SPECIAL SECTION ON ARTIFICIAL INTELLIGENCE AND COGNITIVE COMPUTING FOR COMMUNICATION AND NETWORK

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 1, 2019, accepted March 6, 2019, date of publication March 12, 2019, date of current version March 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2904544

An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks

JIN ZHAO[1], JIFENG HUANG[1], AND NAIXUE XIONG[1,2]

[1]College of Information Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, China
[2]Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK 74464, USA

Corresponding author: Jifeng Huang (jfhuang@shnu.edu.cn)

ABSTRACT Wireless sensor networks (WSNs) are vulnerable to many security threats from compromised nodes, and because the WSNs are resource-constrained, the traditional security methods cannot be used to resist the internal attacks from compromised nodes. The trust and reputation evaluation system is the most effective security mechanisms to protect WSNs from internal attacks. The exponential-based trust and reputation evaluation system (ETRES) is proposed for WSNs' node trust and reputation evaluation. ETRES is used to observe the nodes' behavior, and exponential distribution is applied to represent the distribution of nodes' trust. The trust of the node is used to look for reliable nodes to transmit data and weaken malicious attacks within the wireless sensor networks. More significantly, the entropy theory is used to measure the uncertainty of direct trust values in this paper. Indirect trust is introduced to strengthen interaction information when the uncertainty of direct trust is enough high. It can not only reduce the computing power of nodes but also prolong the lifetime of the network. In addition, the confidence factor is redefined, which can dynamically adjust the node trust value to weaken the harmful effects of the compromised nodes. The simulation results show that the proposed system can more effectively defend the internal attack than the beta-based trust and reputation evaluation system (RFSN) and the binomial-based trust management System (BTMS). The proposed method can be used to strengthen network security by selecting reliable nodes. What is more, the information trust and energy are prone to integrate into ETRES.

INDEX TERMS Wireless sensor networks, trust and reputation evaluation system, exponential distribution, internal attacks.

I. INTRODUCTION

Wireless sensor networks (WSNs) are multi-hop self-organizing distributed sensor network, which consists of hundreds of tiny sensor nodes with sensing capabilities. Commonly, sensor nodes are deployed randomly in unattended areas and terrible environments to perform various complex tasks [1], [2]. WSNs have the ability to acquire process and transmit data and play a significant role in various fields. Such as battlefield surveillance [3], the smart city [4]–[7], healthcare monitoring, intrusion detection, emergency response [8], [9], etc. Unfortunately, the network is more prone to be attacked due to wireless characteristics of WSNs [10], [11]. For example, lack of central authority, distributed cooperation mechanisms, etc. In some cases, the compromised nodes are converted to the legitimated nodes by capturing normal nodes' cryptographic keys [12]. It can bring enormous damage to the network. In addition, once the legitimated nodes become the compromised nodes, the availability and integrity of the network may be damaged by intercepting, deleting, or inserting information in the network.

Information security is designed to protect information systems or information resources from various types of attacks. In WSNs, attacks can be divided into two categories: internal attacks and external attacks. The current literature shows that the internal attack of the wireless sensor network is far more harmful than the external attack [13]–[15]. In fact, although the security mechanism of authentication and protocol can resist external attack effectively, it has little effect on internal attacks [16]. Internal attacks are launched by misbehaving nodes or selfish nodes in WSNs. By the selfish nodes, we mean that it refuses to service requests to

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

save energy. Although selfish nodes cannot launch an attack on WSNs actively, they may give rise to a great disaster to the Internet. Therefore, it is necessary to establish an effective scheme to solve these problems.

At present, the trust management system is an effective way to resist internal attacks. Trust is a multidisciplinary concept, which is characterized by uncertainty and by contextual independent [17]. Trust is also derived from the social science and inherited from human behavior [18], [19]. Inspired by the related literature [20]–[22], we consider that trust is the belief level of an entity that another entity may perform its tasks as expected. If the node is more prone to transmit the received packet continually, it is regarded to be credible and has a good reputation, as a result, its requests are more prone to be accepted. Trust management systems are mainly used to quantify trust and describe the credibility, reliability, or ability of an entity. Apart from this, a large number of the most advanced models have been mentioned in WSNs [23]–[29]. Obviously, the current research findings have greatly promoted the development of related research, but there are still some shortcomings. For example, some researchers have improved trust management system based on beta distribution to enhance the accuracy of trust assessment. Some researchers take little notice of assigning the confidence factor subjectively, which results in inaccurate trust assessment. Others only combine direct and indirect observation to calculate trust without considering the limited energy. It may reduce the lifetime of the network.

In view of the above problems, we proposed an effective exponential-based trust and reputation evaluation system in this paper, short for ETRES. In our proposal, the trust and reputation of the node are represented by the exponential distribution. The performance of trust evaluation of the algorithm is enhanced by improving the related factors allocation scheme. Firstly, we adopt the exponential distribution to represent the nodes' trust and reputation. Secondly, the direct trust is calculated from the interaction records and the indirect trust is computed until the level of uncertainty of direct trust is enough high. The entropy theory is utilized to access the level of uncertainty. The method of assigning weight is proposed to deal with the problem of assigning weight subjectively. Finally, we incorporate a confidence factor into our method to get the total trust. The trust of the node is explored for the scheme of data aggregation. The node with high trust is select reliable relay nodes to transmit data, which can reduce the risk of internal attacks in the network. Furthermore, the proposed method is conveniently incorporated into the existing network. Compared with the existing trust model based on the beta distribution, the exponential distribution represents the time interval of independent random events, which indicates that it can depict the interaction record in the time dimension. What is more, it only uses the time interval between two neighbor cooperation to evaluate trust without considering other states exist in the interaction between nodes. Generally speaking, the main contributions of the paper are as follows:

(1) In our proposal, the exponential distribution is first explored to express trust and reputation. Compared with beta distribution, the exponential distribution only uses the time interval between two adjacent collaboration to calculate trust without considering other states exist in the interaction between nodes. It means that the proposed method is more reasonable to reflect the trust of nodes.

(2) The entropy theory is utilized to access the level of uncertainty. When uncertainty is high, the indirect trust is integrated into the direct trust to strengthen the credibility of trust. It not only effective save the computing power of nodes but also has low energy consumption, which can prolong the service life of the network.

(3) The method of assigning weight is proposed to deal with the problem of assigning weight. In our proposal, the calculation of the confidence factor is redefined, which based on the number of cooperation between nodes. The confidence factor is closely related to the direct trust. When compromised nodes perform bad interactions, the confidence factor will force the direct trust to drop rapidly.

The deployment of the paper is as follows. Section II shows the related work. Section III describes the proposed trust and reputation evaluation system in detail. Section IV talks performance analysis and comparison. Section V discusses the conclusion.

