IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 5, 2019, accepted March 4, 2019, date of publication March 18, 2019, date of current version April 13, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2905550*

# BLTM: Beta and LQI Based Trust Model for Wireless Sensor Networks

**XIAOLING WU[1,2], JUNJIE HUANG[1], JIE LING[1], AND LEI SHU[3,4], (Senior Member, IEEE)**

[1]School of Computer, Guangdong University of Technology, Guangzhou 510006, China
[2]Key Laboratory of Machine Intelligence and Advanced Computing, Ministry of Education, Sun Yat-sen University, Guangzhou, China
[3]College of Engineering, Nanjing Agricultural University, Nanjing 210031, China
[4]School of Engineering, University of Lincoln, Lincoln LN6 7TS, U.K.

Corresponding author: Jie Ling (jling@gdut.edu.cn)

This work was supported in part by the National Key Research and Development Program under Grant 2016YFB0200602, in part by the project of Guangzhou Science and Technology under Grant 201802010043 and Grant 201807010058, and in part by the Foundation of Key Laboratory of Machine Intelligence and Advanced Computing of the Ministry of Education under Grant MSC-201604A.

**ABSTRACT** To defend against internal attacks in wireless sensor networks (WSNs), building a trust model between sensors nodes has been proved to be an effective way in this paper. The most current trust models only consider communication behavior when calculating direct trust, which is directly calculated based on the interactions between sensor nodes. However, this is not enough because of the various types of attacks. Furthermore, the adverse effect of poor-quality links on the trust value of normal nodes is not discussed in the current trust models. In this paper, we propose a beta and link quality indicator (LQI)-based trust model (BLTM) for the WSNs. First, communication trust, energy trust, and data trust are considered when calculating direct trust. Then, the weight of communication trust, energy trust, and data trust are discussed. Finally, an LQI analysis mechanism is proposed to maintain the accuracy and stability of the trust value of normal nodes in a network with poor-quality links. Compared with other models, e.g., beta-based trust and reputation evaluation system (BTRES), the simulation results show that the BLTM can defend against internal attacks, e.g., DoS attack and data tampering attack which the BTRES cannot resist and can reduce the adverse effect of poor-quality links on the trust value of normal nodes effectively.

**INDEX TERMS** Wireless sensor networks, beta distribution, link quality indicator, trust model.

## I. INTRODUCTION

WSNs are promising areas and have been widely applied in various applications, e.g. gas monitoring [1], smart grid [2], decision fusion [3]–[5], and structural health monitoring [6] etc. However, due to the wireless characteristic of the transmission medium and the openness characteristic of the layout environment, WSNs are vulnerable to attacks. According to the source, attacks in WSNs can be divided into external attacks and internal attacks [7], [8]. Traditional encryption and authentication schemes are mainly used to defend against external attacks [9], but cannot effectively resist internal attacks which are caused by the compromised nodes. Once a node has been compromised, the key will be easily captured by the compromised node.

Building trust model [10], [11] to establish a trust relationship between sensor nodes is one of the most effective ways to defend against internal attacks. At present, many researches have been done on building trust models. For example, an Efficient Distributed Trust Model for WSNs (EDTM) is proposed in [12]. In EDTM, both direct trust and recommendation trust are calculated to evaluate the trustworthiness of a sensor node. Meanwhile, communication trust, energy trust, and data trust are considered when calculating the direct trust and the recommendation trust is selectively calculated according to the number of packets received by the sensor nodes. However, the weight of communication trust, energy trust, and data trust are not discussed in EDTM. In [13], a beta-based trust model for clustering WSNs is proposed. It builds a standard Mahalanobis distance based on five trust features, i.e., packet loss rate, message transmission frequency, message receiving frequency, energy consumption rate, and sensor measurement. The standard Mahalanobis distance is used to assess whether a node is normal or abnormal. To build a security route, a Trust Sensing Based Secure Routing Mechanism for WSNs (TSSRM) is proposed in [14].

The associate editor coordinating the review of this manuscript and approving it for publication was Ranjan Bose.

In TSSRM, the trust level and Quality of Service (QoS) are taken into account when a sensor node selects the next hop node. Inspired by social psychology, the sociopsychological trust models are proposed in [15] and [16]. The trust values of sensors nodes in the models are calculated based on three sociopsychological norms, i.e., ability, benevolence, and integrity. In [17], a trust model based on Dempster-Shaffer (D-S) Theory for WSNs is proposed. Considering the recommendation of neighbor nodes, the weighted D-S theory is used to aggregate the recommendations in the model. D-S theory uses belief function to represent the evidence of recommendations. The model considers both communication trust and data trust when calculating the direct trust, while the energy trust is not considered. A distributed Reputation-based Framework for Sensor Networks (RFSN) is proposed in [18]. It first introduces the reputation of a sensor node, which is the probability of the behavior of a sensor node. Then, a conclusion that the reputation of a sensor node follows the beta distribution has been proved. In RFSN, the trust value of a sensor node is the expectation of the reputation. However, in RFSN, the final trust value of a sensor node only consists of direct trust, while the recommendation trust is ignored. A Beta-based Trust and Reputation Evaluation System for WSNs (BTRES) is proposed in [19]. In BTRES, the trust value of a sensor node is calculated based on beta distribution. Both the direct trust and the recommendation trust are calculated to evaluate the trustworthiness of sensor nodes in BTRES. However, it only considers communication trust in the direct trust, while the energy trust and data trust are ignored. Furthermore, BTRES can only be used in the network which has no packet loss.

Link quality indicator (LQI) is frequently used in wireless network [20] to indicate the stability of the communication links. In other words, LQI represents the quality of a communication link [21]. In IEEE802.15.4 standard, the value of LQI ranges from 0 to 255. In some researches, LQI data is used to build up a mechanism to detect external intrusions which can be launched in a node, or a laptop, or other high-power facilities. To determine the number of active nodes in WSNs, RSSI and LQI data are used in [22]. It collects RSSI and LQI data from the unknown wireless topology. Three different clustering methods are applied to the collected data and the clustering results reflect the number of the active nodes in the network. A Granulometric Size Distribution (GSD) method is proposed in [23] based on the erosion method of mathematical morphology, and the LQI data is collected from the network and the GSD method is used to cluster the data. According the GSD clusters, the number of active nodes can be directly monitored.

From the literatures mentioned above, we can find that: 1) the calculation of direct trust for sensor nodes is mainly based on communication interaction, which is not enough due to the various types of internal attacks. For example, DoS attack can make the energy behavior of a sensor node abnormal and data tampering attack can make the data behavior of a sensor node abnormal. Therefore, three trust metrics, i.e., the communication behavior, the energy behavior and the data behavior should be considered when calculating the trustworthiness of a sensor node. 2) The attacks which exist in the network may be harmful to one trust metric only, or two metrics, or three metrics. The weight of communication trust, energy trust, and data trust in different network environment can affect the accuracy of final trust value of a sensor node. Therefore, how to assign the weight of communication trust, energy trust, and data trust in different network environment needs to be solved. 3) Poor-quality links always exist in the real network environment. However, in current research, the network environment when building up trust model is not discussed. The poor-quality links can do harm to the communication behavior and make an adverse effect on trust value of normal nodes. Therefore, take the link quality into account prior to the calculation of trust value is essential. To solve these problems, we propose a Beta and LQI based trust model (BLTM). In BLTM, the calculation of trust value is based on beta distribution. We consider not only communication trust but also energy trust and data trust when calculating direct trust. Furthermore, an LQI analysis mechanism is proposed to make the trust model more robust in a network environment with poor-quality links. RFSN proves that beta distribution can be used to calculate the trust value of sensor nodes for the first time and BTRES is an improvement of RFSN. Therefore, BTRES is chosen as our main comparison models in this paper. According to the simulation results, the proposed BLTM can represent the trust relationship between sensor nodes more stably and accurately. Furthermore, it can prevent more types of attacks, e.g., DoS attack and data tampering attack.

