IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received April 23, 2017, accepted June 13, 2017, date of publication June 20, 2017, date of current version July 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2717387

Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks

ZHIHUA ZHANG[1], HONGLIANG ZHU[1], SHOUSHAN LUO[1], YANG XIN[1], AND XIAOMING LIU[2]

[1]National Engineering Laboratory for Disaster Backup and Recovery, Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China

Corresponding author: Zhihua Zhang (zhangzhihua@bupt.edu.cn)

This work was supported in part by the National High Technology Research and Development Program of China (863 Program), under Grant 2015AA016005 and Grant 2015AA017201 and in part by the National Natural Science Foundation of China under Grant U1536119.

ABSTRACT Security problems have become obstacles in the practical application of wireless sensor networks (WSNs), and intrusion detection is the second line of defense. In this paper, an intrusion detection based on dynamic state context and hierarchical trust in WSNs is proposed, which is flexible and suitable for constantly changing WSNs characterized by changes in the perceptual environment, transitions of states of nodes, and variations in trust value. A multidimensional two-tier hierarchical trust mechanism in the level of sensor nodes (SNs) and cluster heads (CHs) considering interactive trust, honesty trust, and content trust is put forward, which combines direct evaluation and feedback-based evaluation in the fixed hop range. This means that the trust of SNs is evaluated by CHs, and the trust of CHs is evaluated by neighbor CHs and BS; in this way, the complexity of evaluation is reduced without evaluations by all other CHs in networks. Meanwhile, the intrusion detection mechanism based on a self-adaptive dynamic trust threshold is described, which improves the flexibility and applicability and is suitable for cluster-based WSNs. The experiment simulation and evaluation indicate that the mechanism we proposed outperforms the existing typical system in malicious detection and resource overhead.

INDEX TERMS Hierarchical trust, trust evaluation, state context, intrusion detection, wireless sensor network.

I. INTRODUCTION

With the rapid development and advancement of wireless sensor technology, wireless sensor networks (WSNs) are widespread in a variety of areas, including environmental monitoring, battlefield observation, intelligent home systems, forest fire detection, and health monitoring [1]. Due to the self-organizing, dynamic and data-centric characteristics of WSNs, they are deployed in more and more data observation fields, and the nodes in WSNs should cooperate with each other for communication and support of high-level applications.

However, security issues have accompanied the wide use of WSNs. Because of the openness of the deployed environment and the transmission medium, WSNs suffer from various attacks, including hijack attacks, tampering attacks, DoS attacks, selective forwarding attacks, and sinkhole attacks. It is impossible to solve all the security problems by adapting prevention-based technology; thus, detection-based methods are an effective supplement. Therefore, intrusion detection in WSNs is proposed [2], [3], and it plays an irreplaceable role as an important branch in the field of security mechanisms.

Commonly, intrusion detection often detects the crucial features or behaviors of the node. The trust-based model has been widely used in WSNs and P2P networks as an effective means of guarding against internal attacks [4], [5], and it is often used in WSNs for security routing, which selects a secure path according to the trust evaluation of the neighbors of nodes [6]. The first trust model for WSNs is a distributed reputation-based framework described in [7], which could be used for detecting compromised or faulty nodes, and the estimation of reputation is according to transactional data between nodes indicating the cooperativeness of partner nodes. However, the "cooperativeness" in [7] refers to a node's ability to deliver information or the quality of data delivered; i.e., the reputation-based framework merely focused on data accuracy or data authentication in sensor networks. An intrusion detection mechanism using trust for clustered WSNs is implemented in [8], which considers social trust (including intimacy and honesty) and QoS trust (measuring energy and unselfishness) to form the overall trust metric. However, the evaluation of the intimacy trust of nodes only depends on the maximum number of interactions between nodes, which could be misled by malicious nodes exceeding the number of normal interactions.

Based on previous work, an improved hierarchical trust mechanism using multidimensional trust is established for WSNs to detect malicious nodes, which considers not only communication trust (including interactive trust and honesty trust) and content trust (multidimensional sensing data trust) but also the state context of nodes, especially state transitions. Meanwhile, it reduces the possibility of misleading by malicious nodes in the process of interactive trust evaluation by taking the upper bound of the number of normal interactions into account. Besides, the task of trust evaluation and intrusion detection is performed by CHs and BS with abundant resources; thus, the lifetime of the network is prolonged.

State context of nodes is introduced for the calculation of trust value, making nodes in different state transitions adopt different methods to evaluate trust value, which improves the flexibility and applicability of the mechanism. Nodes in WSNs are often set to different states to conserve their energy, and the transitions of states of sensor nodes demonstrate either that the current state has timed out or that the surroundings of the node have changed. State transitions should be focused, and we should distinguish between normal changes and attacks. Transitions between different states may be accompanied by different security issues; thus, the calculation of the trust value will have different emphases, so we should adopt different methods to compute trust to make it more flexible. An example is as follows: If the state of a node changes from a monitoring state to an active state, there will exist two cases; one is normal conversion, which means the node has discovered an abnormal event, such as an occurrence of fire; the other is attack, such as a hijack attack, tampering attack, DoS attack or other packets attack, whose purpose is to consume the energy of the node. So, the interactive trust and data trust become more important measurement factors, and we can distinguish the normal conversion or attack through changes in the trust value. More details are discussed in section IV-B. Therefore, state context is a key factor of trust evaluation and intrusion detection.

The main contributions of our work are as follows:

1) State context construction: By analyzing the states of nodes in WSNs, a state transition context and its judgment rules are established, through which different methods could be adopted to calculate trust value effectively, i.e. a self-adaptive trust calculation method for SNs. Meanwhile, the details of the possible security problem according to the state conversions are analyzed.

2) Hierarchical trust improvement: An improved two-tier hierarchical trust mechanism is proposed, which refers to the trust of SNs and the trust of CHs. The judgment strength of the SNs' trust is reduced by CH-to-SN trust evaluation, whereas the judgment strength of the CHs' trust is enhanced through CH-to-CH, the feedback of 1-hop neighbors of CHs and BS-to-CH trust evaluation. Meanwhile, multidimensional trust is proposed to form overall trust, including interactive trust, honesty trust and content trust. The mechanism is suitable for clustered WSNs with multidimensional observing data.

3) Detection threshold self-adaption: In the malicious detection process, the threshold of detection could be adjusted according to the operation of WSNs rather than a fixed value, which improves the self-adaption and detection rate of the system.

4) Resource conservation considerations: Due to resource limits of WSNs such as storage and energy limits of sensor nodes, measures should be taken to reduce resource consumption, including ten-scale integer representation of trust value, spatial correlation and alleviation of the computing tasks of SNs through CHs and BSs responsible for more computational tasks.

The rest of the paper is organized as follows: Section II summarizes the related works. The network model and assumptions are described in Section III, and an improved hierarchical trust mechanism considering the state context in trust evaluation of SNs is proposed in Section IV. In Section V, intrusion detection based on trust is analyzed. The experiment simulation and performance evaluation are performed in Section VI. Finally, conclusions of the paper are summarized in Section VII.

II. RELATED WORKS

The research on trust mechanisms in WSNs and other networks is widespread, e.g., Underwater Acoustic Sensor Networks (UASNs), Medical Sensor Networks (MSNs) and Vehicular Networks (VNets) [7]–[13]; these approaches are often used to assess data integrity, secure routing, message authenticity, reliability and the security of nodes. Trust-based intrusion detection [14]–[16] is a typical application of reliability and security of nodes.

Bao *et al.* [8] proposed hierarchical trust management for WSNs and applied it to routing and intrusion detection to detect selfish or malicious nodes. In the paper, multidimensional trust attributes were considered, and the trust value was calculated through social trust and QoS trust, including intimacy, honesty, energy, and unselfishness; meanwhile, subjective trust and objective trust were taken into consideration to validate the proposed protocol. However, the node with the maximum number of interactions with neighbors was considered as the most trustworthy in the process of the calculation of the intimacy trust inspired by social networks. The difference in our work is the consideration of the reasonable range of the maximum number of interactions, as interaction that exceeds the range indicates malicious behavior. A new function of interactive trust evaluation is put forward in our work.

Li *et al.* [9] put forward a lightweight and dependable trust system for clustered WSNs, which aims at decreasing resource consumption and enhancing the reliability of CHs' trust evaluation. At the same time, a self-adaptive weighting mechanism for trust calculation of CHs was raised, which was superior to the traditional subjective weight method. A series of theoretical proofs were given in the research to verify the effectiveness of the mechanism. In the process of trust evaluation, only successful and unsuccessful interactions were taken into consideration, with no other trust evaluation factors taken into account. The mechanism in our work takes interactive trust, honesty trust and content trust into account, addressing problems of consuming energy maliciously and tampering multidimensional observing data with lower resource overhead, which is described in the performance evaluation.

He *et al.* [11] put forward a distributed trust evaluation model for Medical Sensor Networks (MSNs) to address some security problems, such as node misbehavior. The authors identified the normal behaviors of nodes by the features of the MSNs and selected some unique features including data rate and leaving time to compute the trust value and detect malicious nodes. Another study [12] by the authors presented attack-resistant and lightweight trust management for MSNs. They pointed out the security risk of the trust mechanism itself and brought forward a two-tier trust architecture called Retrust, which enhanced the trust measurement of nodes and master nodes. However, the mechanisms they presented consume more storage of nodes and CHs because they have to store the trust value of all other nodes, including both the direct trust value and indirect trust value or the recommended trust. The overhead of our method (trust evaluation and intrusion detection) is concentrated on CHs and BSs with much greater resources than SNs, which will prolong the lifetime of WSNs.