II. RELATED WORK

Reputation is defined to mean the evaluation of a target node by a neighbor node to perform a task, while trust is an entity value generated by reputation. On account of the historical record, it reflects positively and negatively. Trust management systems are segmented into two categories, trust model and trust management scheme. Currently, there are many trust models, such as the entropy trust model, fuzzy logic trust model, D-S evidence trust models, and Game Theory trust models [30], [31]. At the same time, a large number of trust models are proposed in WSNs' to observe node behaviors and resist internal attacks from compromised nodes. Some of them are discussed as follows.

With respect to the trust management scheme, Xia *et al.* [32] used an information theoretic framework to quantitatively measure trust and design a novel trust model with multiple trust decision factors. These factors are integrated to represent trust relationship's uncertainty and inhomogeneity from various angles. However, the weight of these factors is undefined in this scheme; Furthermore, renewing a node's trust for next decision-making costs more energy. Wang and Pang [33] utilized a light-weight trust model which considers data aggregation and communication failure due to wireless channels. Direct trust is evaluated by successful or unsuccessful interactions and similar or dissimilar data comparisons. It takes communication ability, the lifetime of node and consistency of data to compute the overall trust value. It costs more energy in computing the trust of the node. Furthermore, the detection rate of the compromised node is not considered. Wang *et al.* [34] firstly proposed a sensor with a changeable sampling frequency, and its control algorithm. The system is established on the basis of multiple factors (e.g. data factor and energy factor et. al.). The scheme gives the reward coefficient of the revised data and the penalty coefficient of the erroneous data. A combined trust model is used to describe the relationship of nodes and the importance of the multiple factors, and the trust value between nodes is calculated by weighting. The proposed model has a low fault detection rate and detects the fault in time duration. Furthermore, it does not take into account energy consumption. Fang *et al.* [35] established a beta-based trust and reputation evaluation system to describe WSNs' node trust and reputation evaluation. The proposed system is based on observing nodes' actions, and the beta distribution is utilized to represent the distribution of nodes' credibility. The overall trust value of the node is used to select relay nodes, mitigating internal attack risks. The method can effectively resist the internal attack of compromised nodes. However, it does not take into account node energy, computation, memory constraints. Luo *et al.* [36] put forward a trust management system for clustered WSNs to keep watch on the sensor nodes' behaviors and evaluate their trust values. Identification labels of sensor nodes are generated by employing a hash algorithm to distinguish external attackers from normal nodes. The compromised nodes are detected by dynamically managing the trust value of each node. The scheme results show that it can detect the malicious nodes quickly, which resists malicious attacks. However, the scheme seems not to detect the malicious nodes quickly, which prevents clustered WSNs from external attacks and internal compromised nodes' attacks. Fang *et al.* [37] proposed a time window-based resilient trust management scheme resisting the reputation time-varying attack in WSNs. In the system, on the basis of beta distribution, the behaviors of compromised nodes are analyzed for a period of time, and the difference of judgment and the trend analysis are used to detect abnormal reputation value of nodes. The control factor and the time window are incorporated to confirm and remove the malicious nodes. It can defend reputation time-varying attacks effectively, but the energy efficiency is not integrated into the trust evaluation system. Based on the above analysis of the trust management system, we find that a large number of trust management schemes mainly focus on a specific behavior; what's more, most of them are inclined to neglect the energy of the node.

With regard to the trust model, Anita *et al.* [38] presented 2-ACKT protocols with 2-ACKT-1 and 2-ACKT-G to establish trust with low communication overhead and memory requirement. The proposed scheme computes the direct trust using a link layer acknowledgment and a two-hop acknowledgment from a downstream neighbor. The trust is calculated by the sensor node based on the number of successful interactions of the data forwarding behavior of a neighbor. The scheme outperforms the conventional multi-hop and trust-based routing schemes in terms of packet delivery ratio, network lifetime, communication overhead, and memory requirements. However, it costs a lot of energy and increases the time complexity. Umarani [39] established an enhanced beta trust model to find a malicious attack. The neighbor node is selected by the sensor node based on trust information in the course of communication. The state of the neighbor node is periodically updated. The recovery procedure is incorporated to raise the throughput of the network. The scheme not only improves the collaboration among sensor nodes by trust value, but also increases the lifetime of the network by the recovery procedure. However, it does not take into account the use of energy and memory constraints to build trust models. Labraoui [40] used a trust model based on risk evaluation to effectively deal with conflicting behaviors of malicious nodes. Reputation is evaluated based on direct and indirect observation, and a cumulative evaluation of long-term behavior. The risk is assessed on the basis of mutual information. Risk factor evaluation can enable the trust model more reliable due to it becomes more sensitive to malicious attacks. It can detect on-off attack effectively but does not consider more attacks in a mobile environment. Ganeriwal *et al.* [41] proposed a Distributed Reputation-based Framework for WSNs (RFSN). There are two key building blocks in RFSN, watchdog and reputation system, respectively. The watchdog is used to observe behaviors of neighbor nodes and rate their behaviors as cooperative or non-cooperative. The reputation system is utilized to maintain the reputation of a node. An aging mechanism is established for trust updating, consequently, a node's trustworthiness is reconsidered continuously. Obviously, it assumes that each node has enough interactions with neighbor nodes so that reputation can reach stationary. More importantly, the RFSN scheme only propagates good reputation information about other nodes. Unfortunately, sensor nodes cannot defend malicious attacks because they cannot share their bad reputation information with each other. The effectiveness of the proposed method is testified by simulation experiments. Many scholars have put forward various improvement schemes based on the scheme and achieved good experimental results. From the perspective of the trust model, currently, a great deal of trust model is improved based on the beta distribution. Furthermore, there are still numerous scholars integrate beta distribution to propose a new method for resisting the internal attack. It seems that trust management schemes are improved by a novel mathematical distribution to improve trust management schemes.

The existing trust management system is complex. Not only the calculation and storage requirements of sensor nodes are high, but also the scope of application is limited. In this paper, an effective exponential-based trust and reputation evaluation system is proposed. The system enables the algorithm of the trust evaluation system simpler and more effective to resist the internal attack. It is noteworthy that the scheme is conveniently incorporated into the existing network.

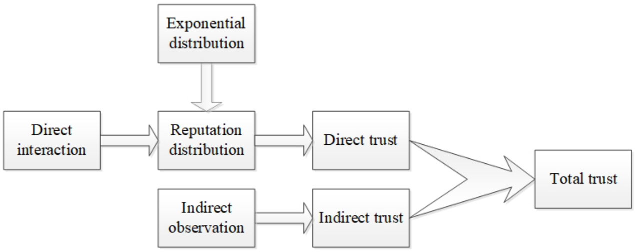

FIGURE 1. The process of the trust assessment.

