IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 17, 2017, accepted May 16, 2017, date of publication May 23, 2017, date of current version June 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2706973

Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network

DANYANG QIN, SONGXIANG YANG, SHUANG JIA, YAN ZHANG, JINGYA MA, AND QUN DING
Key Laboratory of Electronics Engineering, Heilongjiang University, Harbin, 150080, P.R. China

Corresponding author: Danyang Qin (qindanyang@hlju.edu.cn)

This work was supported in part by the National Natural Science Foundation China under Grant 61302074, in part by the Natural Science Foundation of Heilongjiang Province under Grant QC2013C061, in part by the Modern Sensor Technology Research and Innovation Team Foundation of Heilongjiang Province under Grant 2012TD007, in part by the Postdoctoral Research Foundation of Heilongjiang Province under Grant LBH-Q15121, in part by the Postgraduate Innovation Research Foundation of Heilongjiang University under Grant YJSCX2016-019HLJU.

ABSTRACT Aiming at the serious impact of the typical network attacks caused by the limited energy and the poor deployment environment of wireless sensor network (WSN) on data transmission, a trust sensing-based secure routing mechanism (TSSRM) with the lightweight characteristics and the ability to resist many common attacks simultaneously is proposed in this paper, at the same time the security route selection algorithm is also optimized by taking trust degree and QoS metrics into account. Performance analysis and simulation results show that TSSRM can improve the security and effectiveness of WSN.

INDEX TERMS Wireless sensor network, optimal route, security, QoS metrics, trust degree.

I. INTRODUCTION

The rapid development of Internet of things (IoT) promotes cloud computing, social network and the construction of smart city continually [1]–[3]. Smart cities that rely on different types of distributed intelligent devices can provide urban residents with a wide range of applications such as environmental monitoring, traffic management, and social entertainment [4], [5]. WSN with the characteristic of low cost, rapid deployment and self-organization plays a vital role in facilitating the services of smart city. The ubiquitous sensor nodes can both collect the physical information of urban environment and control the public and private facilities in the context of smart urban environment [6], [7]. However, the multi-hop routing is vulnerable to various types of attacks due to the open, distributed and dynamic characteristic of WSN [8]–[11], which has a serious impact on data and information security. At present, the existing secure routing algorithms are usually directed against specific malicious or selfish behavior attacks, since they mainly rely on encryption algorithms and authentication mechanisms, which are not suitable for the multi-hop distributed and energy-constrained WSN [12]–[14].

The research shows that trust management (TM) is an effective way to solve the security problems of WSN [15]–[18], however, the conventional routing protocol based on trust is difficult to ensure the security of multi-hop information transmission, and the reasons can be summarized as follows. Firstly, although the scheme based on trust can handle inherent attacks in WSN, they also prompt some new risks. Secondly, trust is significantly different from other normal route indicators, such as the number of hops, delay or other QoS requirements, but the most credible models do not consider the special property of trust degree in the design of routing protocols. Thirdly, the existing routing protocol based on trust has certain limitations, such as dependence on specific route scheme or platform. In other words, the security mechanism may be invalid if the network routing protocol is changed [19]–[22]. This paper proposes a trust sensing based secure routing mechanism for WSN to solve the network overhead and the security of multi-hop information transmission in this case. And the simulation results show that TSSRM not only improves the security of information for multi-hop communication network, but also reduces the routing overhead in WSN effectively. The main contributions of this paper can be summarized as follows:

1) This paper analyzes the behavior of sensor nodes, including the movement and energy consumption of sensor nodes. The trust degree of sensor node is evaluated according to these characters, and then the trust degree of route is calculated and the trust calculation model of network is established to get the optimal route from the source node to the destination node. At the same time, the trust degree and

QoS metrics are combined as the routing metrics to present an optimized routing algorithm by using the semiring theory.

2) The trust sensing based secure routing mechanism is designed, establishment and working process of TSSRM are also described in this paper. The proposed routing algorithm is applied to the secure routing mechanism to achieve the efficient and reliable transmission of data. At the same time, the maintenance process of TSSRM is also presented to further ensure the security of data transmission.

II. ANALYSIS OF ATTACKS

This section analyzes several typical network attacks in WSN and extracts their characters to provide support for the security assurances of WSN since network attacks aim at different objects using different methods.

