2.2 Trust System for WSNs

The trust system is a favorite scheme which provides a mechanism to monitor the security state of network. For example, it is capable of detecting errors or malicious nodes in a cluster [8]. Many studies have been proposed to discuss the trust systems for WSNs [9–11]. However, these systems suffer from various limitations and consume the overwhelming resources, especially in a large-scale WSN.

Recently, a few trust management systems have been addressed for clustering WSNs. A novel lightweight Group based Trust Management Scheme (GTMS) for clustered WSNs was proposed [12] which divided the trust values into three levels:

sensor node level, CH level and BS level. The innovation of the GTMS was that it evaluated the trust of network from different viewpoints instead of a single trust value. Reliable Data Aggregation and Transmission protocol (RDAT) introduced different functions to compute the reputation and trust values for different activities including sensing, aggregation and routing [13]. The trustworthiness of node is a comprehensive one which depends on the trust of sensing, aggregation and routing protocol.

Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for WSNs (iRTEDA) took the remaining energy and link availability into consideration and prevented the routing path from being overused [14]. Therefore, it ensured that the routing path selected by the trust system was reliable. In addition, watchdog mechanism was employed in many trust systems to monitor the communication behaviors of nodes [7].

2.3 Attack and SDA in WSN

An attacker in a WSN may be an internal node, an external node or both. If the nodes of WSN are equipped with the encryption-based authentication and authorization mechanisms, the external attacks are limited to physical disruption or interference with the communication channel [15]. Internal attacker can initiate various malicious activities such as tampering, eavesdropping and dropping. Among them, packet dropping may have a drastic effect on network performance without being blocked by authentication and authorization [16, 17]. Three typical dropping attacks are described as follows.

- Blackhole Attack. It deserts all received packets and causes the most serious damage to the network. However, it can be easily captured for its activity is rather obvious compared with the normal activity.
- On-Off Attack. When the attack is on, it drops all received packets; when the attack is off, all the received packets are forwarded.
- Selective Forwarding Attack. Different from above mentioned attacks, the selective forwarding attack deserts packet randomly. It may hide the malicious behaviors in normal activities and a sophisticated detection mechanism is indispensable [18].

Recently, several protocols have been proposed for Secure Data Aggregation (SDA) in order to deal with the internal attacks in WSNs. Kefayati discussed a Blind Information Fusion Framework (BIFF) for SDA [19]. The data are transformed from normal space to anonymous space and cannot be deduced after they were fused. A new probabilistic grouping technique, Secure hop-by-hop Data Aggregation Protocol (SDAP), was described which divided the nodes in a tree topology into logical groups (sub trees) of similar size [20]. The commit-and-attest scheme was discussed where the aggregation result could be verified at BS. In addition, trust assessment systems were widely adopted in many protocols including GTMS [12], RDAT [13], Irteda [14] and DCHM [7], which can ensure the security of DA. Therefore, a SDA scheme is proposed in this paper so as to enhance the security of TIDS.

3 Network Model

We develop a trust-based framework for double-CHs-based WSN and design a mechanism to reduce the probability of a malicious node being selected as aggregation node. The nodes in a clustering WSN can be identified as CH and Cluster Member (CM) as shown in Fig. 1.

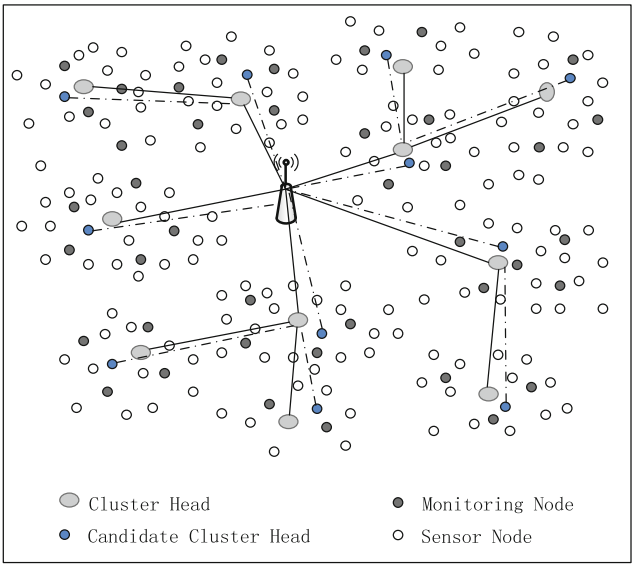

Fig. 1. Network model.

The following assumptions are adopted in our scheme. There are three types of nodes: CM, Monitoring Nodes (MN) and Aggregation Nodes (AN or CH) in a WSN. In addition, we identify a node by a triple $\langle ID, T, S \rangle$ where ID, T and S represent the node identify, the node type and the node subtype, respectively. T defines which type of node is required, such as CM, CH or MN. To prevent trust values from being forged during the transformation from one node to another, a secure communication channel can be established through deploying a key management scheme such as random key distribution mechanism [21].