To this end, the major contributions of our work are summarized as follows:

- A beta distribution and LQI analysis based trust model BLTM is proposed to establish the trust relationship between sensor nodes. Communication trust, energy trust and data trust are considered when calculating direct trust to defend against more types of attacks and the calculation of trust is totally based on beta distribution.
- In this trust model, the weight of communication trust, energy trust, and data trust is discussed to obtain a reliable trust value of a sensor node.
- To reduce the adverse effect of poor-quality links on the trust value of normal nodes, an LQI analysis mechanism is introduced in BLTM. By adding the LQI analysis mechanism, the trust value of normal nodes can maintain stable and accurate in the real network environment.

The rest of paper is organized as follows: In Section II, the network topology and properties of trust model are introduced. In Section III, the overview of BLTM is described. In Section IV, the detailed calculation process of trust value is described. In Section V, the performance of the BLTM is evaluated. Finally, conclusions are made in Section VI.

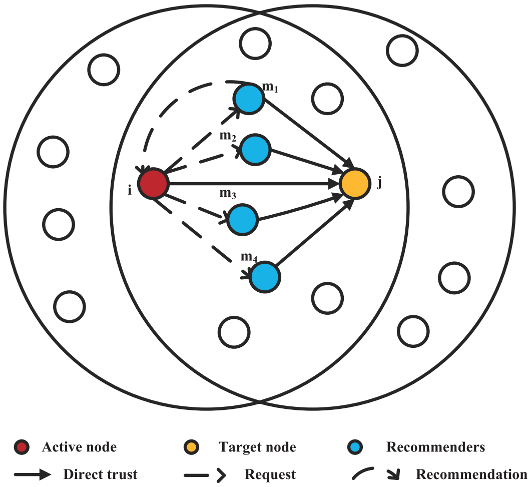

**FIGURE 1.** Network topology.

*Notation:* $P(\cdot)$ refers to the discrete probability as well as continuous probabilistic distribution unless an ambiguity exists; $\Gamma(\cdot)$ denotes the gamma function; $uni(\cdot)$ denotes the uniform distribution; $Bin(\cdot)$ denotes the binomial distribution; $\forall$ means all; $E(\cdot)$ denotes the expectation; $O(\cdot)$ denotes the computational complexity; $|\cdot|$ denotes the absolute value.

## II. NETWORK TOPOLOGY AND PROPERTIES OF TRUST MODEL

In this section, we introduce the network topology and the essential trust properties in the trust model BLTM.

### A. NETWORK TOPOLOGY

In this paper, we assume that all the sensor nodes in the network are randomly deployed without mobility and have the same capability of communication, storage and computation. A homogeneous and static WSN is assumed, where all the sensor nodes stay without mobility and have the same communication range and energy level. The WSNs with non-identical communication ranges and energy levels are not considered in this paper and the effectiveness of the proposed trust model in such networks needs further research. As shown in Fig.1, the network is a multi-hop network. Only when two sensor nodes move into each other's communication range could they communicate with each other. There are three kinds of nodes in the network: active nodes, target nodes, and recommenders. If node $i$ wants to calculate the trust value of node $j$, node $i$ is named as active node and node $j$ is named as target node. Recommenders are the common neighbor nodes between node $i$ and node $j$, which maintain the trust value not less than 0.5, such as nodes $m_1, m_2, m_3, m_4$ shown in Fig.1.

### B. PROPERTIES

#### 1) REPUTATION

If node $i$ wants to predict the behavior of node $j$ for the next event, the concept of reputation is used to describe this prediction. Reputation means the probability of the behavior of a node and is only used to statistically predict the future behavior of other nodes.

#### 2) TRUST

Several definitions are given to trust in [24]. Trust is always defined by reliability, stability, availability, quality of services and other concepts. In this paper, trust is defined as a belief level that one node puts on another node for a specific action according to previous observation of behaviors. Here, trust value is the statistical expectation of the reputation, which ranges from 0 to 1, and can reflect whether a node is normal or abnormal.

#### 3) BETA DISTRIBUTION

Here, the behavior of a node can be described as normal or abnormal. For communication trust, the normal and abnormal behaviors refer to the cooperation and noncooperation of data transmission respectively. For energy trust, the normal and abnormal behaviors refer to the normal energy consumption rate and abnormal energy consumption rate respectively. For data trust, the normal and abnormal behaviors refer to the normal data sequences and the tampered data sequences respectively. Therefore, binomial distribution can be employed to simulate the behavior of a node. For Bayes analysis, the beta function is the conjugate prior for the binomial likelihood distribution, so it can be used to simulate the trust distribution. The beta distribution is indexed by two parameters $(a, b)$ and can be expressed using the gamma function as:

$$P(x) = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1}, \quad \forall 0 \leq x \leq 1 \tag{1}$$

where $a \geq 0$, $b \geq 0$.

Suppose there are $(a + b)$ times of interactions between the nodes. In communication aspect, $a$ and $b$ denote the number of cooperation and noncooperation respectively. In data aspect, $a$ and $b$ denote the number of normal data sequences and the tampered data sequences respectively. In energy aspect, $a$ and $b$ denote the number of times of normal energy consumption rate and abnormal energy consumption rate respectively. Assume that node $i$ wants to predict the behavior of node $j$. The behavior of node $j$ can be denoted as $\sigma$ and complies with uniform distribution, i.e., $P(\sigma) = uni(0, 1) = Beta(1, 1)$. Beta distribution can be used to get the probability of the behavior:

$$P(\sigma) = \frac{Bin(a+b, a) * Beta(1, 1)}{a+b+1} = Beta(a+1, b+1) \tag{2}$$

Eq.(2) shows that the behaviors of nodes are subject to beta distribution.

According to the beta distribution, the reputation of node $j$ maintained at node $i$ can be given by:

$$R_{ij} = Beta(a+1, b+1) \tag{3}$$

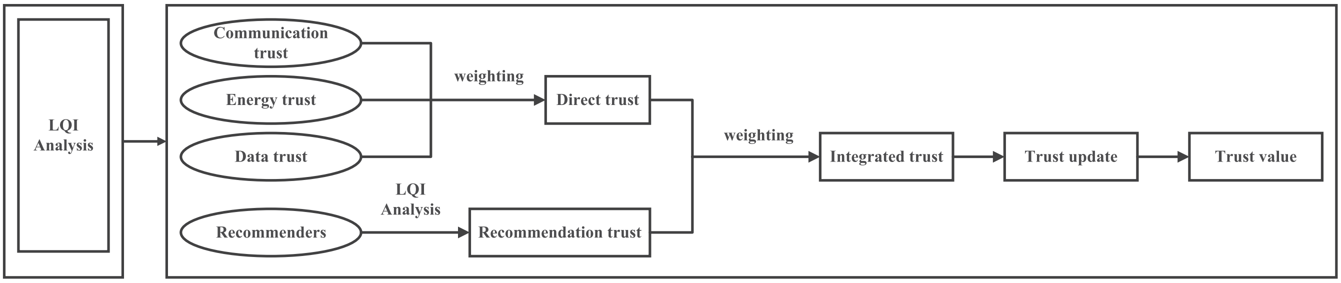

**FIGURE 2.** BLTM structure.

The trust value of node $j$ calculated by node $i$ can be expressed as:

$$Trust_{ij} = E(R_{ij}) = E(Beta(a+1, b+1)) = \frac{a+1}{a+b+2} \quad (4)$$

From Eq.(4), we can see that only two parameters are maintained in the storage of nodes to calculate the trust value. However, the statistics proof is beyond the scope of this paper and interested readers may refer to [18] and [25] for more details.