The common attacks can be divided into routing protocol attacks and trust model attacks according to different attack targets. Multi-hop relay makes the damage of routing protocol attacks to WSN more serious than the general wireless communication network. Generally, routing protocol attacks can be classified into soft attacks and hard attacks according to the behavior of attackers. Soft attacks mean that malicious or selfish nodes steal or destroy the relay data by pretending or cheating fictitious route [23], such as: blackhole attack that adds false available channel information in the routing request, grayhole attack that discards some data packets deliberately [24], sinkhole attack that fabricates local resources, wormhole attack that constructs false links by conspiracy, sniffing attack that eavesdrops routing information by analyzing network traffic, as well as sybil attack that forges multi-identity [25]. Hard attacks mean that malicious nodes damage the information transmission by destroying the existing transmission resources, such as: DoS attack that exhausts the resources of attacked objects [26], tampering attack that tampers routing data and replay attack that occupies bandwidth maliciously [27].

Although the TM system could handle most of network attacks and improve the security of network by encryption and trust mechanisms, it perhaps becomes the new target of attackers [28]. At present, the typical trust model attacks include: on-off attack, conflicting behavior attack, selfish attack, bad mouthing attack and collusion attack [29]. In addition, the trust management algorithm that adopts encryption or trust mechanisms widely used in wireless communication network is not suitable for all wireless networks, because the trust management algorithm focuses on the trust calculation process and ignores the trust derivation process. In fact, in order to ensure the accuracy of trust assessment, trust information is frequently replaced during trust derivation, which leads to a large amount of overhead [30], so TM is difficult to apply to resource-constrained WSN directly. Therefore, the lightweight security routing mechanism proposed in this paper will construct trust degree by behavior and energy, and combine with QoS to design routing metrics so that TSSRM with lower cost can resist several kinds of typical attacks. In addition, sybil attack and sniffing attack are difficult to detect by trust-based mechanism, however, location verification [31] and frequency hopping technology [32] can effectively resist them, but this is not the scope of this paper.

III. ROUTING ALGORITHM

A novel routing algorithm which used for reducing the routing overhead of network is proposed in this section.

A. SYSTEM MODEL

The watchdog is adopted to detect the behaviors of malicious nodes in the proposed detecting mechanism [33]. The results of mutual trust detection among sensor nodes are used as the basis of trust calculation, $td(x, y)$ denotes the trust degree y for x. Considering the number and the distribution of WSN nodes, the behaviors of nodes are evaluated by the combination of direct trust degree, indirect trust degree and incentive factor.

B. ESTABLISHMENT OF TRUST MODEL

Trust degree is an important basis for the evaluation of trust relationship. Analytic hierarchy process (AHP) is adopted in this section to analyze and establish trust calculation model. The trust calculation model of the whole multi-hop route is established by the trust model between two nodes (including direct trust degree, indirect trust degree and incentive factor) to judge the secure route of data transmission.

1) DIRECT TRUST CALCULATION OF NODES

The behavior of sensor nodes can be monitored by neighbor nodes in WSN. Since sensor nodes are highly constrained in computing power, energy, memory and bandwidth, it is not enough to judge the trust degree of nodes only by monitoring the behavior of nodes [34]; therefore, this study will combine behavior with energy to evaluate the trust degree of nodes comprehensively.

(A) Analysis of direct behavior trust

Direct behavior trust is the direct observation of every node involved in communication, a lightweight computing method is proposed in this paper to assess the direct behavior trust degree of sensor nodes in WSN:

$$dtd(x, y)^l = \omega_1 \times dtd_{P(y)}(x, y)^{l-1} + \omega_2 \times dtd_{N(y)}(x, y)^{l-1} + ift(x, y)^l \quad (1)$$

where $dtd_{P(y)}(x, y)^{l-1}$ denotes the direct trust degree of y for x according to the good behavior of node y in the past, $dtd_{N(y)}(x, y)^{l-1}$ denotes the direct trust degree of y for x according to the bad behavior of node y in the past. n stands for the number of neighbor nodes and l denotes the serial number of assessment records. ω_1 and ω_2 denote the self-adaptive exponential decay time factor (SEDTF) of positive and negative evaluation, respectively. $ift(x, y)^l$ represents the evaluation for the current behavior of node y using intrusion

detection system (IDS) [35]. $ift(x, y)$ is given by

$$ift(x,y) = \begin{cases} P(y), & 0 < P(y) < 1 \\ 0, & uncertain \\ N(y), & -1 < N(y) < 0 \end{cases} \quad (2)$$

where $P(y)$ and $N(y)$ denote the positive and negative evaluation for node $y's$ behavior respectively. The judgment for node's behavior will no longer be accurate when the estimated value is in a fuzzy state, so the value of $ift(*)$ will be set as zero at this time.