All nodes are trustworthy in the initial stage and BS is secure with unlimited energy supply. This paper focuses on the selective forwarding which aims to reduce the performance of the network in terms of packet loss rate and prevent the data from being transformed to BS [18]. We propose an intrusion detection mechanism based on Beta model to detect the abnormal behaviors of nodes. The trust value of CM is evaluated by its CHs and MNs when a WSN suffered from an attack. Therefore, each CM does not need to maintain the trust table or communicate with other CMs, which reduces the communication overhead and eliminates the possibility of being attacked by a compromised CM.

4 Trusted Intrusion Detection System with Double CHs for WSNs

The proposed trust intrusion detection system consists of three parts: cluster component, CH component and BS component, as shown in Fig. 2. The main tasks of cluster component are to select CHs, form clusters, monitor the CMs and update the trust system. CH component is in charge of detecting outliers, aggregating data, uploading the aggregation results and trust tables to BS. Two CHs in a cluster execute these operations synchronously with the aim of guaranteeing the reliability of CMs in a cluster and send two aggregation results to BS. According to these aggregation results, BS determines whether the CHs are credible or not.

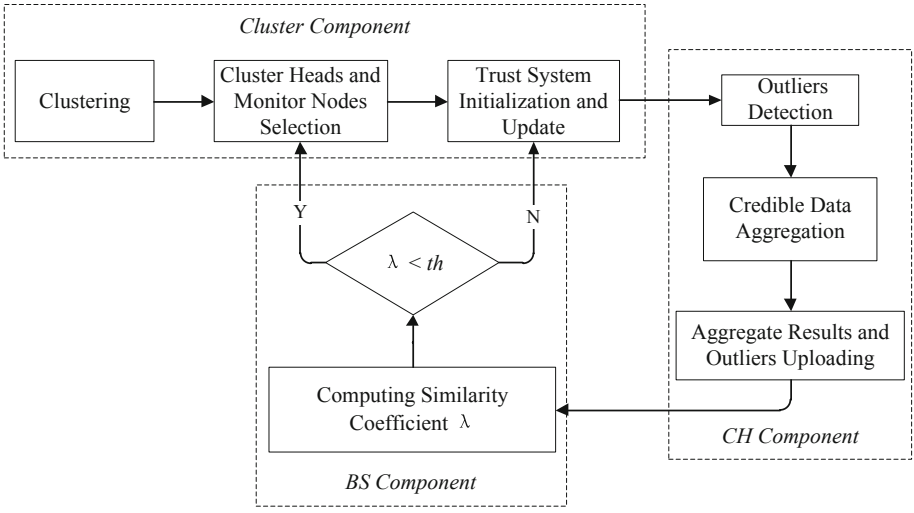

Fig. 2. Overview of the functions of the framework.

4.1 CH Election and Clustering

In the initial phase, sensor nodes are divided into several clusters by improving the clustering algorithm described in DCHM [7]. Different from DCHM, MNs are selected as well when the CHs are selected in our model. MNs need to monitor the behaviors of CMs and maintain a trust table of nodes in a cluster.

The CH and MN selections are two critical parts in the cluster formation. Two indexes are deduced in our model in Eq. (1). The relative residual energy, E_{ri}, can be calculated as

$$E_{ri} = \frac{E_i}{E_{max}} \tag{1}$$

where E_i and E_{max} are the residual energy and the maximum initial energy of node i, respectively. The greater the relative density of node i is, the higher the correlations between i and its neighbors are.

The relative density, Dn_{ri}, can be obtained by Eq. (2).

$$Dn_{ri} = \frac{Dn_i}{Dn_{max}} \tag{2}$$

where the density of node i is expressed as Dn_i. Dn_{max} refers to the largest density in a network. If the distance between them is not up to the predefined threshold d_0, the two nodes are spatially related.

The density of nodes indicates the number of neighbor nodes within the communication radius d_0. Dn_{ri} is regarded as a principle to optimize the CH selection. The choice of CH does not depend on one index and it is a comprehensive one as shown in Eq. (3).

$$F_i = \alpha_1 \times E_{ri} + \alpha_2 \times Dn_{ri} \tag{3}$$

where α_1 and α_2 represent the weight of E_{ri} and Dn_{ri}. The value of weight depends on the application scenario. In this paper, we take E_{ri} as the main factor in the calculation of F_i ($\alpha_1 > \alpha_2$).