Dhakne and Chatur [14] proposed a distributed trust-based intrusion detection approach in WSNs, which considered multidimensional trust on energy, data and communications, evaluating direct trust, recommendation trust and indirect trust of nodes, and detected malicious nodes through the deviation of subjective trust and objective trust. The ability of detection is improved by multidimensional trust, whereas the data trust in DTBID refers to 1-dimensional data, and multidimensional data are not discussed in DTBID. It is essential to take multidimensional observing data into account because it is common for several kinds of sensors to be carried on a node to observe different data. The content trust in our approach could evaluate multidimensional observing data to discover data tampering attacks.

Gerrigagoitia *et al.* [15] presented a reputation-based intrusion detection system for WSNs, which adopted reputation and trust to evaluate the behaviors of nodes. The evaluation considers only communication factors including correct and incorrect interactions using a beta function, which is executed by each node. Every node has evaluation and detection tasks for other nodes; thus, the overhead is still high for WSNs. Our method could decrease the overhead of nodes by executing tasks in CHs and BSs with more resources.

Cervantes *et al.* [16] proposed a method of detecting sinkhole attacks for the Internet of Things (IoT), which could discover sinkhole attacks in the network layer through the watchdog, reputation and trust mechanism together. The system adopts Dempster-Shafer theory to improve the detection rate, and it could be used in the network of fixed nodes and mobile nodes. It is designed for detecting sinkhole attacks, and other attacks would escape from detecting. Our approach is suitable for hybrid attacks including tampering, black hole, selective forwarding and other energy consumption attacks due to multidimensional trust evaluation.

III. NETWORK MODEL AND ASSUMPTIONS

In this section, data transmission features of common WSNs used for monitoring are introduced; then, the spatial correlation of nodes is described for energy preservation. After that, the state transitions of nodes considered in this paper and the network model are explained.

A. DATA TRANSMISSION FEATURES

There are four data transmission models according to [17], including continuous, event-driven, observer-initiated and hybrid, whose features are different. Sensors deliver the observing data continuously at a pre-defined rate in a continuous model, and it is common in WSNs, as is transmitting data at a predetermined period, the feature of which is regularity or periodicity. In the event-driven model, as the name suggests, the observing data are delivered when some events or anomalies are discovered whose characteristic is irregularity and abruptness. The observer-initiated model or request-reply model is triggered by query operations of other nodes, and passivity is the feature. The hybrid model is the most common in practice; it combines continuous, event-driven and observer-initiated models together, and its features are more complex than other three models.

The WSN we focused on is deployed for monitoring events or observing phenomena on some occasions, such as forest fire, pollution, and logistics environments. It is a hybrid model of data transmission using a storage and forwarding mechanism. The observing data are delivered to the sink periodically in normal circumstances, and the data transmission breaks the cycle when events occur or a query is initiated. The data are transmitted to the sink directly or indirectly through other neighbor sensors.

B. SPATIAL CORRELATION

In many scenarios, sensor nodes are deployed densely to acquire more accurate observations to improve the intelligence of the WSNs. As a result, nodes which are close to each other acquire the same observations for the same phenomenon and generate a large amount of redundant data. The data should be transmitted to the sink directly or indirectly, which will consume a lot of energy and reduce the efficiency of the network. Spatial correlation could solve the problem effectively. The closer the distance between nodes, the more redundant the data, and the higher the spatial correlation. Therefore, a small section of nodes in the same area are sorted to deliver their observing data representing nodes that are densely deployed in the area. Thus, the redundant data decrease, and the lifetime of the network is extended.

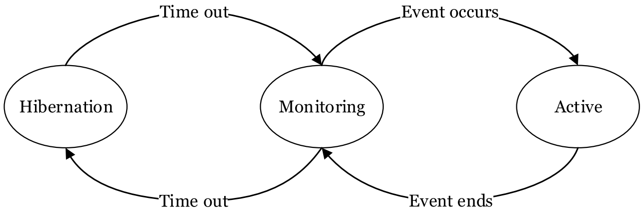

FIGURE 1. States and their transitions.

In [18], spatial correlation has been employed on the Medium Access Control (MAC) layer, and the transmission of redundant data from closely located sensors could be controlled; at the same time, energy consumption is also reduced. Spatial correlation could be utilized to decrease the redundant information.

C. STATES AND TRANSITIONS

Sensor nodes in WSNs are in different states to conserve energy, and it is not necessary for all nodes to appear to be active all the time due to the restriction of resources. The states of nodes are considered including hibernation, monitoring and active, which are three basic and necessary states, and other states are not taken into consideration here. The hibernation state shows that nodes are not working and that there is almost no energy consumption, whereas the monitoring state means that nodes are observing and delivering data at a regular frequency, which will cost more energy. However, the active state demonstrates that the node has discovered an event occurrence and is transmitting a large amount of information about events to sink, and its energy consumption is the largest of the three states. Data transmission is the basis for judging the state of nodes because different states have different data transmission rates [19].

States and their transitions are described in Fig. 1. The transitions of different states depend on pre-defined rules, such as time out or event occurrence. As with spatial correlation described in section III-B, closely located nodes alternate between hibernation and monitoring states according to time rules. If a monitoring node discovers an event, it will revert to an active state to deliver more information about the event. When the event ends, the state of the node returns to monitoring. The data transmission rate in three states listing from high to low is active, monitoring and hibernation.

Transitions between different states may be accompanied by different security issues, especially the transition between monitoring and active. Normal transitions and attacks could be distinguished by trust calculation; hence, state transition is the context of trust calculation, and data transmission rate is the context of state transition. The analysis is detailed in Section IV-B.

D. NETWORK MODEL

The topology of WSN we consider is a cluster-based network, based on which a two-tier hierarchical trust mechanism is put forward. The members of the WSN are categorized into cluster heads (CHs), sensor nodes (SNs) and base station (BS), as shown in Fig.2. In a cluster, a CH possesses more energy than SNs, and all SNs could communicate with CH directly, whereas a CH could forward the fusion data to a BS directly or through other CHs, which is similar to the structure of [19] and [20]. Each SN has a unique identity and belongs to a unique cluster. The composition of clusters is out of the scope of this article and can be found in [20].

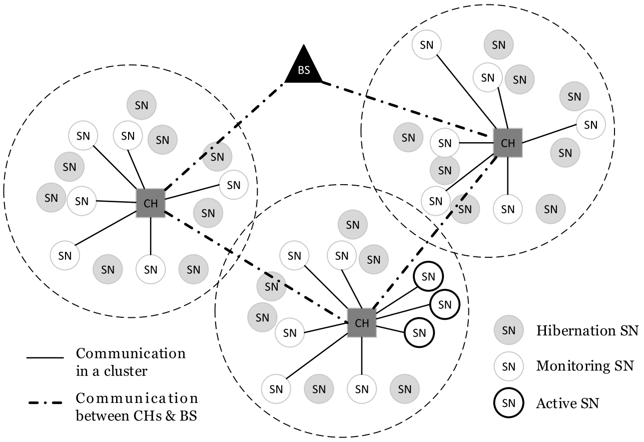

FIGURE 2. The network model of a cluster-based WSN.

In summary, the network we are researching is a cluster-based WSN used for monitoring events with a hybrid data transmission model; meanwhile, spatial correlation is employed in the WSN to reduce the energy cost, and nodes stay within three different states in the network operation process. An example model of WSN is displayed in Fig. 2. Due to spatial correlation, only a few nodes are in the monitoring state, and SNs discovering events revert to an active state. CHs store and forward the data to BSs continuously, and the data are stored in a queue maintained by CHs before forwarding. The increase in length of the data queue indicates an increase in the SNs' data transmission; therefore, the length of the data queue is an important context of state transitions, which is similar to [19].

We make the following assumptions in this paper:

1) 1) The WSN is cluster-based, and SNs in a cluster could communicate with the CH directly, whereas CHs communicate with BSs directly or indirectly through other CHs.

2) Each SN has a unique ID and belongs to a unique cluster, and CHs have more energy than SNs.

3) The data transmission model in a WSN is hybrid, including continuous and event-driven.

4) The states of SNs include hibernation, monitoring and active, and the transition between monitoring and active is taken into consideration during the trust evaluation of SNs.

5) Sensor nodes are deployed densely and redundantly for reliability.

IV. AN IMPROVED HIERARCHICAL TRUST MECHANISM

In this section, an improved two-tier hierarchical trust mechanism is introduced, which consists of SN trust evaluation and CH trust evaluation. The details of trust calculation are described below.