On-off attack is the most common way of trust attacks, therefore, the fixed SEDTF ω_1 and ω_2 in (1) will become self-adaptive, namely $\omega_1 = e^{-\rho_1 \times (t_c - t_{c-1})}$, $\omega_2 = e^{-\rho_2 \times (t_c - t_{c-1})}$, t_c represents the current time and t_{c-1} denotes the time that the last interaction occurred, respectively, ρ_1 and ρ_2 denote the exponential decay strength of positive and negative evaluation, where $t_c > t_{c-1} \geq 0$, $\rho_1 > \rho_2 \geq 0$, It can be seen that the direct behavior trust $dtd(x, y)^l$ will decrease with the increasing of t. It means that the results of recent interactions are more important than those of previous interactions as $\omega \to 0$. Since the behaviors of on-off attackers are good and bad in turn to win higher reputation in the actual environment. At this time, the value ω_1 for normal behavior is reduced and the value ω_2 for malicious behavior is improved by adjusting the SEDTF adaptively, thus ensuring that bad behavior will be memorized for a longer time than good behavior.

(B) Analysis of direct energy trust

The nodes in the network will choose nodes with high trust degree as relay for forwarding information in the traditional security model, which aggravates the energy consumption of nodes with high trust degree, thus resulting in uneven network load or even network segmentation. Therefore, the calculation model will add the energy trust as a measurable indicator of trust degree. The energy consumption of node y during receiving and sending message is shown in (3) and (4), respectively [36].

$$Receiving\_Cost(k, d) = Eelec \times k \quad (3)$$

$$Sending\_Cost(k, d) = Eelec \times k + Eamp \times k \times d^2 \quad (4)$$

where k is the number of message bits, d is the distance between node x and node y, $Eelec$ represents the unit energy consumption for transmitting message at node y, and $Eamp$ represents energy consumption for achieving certain SNR during transmission, $Eelec$ and $Eamp$ are given in this paper.

Therefore, the total energy consumption of node y for forwarding data is:

$$EC = 2 \times Eelec \times k + Eamp \times k \times d^2 \quad (5)$$

If the initial energy of network node is EB, the remaining energy ES of node y is:

$$ES = EB - EC \quad (6)$$

It indicates that the node has the ability to cooperate with other nodes as an energy credible node when the remaining energy ES of the node is greater than the energy trust threshold E_{th}; otherwise, it cannot participate in the information transmission no matter how high the behavior trust degree of the node. The energy trust degree ET_y of node y is defined as:

$$ET_y = \begin{cases} 1, & ES \geq E_{th} \\ 0, & ES < E_{th} \end{cases} \quad (7)$$

The calculation model of direct trust degree $s\_dtd(x, y)^l$ will consider the behavior trust and the energy trust of nodes, as shown in (8):

$$s\_dtd(x,y)^l = \frac{1}{2}\omega_1 \times dtd_{P(y)}(x,y)^{l-1} + \frac{1}{2}\omega_2 \times dtd_{N(y)}(x,y)^{l-1} + \frac{1}{2}ift(x,y)^l + \frac{1}{2}ET_y \quad (8)$$

where the behavior and energy of nodes are equally important for the calculation of trust degree, so the weight of $dtd(x, y)^l$ and ET_y are equally assigned.

2) INDIRECT TRUST CALCULATION OF NODES

Indirect trust is the trust relationship provided by other neighbors in the target node's connected domain. Similar to the direct trust construction model, the indirect trust degree is composed of the indirect behavior trust degree and the indirect energy trust degree. Since energy is an objective parameter, the indirect energy trust degree is the same as the direct energy trust degree. Only the indirect behavior trust degree of node is considered here. If the direct connected domain of target node y in the network is C_y, $itd(x, y)^l$ represents the indirect trust degree calculated by node x according to the suggestions provided by all the nodes in C_y, as shown in (9).