In this way, the node with more energy and density has higher probability to be chosen as a CH. As a result, the CHs can afford more extra workload compared with CMs. In addition, the energy consumption of sensors follows the model as depicted in Eq. (4).

$$E_{TX}(l,d) = E_{TX\_elec}(l) + E_{TX\_amp}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2, d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4, d \geq d_0 \end{cases} \tag{4}$$

where l denotes the number of transmitted bits; d is the transmission distance; E_{elec} indicates the energy required for signal processing; ε_{fs} and ε_{mp} are the energy consumed by the amplifier to transmit data at the shorter distance and the longer distance respectively. Three types of nodes (CH, MN and CM) are deployed in a cluster and these nodes should be initialized before trust system is applied. We choose MNs and CMs according to the following functions.

$$N_{MN} = p \times N_{total}, p \in \left[\frac{1}{4}, \frac{1}{3}\right] \tag{5}$$

$$N_{CM} = N_{total} - p \times N_{total} - 1 = (1-p)N_{total} - 1 \tag{6}$$

where N_{total} represents the total number of nodes in a cluster, N_{MN} and N_{CM} represent the number of MNs and CMs. Parameter p is the proportion of MNs in a cluster and it is between $\frac{1}{4}$ and $\frac{1}{3}$, which has been proved in [22]. It is indispensable that CHs need to be reselected in the following cases. (i) The energy of CH is lower than the threshold E_{th}. (ii) The CH is detected in an abnormal state. If one or both situations occur, the

reselection message is triggered by BS. MCH (Main Cluster Head) keeps in work constantly and CCH (Candidate Cluster Head) sleep and forwards packets periodically. We illustrate the CH selection in Algorithm 1 according to the above-mentioned mechanisms.

Algorithm 1. Cluster Head Selection Algorithm.

Input: Density and energy of node, the energy and trust thresholdE_{th}, Θ_T
Output: CHs and MNs

1. **Begin**
2. **If** $E_i \leq E_{th}$ or the Trust value of CH$\leq \Theta_T$ **then**
3. Broadcast a reelection message;
4. Calculate F_i and trust value of CMs according to Equation (3) and (10) in Section 4.3.2;
5. **If** equality **then**
6. Select two candidates and MNs according to equation (5);
7. **Else**
8. Choose the first and second candidates as MCH and CCH according to F_i;
9. Select MNs in a descending order;
10. **End**
11. Send confirm message to the candidates to ensure that the candidates have enough energy;
12. **If** energy enough **then**
13. Select the candidates as the new CH;
14. **Else**
15. Repeat line 4 to line 10;
16. **End IF**
17. **End IF**
18. **End**

4.2 Trust System Initialization

In the initialization stage of trust system, an aggregation tree is needed so that CHs can transmit the aggregation data to BS hop-by-hop. Therefore, it is necessary to build an aggregation tree rooted at BS for organizing sensor nodes in a network. We adopt the algorithm described in [23] to form an aggregation tree and the message is transmitted along the tree from the leaves to root. The initialization of the trust system is consistent with the traditional trust system, such as GTMS, RDAT in [13, 14].

If the original CH is trusted, BS will send the outlier table T_{BS} to all the CHs in the network. Each CH receives the table, T_{BS} as shown in Table 1, and CH shares this table with MNs in the same cluster. Each MN compares its own trust table T_{MN} with T_{BS}. The trust values are updated if T_{BS} and T_{MN} have different items. On the contrary, the update will be ignored. If the original CH is not trusted, the trust value of CH is initialized to zero.

4.3 Trust Intrusion Detection System

As discussed in Sect. 2.3, the internal attack is a serious problem in a WSN and TIDS should decrease the impact of attacks as soon as possible. TIDS detects internal attacks through the following steps.

4.3.1 Monitoring Mechanism

The MN listens to the activities of CH and CM. The monitoring mechanism operates in a way similar to that of watchdog. Each MN monitors the forwarding activity of CHs. A "good" behavior of CH will be recorded if a packet is forwarded; otherwise, a "bad" behavior of CH will be counted. According to the behaviors of CHs, MN store the different numbers of activities in the trust table T_{MN}. MNs also compute trust value of CMs according to the behaviors of CMs. MN only needs to listen to the channel and maintain the trust table, which consumes less energy than data transmission.

Table 1. Trust table in BS (T_{BS}).

Cluster	Node ID	Trust value	Outlier	Bad behavior	Good behavior
Cluster1	MCH_1	0.9167	No	0	10
Cluster1	CCH_1	0.9167	No	0	10
Cluster1	MN_1	0.6923	No	2	8
Cluster1	MN_2	0.9167	No	0	10
Cluster1	MN_3	0.8333	No	1	9
Cluster1	$Node_6$	0.1579	Yes	5	5
Cluster1	$Node_{10}$	0.5000	Yes	3	7
Cluster2	MCH_2	0	Yes	4	6
Cluster2	CCH_2	0	Yes	2	8
Cluster2	……	……	……	……	……
Cluster2	MN_i	0.8333	No	1	9
Cluster2	$Node_1$	0.3043	Yes	4	6
Cluster2	……	……	……	……	……
Cluster2	$Node_m$	0.0725	Yes	6	4
……	……	……	……	……	……