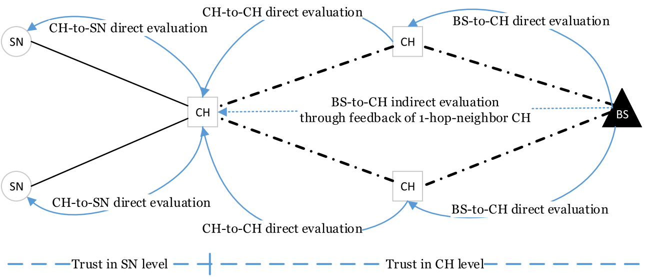
SN
CH-to-SN direct evaluation
CH-to-CH direct evaluation
CH
BS-to-CH direct evaluation
CH
BS-to-CH indirect evaluation
through feedback of 1-hop-neighbor CH
BS
SN
CH
CH-to-SN direct evaluation
BS-to-CH direct evaluation
CH-to-CH direct evaluation
Trust in SN level
Trust in CH level

FIGURE 3. **The structure of two-tier hierarchical trust evaluation.**

A. OVERVIEW OF HIERARCHICAL TRUST MECHANISM

Based on the cluster-based WSN described in section III-D, a two-tier hierarchical trust mechanism is introduced. Unlike prior works, the first level trust is simplified by CH-to-SN evaluation due to the direct communication between SN and CH in a cluster, whereas the second level trust is conducted by CH-to-CH direct evaluation and BS-to-CH direct or indirect evaluation through the feedback of a 1-hop-neighbor CH. This is shown in Fig. 3, in which we can see that the evaluation of trust is executed by CHs and BSs. The evaluation of the trust is periodic, the update cycle of which is Δt, a predefined interval according to the operation of WSN.

Two-tier trust evaluation consists of multidimensional trust, including network related trust and observing data related trust, because the WSN is a data-centric network, and it is essential to take the observing data into consideration. Meanwhile, it is common for sensor nodes to carry various types of sensors with them to acquire information. Therefore, the trust in this article is classified into interactive trust, honesty trust and content trust. The first two are network-related trust, while the last one is data-related trust. Their definitions are as follows:

Interactive trust refers to the trust value computed by the number of interactions between nodes, and an interaction means a node sending/receiving a packet or a request to/from another node. In a certain range, the greater the number of interactions between two nodes, the higher the degree of their trust, and it will reverse when it exceeds the normal range.

Honesty trust means the trust value calculated by the successful and failed interactions between two nodes. The greater the number of successful interactions than failed, the higher the degree of their honesty trust.

Content trust means the trust degree evaluated by the deviation between observing data and the effective average of observing data. The more proximal the data, the higher the content trust value of the node.

In this work, the trust value is mapped to the integer number in the range of [0, 10], where 0 demonstrates the most distrustful, while 10 implies the most trusted, and 5 is the medium trust. Adopting ten-scale integer representation of a trust value could save the memory of sensors [9].

B. SENSOR NODES TRUST EVALUATION

Sensor nodes trust is evaluated by the CH in a cluster, i.e., CH-to-SN trust, which considers multidimensional trust, including *interactive trust*, *honesty trust* and *content trust*, during the procedure of trust calculation.

1) INTERACTIVE TRUST OF SNs

Interactive trust $SIT_{ij}(\Delta t)$ is calculated by the number of interactions between node j and its CH i in Δt. In this paper, interaction refers to all communication behavior including sending and receiving of request and data packets. According to the interaction of members in social networks, the greater the number of interactions of two nodes, the higher the trust value [21]. However, in WSNs, if the number of interactions exceeds a threshold, the trust value will decrease because there may exist malicious interactions such as attacks that send a large amount of packets or requests to exhaust the energy of the node.

Therefore, unlike trust evaluation in social networks, the interactive trust evaluation method in WSNs is put forward. Inspired by Normal Distribution in Statistics, the probability density function, which is normalized to [0, 1] to calculate the interactive trust, is adopted when the number of interactions exceeds a threshold.

Interactions between CH and SNs are abstracted as an undirected weighted graph, the weight of which represents the number of interactions between them. The interactive trust value of SN j evaluated by CH, $SIT_{ij}\ (\Delta t)$ can be defined as:

$$SIT_{ij}(\Delta t)=\begin{cases}\left\lfloor 10\times w_{ij}/\max(w_{ij})\right\rfloor, & j\in G,\ w_{ij}\leq\lambda\mu;\\ \left\lfloor 10\times\exp(-\left|w_{ij}-\mu\right|/\theta)\right\rfloor, & j\in G,\ w_{ij}>\lambda\mu;\end{cases}\tag{1}$$

where $\lfloor x\rfloor$ denotes the largest integer that is equal to or less than x, μ is the mean value of the number of interactions between CH and SNs in the same state, $\lambda\mu$ is taken as the threshold of the interaction range, in which λ is a parameter used to define the upper limit of normal interactions, and θ is a significant factor, which values 1, 10 and 100 when w_{ij} is a single digit, tens digit or hundreds digit, correspondingly, and so on.

Here, states of SNs should be noted because they have a great impact on the interactive trust evaluation between SNs and CH (the number of normal interactions is different based on different states). Therefore, the evaluation process of interactive trust of SNs is classified into three categories according to different states. The judgment of states could refer to section III-D and [19]. For hibernation SNs, they inherit their last nonhibernating trust value, whereas for the interactive trust of monitoring and active SNs is calculated through the number of interactions between CH and SNs, which are at the same state according to (1), respectively.

Two examples are shown in Fig. 4 (a) and (b). In the example graph G, a set of SNs {A, B, C, D, E and F} in the same state (for example, the monitoring state) interact directly with a CH marked as i, and the weight on edges denoted as w_{ij} represents the number of interactions between them in an update cycle Δt, and in this example, we set the parameter $\lambda = 2$.

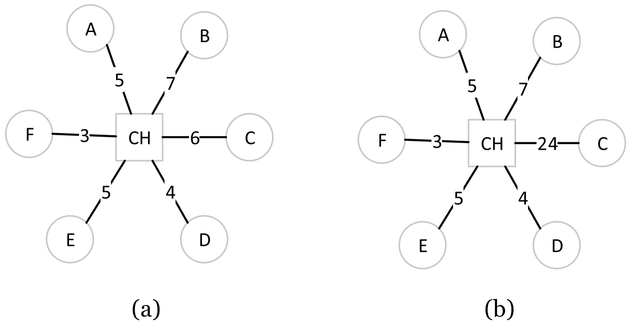

FIGURE 4. An abstracted graph of interactions between CH and SNs (all SNs are in the same state – monitoring state). (a) and (b) The vertexes A, B, C, D, E and F represent the SNs in the monitoring state, CH represents the cluster head. The number on each edge dipicts the number of interatcions between each SN and the CH in an evaluation cycle.

TABLE 1. Interactive trust evaluation results of SNs in Fig. 4.

Nodes	Evaluation Results of Fig. 4 (a)	Evaluation Results of Fig. 4 (b)
A	7	7
B	10	10
C	8	2
D	5	5
E	7	7
F	4	4

Here, the evaluation results of examples in Fig. 4 computed according to (1) are listed in TABLE 1. The results show that node B has the highest interactive trust in both examples, but node C is different. The mean value of the number of interactions in Fig. 4 (a) and (b) is 5 and 8, respectively. Thus, the threshold of normal interactions for (a) and (b) is 10 and 16, respectively. In Fig. 4 (a), the number of interactions is less than the threshold, so nodes with the maximum number of interactions (here, it is 7) have the highest trust value; i.e., the trust value of node B is 10, and the trust value of others is the ratio of the number of interactions to the maximum number of interactions. Whereas in Fig. 4 (b), the number of interactions between node C and CH exceeds the threshold, and thus the trust value of node C is not the highest; and the higher the number of interaction than the threshold, the lower the trust value according to (1).

2) HONESTY TRUST OF SNs

Honesty trust SHT_{ij} (Δt) is calculated by the number of successful and unsuccessful interactions between CH i and a nonhibernating SN j in Δt. The CH i overhears the SN j if j does not deliver a packet in Δt or transmits the packet to another node that is not in its routing table, or if the packets from j do not reach the CH i, the interaction between them is considered an unsuccessful interaction. Otherwise, we consider it a successful interaction. For instance, if a node is compromised and suffers from a black hole or selective forwarding attack, all packets or partial packets from it will not reach the CH. The higher the ratio of the number of successful interactions to the number of all interactions, the higher the trust value.

The number of successful and unsuccessful interactions between nonhibernating nodes and CH i in Δt is denoted as s and f, and the trust value is evaluated with (2) according to the improved beta function.

$$SHT_{ij}(\Delta t) = \begin{cases} \lfloor 10 \times (s+1)/(s+f+2) \rfloor, & when\, f = 0 \\ \lfloor 10 \times (s+1)/(s+f+2) \times f^{-1/2} \rfloor, & when\, f \neq 0 \end{cases} \quad (2)$$

When there are no interactions between nonhibernating members, i.e., $s = f = 0$, the trust value is 5. If there are unsuccessful interactions, the honesty trust value will decrease sharply because of the punishment executed by $f^{-1/2}$ [9]. For hibernation members, they inherit the trust value of their last nonhibernating state.

3) CONTENT TRUST OF SNs

Content trust is the trust evaluation based on observing data, which is data-oriented trust calculated by CH. Content trust is introduced because the WSN is a data-centric network and the observing data are the factor of most concern for applications. Tampering attacks often occur in WSNs to interfere with the network and applications and can be identified by content trust.