### C. LQI

The LQI data can be used to assess the channel with a high degree of reliability, but with the minimum possible resources in terms of both time and energy. Therefore, we use LQI data to estimate link quality when calculating trust value. For the most widespread radio (CC2420), LQI is the first eight symbols of the received packet. Based on [26] and [27], the value of LQI in a good quality link is discussed and we choose 220 as the threshold $LQI_{th}$ of LQI value to evaluate whether a link is stable or not. If the average of the LQI data which is collected from the link between two nodes in a certain time cycle is larger than the threshold $LQI_{th}$, the link is stable in that cycle, otherwise, unstable. However, the threshold $LQI_{th}$ should be changed as the environment and applications change and the proper threshold should be related to the false positive rate, false negative rate and etc. How to choose a proper threshold will be our future work.

## III. OVERVIEW OF BLTM

In this section, we introduce the structure of BLTM and the trust calculation process of sensor nodes.

### A. STRUCTURE OF BLTM

The overall structure of BLTM is depicted in Fig.2. BLTM consists of five components: LQI analysis module, direct trust module, recommendation trust module, integrated trust module and trust update module. The trust value of a node contains direct trust and recommendation trust. Since the attacks existing in WSNs are various, it is insufficient to consider the communication trust only. Thus, the direct trust module consists of three metrics in this paper: communication trust, energy trust, and data trust. The direct trust is directly calculated based on interactions between sensor nodes.

Owing to the malicious attacks, it is not enough to consider the direct trust only. So the recommendation trust is calculated to improve the accuracy of the trust value of a node. Recommendation trust is the direct trust of target node calculated by recommenders.

Because the poor-quality links can cause poor interaction between sensor nodes, e.g. packet loss, which can degrade the trust level of normal nodes. So, BLTM contains an important module, i.e., LQI analysis module. LQI analysis module will be triggered when trust calculation cycle begins. The active node will collect the LQI data between itself and the target node during time $t$ which can be expressed as $LQI_1, LQI_2, \ldots, LQI_n$. If the mean value $aver\_LQI$ of the collected LQI data, which equals to $(LQI_1 + LQI_1 + \ldots + LQI_n)/n$, is lower than $LQI_{th}$, we say the link quality between two nodes is poor or unstable. The whole calculation process will terminate and wait for the next calculation cycle to repeat. However, if the link quality between the active node and the target node is good, the calculation process will continue and the recommenders will also do LQI analysis. If the link quality between a recommender and target node is poor, the recommender will not participate the trust value recommendation, i.e., it will not calculate the direct trust of the target node in current calculation cycle.

### B. CALCULATION PROCESS OF BLTM

Firstly, before starting the trust calculation, the LQI analysis module will be triggered. If the link quality between the active node and the target node is poor, current trust calculation cycle will not proceed, and it will wait for the next cycle. Otherwise, the active node calculates the direct trust of the target node and sends requests to the recommenders. The LQI analysis module will be triggered after recommenders receive the requests. Each recommender will do LQI analysis between itself and the target node. After LQI analysis, the recommender which has a poor-quality link between itself and the target node will be excluded. Each residual recommender continues to calculate the direct trust of target node and send the direct trust to the active node. The active node combines these recommended trust values with a certain weight and obtains the recommendation trust. Finally, the active node combines the direct trust and recommendation trust with a certain weight and the integrated trust is obtained.

## IV. TRUST CALCULATION

In this section, we give a detailed description of trust calculation, including the calculation process of direct trust, recommendation trust, and the trust value update.

### A. DIRECT TRUST CALCULATION

To correctly calculate the trust value of malicious nodes, three metrics are considered: communication trust, energy trust, and data trust.

#### 1) COMMUNICATION TRUST CALCULATION

If a malicious node conducts the selective forwarding attack, the number of uncooperative communications will increase significantly. To correctly reflect such attacks in WSNs, the communication trust is needed. According to the beta distribution, the number of cooperative communications $a_c$ and the number of uncooperative communications $b_c$ during time T should be counted. The communication trust can be expressed as:

$$CT = E(Beta(a_c + 1, b_c + 1)) = \frac{a_c + 1}{a_c + b_c + 2} \tag{5}$$

#### 2) ENERGY TRUST CALCULATION

The energy consumption rate of a normal node always maintains a stable value in a clean network. However, malicious nodes which conduct DoS attack will consume energy faster than normal nodes. We use a concept of energy consumption rate $E_{cr}$ to describe the energy consumption in unit time as:

$$E_{cr} = \frac{|E_{t+\Delta t} - E_t|}{\Delta t} \tag{6}$$

where $E_{t+\Delta t}$ represents the residual energy of a sensor node at time $t+\Delta t$ and $E_t$ represents the residual energy of a sensor node at time $t$. When malicious nodes conduct attacks such as flooding and DoS, the value of $E_{cr}$ will behave abnormally.

Assume that node $i$ calculates the energy trust of node $j$. Within time T, node $i$ compares the energy consumption rate of itself with the energy consumption rate of node $j$ in every $\Delta t$ time. The energy consumption rates of node $i$ and node $j$ during $\Delta t$ are denoted as $E_{cri\_\Delta t}$ and $E_{crj\_\Delta t}$ respectively. If $E_{crj\_\Delta t} - E_{cri\_\Delta t} > \epsilon$ where $\epsilon$ is the energy threshold, we say that the energy consumption rate of node $j$ is abnormal, and node $j$ may be a malicious node and conducts DoS attack or other attacks which can result in abnormal energy consumption. However, the energy threshold $\epsilon$ should change with different applications. Count the number of times of normal energy consumption rate $a_e$ and abnormal energy consumption rate $b_e$ within time T. According to beta distribution, energy trust can be expressed as:

$$ET = E(Beta(a_e + 1, b_e + 1)) = \frac{a_e + 1}{a_e + b_e + 2} \tag{7}$$

#### 3) DATA TRUST CALCULATION

The perceptual data of nodes always follows certain distribution, e.g. Gaussian distribution [28], [29]. For simplicity, the perceptual data of nodes in this paper is modeled as a Gaussian distribution. In neighborhood range, the perceptual data of nodes is always similar. If a malicious node conducts data tempering attack, the perceptual data sequences from the malicious node and the normal node will show significant difference. The concept of the significant difference in statistics is used to indicate whether two sets of data are from the same population. For WSNs, in neighborhood range, two data sets which have significant difference can be regarded as that one set is a normal perceptual data sequence, and the other is a tampered data sequence. We use the t-test to verify whether there is a significant difference between two data sets which are collected from two nodes.

Assume that node $i$ calculates the data trust of node $j$. In every $\Delta t$ within time T, node $i$ collects the perceptual data sequences from node $j$ and itself, denoted as $d_{j\_\Delta t}$ and $d_{i\_\Delta t}$ respectively, where $i, j = 1, 2, \ldots, n$. Node $i$ will test these two data sequences using the t-test. According to the t-test, give the hypothesis $H0$ firstly: there is no significant difference between the two sets of data. Then assign the significant level $\rho = 0.05$. If the probability $p(H0)$ for the given hypothesis $H0$ is less than 0.05, the hypothesis will be rejected which indicates that there exists the significant difference between the two sets of data, otherwise, accept the hypothesis. Count the number of times of existing significant difference $b_d$ and those of no significant difference $a_d$. Then, the data trust can be expressed as:

$$DT = E(Beta(a_d + 1, b_d + 1)) = \frac{a_d + 1}{a_d + b_d + 2} \tag{8}$$

According to communication trust, energy trust, and data trust we can derive the direct trust:

$$dir\_Trust = \omega_c CT + \omega_e ET + \omega_d DT \tag{9}$$

where $\omega_c$, $\omega_e$, $\omega_d$ are the weight of communication trust, energy trust and data trust respectively and $\omega_c + \omega_e + \omega_d = 1$.