III. THE PROPOSED TRUST AND REPUTATION EVALUATION SYSTEM

In this part, a novel trust and reputation evaluation system based on the exponential distribution is proposed for WSNs, which named an effective exponential-based trust and reputation evaluation system (ETRES). When nodes need to interact, nodes will decide whether to interact with another node based on trust. The trust assessment process is illustrated in Figure 1.

A. TRUST AND REPUTATION MODELING

The trust and reputation of the node are represented by the beta distribution among the related trust systems [18], [42], which assumes that only the cooperation and the non-cooperation in the process of interaction between nodes. Aiming at avoiding the existing states between interactions, the time interval between two adjacent collaboration is used to represent the trust and reputation of the node. Furthermore, we derive the expression of the nodes' trust and reputation according to the relationship between beta distribution and exponential distribution. In order to simplify the model of trust and reputation, we divide the behavior of nodes into two categories in two adjacent collaboration, namely, cooperation and non-cooperation. Undoubtedly, it is not adopting the potential hypothesis, because trust and reputation mainly depend on the cooperation between nodes. We assume that interaction between the nodes has remained $(a + b)$ times. The modeling as follows.

$$f(p) = exponential(x = a) = \frac{1}{(a+b)p} e^{-\frac{a}{(a+b)p}} \tag{1}$$

where variable a and b represents the number of successful interactive behaviors and unsuccessful interactive behaviors of the node, respectively. P represents the probability of successful cooperation. Obviously, node i holds about the reputation distribution of node j, marked as R_{ij}, the representation is as follows.

$$R_{ij} = \frac{1}{(a+b)p} e^{-\frac{a}{(a+b)p}} \tag{2}$$

Since $f(p)$ is the probability distribution of reputation p, the maximum of the function is used to express the maximum probability of p. Thus, we defined the maximum value of the function as the trust value of the node. This process can be expressed by formulas 3-5.

$$f'(p) = [\frac{1}{(a+b)p} e^{-\frac{a}{(a+b)p}}]' = 0 \tag{3}$$

After the derivation, we can get the maximum of the above function, which is represented as follows.

$$p = \frac{a}{a+b} \tag{4}$$

Trust is represented by the maximum value of the reputation distribution [33], [37], [41]. Consequently, the node's trust is defined as,

$$T_{ij} = \frac{a}{a+b} \tag{5}$$

In order to verify the effectiveness of the algorithm, we should proof the trust will still converge regardless of the increase in the number of malicious nodes. The proof is as follows.

$$\lim_{b\to 0} \frac{a}{a+b} = 1, \quad \lim_{b\to\infty} \frac{a}{a+b} = 0 \tag{6}$$

Formula (6) represents the function of trust is bounded. We verify the monotonicity of the function of trust by formula (7).

$$T'_{ij} = (\frac{a}{a+b})' = -\frac{1}{(a+b)^2} \tag{7}$$

Obviously, $T'_{ij} < 0$, it indicates that the function is strictly monotone decreasing. According to the Monotone Convergence Theorem, the function of trust will still converge regardless of the increase in the number of malicious nodes.

B. TRUST AND REPUTATION EVALUATION SYSTEM MODELING

On the basis of the above modeling, we get an expression of the nodes' reputation and trust, which based on the exponential distribution. Now, we will build a trust and reputation system to resist attacks from the network. The detailed process of building trust and reputation system is as follows.

1) INTRODUCTION OF ENTROPY

Entropy is a key concept in information theory. It is a measure of uncertainty in random events. Entropy reflects the degree of order of a system, and the higher the entropy, the lower the degree of order. Normally, the entropy of a random variable x is represented as follows.

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \tag{8}$$

where $p(x)$ represents the probability density function of random variables x. The entropy function is a symmetric function in its definition domain [0,1]. As shown in Figure 2, the probability of a random event x_i is denoted by $p(x_i)$. When $p(x_i) = 0$ (or $p(x_i) = 1$), $H(x) = 0$. It means that a random event x_i will (or will not) occur without uncertainty. Contrarily, when $p(x_i) = 0.5$, $H(x)$ take the maximum value. It means that a random event is completely uncertain under any conditions.

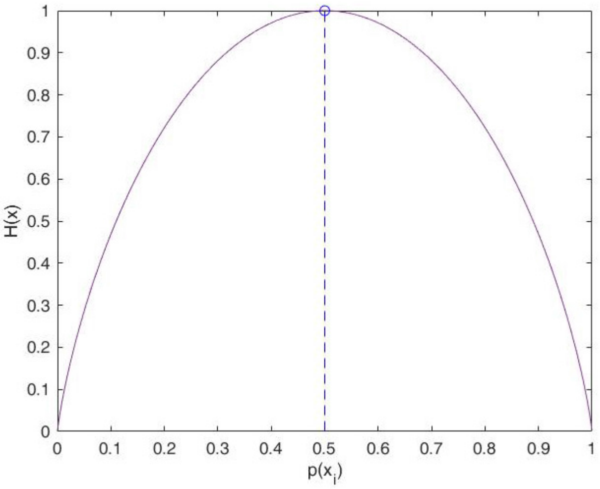

FIGURE 2. Function plot of H(x).

2) DIRECT TRUST

Direct observation is an interactive record between two entities obtained by observation without a third party. The direct trust is originated from the direct observation between node i and node j, which is represented as D_{ij}. Where node i or node j represents an index between nodes.

Due to the exponential distribution denotes the probability of the time interval between two adjacent events occurring, the exponential distribution is adopted as the prior distribution of interactions between nodes. Supposing that the future interacts in the same way as the former, we can represent the direct trust as follows.

$$D_{ij} = \frac{a}{a+b} \tag{9}$$

3) DIRECT TRUST UPDATE

Assume that the reputation indicator of node i and node j is founded between nodes. The interaction between node i and node j requires $(m+n)$ times, where m indicates the number of successful interactions and n expresses the number of unsuccessful interactions. The reputation of the node j is updated. The representation is as follows.

$$R_{ij}^{new} = \frac{1}{(a+m+b+n)p} e^{-\frac{(a+m)}{(a+m+b+n)p}} \tag{10}$$

As we can see from the above, the reputation update is only related to two parameters.

$$a^{new} = a+m, \quad b^{new} = b+n \tag{11}$$

4) WEIGHT ASSIGNMENT

More weight should be given to up-to-date interactive information. Thus, the added weight value can be represented as below.

$$a^{new} = (s_{age} \times a) + m, \quad b^{new} = (s_{age} \times b) + n \tag{12}$$

where s_{age} is weight, $0 < s_{age} < 1$. The weight ensures that all nodes interact together. The reasonable weight value makes the historical reputation weight decreased gradually. Furthermore, the nodes need to successful interaction together to maintain a good reputation.