In WSNs, nodes often carry different sensors with them, such as temperature sensors, humidity sensors, light intensity sensors, and air pressure sensors. They will transmit multidimensional observing data to the CH, and the deviation between the observing data and the effective average of observing data determines the content trust. Euclidean distance is adopted to evaluate the content trust in this work. As for the effective average, we denote m_{ak} and σ_k as the mean value and standard deviation of the *kth*-dimension observing data of nonhibernating SNs; the effective average of the *kth*-dimension data is the mean value of the observing data that are in the range of $[m_{ak} - \sigma_k, m_{ak} + \sigma_k]$. For instance, if a 1-dimension observing data set is {10, 11, 10, 14, 10}, the mean value and standard deviation is 11 and 1.55, respectively. The effective average is the mean value of observing data that are in the range of [9.45, 12.55]; i.e., the mean value of {10, 11, 10, 10} and {14} is excluded because it is out of range. Due to the dense deployment of nodes, if an observing event occurs, most nodes around the event will report the observing data, and it is impossible for only one node to observe obviously different data, unless the node is compromised or attacked.

Therefore, content trust SCT_{ij} (t) is calculated as follows:

$$SCT_{ij}(t) = \lfloor 10 \times \exp(-D_{ij}) \rfloor, \; D_{ij} = \left(\sum_{k=1}^{d_m} (x_{ik} - x_{jk})^2 \right)^{1/2} \quad (3)$$

where D_{ij} denotes the Euclidean distance between the multidimensional effective average calculated by CH i and the multidimensional data observing by SN j, d_m indicates the dimensions of observing data; and x_{ik} and x_{jk} represent the effective average of the *kth*-dimension data stored in CH *i* and the *kth*-dimension data of SN *j*, respectively. Hibernation SNs inherit the trust value of their last nonhibernating state.

4) OVERALL TRUST OF SNs

The overall trust of SN j evaluated by CH i is calculated as (4), which aggregates the interactive trust, honesty trust and content trust.

$$SOT_{ij} = \lfloor \alpha SIT_{ij} + \beta SHT_{ij} + (1 - \alpha - \beta) SCT_{ij} \rfloor \tag{4}$$

where parameters $\alpha, \beta \in [0,\ 1]$ are weights for each subtrust value. The higher the weight, the more important that subtrust is to overall trust and vice versa. The parameters are different according to different occasions considering state transitions, and discussions are as follows:

We consider hibernation state, monitoring state and active state as described in section III-C. The state transition between hibernation and monitoring depends on the predefined time period, and we assume that there is no security event during the occasion. However, the transition between monitoring and active state may be accompanied by the occurrence of security issues. Therefore, three occasions are discussed, including No state transitions between monitoring and active, State transition from monitoring to active and State transition from active to monitoring.

Case 1: No state transitions between monitoring and active.

In this occasion, states of nodes periodically alternate between monitoring and hibernation, which is common in WSNs. According to the assumption above, it has no effect on the evaluation of trust; therefore, the calculation is executed by (4) with the parameter $\alpha = \beta = 1/3$, which means the interactive trust, honesty trust and content trust have the same importance.

Case 2: State transition from monitoring to active.

When there exists state transition from monitoring to active, the most significant change is that the queue length of corresponding CH increases sharply. According to data transmission features and the network model described in section III-A and III-D, abnormal events may occur in the environment; otherwise, attacks may occur, especially DoS attacks, tampering attacks or other attacks whose purpose is to consume energy. Therefore, the interactive trust and content trust are of greater concern among the three trusts, and the evaluation of the trust of active nodes is executed by (4) with the parameter $\alpha = 1/2$ and $\beta = 0$. If the abnormal event of the environment is true, the neighbors of the node will also increase the transmission rate, and the effective average of observing data will also be very proximate with the data of the node, which means the trust value of the active node is still at a high level. Otherwise, if only the active node changes its behavior or observing data, its trust value will decrease significantly, which means the active node may be attacked.

Case 3: State transition from active to monitoring

When a normal active node converts its state to monitoring, there exists two cases: One is that the abnormal event of an environment is ended, and the other is that a node is suffering from a tampering attack or a black hole attack or selective forwarding attack. Therefore, honesty trust and content trust are of more concern, and the trust evaluation is calculated by (4) with the parameter $\alpha = 0$ and $\beta = 1/2$. If the abnormal event indeed ends, the effective average of observing data will be similar to the observing data of the node, and the honesty trust will not fall to a low level, which means the trust of the node will be at a high level. Otherwise, the difference in observing data or decrease in transmission rate (the CH will not receive enough packets from the node as with others) makes the trust value decrease in an obvious way, which means that the observing data of the node are tampered with or the node drops all the packets or part of the packets.

C. CLUSTER HEADS TRUST EVALUATION

Cluster heads trust evaluation is enforced in this work by CH-to-CH evaluation, BS-to-CH evaluation and feedback from 1-hop neighbors of CH in order to avoid malicious CHs in WSNs. Similar to the trust of SNs, CH trust evaluation also includes interactive trust, honesty trust and content trust. Interactive trust and honesty trust are computed by BS-to-CH and feedback from 1-hop neighbors of CHs, whereas content trust is evaluated by BS-to-CH evaluation through the proximity between the fusion data and the effective average observing data of non-hibernating SNs in its cluster.

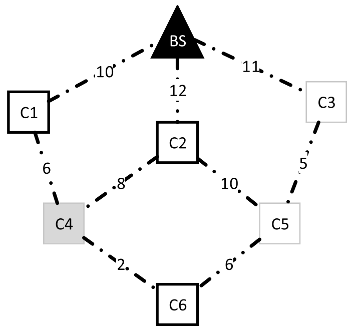

FIGURE 5. The schematic diagram of interactions between BS and CHs, and the interactive trust of C4 evaluated by BS is based on the feedback of C1, C2 and C6.

1) INTERACTIVE TRUST OF CHs

Interactive trust of CHs is divided into direct trust and indirect trust. The former is evaluated by BS for its 1-hop-neighbor CHs, and the latter is evaluated by feedback from CHs that are 1-hop neighbors of a CH that is a non-1-hop neighbor of a BS. Here, feedback is defined as positive feedback and negative feedback, which means the trust value calculated by its 1-hop neighbors is greater than or equal to 5 and less than 5, respectively.

As shown in Fig. 5, C1, C2 and C3 are 1-hop neighbors of BS, whereas C4, C5 and C6 are non-1-hop neighbors of BS; therefore, the trust of C1, C2 and C3 is evaluated by BS directly, and the trust of C4, C5 and C6 is calculated by the feedback of the respective 1-hop neighbors of each CH; i.e., the interactive trust of C4 is computed by the feedback of

C1, C2 and C6, which are 1-hop neighbors of C4; similarly, the trust of C5 (respectively, C6) is evaluated by the feedback of C2, C3 and C6 (respectively, C4 and C5). The numbers on edges represent the number of interactions between two CHs.

The interactive trust of each CH is initialized to 5, and the trust between a CH and its 1-hop neighbors is updated with (5).

$$IT_{ij}(\Delta t)=\begin{cases}\left\lfloor 10\times w_{ij}/\max(w_{ij})\right\rfloor, & w_{ij}\le\lambda\mu;\\ \left\lfloor 10\times \exp(-\left|w_{ij}-\mu\right|/\theta)\right\rfloor, & w_{ij}>\lambda\mu;\end{cases}\tag{5}$$

where *j* is 1-hop neighbors of *i*, and w_{ij} represents the number of interactions between *i* and *j*, μ denotes the mean value of w_{ij}, λ is a parameter used to define the upper limit of the normal interactions, and θ is a significant factor, which values 1, 10 and 100 when w_{ij} is a single digit, tens digit or hundreds digit, correspondingly, and so on.

Interactive trust evaluation of 1-hop-neighbor CHs of BS *b* is based on (5) denoted as IT_{bj} (Δt), which means $i=b$, and for non-1-hop-neighbor CHs of BS, the value is calculated by BS according to the feedback of their 1-hop neighbors. The 1-hop neighbors of CH *j* compute the interactive trust between each of them and CH *j* with (5); then, BS evaluates the interactive trust according to the feedback with the beta function:

$$FIT_j(\Delta t)=\lfloor 10\times(f_P+1)/(f_P+f_N+2)\rfloor\tag{6}$$

where *j* represents the destination CH, f_P and f_N denote the number of instances of positive feedback $[IT_{ij}(\Delta t)\ \geq\ 5]$ and negative feedback $[IT_{ij}(\Delta t)5]$ of CH *j*'s 1-hop neighbors, respectively. In order to improve the quality of feedback, BS considers only the feedback of CH *j*'s 1-hop neighbors whose interactive trust in last Δt is larger than or equal to 5. If there are no neighbors that meet this condition, the interactive trust of the CH is set to 5.

Therefore, the interactive trust of CH *j* evaluated by BS *b* denoted as CIT_{bj} (Δt) is calculated as follows:

$$\begin{aligned}&CIT_{bj}(\Delta t)\\&\quad=\begin{cases}IT_{bj}(\Delta t), & j\ is\ the\ 1-hop\ neighbor\ of\ b;\\ FIT_j(\Delta t), & j\ is\ non-1-hop\ neighbor\ of\ b;\end{cases}\end{aligned}\tag{7}$$

Take C4 in Fig. 5 as an example; the interactive trust of C4 is evaluated by C1, C2 and C6 with (5) as 6, 6 and 3, which means the number of positive feedback and negative feedback are 2 and 1, respectively. Therefore, the interactive trust of C4 calculated by BS denoted as CIT_{b4} (Δt) is 6 according to (6) and (7).