4.3.2 Trust Evaluation

Based on the monitoring mechanism in Sect. 4.3.1, MNs evaluate the trustworthiness of nodes with a trust model. In the Beta trust model, MN_i calculates the reputation $R_{i,j}$ according to the behaviors of CM_j. For example, MN_i counts the number of good and bad behaviors of CM_j as $r_{i,j}$, $s_{i,j}$ and records the credibility of node CM_j using Eq. (7).

$$R_{i,j} = Beta(p|r_{i,j}+1, s_{i,j}+1) \tag{7}$$

Beta model can be represented by a Γ function

$$Beta(p|r_{i,j}+1, s_{i,j}+1) = \frac{\Gamma(r_{i,j}+s_{i,j}+2)}{\Gamma(r_{i,j}+1)\Gamma(s_{i,j}+1)} p^{r_{i,j}}(1-p)^{s_{i,j}} \tag{8}$$

Then the trust value of CM_j in MN_i, $T_{i,j}$, can be expressed as

$$T_{i,j} = E(R_{i,j}) = \frac{r_{i,j}+1}{r_{i,j}+s_{i,j}+2} \tag{9}$$

where $0 \le p \le 1$, $r_{i,j} \ge 0$ and $s_{i,j} \ge 0$. We introduce a parameter θ which is called the attenuation factor and substitute $s_{i,j}$ with $\theta^{S_{i,j}} - 1$ into Eq. (9). $T_{i,j}$ can be transformed to Eq. (10).

$$T'_{i,j} = \frac{r_{i,j}+1}{r_{i,j}+(\theta^{s_{i,j}}-1)+2} = \frac{r_{i,j}+1}{r_{i,j}+\theta^{s_{i,j}}+1} \tag{10}$$

The improved Beta trust model has at least three characteristics compared with the traditional Beta model. (i) The trust value of node decreases dramatically when a bad behavior emerges. (ii) The trust is based on the computation rather than the communication, which consumes less energy. (iii) The data received from the trust nodes will be fused and the other ones will be ignored by CHs, which improve the accuracy of DA.

4.3.3 Intrusion Detection

Each MN generates the trust table for all the nodes in a cluster as shown in Table 2.

Table 2. Trust table in MN (T_{MN}).

Cluster	Node ID	Trust value	Outlier	Bad behavior	Good behavior
Cluster1	MCH_1	0.9167	No	0	10
Cluster1	CCH_1	0.9167	No	0	10
Cluster1	MN_1	0.6923	No	2	8
Cluster1	MN_2	0.9167	No	0	10
Cluster1	MN_3	0.8333	No	1	9
Cluster1	$Node_1$	0.3043	Yes	4	6
Cluster1	$Node_2$	0.9167	No	0	10
Cluster1	$Node_3$	0.9167	No	0	10
Cluster1	$Node_4$	0.5000	Yes	3	7
Cluster1	……	……	……	……	……
Cluster1	$Node_{10}$	0.5000	Yes	3	7

Here, we take cluster 1 as an example to describe the detection mechanism. We divide the intrusion detection into intra-cluster and inter-cluster detections.

(1) Intra-Cluster Detection. The MNs mainly monitor the behavior of CHs and CMs. Assumed that a cluster consists of many sensor nodes, $N = \{n_k | k = 1, 2, \ldots, \mathrm{n}\}$. Take $k = 10$ for example, the number of MNs is 3 (an integer between 10/4 and 10/3 according to Eq. (3)). Three MNs are symbolized as MN_1, MN_2 and MN_3. They are assigned to evaluate the trust values of a CM, CM_j, in the same cluster. They evaluate

the trust values, $T'_{1,j}$, $T'_{2,j}$ and $T'_{3,j}$ of CM_j respectively and exchange trust tables with each other. Then, a comprehensive trust value of CM_j and CT_j can be formulized as Eq. (11)

$$CT_j = a_1 T'_{1,j} + a_2 T'_{2,j} + a_3 T'_{3,j} \tag{11}$$

where a_1, a_2, a_3 are the weight of trust values and $a_1 + a_2 + a_3 = 1$. The weight value is based on F_i according to Algorithm 1.

By comparing the comprehensive trust value with a predefined threshold Θ_T, a MN determines whether CM_j is trustworthy or not. A node will be considered as malicious one if CT_j is less than Θ_T. A MN inserts a malicious item into the outlier table. After that, MN shares the table with CHs and other MNs. CH records this outliers table and send it to upstream node in aggregation tree until BS reaches. Then, BS isolates the malicious node from the network according to this outlier table. This process is depicted in Algorithm 2.

Algorithm 2. Intra-Cluster Detection Mechanism.