$$itd(x,y)^l = \sum_{z \in C_y, z \neq x} \left(dtd(x,z)^l \times dtd(z,y)^l \right) \quad (9)$$

Considering that bad mouthing attack and collusion attack can avoid the check of direct trust, it is necessary to verify the suggestions provided by all the nodes in C_y. The dissimilarity check degree $cs(x, y)^l$ of target node y for node x is:

$$cs(x,y)^l = \frac{itd(x,y)^l + dtd(x,y)^l}{\sum_{z \in C_y, z \neq x} dtd(x,z)^l + 1} \quad (10)$$

For any neighbor node z in the direct connected domain of target node y, $|dtd(z, y)^l - cs(x, y)^l| > \delta$, the suggestion of node z will not be adopted. The dissimilarity check threshold δ is the predetermined value associated with the particular network environment and information. As a result, the malicious nodes in the set of credible nodes can be detected, and false suggestions provided by them will be excluded from the network.

TABLE 1. 1-9 scale method of AHP.

Scale	Definition
1	The two factors have the same importance
3	A factor is a little more important than another factor when two factors compare with each other
5	A factor is significantly more important than another factor when two factors compare with each other
7	A factor is intensely more important than another factor when two factors compare with each other
9	A factor is extremely more important than another factor when two factors compare with each other

Similar to the calculation of direct trust degree, node x obtains the indirect trust degree of target node y:

$$s\_itd(x,y)^l = \frac{1}{2}itd(x,y)^l + \frac{1}{2}ET_y = \frac{1}{2}\sum_{z\in C_y, z\neq x}\left(dtd(x,z)^l \times dtd(z,y)^l\right) + \frac{1}{2}ET_y \tag{11}$$

where the weight of $itd(x,y)^l$ and ET_y are also equally assigned as (8).

3) INCENTIVE FACTOR

Considering the limited energy of WSN and the vulnerability of malicious nodes, an incentive mechanism is established to punish the malicious nodes while encouraging the nodes to cooperate. Incentive is that the node will increase the number of participating in the network cooperation to improve the trust degree of node actively when the trust degree of node is reduced. Punishment is mainly manifested in two aspects: (1) if the node does not participate in network cooperation, then the trust degree of node will be reduced. The node is considered as a failure node or a malicious node and will be removed out of the network when its trust degree is below a certain level. (2) If the node already has higher trust degree, the node is still very involved in the cooperation between the networks, and then the network will consider the node as a malicious node and remove it out of WSN directly. Therefore, in the case of that the number of node participating in the network cooperation is more, the incentive factor value has much positive impact on the trust degree, on the contrary, the trust degree of node which has much more malicious behaviors must be reduced to encourage effective cooperation between nodes. For the incentive factor, the cooperative frequency is an important factor to reflect the behavior of node and also has a great impact on evaluation of node's trust degree. Therefore, the maximum effective historical time τ is defined since the information interaction has timeliness firstly, and then the incentive factor is also defined according to the interaction between nodes in τ. Since the incentive factor e_{xy} is used to solve the binary problem finally, the model is constructed using the Bernoulli distribution:

$$e_{xy} = 1 - \frac{F_{xy}^{\tau}}{F_{xy}^{\tau} + S_{xy}^{\tau}} \tag{12}$$

where S_{xy}^{τ} and F_{xy}^{τ} are the number of successful direct interaction and failing direct interaction in the maximum effective historical time τ, respectively.

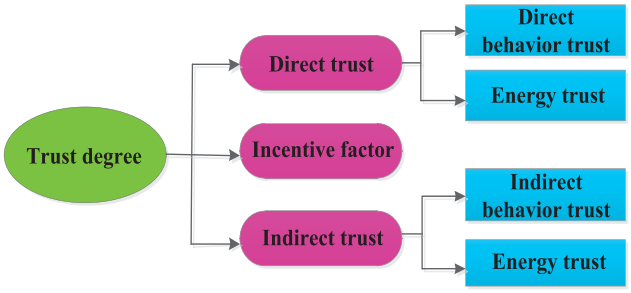

FIGURE 1. Trust model based on AHP.

4) TRUST CALCULATION MODEL BASED ON AHP

Analytic hierarchy process (AHP) is adopted in this paper to establish a comprehensive trust model, which is based on direct trust, indirect trust and incentive factor, as shown in Fig.1.