2) HONESTY TRUST OF CHs

Similar to interactive trust evaluation, the honesty trust of CHs is evaluated by BS-to-CH evaluation and feedback of 1-hop neighbors of CHs. The direct CH evaluation is executed with (8).

$$\begin{aligned}&HT_{ij}(\Delta t)\\&\quad=\begin{cases}\lfloor 10\times(s+1)/(s+f+2)\rfloor, & when\,f\ =0\\ \left\lfloor 10\times(s+1)/(s+f+2)\times f^{-1/2}\right\rfloor, & when\,f\ \neq 0\end{cases}\end{aligned}\tag{8}$$

where *i* and *j* represent 1-hop-neighbor CHs in WSN, and *s* and *f* denote the number of successful and unsuccessful interactions between them, respectively. CH *i* sends a packet to *k* through *j* and overhears the behavior of *j*; if *j* does not forward the packet in a predefined period or forwards it to another node that is not in the routing table, the interaction is unsuccessful (dishonest); otherwise, it is successful (honest). The trust evaluation of 1-hop-neighbor CHs of BS is directly computed by BS *b* denoted as HT_{bj} (Δt), where $i=b$ in (8).

For CHs that are not 1-hop neighbors of BS, the evaluation is executed by the feedback of their 1-hop neighbors with (8) and (9).

$$FHT_j(\Delta t)=\lfloor 10\times(f_P+1)/(f_P+f_N+2)\rfloor\tag{9}$$

where *j* represents the destination CH and f_P and f_N denote the number of positive feedback $[HT_{ij}(\Delta t)\geq 5]$ and negative feedback $[HT_{ij}(\Delta t)5]$ of CH *j*'s 1-hop neighbors, respectively. Similarly, BS also considers only the feedback of CH *j*'s 1-hop neighbors whose honesty trust in last Δt is larger than or equal to 5.

Therefore, the honesty trust of CH *j* evaluated by BS *b* denoted as CHT_{bj} (Δt) is calculated as follows:

$$\begin{aligned}&CHT_{bj}(\Delta t)\\&\quad=\begin{cases}HT_{bj}(\Delta t), & j\ is\ the\ 1-hop\ neighbor\ of\ b;\\ FHT_j(\Delta t), & j\ is\ non-1-hop\ neighbor\ of\ b;\end{cases}\end{aligned}\tag{10}$$

3) CONTENT TRUST OF CHs

CHs fuse the observing data of SNs in respective clusters and transmit to the BS directly or indirectly through other CHs. Content trust of the CH is evaluated by BS according to the proximity between the fusion data and the effective average observing data of nonhibernating SNs in the cluster; the proximity D_{pj} is defined as:

$$D_{pj}=\left(\sum\nolimits_{k=1}^{d_m}(x_{jk}-x_{jfk})^2\right)^{1/2}\tag{11}$$

where d_m indicates the dimensions of observing data, x_{jk} and x_{jfk} represent the effective average of the *kth*-dimension data of SNs calculated by CH *j* and the *kth*-dimension fusion data of CH *j*, respectively. The CH is required to transmit the effective average and fusion data to BS *b* for content trust evaluation, which is conducted as:

$$CCT_{bj}(\Delta t)=\left\lfloor 10\times\exp(-D_{pj})\right\rfloor\tag{12}$$

where CCT_{bj} (Δt) represents the content trust of CH *j* evaluated by BS *b* in update cycle Δt, and D_{pj} is the proximity calculated by (11).

4) OVERALL TRUST OF CHs

The overall trust of CH j evaluated by BS b is calculated as (13), which aggregates the interactive trust, honesty trust and content trust.

$$COT_{bj} = \lfloor \omega_1 CIT_{bj} + \omega_2 CHT_{bj} + (1 - \omega_1 - \omega_2) CCT_{bj} \rfloor \quad (13)$$

where parameters $\omega_1, \omega_2 \in [0,\ 1]$ are weights for each subtrust value. We consider each subtrust as an equally important trust; thus, parameter $\omega_1 = \omega_2 = 1/3$, and they could be set to different weights according to different occasions.

V. INTRUSION DETECTION BASED ON HIERARCHICAL TRUST

According to the two-tier hierarchical trust mechanism, an intrusion detection method at the SN level and CH level is proposed in this section to discover malicious SNs or CHs. The process of the method is introduced, and then the detection at the SN level and CH level is described.

A. THE MODULES OF THE SYSTEM

The modules of the system include the formation of cluster-based WSN, the evaluation of the hierarchical trust, intrusion detection at different levels and the measures taken after a malicious SN or CH is detected. The process of the method is shown in Fig. 6.

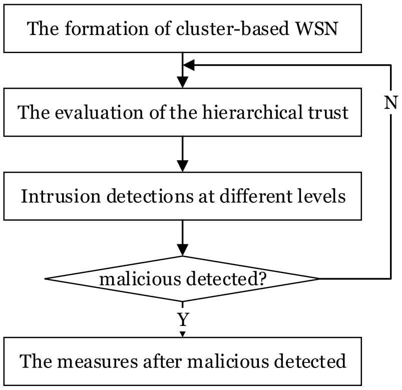
The formation of cluster-based WSN
The evaluation of the hierarchical trust
Intrusion detections at different levels
malicious detected?
N
Y
The measures after malicious detected

FIGURE 6. The process of IDS based on two-tier hierarchical trust.

The task in formation of cluster-based WSN is the partition of clusters after the network deployment, which is not the scope of this work and may be found in [20]. The evaluation of two-tier hierarchical trust is described in detail in Section IV, in which the trust value of SNs is evaluated by their respective CH, and the trust of CHs is calculated by BS, reducing the burden on SNs. Intrusion detection at different levels is introduced in section V-B and section V-C, and the measures taken include alarm, isolation of the malicious SN, re-selection of the CH when malicious CH is discovered, etc., which are not discussed in detail in this work.

B. INTRUSION DETECTION AT SN LEVEL

Malicious SN detection is executed by the respective CH. The CH c evaluates and maintains the trust value of SN j in the same cluster and selects a trust threshold TS^{thi} according to the trust value of SNs in cluster i, which is calculated as:

$$TS^{thi} = \begin{cases} \lfloor avg_{j \in CL \text{ and } SOT_{cj} \geq 5} \{SOT_{cj}\} \rfloor; \ \exists j, & s.t.\ SOT_{cj} \geq 5 \\ 5; & others \end{cases} \quad (14)$$

where i represents the identification of a cluster, CL is the cluster with CH c and SN j, and avg is the average function.

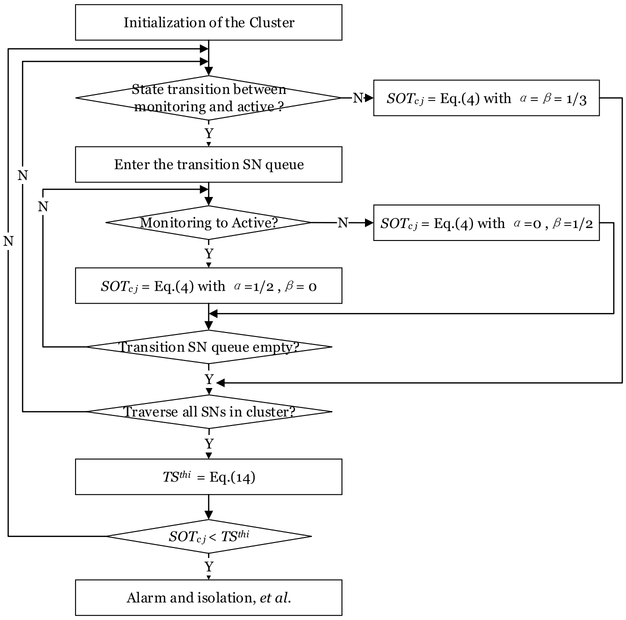
Initialization of the Cluster
State transition between monitoring and active ?
N
SOT_{cj} = Eq.(4) with $\alpha = \beta = 1/3$
Y
Enter the transition SN queue
Monitoring to Active?
N
SOT_{cj} = Eq.(4) with $\alpha = 0$, $\beta = 1/2$
Y
SOT_{cj} = Eq.(4) with $\alpha = 1/2$, $\beta = 0$
Transition SN queue empty?
N
Y
Traverse all SNs in cluster?
N
Y
TS^{thi} = Eq.(14)
$SOT_{cj} < TS^{thi}$
N
Y
Alarm and isolation, *et al.*

FIGURE 7. The process of malicious SN detection by a CH.

According to the state context described in Section IV-B, the trust value of SN who has state transition between monitoring and active is evaluated preferentially, and the process of the calculation and detection is demonstrated in Fig. 7. After the deployment of WSN, the formation and initialization of clusters are conducted. Before evaluating the trust of SNs, a CH observes if there exists state conversion of SNs between monitoring and active. If it exists, the CH calculates the trust of SNs with different parameters according to the state context. Then, the trust of other SNs in the cluster is calculated, and the threshold of SN trust is not selected until all SNs in the cluster are traversed. Finally, the trust of each SN is compared with the threshold, below which the SN is regarded as a malicious one and measures should be taken to avoid its further damage.