5) JUDGEMENT OF DIRECT TRUST

Direct trust and indirect trust are considered within the conventional method, which costs more extra energy and enables the load of resource-constrained wireless sensor nodes heavy. Inspired by human social relations, if the level of uncertainty goes down to a low level, it is unnecessary to consider the recommendation of others. That is to say, direct observation is able to execute the trust assessment. Entropy theory is a concept in the realm of thermodynamics, statistics, and information theory [42]. It is the measurement of uncertainty or information quantity in a random signal or event [18]. Therefore, assume $H(D_{ij})$ is the entropy of direct observation and thr is the threshold of non-determinacy. The setting of the threshold is closely related to the security of the network system. The greater the entropy threshold, the lower the system security. If $thr \leq H(D_{ij}) \leq 1$, which expresses that the non-determinacy of direct trust is high and more related information is needed, then the indirect trust calculation is introduced. If not, the total trust that node i holds about node j is simply set to direct value, i.e. $OT_{ij} = D_{ij}$.

6) INDIRECT TRUST

When a node is deemed as ''uncertain,'' the recommendation from third parties is required. The assessing node i obtains the recommendation of node j through their common neighbor nodes k, marked as N_k. Node i has a prior reputation distribution of common neighbor nodes k already. Node i sends an inquiry message to its neighbors and the common neighbors are shared by node i and node j send back their interaction records with (a_{kj}, b_{kj}) in response. Accordingly, the reputation of node i and node j can be represented as (a_j, b_j). The working mechanism can be illustrated with the help of the flow diagram shown in Figure 3. The circles express the communication range of node i and node j, respectively. More notably, the communication range of selecting neighbor nodes is one-hop.

Assume the recommendation offered by the common neighbor nodes k is R_{ij}^k. Given (a_{kj}, b_{kj}) and (a_{ik}, b_{ik}), the recommendation trust value is calculated as follows, where (Ra_{ij}^k, Rb_{ij}^k) is the recommendation interaction record, Ra_{ij}^k represents the cooperation interaction record by the common neighbor nodes observes. Rb_{ij}^k represents the noncooperation interaction record by the common neighbor nodes observes.

$$Ra_{ij}^k = a_j + \frac{a_{ik}}{a_{ik}+b_{ik}} \times a_{kj} \tag{13}$$

$$Rb_{ij}^k = b_j + \frac{a_{ik}}{a_{ik}+b_{ik}} \times b_{kj} \tag{14}$$

$$R_{ij}^k = \frac{Ra_{ij}^k}{Ra_{ij}^k + Rb_{ij}^k} \tag{15}$$

According to the information that node i have, not every recommendation is reliable and trustless feedback cause

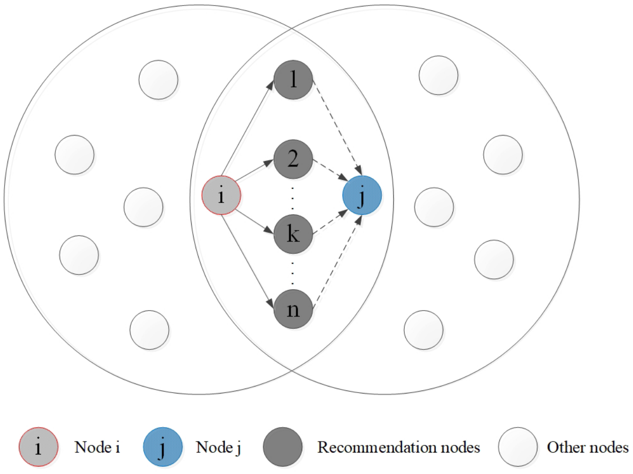

FIGURE 3. **The conveying path of recommendation.**

error outcome. Apparently, it is significant to estimate the credibility of recommenders to ensure accuracy in calculating indirect trust. Only the recommendations from dependable nodes are acceptable. The trust levels of node i towards recommender k, which is symbolized as follows.

$$T_{ik} = \frac{a_{ik}}{a_{ik} + b_{ik}} \tag{16}$$

Assume there are r advisers and their trust values held by node i are marked as $T_{i1}, \cdots, T_{i(r-1)}, T_{ir}$. If $T_{ik} \geq \chi$, the recommendation from node k is utilized. Oppositely, it will be completely ignored. Where $\chi (0 \leq \chi \leq 1)$ is a self-defined threshold, and $k = 1, 2 \ldots, r$. In our proposed model, we assign weights based on the trust level of recommenders to mitigate the impact of personal preference. The following method is proposed to compute the weight of R_{ij}^k.

$$s_k = \frac{T_{ik}}{\sum\limits_{k=1}^{q} T_{ik}}, \quad k = 1, 2, \cdots, q. \tag{17}$$

where $s_k (0 \leq s_k \leq 1, \sum_{k=1}^{q} s_k = 1)$ is the weight of R_{ij}^k. q is the number of received recommendations. The indirect trust is as follows.

$$ID_{ij} = \sum_{k=1}^{q} s_k \times R_{ij}^k \tag{18}$$

7) TOTAL TRUST AGGREGATION

The total trust value OT_{ij}, which node i holds about node j, is utilized via the following expression.

$$OT_{ij} = \begin{cases} D_{ij} & 0 \leq H(D_{ij}) < thr \\ \alpha \times D_{ij} + (1 - \alpha) \times ID_{ij} & thr \leq H(D_{ij}) < 1 \end{cases} \tag{19}$$

where α is considered as a confidence factor. Importing confidence factor is a significantly effective strategy to resist the false recommendation from malicious nodes. Furthermore, it conforms to human interaction customary. It can be calculated as follows.

$$\alpha = 1 - t^{-z}, \quad z \in (0, 1) \tag{20}$$

where t represents the number of cooperation between node i and node j. z is a dynamic value with a range of (0,1) and varies with the application scenario. Apparently, the weight of direct trust value is positively correlated with the number of direct interactions, that is, direct trust value changes with the number of direct interactions.

C. EXPONENTIAL-BASED TRUST AND REPUTATION EVALUATION SYSTEM FOR RESISTING THE INTERNAL ATTACKS

The trust and reputation system is considered as the most effective methods to resist the internal attack, which includes the selective forwarding attack, the on-off attack, the slander attack, and the collusion attack. The on-off attack is considered that nodes behave well or badly alternatively trying to remain undetected while causing damage [43]. The selective forwarding attack is deemed that malicious nodes can transmit or discard specific messages probabilistically, which makes the packets unable to reach the destination, resulting in a chaotic state of the network. Both the on-off attack and the selective forwarding attack are harmful to the internet. Obviously, the trust evaluation system is the most appropriate and effective method to resist them due to the trust of malicious nodes may decrease continuously with the number of noncooperation. Compromised nodes can also act as normal nodes and gain high credibility by the cooperation continues to offer a good reputation for the same type of nodes, which named the collusion attack. For the above internal attack, we can discard the misbehaving nodes by setting a threshold value.