Input: Original data from CMs, trust value of CMs and the threshold trust Θ_T
Output: Trust data and outliers table T_{MN}

1. **Begin**
2. Compute comprehensive trust value CT_j of CM_j
3. **If** $CT_j < \Theta_T$
4. CM_j is a malicious node, then store it in T_{MN};
5. **Else**
6. CM_j is a normal node and CH accepts its data;
7. **End IF**
8. **End**

(2) Inter-Cluster Detection. Inter-cluster detection is mainly performed at BS and the main work of BS is to calculate the similarity of the aggregated results. The MCH, $MCH_i (i = 1, \ldots, m)$, where m is the number of CH in a WSN, submits the aggregation result R_{MCH_i} and the outliers table T_{MN_i}. The CCH, $H_j (j = 1, \ldots, m)$, keeps sleeping and working according to the sleeping strategy. In a time window t, CCH sleeps $t/2$ and works for $t/2$. In working time, CCH_j sends the aggregation result R_{CCH_j} and the outliers table T_{MN_j} to BS. Then, the similarity coefficient can be verified using Eq. (12).

$$\lambda = \varepsilon_1 * \left(1 - \frac{2 * \left|R_{MCH_i} - R_{CCH_j}\right|}{\left|R_{MCH_i} + R_{CCH_j}\right|}\right) + \varepsilon_2 * \frac{\left|T_{MN_i} \cap T_{MN_j}\right|}{\left|T_{MN_i} \cup T_{MN_j}\right|} \tag{12}$$

where ε_1 and ε_2 are the weights and $\varepsilon_1 + \varepsilon_2 = 1$. $\left|T_{MN_i} \cap T_{MN_j}\right|$ denotes the number of common outliers in T_{MN_i} and T_{MN_j}. $\left|T_{MN_i} \cup T_{MN_j}\right|$ is the number of all outliers in T_{MN_i} and T_{MN_j}. The R_{MCH_i} and R_{CCH_j} will be accepted by BS, if λ is more than a similarity threshold Θ_S. Otherwise, MCH and CCH are both reassigned by BS when $\lambda < \Theta_S$.

Algorithm 3 shows the pseudo code of inter-cluster detection. In this way, BS only accepts the trust aggregation result and the accuracy is ensured.

Algorithm 3. Inter-Cluster Detection Mechanism.

Input: Aggregation results, outliers tables T_{MN} and similarity threshold Θ_S
Output: Outliers table T_{BS}

1. **Begin**
2. BS computes the similarity coefficient λ
3. **If** $\lambda \geq \Theta_S$
4. R_{CH} will be accepted by BS;
5. **Else**
6. Reelect CHs according to Algorithm 1;
7. **End IF**
8. **End**

4.4 Trusted Data Aggregation

DA is an effective technology to eliminate data redundancy and improve energy efficiency in a WSN. The basic idea is to fuse the data received from different sources to a single packet and reduce the energy consumption in data transmission. In TIDS, the reliable data are obtained and the malicious nodes are detected. The aggregation is carried out within the trust data. CH calculates the sum of the sensing data and sends the result to BS. Then, the final aggregation result can be expressed as follows:

$$R_{CH_i} = \sum_{i=o}^{k} data_i \tag{13}$$

$$R_{DA} = Avg(R_{CH_1}, R_{CH_2}, \ldots, R_{CH_n}) = \frac{\sum_{i=0}^{m} R_{CH_i}}{m} \tag{14}$$

where k is the number of trust CMs and m is the number of trust ones in n CHs.

5 Simulation

In this section, theoretical analysis and simulation studies will be done to verify our scheme by examining parameters in terms of security, energy consumption and network lifetime. A network with 150 sensor nodes is randomly deployed in a 400 m * 400 m area. The communication radius of the sensor node is 50 m and the transmission rate of the node is 1 Mbps. All the simulation parameters are displayed in Table 3.

As discussed previously, the compromised sensor nodes can attack the network in several traditional ways such as jamming, message dropping and falsifying. In this study, only take dropping attack is considered and packet loss ratio is 50% for a compromised sensor node and 10% for a credible sensor node. Besides, the sensor node measurement model approximately accords with Gaussian distribution.

Table 3. Simulation parameters.

Parameter	Value	Parameter	Value
Packet size	27 bytes	θ	2
E_{max}	0.01 J	α_1	0.6
E_{elec}	50 nJ bit^{-1}	α_2	0.4
ε_{fs}	10 pJ bit^{-1} m^{-2}	ε_1	0.5
ε_{mp}	0.0013 pJ bit^{-1} m^{-2}	ε_2	0.5
E_{th}	0.001 J	a_1	0.5
Θ_T	0.5000	a_2	0.3
Θ_S	0.80	a_3	0.2

5.1 Average Energy Consumption and Network Lifetime

A sensor node is composed of a sensor module, a processing module, a wireless communication module and an energy supply module. The sensing module and the processing module only consume a small amount of energy. The communication module being the most important part needs to be evaluated.