#### 4) CHOOSE THE WEIGHT

Direct trust contains three parts: communication trust, energy trust, and data trust. How to weigh these three aspects can influence the accuracy of the final trust value. Thus, we give a solution on how to choose the weight of communication trust, energy trust, and data trust. Here, we discuss how to choose the value of $\omega_c$, $\omega_e$, $\omega_d$.

Firstly, if the values of $CT$, $ET$, and $DT$ are all greater than 0.5, the value of $\omega_c$, $\omega_e$, and $\omega_d$ are assigned to 1/3 respectively.

Secondly, if the values of $CT$, $ET$, and $DT$ are all less than 0.5, the value of $\omega_c$, $\omega_e$, and $\omega_d$ are assigned to 1/3 respectively.

Finally, if there exist items in $CT$, $ET$, and $DT$ with the values less than 0.5, the weight of items which have the values greater than 0.5 will be assigned to 0. The weight of the rest items will be assigned evenly, and the sum of the weight must be 1. When there exists a certain factor with the trust value less than 0.5, it means that there exist attacks against this aspect. In this situation, if we still consider the remaining aspects with the trust value greater than 0.5 when calculating direct trust, the attack will be masked by the aspects with the trust value greater than 0.5. This will cause the direct trust value fail to reflect the attacks that exist in the network. For example, assume that we have calculated the value of $DT$ as 0.4, and the value of $CT$ and $ET$ are 0.8 and 0.7 respectively. The trust value indicates that there may exist attacks that tamper the perceptual data. If we still consider communication trust and energy trust when calculating direct trust, the direct trust can be obtained: $\frac{1}{3}(0.4 + 0.8 + 0.7) = 0.63$. The result indicates that the node behaves well and the active node will trust the target node according to the direct trust value. The attack has been masked and the direct trust cannot reflect the trust value of the malicious node correctly.

### B. RECOMMENDATION TRUST CALCULATION

Assume that node $i$ calculates the recommendation trust of node $j$. As mention above, LQI analysis mechanism plays a crucial role in the calculation of recommendation trust. After LQI analysis, the recommender which has poor-quality link between itself and node $j$ will be excluded. Each residual recommender calculates and sends the direct trust of node $j$ to node $i$ respectively. Node $i$ combines these direct trust values with a certain weight. Finally, the recommendation trust of node $i$ is obtained and can be expressed as:

$$rec\_Trust = \sum_{x=1}^{m} \varphi_x \cdot dir\_Trust_{r_x}^{j} \tag{10}$$

where $m$ denotes the number of residual recommenders after LQI analysis, $dir\_Trust_{r_x}^{j}$ represents the direct trust of node $j$ for recommender $r_x$, and $\varphi_x$ denotes the weight of direct trust recommended by recommender $r_x$. $\varphi_x$ can be expressed as:

$$\varphi_x = \frac{dir\_Trust_i^{r_x}}{\sum_{x=1}^{m} dir\_Trust_i^{r_x}} \tag{11}$$

where $dir\_Trust_i^{r_x}$ represents the direct trust of recommender $r_x$ for node $i$.

According to the direct trust and recommendation trust, we can obtain the integrated trust which can be expressed as:

$$int\_Trust = \alpha \cdot dir\_Trust + \beta \cdot rec\_Trust \tag{12}$$

where $\alpha$ and $\beta$ are the weight of direct trust and recommendation trust respectively and $\alpha + \beta = 1$. The weight should be selected depending on specific applications.

### C. UPDATE TRUST VALUE

In WSNs, the network status changes dynamically. A well-behaved node may be compromised at a certain time, and the quality of a link changes according to the environment. Thus, the trust values of sensor nodes also need to change dynamically to reflect the status of the network correctly. We use a concept of the sliding time window to update the trust value of sensor nodes. The time window consists of several time slots and every time slot is an update cycle. In every time slot, the active node will calculate the trust value of the target node and can be expressed as: $int\_Trust(i)$, where $i = 1, 2, \ldots, n$, $n$ denotes the number of time slots. The updated trust value can be expressed as:

$$\begin{aligned} &int\_Trust(i+1)_{update} \\ &\qquad = \delta_i int\_Trust(i) + \delta_{i+1} int\_Trust(i+1) \end{aligned} \tag{13}$$

where $i = 1, 2, \ldots, n$, $\delta_i$ and $\delta_{i+1}$ represent the weight of the historical trust value and current trust value respectively.

The historical trust value reflects the trust value of sensor nodes in the past. The current trust value is the latest trust value of sensor nodes. However, the current trust value is more important and has a higher weight. We define aging factor $\theta$ to describe the damping of trust value, and $\delta_i = \theta$, $\delta_{i+1} = 1 - \theta$. The value of aging factor should be selected depending on specific applications and how important the historical trust is.

### D. COMPUTATIONAL COMPLEXITY

#### 1) TIME COMPLEXITY

We assume that the problem size is $n$. For the calculation of communication trust, $n$ is needed to judge whether the communication is cooperative or uncooperative and the time complexity of communication trust is denoted as $T(n)\_c = O(n)$. For the calculation of energy trust and data trust, $n$ is needed to do comparison and the time complexity of them is denoted as $T(n)\_e = O(n)$ and $T(n)\_d = O(n)$ respectively. When an active node calculates the trust value of a target node, the active node and the recommenders will do the calculation. Therefore, the total time complexity of the calculation of trust value of the target node is $T(n) = O(n^2)$.

#### 2) SPACE COMPLEXITY

For BLTM, two parameters need to be stored: $a$ and $b$ which represent the number of times being normal and abnormal respectively. Therefore, the space complexity of BLTM is $S(n) = O(1)$.

## V. SIMULATION ANALYSIS

Our experiments are performed in Matlab. We implemented two different sets of simulations. First, we evaluate the performance of BLTM with LQI analysis mechanism and without LQI analysis mechanism. Then, we compare the performance of BLTM with BTRES and RFSN in different network environments. We simulate six nodes in the network to verify the model and they are named as node $i$, node $j$, and nodes $m_1$, $m_2$, $m_3$, $m_4$. We set node $i$ as the active node, node $j$ as the target node, and nodes $m_1$, $m_2$, $m_3$, $m_4$ as the recommenders. All sensor nodes are randomly arranged in the sensing area without mobility. The malicious nodes are simulated by three kinds of attacks, i.e., selective forwarding attack, DoS

**TABLE 1. Simulation parameters.**

| Parameters | Value |
|---|---|
| Initial trust value of sensor nodes | 0.5 |
| $LQI\_th$ | 220 |
| $\alpha$ | 0.6 |
| $\beta$ | 0.4 |
| $\theta$ | 0.1 |
| Active node | node $i$ |
| Target node | node $j$ |
| Recommenders | nodes $m_1, m_2, m_3, m_4$ |