AHP is a decision-making method that decomposes elements which are always related to decision-making into objectives, criteria and schemes, and then performs qualitative and quantitative analysis. This paper also cites the 1-9 scale method to calculate the weight of each factor associated with trust degree, as shown in Table 1.

A lightweight calculation method based on the constrained resource of WSN is proposed, the comprehensive trust degree $td(x,y)^l$ of target node y for node x is:

$$td(x,y)^l = \alpha \times s\_dtd(x,y)^l + \beta \times \frac{s\_itd(x,y)^l}{n-1} + \gamma \times e_{xy} \tag{13}$$

where α, β and γ are the weighted factor associated with security policy, where $\alpha + \beta + \gamma = 1$, $\alpha, \beta, \gamma > 0$. The values of parameters can be obtained by the 1-9 scale method of AHP, namely $\alpha = 0.6986$, $\beta = 0.2370$, $\gamma = 0.0643$. The comprehensive trust degree $td(x,y)^l$ satisfies [0, 1], the higher the value of td is, the more trustworthy the node is.

C. TRUST COMPUTATION OF ROUTES

In order to maintain the generality, the given route trust calculation model will not distinguish the routing algorithm used by WSN. When the nodes in the network complete the route discovery process according to the adopted routing protocol, it will not directly determine the route and enter the information transmission phase, but calculate the trust degree of route firstly. In general, the design of trust calculation for route must meet the rules below [37]: (1) credible message

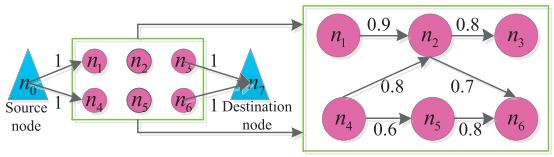

FIGURE 2. Multi-hop route trust calculation model.

cannot be increased through dissemination; (2) the destination node is identified as credible node, and its initial trust degree will be set as 1 since it is no significance to evaluate the trust degree of destination node. Thus, the trust degree $td(r)$ of single-hop link r between node x and its downstream node y is:

$$td(r) = \prod(\{td(x, y)|x, y \in r, x \to y\}) \tag{14}$$

The route of any source node to the destination node in WSN is often composed of multiple links, the trust calculation model is shown in Fig. 2, where n_0 is the source node and n_7 is the destination node. There are five routes from the source node to the destination node, their trust degree are $td(n_0, n_1, n_2, n_3, n_7) = 0.72$, $td(n_0, n_1, n_2, n_6, n_7) = 0.63$, $td(n_0, n_4, n_5, n_6, n_7) = 0.48$, $td(n_0, n_4, n_2, n_6, n_7) = 0.56$, $td(n_0, n_4, n_2, n_3, n_7) = 0.64$, respectively. It can be seen that the most credible route is $n_0 \to n_1 \to n_2 \to n_3 \to n_7$.

D. ROUTING METRICS

This section presents the basis of determining the final transmission route, namely, the routing metrics, which consist of trust degree $td(r)$ and a variety of QoS metrics $q_1(r), q_2(r), \ldots, q_n(r)$. The routing metrics can be expressed as an ordered set $m(r) \triangleq [td(r), q_1(r), q_2(r), \ldots, q_n(r)]'$, and the order of parameters in the set reflects the priority of quantization sorting. Considering the non-uniqueness of QoS and the semi-closed correlation property between $td(r)$ and $q(r)$, the theory of semiring [38] in the process of constructing the calculation model of routing metrics is introduced in this study.

Definition: The semiring is an algebraic expression $(S, \oplus, \otimes, \overline{0}, \overline{1}, \leq)$, where S is a set. $\oplus$, $\otimes$ and $\leq$ denote operational character with the features below: $(a, b, c \in S)$

$$\begin{aligned} a \oplus b &= b \oplus a \\ (a \oplus b) \oplus c &= a \oplus (b \oplus c) \\ a \oplus \overline{0} &= a \end{aligned} \tag{15}$$

$$\begin{aligned} (a \otimes b) \otimes c &= a \otimes (b \otimes c) \\ a \otimes \overline{0} &= \overline{0} \\ a \otimes \overline{1} &= a \end{aligned} \tag{16}$$

$$\forall a, b \in S : a \leq b, c \leq d \Rightarrow a \oplus c \leq b \oplus d, a \otimes c \leq b \otimes d$$

$$\forall a, b \in S : a \leq b \Leftrightarrow \exists c \in S : a \oplus c = b \tag{17}$$