In this paper, an effective method is proposed to resist internal attacks in WSNs, which named exponential-based trust and reputation system, short for ETRES. In this method, the behaviors of nodes are largely depended on the trust value of nodes, which are calculated by the interaction between nodes. Consequently, the system is used to resist the on-off attack and the selective forwarding attack. Additionally, it is also utilized to detect the compromised node, which can launch the collusion attack.

1) WEAKENING THE IMPACT OF THE ON-OFF ATTACK

The on-off attack is launched by malicious nodes. Thus, rejecting to cooperate with malicious nodes is an appropriate way to defense the on-off attack and the selective forwarding attack. In this part, the property of the node is estimated based on the total trust. For the bad nodes, it takes little effect on the total trust, good node versa. The total trust value is calculated by direct trust, which based on direct observation or indirect trust is integrated as needed, which based on indirect observation. The detail process is shown in Algorithm 1.

Algorithm 1 Resisting On-Off Attack

```
Input:  Direct observation and indirect observation
Output:  The total trust
While
  Calculate the direct trust
    If $0 \leq D_{ij} \leq thr$
        The total trust ⟵ the direct trust
    Else
        Calculate the indirect trust
        The total trust ⟵ $\alpha \times$the direct trust + $\beta \times$the
          indirect trust
      End
End
```

2) DETECTING THE COMPROMISED NODES

The collusion attack is launched by neighbor nodes. Therefore, the trust of the neighbor node should be accessed when the indirect trust needs to be considered. In our method, there is an attractive way to resist attacks from compromised nodes. When the certainty of direct trust is relatively high, it is unnecessary to compute the indirect trust from indirect observations. It means that the scheme can save more energy and prolong the lifetime of the network. In more detail, resisting internal attacks from the compromised node are two main advantages of our method. One is that when the certainty of the target node is relatively high, the trust of the evaluating node can be calculated by the direct trust. Defending the attacks from compromised nodes can be avoided by without considering indirect information from neighbor nodes. The other is that when the uncertainty of the trust of the target node is relatively high, the indirect trust is integrated to enhance the trust of the evaluating node, which can be calculated by indirect information. However, not all indirect information is trustworthy. It is necessary to evaluate the indirect information from third parties to discard the compromised nodes, which may result in the adverse evaluation of normal nodes. In the course of evaluating the indirect information, compromised nodes can be determined by setting a threshold value χ. It can offer more credible information to evaluate the target node and detect the compromised node. The detail process is shown in Algorithm 2.

Algorithm 2 Resisting the Collusion Attack

```
Input:  Direct observation and indirect observation
Output:  The total trust
While
  Calculate the direct trust
    If $0 \leq D_{ij} \leq thr$
        The total trust ⟵ the direct trust
    Else
        Calculate neighbor nodes' trust value $T_{ik}$
        If $T_{ik} \geq \chi$
            Calculate the indirect trust
              The total trust ⟵ $\alpha \times$the direct trust + $\beta \times$
              the indirect trust
          Else
            Discard the compromised nodes
          End
    End
End
```

IV. PERFORMANCE ANALYSIS AND COMPARISON

In this section, performance and security evaluations are implemented on MATLAB platform. Without considering the internal security in a random appearance, we focus on the efficiency of resisting the internal attacks that keep exist in medium and small scale WSNs. Since RFSN [41] is the benchmark in WSNs, and BTMS [18] has been a highly valued method and received much attention in recent years. Therefore, we contrast ETRES model with typical RFSN [41] and BTMS [18]. The results show that ETRES has a powerful capability of trust assessment and attack defense.

Typically, in the phase of initializing trust values, all nodes are defined as the same initial trust value. We assume that all nodes are good nodes. It does not require initialization time, but encourages malicious nodes to create a new ID and reenter the network in a form of new reputation. Conversely, it can resolve the problem of forgery of new IDs, but it takes a lot of time to build trust in the system. Based on the above hypothesis, we propose a neutral method that set the initial trust as 0.5. In other words, let $a = b$. Unfortunately, it is difficult to determine the number of interactions of a or b. When the number of interactions between nodes is scarce, the trust value is not accurate enough. Contrarily, it not only increases the weight of the historical trust information, affects the evaluation of trust, but also increases the convergence time of the trust value and affects the stability of the network. For a or b, the selection of reasonable value is significant.

In the real world, the base station will collect the sensing data from the sensor node and transmit it to the next hop node. Then, the interaction records are confirmed by comparison. To simplify the simulation, the packet modification/ packet dropping is ignored to verify the proposed evaluation system. Suppose that the signal channel is perfect, and normally transmits packets in ideal condition. In the initial phase, we define the initial trust is 0.5. That is a equals b. The simulation conditions are as followings. Generally speaking, the higher the reliable neighbor nodes of the one-hop communication range, the higher the evaluation. But we set two or three neighbor nodes for simulating simply the proposed method.

The neighbor node number of node j is 2. Node i evaluates the trust value of neighbor node j, then it is renewed for each interaction. The performance of the proposed method, RFSN [41] and BTMS [18] will be compared in four different scenarios.

A. SCENARIO 1

Assume node i and node j are reliable, and the neighbor node is also reliable. Node i intends to interact with node j, and

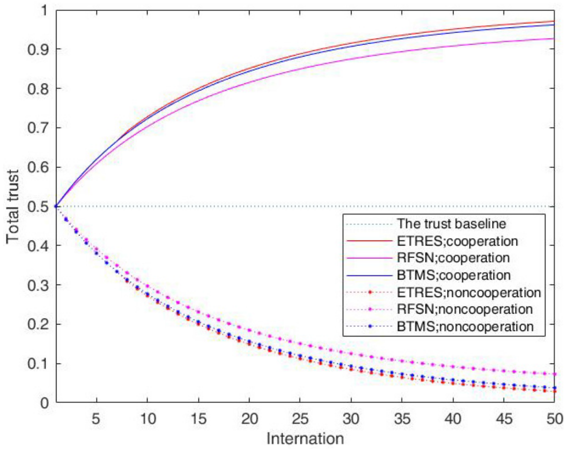

FIGURE 4. **The total trust of normal nodes.**

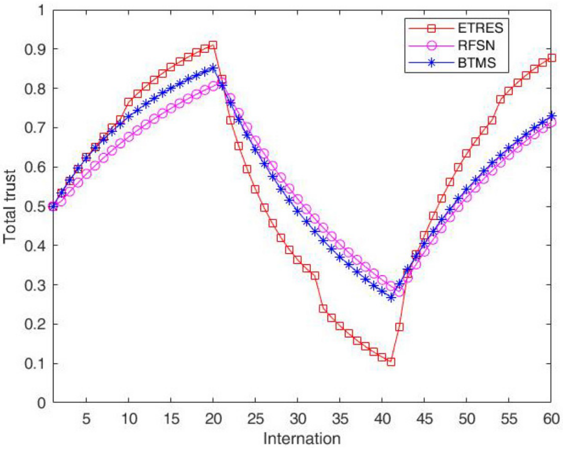

FIGURE 5. **Direct trust value under on-off attack.**

node *i* needs to evaluate the trust of node *j* firstly. Suppose the trust of the node *i* to node j as (7, 7). Suppose the trust of the neighbor nodes to node *j* as (7, 7). Suppose the trust of node *i* to neighbor nodes as (25,5). Finally, we compare ETRES with RFSN [41] and BTMS [18] in trust evaluation. The simulation result is shown in Figure 4.