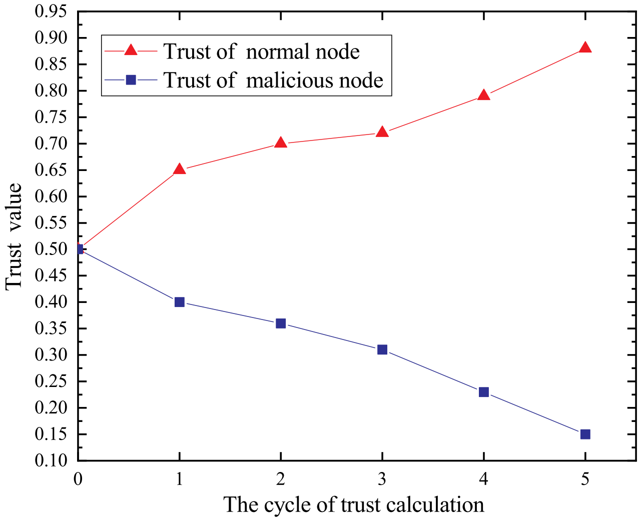

**FIGURE 3.** Trust value of the normal node and malicious node.

attack, and data tampering attack. For better comparison, the parameters are set to be the same as BTRES [19]. Firstly, the trust value of sensor nodes is initialized to 0.5. If the trust value of a node is not less than 0.5, we say the node behaves normal, otherwise, abnormal. However, the standard of being normal or abnormal should depend on specific applications and the selection of value is based on the security level required in specific applications. Then, the weight $\alpha$ and $\beta$ of direct trust and recommendation trust are set to 0.6 and 0.4. Finally, the aging factor $\theta$ of trust value is set to 0.1. The simulation parameters can be found in Table.1.

## A. EFFECTIVENESS OF BLTM

In this section, we verify the effectiveness of BLTM. We mainly focus on the correctness of the trust value of sensor nodes when using BLTM. Experimental results show that BLTM can correctly reflect the trust value of normal nodes and malicious nodes.

### 1) SCENARIO 1: USING BLTM IN A NETWORK WITHOUT POOR-QUALITY LINKS

In this scenario, we set the quality of all links in the network to be good. Node *j* is set to be a normal node and a malicious node respectively. When node *j* is set to be a malicious node, it conducts three types of attacks at the same time. The trust value of target node $j$ is shown in Fig.3. The result shows that in a good-quality link environment, BLTM can reflect the trust value of the target node correctly when the target node behaves good and malicious.

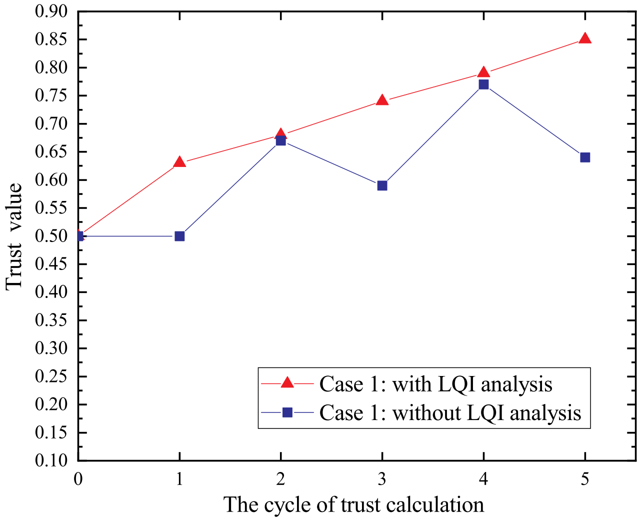

**FIGURE 4.** Trust value of normal node *j* in case 1.

### 2) SCENARIO 2: USING BLTM IN A NETWORK WITH POOR-QUALITY LINKS

We assume that there are poor-quality links in the network and node *j* is set to be a normal node. Then, we assume that there are three cases in this scenario. In each case, the trust values of sensor nodes are calculated by BLTM with LQI analysis and without LQI analysis respectively. Through the results, we can see if BLTM with LQI analysis can reduce the adverse effect of poor-quality links on trust value of normal nodes.

- Case 1. Within all calculation cycles, the link quality between active node *i* and target node *j* is set to be good and it is also good between recommender $m_4$ and node *j*. For recommenders $m_1$, $m_2$, and $m_3$, the link quality between each of them and node *j* is set to be poor in calculation cycle 1, 3, and 5 respectively. The calculated trust value of node *j* in the scenarios of BTLM with LQI analysis and BLTM without LQI analysis are shown in Fig.4.
- Case 2. The link quality between node *i* and node *j* in cycle 1, 3, and 5 is set to be poor respectively, while it is good between each recommender and node *j* in all cycles. The calculated trust value of node *j* in the scenarios of BTLM with LQI analysis and BTLM without LQI analysis are shown in Fig.5 respectively.
- Case 3. The link quality between node *i* and node *j* is set to be poor in cycle 1, 3, and 5. For recommenders $m_1$, $m_2$, and $m_3$, the link quality between each of them and node *j* is also set to be poor in all cycles, while it is good between recommender $m_4$ and node *j* in all cycles. The calculated trust value of node *j* in the scenarios of BTLM with LQI analysis and BTLM without LQI analysis are shown in Fig.6.