C. INTRUSION DETECTION AT CH LEVEL

The intrusion detection at CH level is conducted by BS b, reducing the possibility of being deceived by CHs and decreasing the energy consumption of CHs. The trust calculation of each CH is different from SN since there is no state transition of CHs in this work. Malicious CH detection is similar to malicious SN discovery, which also detects by a threshold of trust of CHs. The BS b computes and maintains the trust value of each CH j and selects a threshold trust TC^{th} as the detection metric, which is computed as follows:

$$TC^{th} = \begin{cases} \left\lfloor avg_{j\in CHS \text{ and } COT_{bj}\geq 5}\left\{COT_{bj}\right\}\right\rfloor; \ \exists j, & s.t.\ COT_{bj} \geq 5 \\ 5; & others \end{cases} \tag{15}$$

where CHS is the set of CH in WSN, and avg is the average function. The BS b compares the trust of each CH in WSN to the threshold calculated by (15) and considers the CH whose trust value is less than the threshold as malicious or compromised. Measures should be taken to reduce harm to the WSN, for instance, isolation of CH and re-election of a new CH, which is not the scope of this work.

VI. EXPERIMENT SIMULATION AND PERFORMANCE EVALUATION

A. DETECTION RATE EVALUATION OF IDSHT

Our experiments are conducted with the NS2 simulator, and we predefine 111 members including 100 SNs, 10 CHs and a base station in cluster-based WSN with 10 clusters deployed randomly in an area of 50 × 50 square meters. All SNs and CHs are stationary, and CHs are predefined whose energy, computation and memories are more than SNs, and the energy, computation and storage of BS is not limited. According to assumptions, part of nodes (we set 70%) are in a monitoring or active state, and the data update cycle is set to 10 seconds, and experiments last for 1000 seconds.

In experiments, 2-dimensional observing data with temperature and humidity as examples are considered. Malicious behaviors including DoS attacks, selective forwarding attacks, tampering attacks and energy exhaustion attacks are simulated. Malicious nodes with DoS attacks perform sending requests and data information constantly, and nodes with selective forwarding attacks forward the receiving packets with a probability of 20%; meanwhile, nodes with tampering attacks tamper the observing data randomly, and the energy exhaustion attack performs communication with other nodes constantly.

The average trust value of normal members and abnormal members in an update cycle is calculated during the experiments; meanwhile, the trust threshold for malicious detection is counted. Fig. 8 demonstrates the average trust value and threshold of normal and abnormal members in 10 update cycles, from which we could see that the average trust value of normal and abnormal members is in the vicinity of 8 and 4, respectively, and the dynamic trust threshold for malicious detection is different in each update cycle. Based on the mechanism we proposed, normal members and abnormal members could be distinguished apparently. The trust value of abnormal members in our mechanism is not decreasing sharply because the trust evaluation combines the interactive, honesty and content trust, and only when all three trust values reduce will the overall trust value decrease significantly.

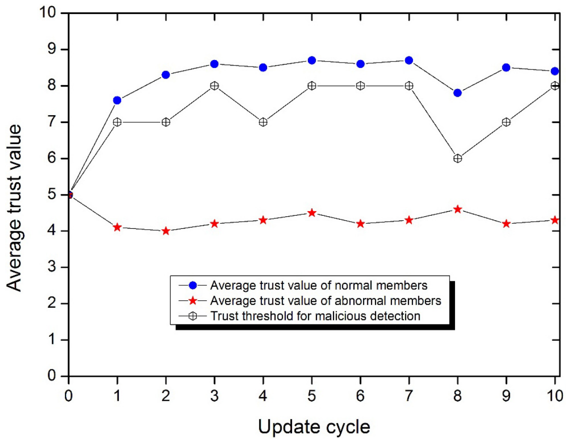

FIGURE 8. The trust value and threshold of normal and abnormal members.

The proposed method IDSHT is compared with DTBID (Distributed Trust based Intrusion Detection) proposed in [14], which also considers multidimensional trust including energy, data and communications, and detects malicious nodes through comparison of subjective and objective trust. But the data trust in DTBID refers to 1-dimensional data, and multidimensional data are not discussed.

For detection of each single attack type, only a type of attack is injected to the network, and the number of malicious members is set to 20% of the whole members, distributed evenly to each cluster. Experiments are executed 10 times independently for detecting each type of attack, the detection rate of which is the average of the results of 10 experiments.

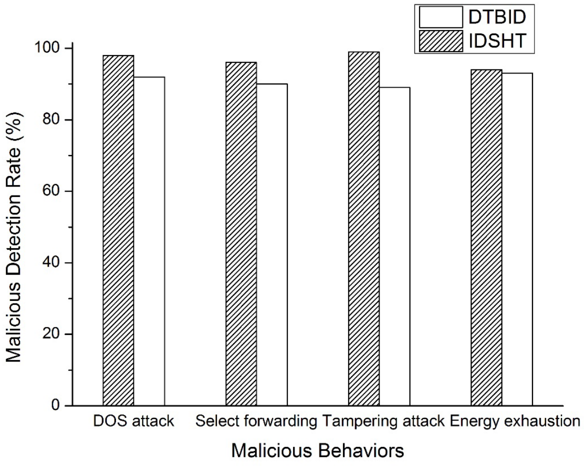

FIGURE 9. Malicious detection rate of different behaviors using IDSHT and DTBID.

Fig. 9 shows the malicious detection rate of different attacks using IDSHT and DTBID. Both methods have a high detection rate for DoS attacks, selective forwarding attacks, tampering attacks and energy exhaustion attacks because both of them consider multidimensional trust factors. However, the detection rate of IDSHT we proposed is higher than that of

DTBID due to more strict punishment in the process of trust calculation. The detection rate of tampering attacks is nearly 100% according to the content trust for both 1-dimensional and multidimensional observing data, whereas DTBID only considers 1-dimensional data.

For the overall detection rate with all types of attacks above, we set the number of malicious members with different attacks as 5%-60% of the whole members with a 5% increase, and the malicious members are distributed evenly in each cluster. Four types of attacks are considered and shown in Fig. 9, and a member could be attacked by one or more attacks simultaneously. Malicious detection with the same number of malicious members is conducted 10 times independently, and the overall detection rate is the average of 10 results. In this process, the overall false positive rate and false negative rate are evaluated simultaneously.

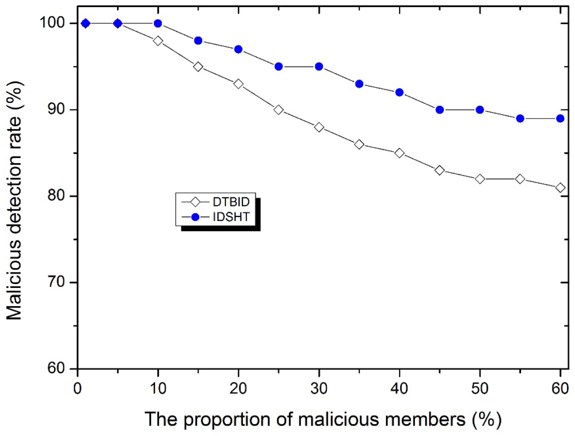

FIGURE 10. Comparison of detection rate of IDSHT and DTBID.

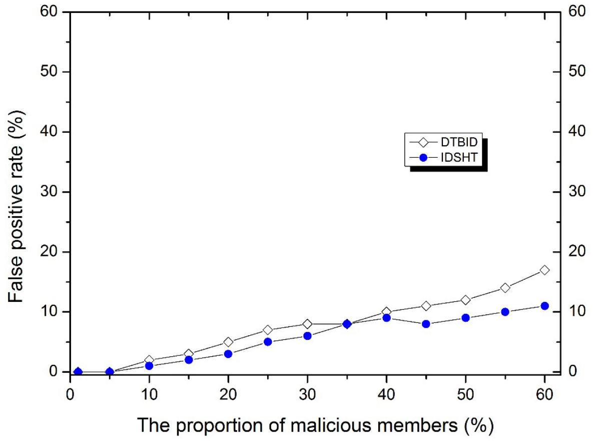

FIGURE 11. Comparison of False positive rate of IDSHT and DTBID.

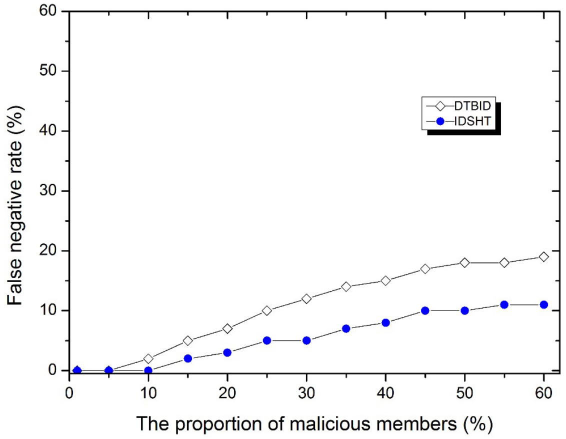

FIGURE 12. Comparison of False negative rate of IDSHT and DTBID.

The comparison of the detection rate of two methods is shown in Fig. 10, which indicates that the detection rate of both methods is decreasing with the increase in the proportion of malicious members. However, the IDSHT maintains a higher detection rate due to the dynamic threshold of trust as shown in Fig. 8, whereas the threshold of difference between subjective trust and objective trust in DTBID is not self-adaptive according to the introduction in [14]. In the simulation, the proportion of malicious members increases from 5% to 60%, and the detection rate of IDSHT and DTBID is decreasing from 100% to 89% and 81%, respectively.