On account of the above simulation results, RFSN [41], BTMS [18] and ETRES are utilized to evaluate reliable nodes, the trust of reliable nodes is gradually increasing, and the performance of RFSN, BTMS and ETRES are good. Relatively, ETRES is better than RFSN and BTMS due to the fast growth of the trust curve indicates that the initialization time is short. It can save more energy. As shown in Figure 4. A dotted line represents a trust baseline line. Above this line means a good reputation, and below this line means a bad reputation. The red solid line represents the simulation results of ETRES under cooperation. The red dot line represents the simulation results of ETRES under noncooperation. The magenta dot line represents the simulation results of RFSN under noncooperation. The magenta solid line represents the simulation results of RFSN under cooperation. The blue solid line represents the simulation results of BTMS under cooperation. The blue dot line represents the simulation results of BTMS under noncooperation.

B. SCENARIO 2

Opponents can launch an on-off attack whereby nodes behave well or badly alternatively trying to remain undetected while causing damage [43]. Suppose the trust of the node *i* to node *j* as (7,7). Suppose the trust of the neighbor nodes to node *j* as (7,7). Suppose the trust of node *i* to neighbor nodes as (25,5). Based on the definition of the on-off attack, we set an attacker to behave well in the first 20 interactions to set up a good reputation but behave badly in the next 40 interactions. And then it behaves well continuously. We compare ETRES with RFSN [41], and BTMS [18] in trust evaluation. The simulation result is illustrated in Figure 5.

On account of the above simulation results, RFSN [41], BTMS [18] and ETRES are utilized to resist the on-off attack. For on-off attack, although ETRES, BTMS and RFSN have a similar performance, we can see that the trust value of ETRES falls much faster than that of RFSN and BTMS. It means that the nodes need only a small amount of bad behavior to cause the loss of trust quickly in a short time. Apparently, it also obeys human interaction rules. As shown in Figure 5. The red square solid line represents the simulation result of ETRES. The magenta round solid line represents the simulation result of RFSN. The blue asterisk solid line represents the simulation result of BTMS.

In order to verify the extensiveness of the algorithm, we assume the neighbor node number of node *j* is 3. At the same time, various parameters will be set in this simulation.

C. SCENARIO 3

Assume node *j* is unreliable node and one of the neighbor nodes between node *i* and node *j* is an unreliable node. But the other two shared neighbors are normal nodes. Node *i* intends to interact with node *j*, and node *i* needs to evaluate the trust of node j firstly.

Suppose the trust of the node *i* to node *j* as (20,20). Suppose the trust of the neighbor nodes to node *j* as (0,0). Suppose the trust of node *i* to neighbor nodes as (2,15), (9,9), (30,2) respectively. Finally, we compare ETRES with RFSN [41] in trust evaluation. The simulation result is shown in Figure 6.

On account of the above simulation results, RFSN [41], BTMS [18] and ETRES are utilized to resist attacks launched by the compromised nodes. From Figure 6 we can know, compared with RFSN and ETMS, the trust of ETRES decrease quickly than RFSN, which means ETRES has a better performance to resist attacks launched by the compromised nodes. The magenta double solid line represents the simulation result of ETRES. The blue line represents the simulation result of BTMS. The red dotted line represents the simulation result of RFSN.

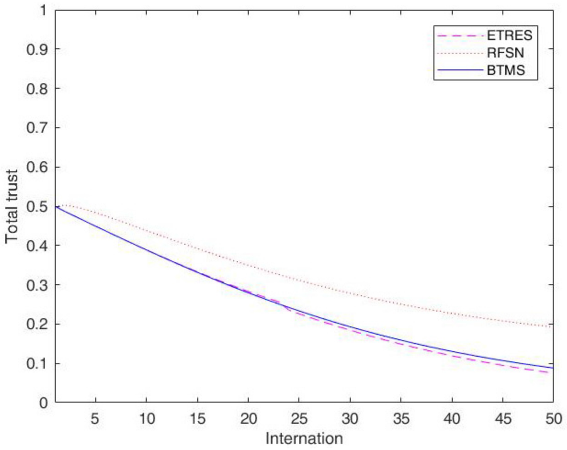

FIGURE 6. The total trust of compromised nodes.

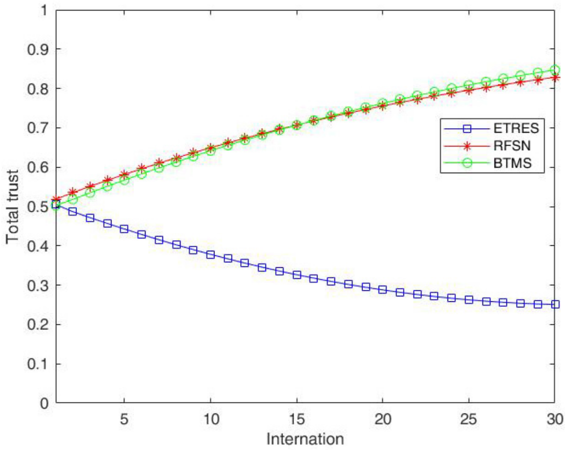

FIGURE 7. The total trust of compromised nodes under collusion attack.

D. SCENARIO 4

In this part, we assume that node j is unreliable. What's more, neighbor nodes are compromised nodes. Node i intends to interact with node j, and node i needs to evaluate the trust of node j firstly.

Suppose the trust of the node i to node j as (15, 15). Suppose the trust of the neighbor nodes to node j as (8,8), (6,1), (6,1), respectively. Suppose the trust of node i to neighbor nodes as (10,1). Finally, we compare ETRES with RFSN [41] and BTMS [18] in trust evaluation. The simulation result is shown in Figure 7.

On account of the above simulation results, RFSN [41], BTMS [18] and ETRES are utilized to resist the collusion attack. As for Figure 7, our proposed method can effectively resist the collusion attack, while RFSN and BTMS have a poor performance to resist the collusion attack.