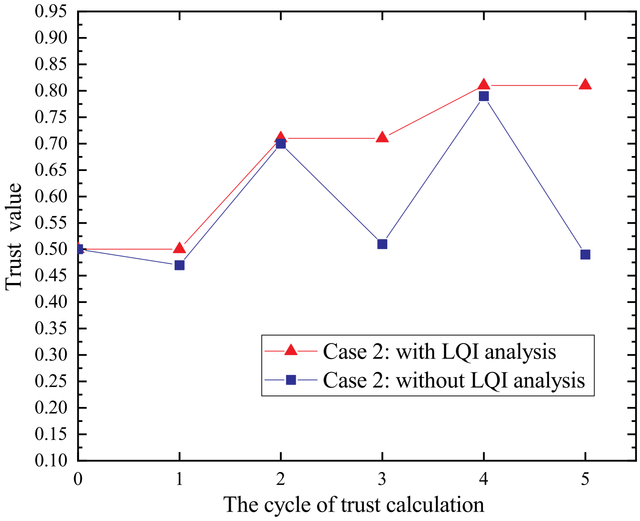

**FIGURE 5.** Trust value of normal node *j* in case 2.

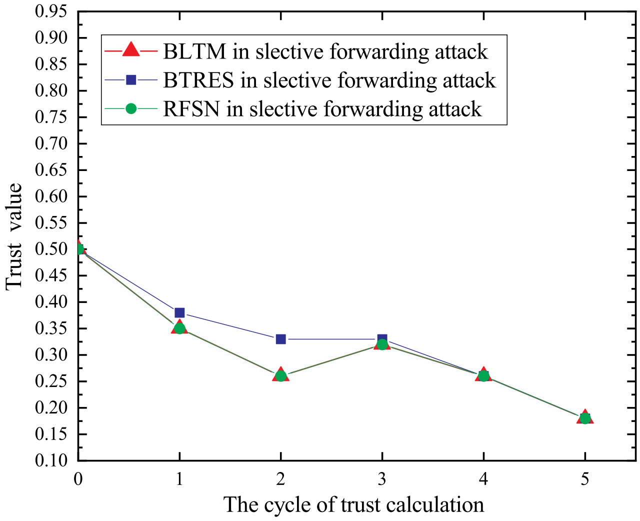

**FIGURE 7.** Trust value of node *j* under selective forwarding attack.

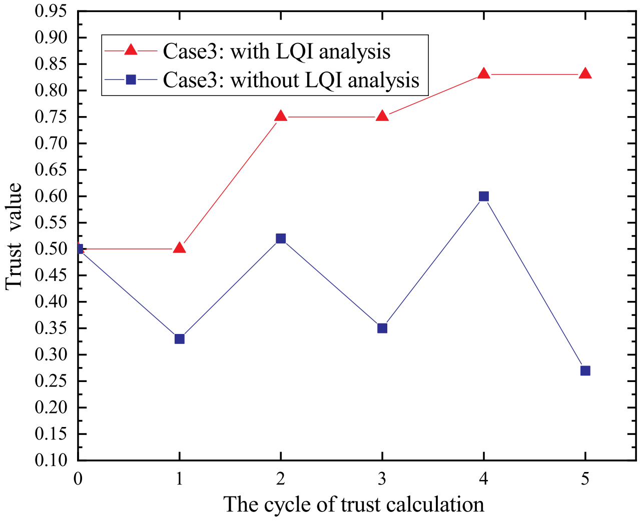

**FIGURE 6.** Trust value of normal node *j* in case 3.

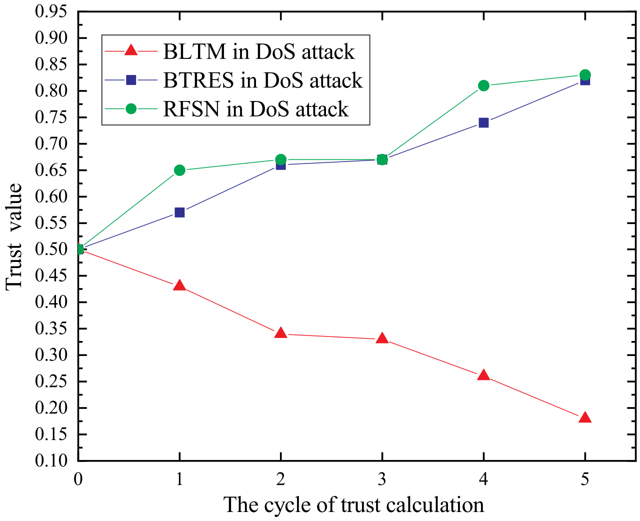

**FIGURE 8.** Trust value of node *j* under DoS attack.

The results in Fig.4 to Fig.6 show that the trust values of normal nodes fluctuate significantly in the scenario of BLTM without LQI analysis when there are poor-quality links in the network. The results indicate that the poor-quality link can adversely affect the trust value of a normal node, and even mistakenly regard a normal node as a malicious node. However, with LQI analysis, BLTM can effectively reduce the adverse effect of poor-quality links, and the trust value of normal nodes can maintain stable and accurate.

### B. COMPARISON OF TRUST MODELS

In this section, we compare the performance of BLTM with RFSN and BTRES. In a network environment with poor-quality links, we compare their performance when the target node behaves well. The results show that the proposed BLTM outperforms the other two trust models.

#### 1) COMPARISON OF TRUST MODELS UNDER SELECTIVE FORWARDING ATTACK

With the same network environment as BTRES which has no packet loss, target node *j* is set to be a malicious node and conducts selective forwarding attack only. The selective forwarding attack can make the number of failed communications increase. The calculated trust value of node *j* is shown in Fig.7. The result shows that the models perform well and can correctly reflect the trust value of malicious node which conducts selective forwarding attack.

#### 2) COMPARISON OF TRUST MODELS UNDER DOS ATTACK

With the same network environment as BTRES which has no packet loss, target node *j* is set to be a malicious node and conducts DoS attack only. The DoS attack can make the energy of a malicious node consume faster than a normal node. The calculated trust value of node *j* is shown in Fig.8.

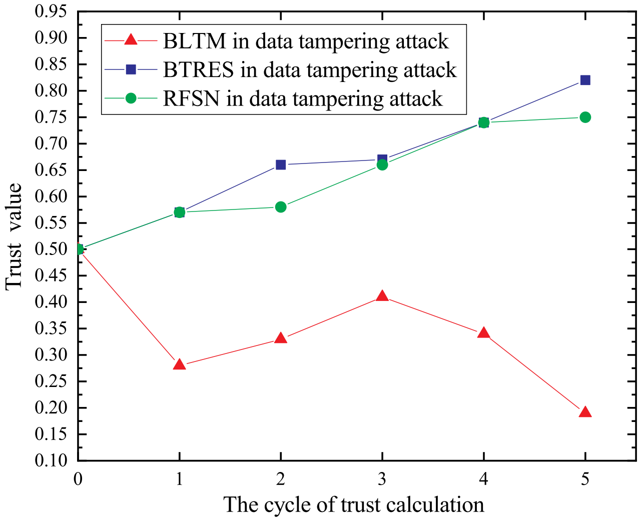

**FIGURE 9.** Trust value of node *j* under data tampering attack.

The result shows that BLTM can correctly reflect the trust value of malicious node *j*, while the trust values of a malicious node calculated by BTRES and RFSN are similar to a normal node. BTRES and RFSN cannot detect the DoS attack which influences the energy aspect adversely because they only consider the communication aspect.

### 3) COMPARISON OF TRUST MODELS UNDER DATA TAMPERING ATTACK

With the same network environment as BTRES which has no packet loss, target node *j* is set to be a malicious node and conducts data tampering attack only. The data tampering attack can result in significant differences between two data sequences from a malicious node and a normal node respectively. The calculated trust value of node *j* is shown in Fig.9. The result shows that the proposed BLTM can correctly reflect the trust value of malicious node *j*. However, because data tampering attack only affects the perceptual data when the communication between two nodes is normal, BTRES and RFSN reflect the trust value of a malicious node the same as a normal node.

### 4) COMPARISON OF TRUST MODELS UNDER TWO TYPES OF ATTACKS

With the same network environment as BTRES which has no packet loss, target node *j* is set to be a malicious node and conducts DoS attack and data tampering attack at the same time. The calculated trust value of node *j* is shown in Fig.10. The result shows that the proposed BLTM can correctly reflect the trust value of a malicious node *j* which conducts two attacks at the same time. However, BTRES and RFSN reflect the trust value of the malicious node incorrectly because they only consider the communication aspect. When the attacks conducted by the malicious node do not affect communication, BTRES and RFSN cannot detect such attacks.

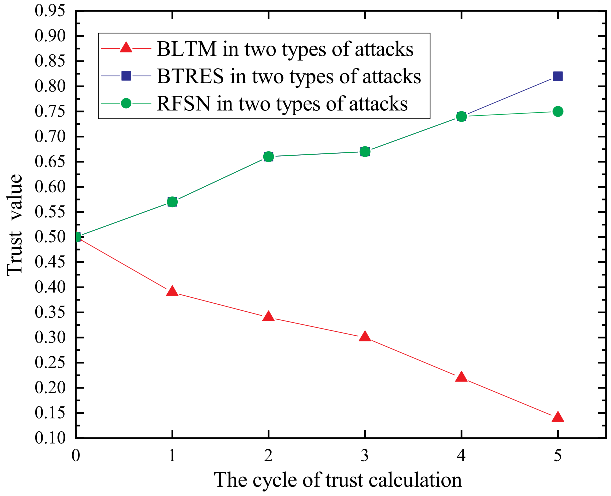

**FIGURE 10.** Trust value of node *j* under two types of attacks.

### 5) COMPARISON OF TRUST MODELS UNDER THREE TYPES OF ATTACKS

With the same network environment as BTRES which has no packet loss, target node *j* is set to be a malicious node and conducts three types of attacks: selective forwarding attack, DoS attack, and data tampering attack at the same time. The calculated trust value of node *j* is shown in Fig.11. The result shows that the trust value of the malicious node calculated by the trust models is less than 0.5. BTRES and RFSN can detect such kind of attacks which affect the communication aspect adversely e.g. the selective forwarding attack. However, the trust value of the malicious node calculated by BTRES and RFSN only reflects selective forwarding attack, but cannot reflect the other two types of attacks, i.e., DoS attack and data tampering attack.