When the node is in a sending state, the relationship between the energy consumption and distance is $E = kd^n$, where n is a signal attenuation index, which is a real number between 2 and 4. In our simulation, the initial energy (E_{max}) of CMs is 0.01 J. According to Eq. (4), the energy consumption of the sender is $E_{TX}(l,d) = E_{TX\_elec}(l) + E_{TX\_amp}(l,d) + l \times E_{elec} + l \times \varepsilon_{fs} \times d^2$ when sending l bit data between nodes. And the energy consumption of the receiver is $E_{RX}(l) = l \times E_{elec}$.

The average energy consumption refers to the ratio of the total dissipation energy of the entire network in one second to the number of all the sensor nodes. The simulation results of average energy consumption and lifetime are shown in Figs. 3 and 4, respectively. It can be found that the average energy consumption of TIDS is smaller than that of DCHM. The energy consumption of TIDS is larger than that of a network without any security mechanism. This is mainly due to the fact that some extra data are calculated, stored, transmitted in TIDS. However, our scheme guarantees the security and accuracy for DA and it is a reasonable tradeoff among different network parameters.

Figure 4 shows the number of surviving nodes in a network. Most of the nodes are active in the initial 6×10^4 s in the condition that d_0 = 50 m. But the number of surviving nodes decreases significantly after 6×10^4 s in DCHM. TIDS can keep working in 6.5×10^4 s in TIDS. Although the lifetime of TIDS is shorter than that of the network without any mechanism (7.5×10^4 s), TIDS demonstrates a better performance in lifetime than DCHM. Figures 3 and 4 denote a fact that the energy consumption is an unavoidable overhead when a security mechanism is applied in a WSN and SDA should provide security at a price as low as possible.

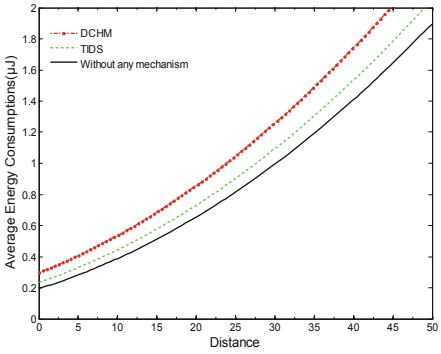

Fig. 3. Average energy consumption.

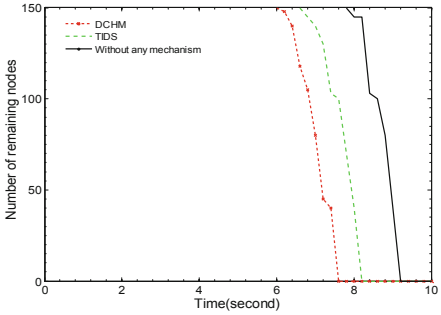

Fig. 4. Number of remaining nodes.

5.2 Security Analysis

The compromised node is a huge threat to a WSN. The performances of TIDS are verified in two cases, compromised CH and the evolution pattern of trust value. Assumed that t_i is the working time of a compromised node, C_i, in a cluster, the probability of C_i being selected as a CH is defined as follows:

$$P_c = \frac{1}{2} \times \frac{t_1}{T_{life}} + \frac{1}{2} \times \frac{t_2}{T_{life}} + \cdots + \frac{1}{2} \times \frac{t_c}{T_{life}} = \frac{\sum_{i=1}^{c} t_i}{2 * T_{life}} \tag{15}$$

where c is the number of compromised nodes, T_{life} is the lifetime of the whole network. For example, the lifetime of the network is 10000 s when there is no compromised node in cluster 1. In cluster 2, the working time of compromised MCH is 100 s. In cluster 3, the compromised MCH is operated for 500 s and CCH is dominated by a malicious activity for 400 s. Therefore, P_c is equal to 5% according to Eq. (15).

We compared TIDS with DCHM and demonstrated their performances in Fig. 5. The P_c increases linearly with the number of compromised nodes increase if CHs are randomly selected without any security mechanism. Both DCHM and TIDS perform well, especially when the ratio of compromised nodes is less than 10%, and TIDS presents a better performance than DCHM in other cases. Our mechanism is acceptable because P_c is below than 50% even if the compromised nodes are more than 75%.

A normal node should not be reported as a malicious one although it may act as an abnormal one occasionally due to the unreliable channel. In our experiments, TIDS are tested in two situations: (1) a normal node operates in a network scene with communication errors and (2) a normal node operates in a network scene without any communication error. The simulation results are shown in Fig. 6. As time goes on, the trust value of the normal node gradually increases to a higher level. It should be noted that a few errors may result in a severe fluctuation of trust value. This proves that our trust evaluation model in Sect. 4.3.2 can actualize the decline-quick-rise-slow which makes it easier to recognize a malicious node.

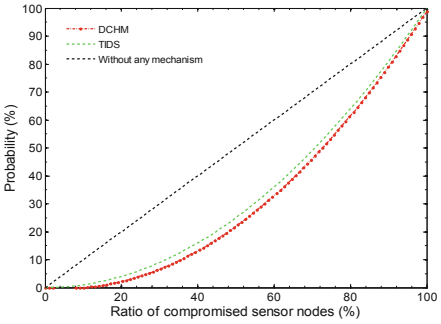

Fig. 5. Probability of selecting compromised CH.