Briefly speaking, the simulation results based on the above results show that the proposed scheme ETRES has a powerful ability to trust assessment and attack defense. Compared with RFSN and BTMS, there are several reasons for obtaining such simulation results. Firstly, we use entropy theory to evaluate the uncertainty of direct trust. Only when the uncertainty is high enough, indirect trust is introduced to enhance the certainty of direct trust. It is beneficial to improve the security of the network by obtaining high trust value in a short time. Furthermore, the trust and reputation evaluation system can save a lot of energy due to indirect trust is calculated as needed. As shown in Figure 4. Secondly, when a node behaves badly, other nodes refuse to interact with it. The uncertainty of the direct trust of the node increases dramatically over time, and then the direct trust declines rapidly. As shown in Figure 5. Thirdly, as for the attacks launched by compromised nodes on the internet, the confidence factor is integrated into the trust management system to resist the internal attack dynamically, which is computed based on the number of operations. Especially when the compromised node performs a bad behavior, this method can make the trust value of the node drop quickly. As shown in Figures 6-7.

V. CONCLUSION

Trust management system is an effective method to detect misbehaving from malicious nodes. At present, a large number of trust management systems based on the beta distribution are proposed. Unfortunately, there is a potential hypothesis which two states exist in the process of interaction between nodes. In fact, it may lead to inaccurate trust values due to multiple states exist in WSNs. Therefore, a trust and reputation system based on the exponential distribution, ETRES for short, is proposed. In our method, the exponential distribution is used to express the trust and reputation of nodes. It can establish a trust management system based on the state of successful interaction without considering other states. The confidence factor is redefined, which is computed by the number of successful interactions. It can force the direct trust to drop rapidly, which can weaken the impact of malicious nodes. Compared with RFSN and BTMS, ETRES evaluates the total trust of nodes by its reputation distribution and its confidence factor that on the basis of the successful interaction information. The simulation results show that ETRES can evaluate the trust of nodes reasonably, and it can resist internal attacks, especially on-off attacks. The trust of nodes is used for the scheme of data aggregation. The node with high trust is selected reliable relay nodes to transmit data, which can reduce the risk of internal attacks in the network. Furthermore, the proposed method is conveniently incorporated into the existing network. Unfortunately, there are still some drawbacks in our method. Although the proposed method can effectively resist the internal attacks, the performance difference between the above method seems to be very close. Therefore, in the future, we will be committed to improving the algorithm for detecting compromised nodes effectively and enhancing network security. In addition, we would like to concentrate on the application of the trust management system and seek a better way to balance between energy and security.

REFERENCES

[1] 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.

[2] A. A. Anasane and R. A. Satao, "A survey on various multipath routing protocols in wireless sensor networks," *Procedia Comput. Sci.*, vol. 79, no. 20, pp. 610–615, 2016.

[3] T. Qiu, X. Liu, L. Feng, Y. Zhou, and K. Zheng, "An efficient tree-based self-organizing protocol for Internet of Things," *IEEE Access*, vol. 4, pp. 3535–3546, 2016.

[4] J. He and N. Xiong, "An effective information detection method for social big data," *Multimedia Tools Appl.*, vol. 77, pp. 11277–11305, May 2018.

[5] X. Li, C. Zhou, Y.-C. Tian, N. Xiong, and Y. Qin, "Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 608–618, Feb. 2018.

[6] M. Wu, N. N. Xiong, and L. Tan, "An Intelligent Adaptive Algorithm for Environment Parameter Estimation in Smart Cities," *IEEE Access*, vol. 6, pp. 23325–23337, 2018.

[7] C. Chen, H. Zhao, Q. Tie, R. Hou, and A. K. Sangaiah, "A multi-station block acknowledgment scheme in dense IoT networks," *Comput. Commun.*, vol. 119, pp. 179–190, Apr. 2018.

[8] T. Qiu, Y. Lv, F. Xia, N. Chen, J. Wan, and A. Tolba, "ERGID: An efficient routing protocol for emergency response Internet of Things," *J. Netw. Comput. Appl.*, vol. 72, pp. 104–112, Sep. 2016.

[9] N. Xiong, L. Zhang, W. Zhang, A. Vasilakos, and M. Imran, "Design and analysis of an efficient energy algorithm in wireless social sensor networks," *Sensors*, vol. 17, no. 10, p. 2166, 2017.

[10] A. Liu, Z. Chen, and N. N. Xiong, "An adaptive virtual relaying set scheme for loss-and-delay sensitive WSNs," *Inf. Sci.*, vol. 424, pp. 118–136, Jan. 2018.

[11] J. Li, H. Hu, Q. Ke, and N. Xiong, "A novel topology link-controlling approach for active defense of nodes in networks," *Sensors*, vol. 17, no. 3, p. 553, 2017.

[12] J. Zhao and W. D. Fang, "PTMS: Poisson-based Trust Management System in Wireless Sensor Networks," presented at the 18th IEEE Int. Conf. Comput. Inf. Technol., Halifax, NS, Canada, Jul./Aug. 2018.

[13] Y. Liu *et al.*, "QTSAC: An energy-efficient MAC protocol for delay minimization in wireless sensor networks," *IEEE Access*, vol. 6, pp. 8273–8291, 2018.

[14] J. Tang, A. Liu, J. Zhang, N. N. Xiong, Z. Zeng, and T. Wang, "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*, vol. 18, no. 3, pp. 751, 2018.

[15] M. Huang *et al.*, "A services routing based caching scheme for cloud assisted CRNs," *IEEE Access*, vol. 6, pp. 15787–15805, 2018.

[16] T. Qiu, Y. Zhang, D. Qiao, X. Zhang, M. L. Wymore, and A. K. Sangaiah, "A robust time synchronization scheme for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3570–3580, Aug. 2018.

[17] R. Feng, Q. Liu, Q. Liu, and N. Yu, "A credible Bayesian-based trust management scheme for wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 2015, no. 2, p. 10, 2015.

[18] W. Fang, X. Zhang, Z. Shi, Y. Sun, and L. Shan, "Binomial-based trust management system in wireless sensor networks," *Chin. J. Sens. Actuators*, vol. 28, no. 5, pp. 703–708, 2017.

[19] P. Dong, J. Guan, X. Xue, and H. Wang, "Attack-resistant trust management model based on beta function for distributed routing in Internet of Things," *China Commun.*, vol. 9, no. 4, pp. 89–98, 2012.

[20] Y. Wang *et al.*, "Dynamic propagation characteristics estimation and tracking based on an EM-EKF algorithm in time-variant MIMO channel," *Inf. Sci.*, vol. 408, pp. 70–83, Oct. 2017.

[21] X. Xu *et al.*, "A cross-layer optimized opportunistic routing scheme for loss-and-delay sensitive WSNs," *Sensors*, vol. 18, no. 5, p. 1422, 2018.

[22] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16–22, Feb. 2018.

[23] X. Li, A. Liu, M. Xie, N. N. Xiong, Z. Zeng, and Z. Cai, "Adaptive aggregation routing to reduce delay for multi-layer wireless sensor networks," *Sensors*, vol. 18, no. 4, p. 1216, 2018.