### 6) COMPARISON OF TRUST MODELS IN A NETWORK WITH POOR-QUALITY LINKS

In this section, we compare the performance of BLTM with RFSN and BTRES in a network environment where poor-quality links exist. Meanwhile, the target node *j* is set to be a normal node. We assume that there are two situations.

- Situation 1. We set the link quality between active node *i* and target node *j* to be poor in the calculation cycles 1, 3, and 5 respectively, while it is good between each recommender and target node *j* in all cycles. Three trust models are used to calculate the trust value of node *j* respectively, and the calculated trust value of node *j* is shown in Fig.12.
- Situation 2. The link quality between active node *i* and target node *j* is set to be poor in cycles 1, 3, and 5. For recommenders $m_1$, $m_2$, and $m_3$, the link quality between each of them and node *j* is set to be poor in all calculation cycles, while it is good between recommender $m_4$ and node *j* in all calculation cycles. Three trust models are used to calculate the trust value of node *j* respectively. The calculated trust value of node *j* is shown in Fig.13.

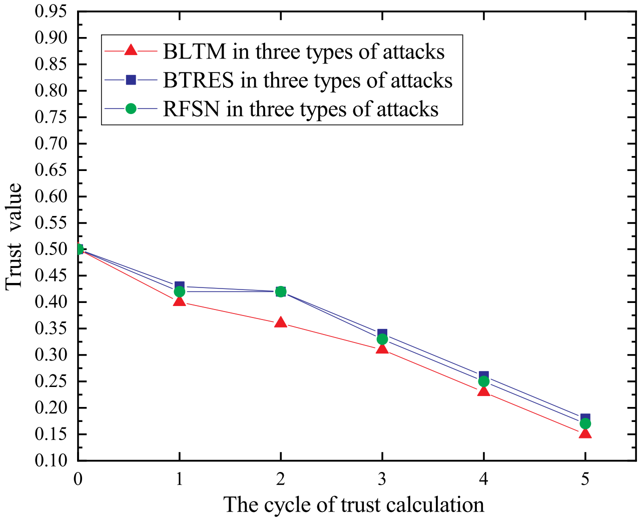

**FIGURE 11.** Trust value of node *j* under three types of attacks.

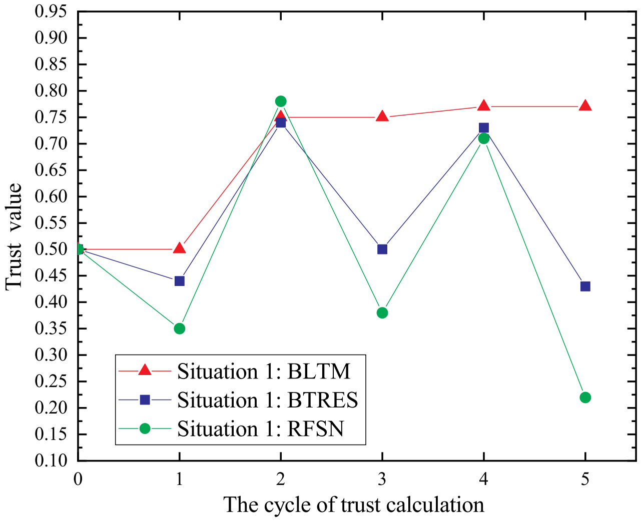

**FIGURE 12.** Trust value of node *j* in situation 1.

The results of these two situations show that the trust value of a normal node calculated by BLTM can maintain stability and accuracy in a network with poor-quality links even though the poor-quality links take the majority of proportion. Due to the LQI analysis module, the adverse effect of the poor-quality links on trust value of a normal node can be reduced effectively in BLTM. However, BTRES and RFSN cause the trust value of a normal node to fluctuate dramatically and cannot alleviate the adverse effect of the poor-quality links on the trust value of a normal node because of the lack of LQI analysis mechanism. Due to the lack of recommendation trust, the volatility of RFSN is even greater than BTRES. In BTRES and RFSN, the failed communications which are caused by the poor-quality links will be considered as that caused by the attacks and the normal node may be mistakenly regarded as a malicious node with a great probability. From the results, we can see that the BLTM

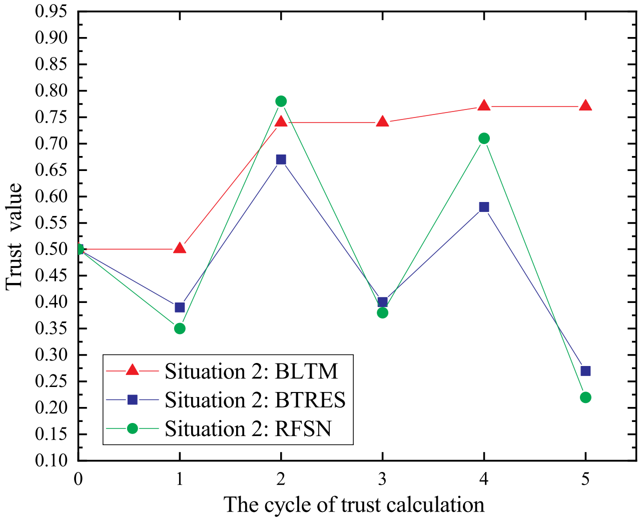

**FIGURE 13.** Trust value of node *j* in situation 2.

outperforms BTRES and RFSN when calculating the trust values of normal nodes in the network environment with poor-quality links.

## VI. CONCLUSION

In WSNs, trust model can effectively help recognize the normal nodes and malicious nodes. Thus, it is an effective way to defend against the internal attacks. We proposed BLTM in this paper to establish a trust relationship between sensor nodes. In BLTM, the direct trust consists of communication trust, energy trust, and data trust. We discussed how to weight communication trust, energy trust, and data trust. An LQI analysis module was introduced in BLTM to reduce the adverse effect of poor-quality links on the trust value of normal nodes. Compared with the existing schemes BTRES and RFSN, BLTM can defend against the internal attacks which not only adversely affect communication but also energy and data. By using BLTM, the adverse effect of poor-quality links on trust value of normal nodes can be reduced. Even in a network environment with a large proportion of poor-quality links, BLTM still works well, and the trust value of normal nodes can maintain stable and accurate. We will further improve our work by generalizing the proposed BLTM to mobility models and the heterogeneous networks with non-identical communication ranges and energy levels. The conjunction of the BLTM and the cryptographic schemes, such as SERP, SIA, SPINS etc., will also be considered to provide a complete solution for highly integrated sensor networks. How to correctly evaluate the trust values of malicious nodes which coexist with poor-quality links in the network and how to select the proper value of the weight and the threshold will also be our future work.

## REFERENCES

[1] M. Mukherjee, L. Shu, L. Hu, G. P. Hancke, and C. Zhu, "Sleep scheduling in industrial wireless sensor networks for toxic gas monitoring," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 106–112, Aug. 2017.

[2] S. Kurt, H. U. Yildiz, M. Yigit, B. Tavli, and V. C. Gungor, "Packet size optimization in wireless sensor networks for smart grid applications," *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2392–2401, Mar. 2017.

[3] D. Ciuonzo, A. Buonanno, M. D'Urso, and F. A. N. Palmieri, "Distributed classification of multiple moving targets with binary wireless sensor networks," in *Proc. 14th Int. Conf. Inf. Fusion*, Jul. 2011, pp. 1–8.