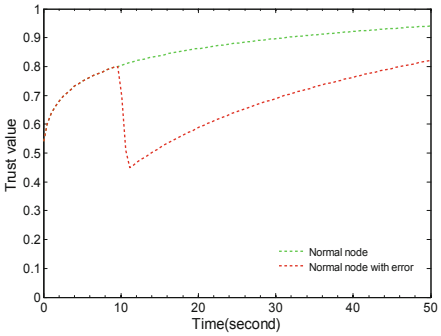

Fig. 6. Trust value changes of node.

5.3 Accuracy of TIDS

The detection rate of malicious nodes is related to the number of malicious nodes. If there are many malicious nodes in a WSN, the detection rate is lower; otherwise, the detection rate is higher. Our experimental network is operated with different proportions of malicious nodes (0%, 10%, 20%, 30%, 40% and 50%) between TIDS and FDSR [22]. For each proportion, our experiment is repeated 20 times with the malicious nodes being deployed to a random location in each experiment. Then, the average detection rate is obtained which is shown in Fig. 7. It is clear that the detection rate keeps declining with the proportion of malicious nodes increasing. Both TIDS and FDSR can detect the malicious nodes at a higher level (more than 90%) when the compromised nodes are less than 10%. However, the detection rate drops to nearly 70% when the proportion of compromised nodes rises to 50%. This illustrates that a more accurate detection mechanism needs to be explored in subsequent studies.

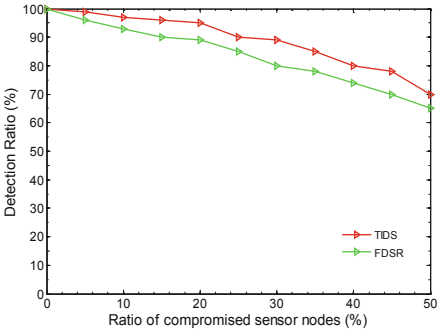

Fig. 7. Detection ratio with compromised nodes.

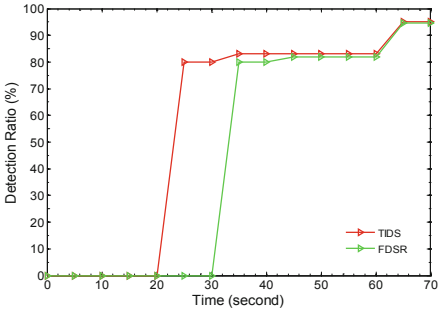

Fig. 8. Detection ratio changes with time.

The evolution of detection rate is also tested a fixed proportion of malicious nodes (25%) at different times. Figure 8 shows that the detection rate increases with the time goes on. It is obvious that the detection rate of TIDS is better than FDSR, which is mainly because the trust values of nodes may be more accurate with the updating of trust table.

Aggregation accuracy is a key criterion for data aggregation in WSNs. Figure 9 displays a comparison between the FDSR, DCHM and TIDS in accuracy of aggregation. The accuracy of these three protocols grows slowly in the initial stage and the malicious behaviors of the compromised nodes are not detected, which means that the compromised nodes are not excluded from the network. The aggregation accuracy increases sharply after 1200 s because TIDS collects enough malicious behaviors and the trust tables are exchanged among MNs in a cluster. Meanwhile, BS isolates most of the malicious nodes from the network and aggregates the data received from trust nodes only. The aggregation accuracy of TIDS increases to 91.1%, while FDSR is 85.7% and DCHM is 85% after the network runs for 3000 s. Although the improvement of accuracy does not reach a prominent degree, the promotion made by our scheme is significant compared with DCHM and FDSR.

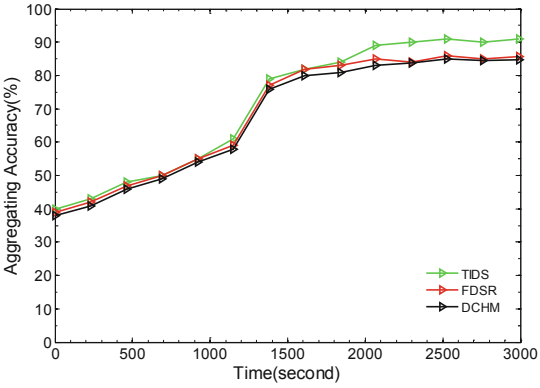

Fig. 9. Comparison of aggregating accuracy.