There are two important indexes in intrusion detection systems - false positives and false negatives; the former indicates normal nodes recognized as malicious nodes, and the latter indicates malicious nodes recognized as normal nodes. The false positive rate is defined as the ratio of the number of normal nodes recognized as malicious ones to the number of whole normal nodes. The false negative rate is the ratio of the number of malicious nodes recognized as normal ones to the number of whole malicious nodes. Fig. 11 and Fig. 12 depict the false positive rate and false negative rate of both methods with the increase in proportion of malicious members, from which we can see that both the false positive rate and false negative rate of IDSHT is from 0 to 11%, whereas that of DTBID is from 0 to 17% and 19%, respectively. The false positive rate of both methods is equal when the proportion of malicious members is 35%, just as shown in Fig. 11. The reason is that the dynamic detection threshold in our method is just the same as that of DTBID. There after the false positive rate decreases and grows slowly due to the dynamic detection threshold which is adaptive to the operation of the network. This indicates that the performance of IDSHT is better than that of DTBID because in the simulation, both the false positive rate and false negative rate of IDSHT are lower than that of DTBID. The reason is that the dynamic detection threshold excludes some normal fluctuation in trust value, which makes the system more flexible.

The value of the parameter λ in (1) and (5) has a significant impact on the performance of the system. When the value is small, it will result in a higher false positive rate because some normal interactions exceed the threshold leading to a decrease in trust value. However, when the value is large, it will result in a higher false positive rate and false negative rate because the abnormal interactions are treated as normal ones and become the most trustable, making nodes with normal interactions acquire lower trust values according to (1) and (5).

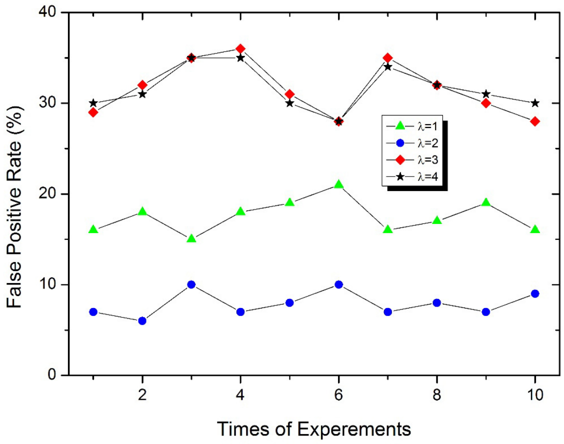

FIGURE 13. The false positive rate according to different λ.

The relationship between the value of λ and the performance of the system is shown in Fig. 13, on the condition that there are 30% malicious nodes in the WSN. From Fig. 13, we could infer that the parameter λ has an impact on the performance of the system, and the false positive rate is around 17%, 8%, 32% and 32% when $\lambda = 1, 2, 3$ and 4, respectively. Therefore, $\lambda = 2$ is the most suitable for our work.

B. OVERHEAD EVALUATION OF IDSHT

In this section, the maximum communication overhead and storage overhead of the proposed IDSHT are analyzed and compared with LDTS [9], which is a lightweight and dependable trust system for clustered WSNs and similar to our work.

1) THE MAXIMUM COMMUNICATION OVERHEAD ANALYSIS

The communication overhead evaluation is conducted on the condition that the WSN is at a heavy load and consumes maximum communication. Here, some variables and assumptions are defined to compute the communication overhead. There are m clusters in WSN, i.e., m CHs and n SNs in each clusters, the communication between which is through packet transmission. According to the assumption described in section III-D, SNs in a cluster communicate with CH directly and the communication between CHs and BS is direct or indirect through other CHs. Therefore, the communication overhead consists of SN with CH, CH with CH and BS with CH.

In a cluster, an SN interacts with its CH by sending a packet and receiving a feedback packet, which means 2 packets transmit during this interaction. Thus, all SNs in the cluster communicate with its CH at the worst occasion, and $2n$ packets are consumed in a cluster. The total number of packets of all m clusters is $2mn$.

The communication between CHs also consists of packet and feedback packet. If a CH communicates with another CH, 2 packets are consumed, and it will cost $2(m-1)$ packets when the CH communicates with all other CHs. Therefore, at the worst condition, it will consume $2(m-1)\,(m-1)$ packets when all CHs communicate with other CHs. Meanwhile, the BS communicating with all CHs will cost $2m$ packets.

Above all, the maximum of the communication overhead of IDSHT in WSN is computed as $2mn+2(m-1)(m-1)+2m$, and the communication overhead of LDTS is computed as $2mn^2 + 2m^2 - 4mn + 2m + 2$, correspondingly.

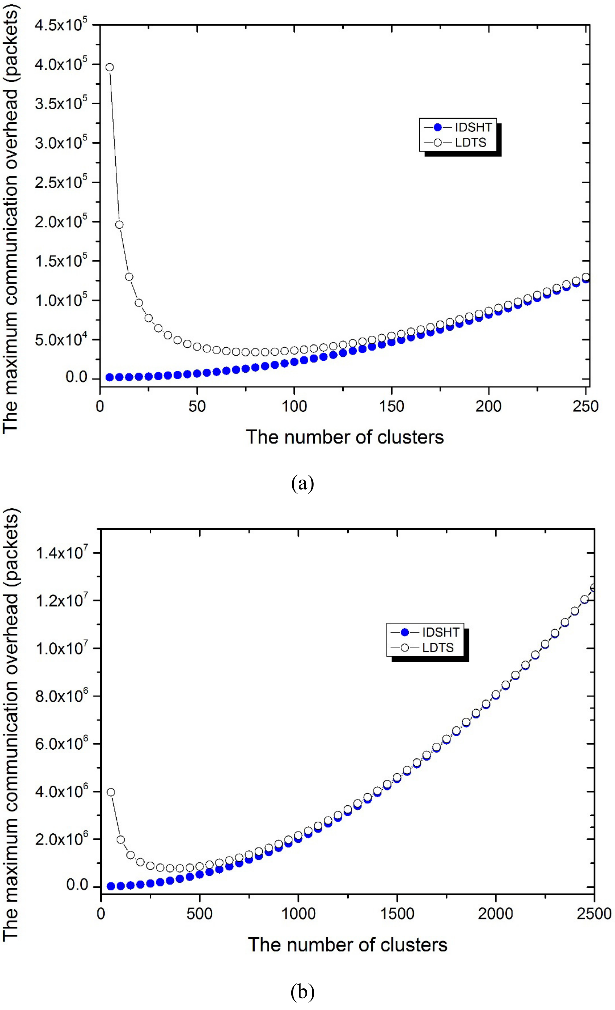

FIGURE 14. Communication overhead with 1,000 nodes (a) and with 10,000 nodes (b).

The comparison of the maximum communication overhead of IDSHT and LDTS is shown in Fig.14 (a) and (b) for the condition where there are 1,000 and 10,000 nodes in clustered WSNs, respectively. The curves in Fig.14 (a) and (b) show that the communication overhead of IDSHT is lower than that of LDTS overall, especially when the number of clusters is at a low level, and the overhead is tending to approach with the increase in the number of clusters and the expansion of the scale of WSNs.

2) THE MAXIMUM STORAGE OVERHEAD ANALYSIS

The SN in each cluster interacts with its CH directly, and it does not need to store information of other SNs in the process of trust evaluation. Therefore, the SN only stores the

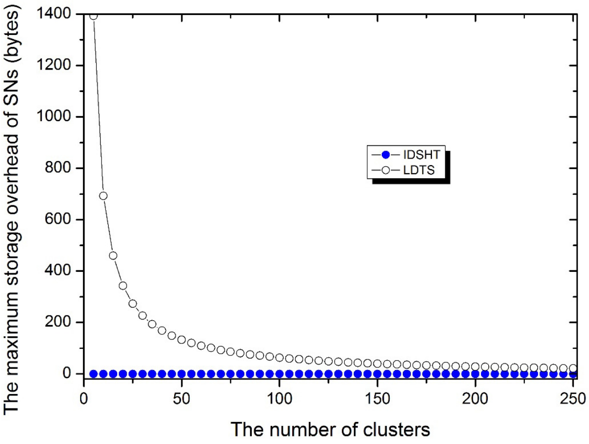

FIGURE 15. Storage overhead of SNs with 1,000 nodes.

ID of itself and the observing data. That means there is no additional storage overhead caused by trust evaluation in SNs, whereas the storage overhead of SNs of LDTS is $7n$, where n represents the number of SNs in a cluster; the reason is that SNs of LDTS have to store the trust information of all other SNs in a cluster.

The comparison of SNs' storage overhead caused by trust evaluation of IDSHT and LDTS is shown in Fig. 15 according to the number of clusters with 1,000 nodes in WSN. Since the trust of SNs in the proposed IDSHT is evaluated by corresponding CH and that of LDTS is calculated by other SNs in a cluster, we could see from Fig. 15 that the storage of SNs of IDSHT is less than that of LDTS, and the larger the number of clusters, the smaller the gap in SNs' storage overhead. The reason is that the number of SNs in a cluster decreases as the number of clusters increases, so the storage of SNs decreases.

The storage overhead of CHs should be considered important because CHs bear the heavier task, including trust calculation of SNs and their 1-hop neighbor CHs and malicious SNs detection. Each CH maintains two databases during malicious detection, including an SN dependent database and a 1-hop-neighbor-CH dependent database. Here, the variable m, n, d_m represent the number of clusters, the number of SNs in a cluster and the dimension of observing data, respectively. The storage of trust value is 0.5 bytes just because we have normalized the trust value to the integer in [0, 10], which could be denoted and stored with 4 bits.

The SN dependent database and 1-hop-neighbor-CH dependent database maintained by each CH during the trust evaluation and malicious detection are shown in Table 2 and Table 3, respectively, which describe the items, storage and relevant implications in detail.