[4] D. Ciuonzo, G. Romano, and P. S. Rossi, "Channel-aware decision fusion in distributed MIMO wireless sensor networks: Decode-and-fuse vs. Decode-then-fuse," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 2976–2985, Aug. 2012.

[5] P. S. Rossi, D. Ciuonzo, and T. Ekman, "HMM-based decision fusion in wireless sensor networks with noncoherent multiple access," *IEEE Commun. Lett.*, vol. 19, no. 5, pp. 871–874, May 2015.

[6] P. Guo, X. Liu, S. Tang, and J. Cao, "Enabling coverage-preserving scheduling in wireless sensor networks for structural health monitoring," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2456–2469, Aug. 2016.

[7] A. Ghosal and S. Halder, "A survey on energy efficient intrusion detection in wireless sensor networks," *J. Ambient Intell. Smart Environ.*, vol. 9, no. 2, pp. 239–261, Feb. 2017.

[8] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.

[9] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2643–2655, Oct. 2016.

[10] Q. Jing, T. Li-Yong, and C. Zhong, "Trust management in wireless sensor networks," *J. Softw.*, vol. 19, no. 7, pp. 1716–1730, 2008.

[11] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, May 2014.

[12] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.

[13] W. M. Tong, J. Q. Liang, L. Lu, and X. J. Jin, "Intrusion detection scheme based node trust value in WSNs," *Syst. Eng. Electron.*, vol. 37, no. 7, pp. 1644–1649, Jul. 2015.

[14] D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma, and Q. Ding, "Research on trust sensing based secure routing mechanism for wireless sensor network," *IEEE Access*, vol. 5, pp. 9599–9609, 2017.

[15] H. Rathore, V. Badarla, and S. Shit, "Consensus-aware sociopsychological trust model for wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 12, no. 3, pp. 21:1–21:27, Aug. 2016.

[16] H. Rathore, V. Badarla, and K. J. George, "Sociopsychological trust model for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 62, pp. 75–87, Feb. 2016.

[17] V. B. Reddy, S. Venkataraman, and A. Negi, "Communication and data trust for wireless sensor networks using D-S theory," *IEEE Sensors J.*, vol. 17, no. 12, pp. 3921–3929, Jun. 2017.

[18] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, pp. 66–77, May 2008.

[19] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 59, pp. 88–94, Jan. 2016.

[20] T. Liu and A. E. Cerpa, "Data-driven link quality prediction using link features," *ACM Trans. Sensor Netw.*, vol. 10, no. 2, pp. 37:1–37:34, Jan. 2014.

[21] G. Hu, "A link quality evaluation model based on the three-dimensional space in wireless sensor network," *Inf. Technol. J.*, vol. 13, no. 4, pp. 720–724, Jan. 2014.

[22] Y. Wang, I. G. Guardiola, and X. Wu, "RSSI and LQI Data clustering techniques to determine the number of nodes in wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 10, no. 5, Mar. 2014, Art. no. 380526.

[23] Y. Wang, X. Wu, and H. Chen, "An intrusion detection method for wireless sensor network based on mathematical morphology," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2744–2751, Oct. 2016.

[24] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279–298, 2nd Quart., 2012.

[25] *Beta Distribution From Mathword*. Accessed: Feb. 3, 2019. [Online]. Available: http://mathworld.wolfram.com/BetaDistribution.html

[26] N. Baccour *et al.*, "Radio link quality estimation in wireless sensor networks: A survey," *ACM Trans. Sensor Netw.*, vol. 8, no. 4, pp. A:1–A:34, Sep. 2012.

[27] H. Du, Q. Li, G. Ding, Y. Wang, and L. Zhu, "The research of AODV routing protocol based on link quality and node energy in WSN," *Chin. J. Sens. Actuators*, vol. 29, no. 7, pp. 1042–1048, Jul. 2016.

[28] M. Rabbat and R. Nowak, "Distributed optimization in sensor networks," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw.*, Apr. 2004, pp. 20–27.

[29] K. Shao, F. Luo, N. X. Mei, and Z. T. Liu, "Normal distribution based dynamical recommendation trust model," *J. Softw.*, vol. 23, no. 12, pp. 3130–3148, Dec. 2012.

**XIAOLING WU** received the B.S. and M.S. degrees from the Harbin Institute of Technology, Harbin, China, in 2001 and 2003, respectively, and the Ph.D. degree from the Department of Computer Engineering, Kyung Hee University, South Korea, in 2008. From 2008 to 2012, she was a Senior Engineer with the R&D Center, ATLab Inc., South Korea. Since 2012, she has been with the Guangzhou Institute of Advanced Technology, Chinese Academy of Sciences, as an Associate Professor. She is currently an Associate Professor with the School of Computer, Guangdong University of Technology, and an Evaluation Expert in Guangdong and Guangzhou Bureau of Science and Technology. Her research interests include wireless sensor networks, touch sensing, and the IoT security.

**JUNJIE HUANG** received the bachelor's degree in computer science and technology from Shaoguan University, in 2015. He is currently a Postgraduate Fellow with the School of Computer Science, Guangdong University of Technology. His current research interest includes the key technologies in wireless sensor networks.

**JIE LING** received the Ph.D. degree in computer science from Sun Yat-sen University, China, in 1998. He is currently a Professor with the School of Computer Science, Guangdong University of Technology. His main research interests include computer applications and intelligent video processing technology.

**LEI SHU** (M'07–SM'15) received the B.Sc. degree in computer science from South Central University for Nationalities, China, in 2002, the M.Sc. degree in computer engineering from Kyung Hee University, South Korea, in 2005, and the Ph.D. degree from the Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland, in 2010. Until 2012, he was a Specially Assigned Researcher with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University, Japan. He is currently a Distinguished Professor with Nanjing Agricultural University, China, and a Lincoln Professor with the University of Lincoln, U.K, where he is also the Director of the NAU-Lincoln Joint Research Center of Intelligent Engineering. He has published more than 380 papers in related conferences, journals, and books in the area of sensor networks. His main research interests include wireless sensor networks and the Internet of Things. He was awarded the Globecom 2010, the ICC 2013, the ComManTel 2014, the WICON 2016, and the SigTelCom 2017 Best Paper Awards, the 2017 and 2018 IEEE Systems Journal Best Paper Awards, the 2017 *Journal of Network and Computer Applications* Best Research Paper Award, the Outstanding Associate Editor Award of the 2017 IEEE Access, the 2014 Top Level Talents in ''Sailing Plan'' of Guangdong Province, China, and the 2015 Outstanding Young Professor of Guangdong Province, China. He served as the Co-Chair for more than 50 various international conferences/workshops, e.g., IWCMC, ICC, ISCC, ICNC, and Chinacom, especially the Symposium Co-Chair for IWCMC 2012 and ICC 2012, the General Co-Chair for Chinacom 2014, Qshine 2015, Collaboratecom 2017, DependSys 2018, and SCI 2019, the TPC Chair for InisCom 2015, NCCA 2015, WICON 2016, NCCA 2016, Chinacom 2017, InisCom 2017, WMNC 2017, and NCCA 2018, and a TPC Member of more than 150 conferences, e.g., ICDCS, DCOSS, MASS, ICC, Globecom, ICCCN, WCNC, and ISCC. He has been serving as an Associate Editors for the IEEE Transactions on Industrial Informatics, the *IEEE Communications Magazine*, the *IEEE Network Magazine*, the IEEE Systems Journal, the IEEE Access, the IEEE/CAA Journal of Automatic Sinica, and *Sensors*. Currently, his H-index is 43 and i10-index is 162 in Google Scholar Citation.