6 Conclusion

In this paper, we discuss a trust-based intrusion detection mechanism and the secure data aggregation issues in WSNs. We attempt to solve these problems by clustering technique, trust system, and data aggregation. We ensure certain levels of security in case of compromised nodes and prevent the aggregation result from being deviated through trust evaluation, trust exchange and outlier detection. Our scheme promotes the system performance in terms of security and accuracy at a relatively low price of energy consumption. Simulation verifications show that TIDS significantly improves the detection rate, the lifetime and the aggregation accuracy of WSNs. Although TIDS

is a favorable trade-off between network security and energy efficiency, we are a long way from a good solution to make the network run in a reasonable manner. For future work, a more accurate aggregation scheme is required and a novel trust model is an important design goal in subsequent studies. In addition, the threshold plays a significant role in trust-based intrusion detection system and an optimal threshold should be determined, which is one of the valuable topics we are pursuing in the future.

Acknowledgements. This work is supported by NSF of China under Grants 61373027 and 61672321; Shandong Graduate Education Quality Improvement Plan (SDYY17138).

References

1. Butun, I., Morgera, S.D., Sankar, R.: A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutorials **16**(1), 266–282 (2014)
2. Parmar, K., Jinwala, D.C.: Concealed data aggregation in wireless sensor networks. Comput. Netw. **103**(C), 207–227 (2016)
3. Baker, D.: The architectural organization of a mobile radio network via a distributed algorithm. IEEE Trans. Commun. **29**(11), 1694–1701 (2003)
4. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Hawaii International Conference on System Sciences, pp. 1–10. IEEE, Maui (2000)
5. Zhang, H., Arora, A.: Gs^3: scalable self-configuration and self-healing in wireless sensor networks. Comput. Netw. **43**(4), 459–480 (2003)
6. Wei, D., Jin, Y., Vural, S., Moessner, K., Tafazolli, R.: An energy-efficient clustering solution for wireless sensor networks. IEEE Trans. Wirel. Commun. **10**(11), 3973–3983 (2011)
7. Fu, J.S., Liu, Y.: Double cluster heads model for secure and accurate data fusion in wireless sensor networks. Sensors **15**(1), 2021–2040 (2015)
8. Bao, F., Chen, I.R., Chang, M.J., Cho, J.H.: Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Netw. Serv. Manag. **9**(2), 169–183 (2012)
9. Ganeriwal, S., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 66–77. ACM, Washington DC (2004)
10. Zhan, G., Shi, W., Deng, J.: Design and implementation of TARF: a trust-aware routing framework for WSNs. IEEE Comput. Soc. **9**(2), 184–197 (2012)
11. Aivaloglou, E., Gritzalis, S.: Hybrid trust and reputation management for sensor networks. Wirel. Netw. **16**(5), 1493–1510 (2010)
12. Shaikh, R.A., Jameel, H., Lee, S., Rajput, S., Song, Y.J.: Trust management problem in distributed wireless sensor networks. In: Proceedings of the 12th IEEE Conference on Embedded and Real-Time Computing Systems and Applications, pp. 411–414. IEEE, Sydney (2006)
13. Ozdemir, S.: Functional reputation based reliable data aggregation and transmission for wireless sensor networks. Comput. Commun. **31**(17), 3941–3953 (2008)
14. Liu, C.X., Liu, Y., Zhang, Z.J.: Improved reliable trust-based and energy-efficient data aggregation for wireless sensor networks. Int. J. Distrib. Sens. Netw. 1–11 (2013)

15. Su, X., Boppana, R.V.: On mitigating in-band wormhole attacks in mobile ad hoc networks. In: Proceedings of IEEE International Conference on Communications, pp. 1136–1141. IEEE, Glasgow (2007)
16. Karlof, C., Wangner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Netw. **1**(2), 293–315 (2003)
17. Cho, Y., Qu, G., Wu, Y.: Insider threats against trust mechanism with watchdog and defending approaches in WSN. In: Proceedings of IEEE Symposium on Security and Privacy Workshops, pp. 134–141. IEEE, San Francisco (2012)
18. Cho, Y., Qu, G.: Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs. Int. J. Distrib. Sens. Netw. 1–16 (2013)
19. Kefayati, M., Talebi, M.S., Rabiee, H.R., Khalaj, B.H.: On secure consensus information fusion over sensor networks. In: Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, pp. 108–115. IEEE, Amman (2007)
20. Yang, Y., Wang, X., Zhu, S., Cao, G.: SDAP: a secure hop-by-hop data aggregation protocol for sensor networks. In: Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 356–367. ACM, Florence (2006)
21. Sen, J.: Secure and energy-efficient data aggregation in wireless sensor networks. In: Proceedings of the 2nd IEEE Computational Intelligence and Signal Processing. IEEE, Guwahati (2012)
22. Xiaomei, D.: Secure data aggregation approach based on monitoring in wireless sensor networks. China Commun. **3**(3), 101–148 (2012)
23. Hua, P., Liu, X., Yu, J., Dang, N., Zhang, X.: Energy-efficient adaptive slice-based secure data aggregation scheme in WSN. Procedia Comput. Sci. **129**, 188–193 (2018)