[24] G. Zhang, S. Cai, and N. Xiong, "The application of social characteristic and L1 optimization in the error correction for network coding in wireless sensor networks," *Sensors*, vol. 18, no. 2, p. 450, 2018.

[25] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *J. Supercomput.*, vol. 74, no. 4, pp. 1779–1801, 2018.

[26] C. Zhu, V. C. M. Leung, K. Wang, L. T. Yang, and Y. Zhang, "Multi-method data delivery for green sensor-cloud," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 176–182, May 2017.

[27] C. Zhu, X. Li, V. C. M. Leung, L. T. Yang, E. C.-H. Ngai, and L. Shu, "Towards pricing for sensor-cloud," *IEEE Trans. Cloud Comput.*, to be published.

[28] S. Wen, C. Huang, X. Chen, J. Ma, N. Xiong, and Z. Li, "Energy-efficient and delay-aware distributed routing with cooperative transmission for Internet of Things," *J. Parallel Distrib. Comput.*, vol. 118, pp. 46–56, Aug. 2018.

[29] X. Liu, N. Xiong, N. Zhang, A. Liu, H. Shen, and C. Huang, "A trust with abstract information verified routing scheme for cyber-physical network," *IEEE Access*, vol. 6, pp. 3882–3898, 2018.

[30] Y. Chen, S. Weng, W. Guo, and N. Xiong, "A game theory algorithm for intra-cluster data aggregation in a vehicular ad hoc network," *Sensors*, vol. 16, no. 2, p. 245, 2016.

[31] Q. Fan, N. Xiong, K. Zeitouni, Q. Wu, A. Vasilakos, and Y. C. Tian, "Game balanced multi-factor multicast routing in sensor grid networks," *Inf. Sci.*, vols. 367–368, pp. 550–572, Nov. 2016.

[32] H. Xia, Z. Jia, and E. H.-M. Sha, "Research of trust model based on fuzzy theory in mobile ad hoc networks," *IET Inf. Secur.*, vol. 8, no. 2, pp. 88–103, Mar. 2014.

[33] N. Wang and Y. Pang, "An improved light-weight trust model in WSN," *Comput. Model. New Technol.*, vol. 18, no. 4, pp. 57–61, 2014.

[34] W. Na and L. DongQian, "Trust model based on changeable sampling frequency for wireless sensor network," in *Proc. IEEE/ACIS 15th Int. Conf. Comput. Inf. Sci. (ICIS)*, Jun. 2016, pp. 1–4.

[35] 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.

[36] W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 7, pp. 613–621, 2016.

[37] W. Fang, W. Zhang, Y. Yang, Y. Liu, and W. Chen, "A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution," *Sci. China-Inf. Sci.*, vol. 60, Apr. 2017, Art. no. 040305.

[38] X. Anita, J. M. L. Manickam, and M. A. Bhagyaveni, "Two-way acknowledgment-based trust framework for wireless sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 2013, no. 2, pp. 140–154, 2013.

[39] V. Umarani, K. S. Sundaram, and D. Jayashree, "Enhanced beta trust model in wireless sensor networks," in *Proc. Int. Conf. Inf. Commun. Embed. Syst.*, Feb. 2016, pp. 1–5.

[40] N. Labraoui, "A reliable trust management scheme in wireless sensor networks," in *Proc. IEEE Int. Symp. Program. Syst. (ISPS)*, Apr. 2015, pp. 1–6.

[41] 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, 2008.

[42] D. Hongjun, J. Zhiping, and D. Xiaona, "An entropy-based trust modeling and evaluation for wireless sensor networks," in *Proc. Int. Conf. Embedded Softw. Syst.*, 2008, pp. 27–34.

[43] C. Zhu, Z. Sheng, V. C. M. Leung, L. Shu, and L. T. Yang, "Toward offering more useful data reliably to mobile cloud from wireless sensor network," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 84–94, Mar. 2015.

JIN ZHAO was born in Xinyang, Henan, China, in 1994. He received the B.S. degree in mechanical design, manufacture and automation from the College of Mechanical Engineering, Shangqiu Institute of Technology, Henan, in 2016. He is currently pursuing the master's degree with the College of Information Mechanical and Electrical Engineering, Shanghai Normal University, China. His current research interests are wireless sensor networks and natural language processing.

JIFENG HUANG received the B.S. degree in radio engineering from Zhengzhou University, Zhengzhou, Henan, China, in 1984, the M.S. degree in communication and electronic systems from Xi'an Jiaotong University, Xi'an, China, in 1989, and the Ph.D. degree in measurement and control technology and automation instruments from the East China University of Science and Technology, Shanghai, China, in 2006.

From 1989 to 1999, he was a Teacher with the Zhengzhou University of Aeronautics, Zhengzhou. Since 1999, he has been a Professor with the College of Information, Mechanical and Electrical Engineer, Shanghai Normal University. His research interests include pattern recognition, machine learning, and automation instrument.

Dr. Huang received the award for the scientific and technological advancement from the Aviation Ministry of China.

NAIXUE XIONG received the Ph.D. degree in sensor system engineering from Wuhan University, and the Ph.D. degree in dependable sensor networks from the Japan Advanced Institute of Science and Technology.

He was with Georgia State University, Wentworth Technology Institution, and Colorado Technical University (as a Full Professor for five years), for about 10 years. He is currently an Associate Professor (with three-year credits) with the Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK, USA. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory. He has published over 300 international journal papers and over 100 international conference papers. Some of his papers were published in the IEEE JSAC, the IEEE / ACM transactions, the ACM Sigcomm Workshop, the IEEE INFOCOM, ICDCS, and IPDPS. He is a Senior Member of the IEEE Computer Society. He has received the Best Paper Award at the 10th IEEE International Conference on High-Performance Computing and Communications (HPCC-08) and the Best Student Paper Award at the 28th North American Fuzzy Information Processing Society Annual Conference (NAFIPS2009). He is the Chair of the Trusted Cloud Computing Task Force, the IEEE Computational Intelligence Society, and the Industry System Applications Technical Committee. He has been the General Chair, the Program Chair, the Publicity Chair, a PC member, and an OC member of over 100 international conferences, and as a Reviewer of about 100 international journals, including the IEEE JSAC, the IEEE SMC (Park: A/B/C), the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON MOBILE COMPUTING, and the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. He is serving as the Editor-in-Chief, and an Associate Editor or Editor Member for over 10 international journals, including an Associate Editor for the IEEE TRANSACTIONS ON SYSTEMS, MAN CYBERNETICS: SYSTEMS, an Associate Editor for the *Information Science*, the Editor-in-Chief of the *Journal of Internet Technology*, and the Editor-in-Chief of the *Journal of Parallel Cloud Computing*, and a Guest Editor for over 10 international journals, including the *Sensor Journal*, WINET, and MONET.