A CH has to store all items in table 2 for each SN except μ, θ, m_{ak}, σ_k, x_{ik}, TQ and TS^{thi} because these seven items are shared in a cluster. Therefore, the total storage of an SN dependent database with n SNs in a cluster is computed as:

$$STOR_{SN-dp} = 18n + 12d_m + 8.5 \tag{16}$$

TABLE 2. The structure of SN dependent database maintained by a CH.

Items	Storage (bytes)	Implications
ID	2	The ID of a SN
w_{ij}	2	The number of interactions between CH i and SN j
μ	4	The mean value of interactions between a CH and SNs that are at the same state in a cluster
θ	4	The significant factor based on the value of w_{ij}
s	2	The number of successful interactions between i and j
f	2	The number of unsuccessful interactions between i and j
m_{ak}	$4d_m$	The mean value of the kth-dimension data of SNs
σ_k	$4d_m$	The standard deviation of the kth-dimension data of SNs
x_{ik}	$4d_m$	The effective average of the kth-dimension data stored in CH i
D_{ij}	4	The Euclidean distance of data between average and j
SIT_{ij}	0.5	The interactive trust of SN j evaluated by CH i
SHT_{ij}	0.5	The honesty trust of SN j evaluated by CH i
SCT_{ij}	0.5	The content trust of SN j evaluated by CH i
SOT_{ij}	0.5	The overall trust of SN j evaluated by CH i
QL	2	The length of data queue
TQ	$2n$	The queue of SNs with state conversion (monitoring - active)
TS^{thi}	0.5	The threshold of malicious SN detection

TABLE 3. The structure of 1-hop-neighbor CH dependent database of a CH.

Items	Storage (bytes)	Implications
ID	2	The ID of a 1-hop-neighbor CH
w_{ij}	2	The number of interactions between CH i and CH j
μ	4	The mean value of interactions between CH and its neighbors
θ	4	The significant factor based on the value of w_{ij}
s	2	The number of successful interactions between i and j
f	2	The number of unsuccessful interactions between i and j
CIT_{ij}	0.5	The interactive trust of CH j evaluated by CH i
CHT_{ij}	0.5	The honesty trust of CH j evaluated by CH i
CCT_{ij}	0.5	The content trust of CH j evaluated by CH i

Similarly, a CH should store all items in table 3 for each 1-hop-neighbor CH except μ and θ since they are shared among neighbors. We assume that all other $m - 1$ CHs are 1-hop neighbors of a CH, which is the worst case, and the CH needs to maintain the information of other $m - 1$ CHs. Therefore, the total storage of a 1-hop-neighbor CH dependent database is computed as:

$$STOR_{CH-dp} = 9.5(m - 1) + 8 \tag{17}$$

Therefore, the overall maximum storage of a CH with trust evaluation is computed by (18) with the sum of (16) and (17).

$$STOR_{overall} = 18n + 9.5m + 12d_m + 7 \tag{18}$$

whereas the storage of a CH in LDTS is computed as $0.5mn^2 + 7(m - 1)$.

The comparison of CHs' maximum storage overhead of IDSHT with 1-dimensional data and LDTS caused by trust evaluation is shown in Fig. 16. We can see that the storage overhead of IDSHT with 1-dimensional data is lower than the overhead of LDTS on the whole, and the overhead tends to approach as the number of clusters increases. With the increase in the dimension of observing data, the storage

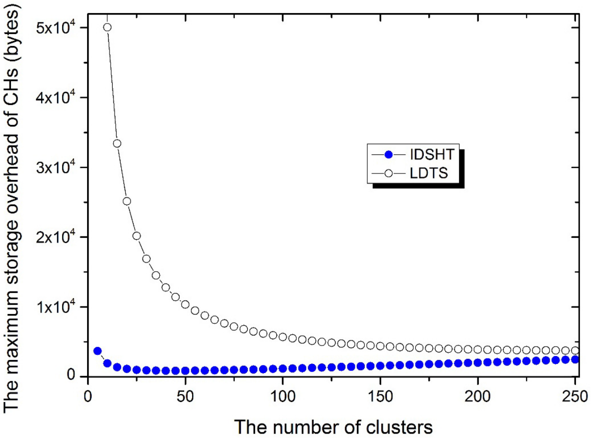

FIGURE 16. **Storage overhead of CHs with 1,000 nodes.**

overhead of CHs in IDSHT is increasing at an extremely low level, essentially constant, so the dimension of observing data almost has no impact on the storage overhead of CHs. This demonstrates that the storage overhead of the proposed IDSHT is better than that of LDTS, especially when the number of clusters is at a lower level.

VII. CONCLUSION

In this article, an intrusion detection mechanism based on state context and hierarchical trust (IDSHT) for cluster-based and constantly changing WSNs is proposed; it considers trust evaluation and the self-adaptation detection threshold. During trust evaluation, factors of communication, multidimensional observing data and state transitions of SNs are considered. Meanwhile, the judgment strength of SNs' trust is reduced by CH-to-SN trust evaluation, whereas the judgment strength of CHs' trust is increased through CH-to-CH, feedback of 1-hop neighbors of CHs and BS-to-CH trust evaluation. Moreover, the mechanism could adapt different weights to evaluate SNs' trust value according to the state transitions, improving the efficiency of the system. Malicious behaviors could be detected based on the trust and dynamic threshold, which improves the adaptability of the system. Simulation results demonstrate that the proposed IDSHT requires less storage and communication overhead compared with existing typical systems, and it performs well in malicious detection with a higher detection rate and lower false positive rate and false negative rate.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Proc. IEEE Int. Conf. Wireless Mobile Comput. Netw. Commun.*, Aug. 2005, pp. 253–259.

[3] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 234–241, 1st Quart., 2014.

[4] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, May 2012.

[5] O. Khalid *et al.*, "Comparative study of trust and reputation systems for wireless sensor networks," *Secur. Commun. Netw.*, vol. 6, no. 6, pp. 669–688, 2013.

[6] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in *Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst.*, Sep. 2006, pp. 437–446.

[7] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 4, pp. 66–77, Oct. 2004.

[8] F. Bao, I.-R. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[9] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.

[10] G. Han, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Trans. Mobile Comput.*, vol. 14, no. 12, pp. 2447–2459, Dec. 2015.

[11] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1164–1175, Nov. 2012.

[12] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 623–632, Jul. 2012.

[13] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 121–132, Apr. 2015.

[14] A. Dhakne and P. Chatur, "Distributed trust based intrusion detection approach in wireless sensor network," in *Proc. IEEE Int. Conf. Commun. Control Intell. Syst.*, Nov. 2015, pp. 96–101.

[15] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, and I. Arenaza, "Reputation-based intrusion detection system for wireless sensor networks," in *Proc. IEEE Complex. Eng.*, Jun. 2012, pp. 1–5.

[16] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage.*, Jun. 2015, pp. 606–611.

[17] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *ACM Sigmobile Mobile Comput. Commun. Rev.*, vol. 6, no. 2, pp. 28–36, Apr. 2002.

[18] M. C. Vuran and I. F. Akyildiz, "Spatial correlation-based collaborative medium access control in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 14, no. 2, pp. 316–329, Apr. 2006.

[19] S. Misra, S. Das, and M. Obaidat, "Context-aware quality of service in wireless sensor networks," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 16–23, Jun. 2014.

[20] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 3, pp. 366–379, Oct. 2004.

[21] F. Hao, G. Min, M. Lin, C. Luo, and L. Yang, "MobiFuzzyTrust: An efficient fuzzy trust inference mechanism in mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2944–2955, Nov. 2014.

ZHIHUA ZHANG was born in 1984. He received the B.Sc. degree in computer science and technology from Beijing Union University in 2008, and the M.Sc. degree in computer application technology from Shijiazhuang Tiedao University in 2011.

He is currently pursuing the Ph.D. degree with the School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include network security with a focus on WSN security.

HONGLIANG ZHU was born in 1982. He received the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China.

He is currently a Vice Director of Beijing Engineering Lab for Cloud Security Technology and Information Security Center of BUPT, where he is also a Lecturer and a Master Supervisor. His current research interests include big data security, cloud computing security, and network security.

SHOUSHAN LUO received the B.Sc. degree in mathematics from Beijing Normal University in 1985, and the M.Sc. degree in applied mathematics and the Ph.D. degree in signal and information processing from the Beijing University of Posts and Telecommunications (BUPT) in 1994 and 2001, respectively.

He is currently a Professor with the School of Cyberspace Security, BUPT, Beijing, China. His research interests include cryptography and information security.

YANG XIN was born in 1977. He received the B.Sc. degree in signal and information system and the M.Sc. degree in circuits and systems from Shandong University in 1999 and 2002, respectively, and the Ph.D. degree in signal and information processing from the Beijing University of Posts and Telecommunications (BUPT) in 2005.

He is currently an Associate Professor with the School of Cyberspace Security, BUPT, Beijing, China. His research interests include big data security, cloud computing security, and network security.

XIAOMING LIU received the B.Sc. degree in applied physics from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2006, and the Ph.D. degree in electronic engineering from the School of Electronic Engineering and Computer Science, Queen Mary University of London, London, U.K., in 2012.

In 2012, he joined the School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include terahertz science and technology, quasi-optical techniques and systems, millimeter and submillimeter wave antenna measurement techniques, and bioelectromagnetics.