It can be seen that the semiring of trust degree can be expressed an algebraic expression $(T, \oplus_T, \otimes_T, \overline{0}_T, \overline{1}_T, \leq)$, where T is a set of trust degree. $\otimes_T$ and $\oplus_T$ denote an operational character to connect with trust degree along a route and converge trust degree traverse routes, respectively. The semiring of QoS can be expressed an algebraic expression $(Q, \oplus_Q, \otimes_Q, \overline{0}_Q, \overline{1}_Q, \leq)$, where Q is a set of QoS metrics. $\otimes_Q$ and $\oplus_Q$ denote an operational character to connect with QoS metrics along a route and converge QoS metrics traverse routes, respectively.

E. ROUTING SELECTION

The optimal routing metrics $m(r)$ should be determined before selecting the optimal route, and $m(r)$ is an ordered set consisting of trust degree and QoS, so the quantitative sorting of trust degree will be considered at first. According to the semiring algebraic structure model of trust degree, the trust degree set $TD(r)$ of the route from node n_1 to node n_n in WSN is:

$$TD(r) = \oplus_T[td(r(n_1, n_z)) \otimes_T td(r(n_z, n_n))] \tag{18}$$

where $n_z \in r(n_1, n_n)$, $\otimes_T$ denotes "$\times$", $\oplus_T$ denotes "$sort(*)$". Thus, the first row parameter $TD(r)$ of $m(r)$ is the set vector in descending order of route trust. The route $r_i(n_1, n_n)$ corresponding to the current maximum trust degree $td_i(r_i)$ (denoted by td^*) is defined as the current most credible route, denoted by $r^*(n_1, n_n)$.

However, the most credible route may not meet the QoS requirements, so a number of QoS metrics must be considered to meet environmental requirements, namely, $q_1, \ldots, q_n$ in $m(r)$ (such as delay, throughput, jitter, load overhead, etc.). After this algorithm sorts the route to select an ordered route set satisfying the network trust requirements by semiring algebraic model, if any node x can find non-empty candidate optimal credible route set $R^*(n_x, n_n) = \{r_i(n_x, n_n), ...\}$, node x will sort $R^*(n_x, n_n)$ based on other QoS metric priority and continue to traverse the route selection process according to the semiring algebraic model until the optimal route satisfying both the trust degree and QoS metrics is obtained. The details of the proposed routing algorithm in this paper are shown in Table 2.

IV. SCHEME OF TSSRM

A trust sensing based secure routing mechanism (TSSRM) is proposed according to the constructed routing metrics and the optimal credible route selection algorithm.

A. NETWORK INITIALIZATION PROCESS

This paper will choose the node with higher initial trust degree as the cluster head. The higher the node's trust degree is, the higher its energy is, and the longer the node lifetime is, which is more favorable for the stability of cluster structure. The cluster head selection process of clustering topology network model composed of 6 nodes is shown in Fig. 3. In the network initialization phase of Fig. 3 (a), the nodes are non-clustered, and each node has a random initial trust degree TD_s which satisfies $0.5 \leq TD_s \leq 1$. Each node will monitor the behaviors of neighbor nodes and exchanges their initial trust degree with each other to select the new cluster head according to the cluster head selection mechanism.

TABLE 2. Routing algorithm

(1) Begin
(2) Add n_n to N^* $\quad\%n_n$ represents the destination node, N^* denotes the set of nodes which have optimal paths to n_n
(3) **while** $N \neq N^*$ $\quad\%N$ represents a set of all nodes in the network
(4) **for** node $n_x \in N - N^*$ $\quad\%n_x$ represents the source node
(5) Determine $m(r(n_x, n_n)) = [q_0, q_1, ..., q_t]'$ $\quad\%m(r(n_x, n_n))$ represents routing metrics, $q_0 = TD(r(n_x, n_n))$ has the highest priority
(6) **for** $n_z \in \Gamma(n_x)$ $\quad\%\Gamma(n_x)$ represents represents the set of candidate nodes can be selected as the next hop of message transmission
(7) **if** $td(r(n_x, n_z)) \otimes_T td(r(n_z, n_n)) \geq td(r(n_x, n_n))_{th}$ $\quad\%td(r(n_x, n_n))_{th}$ represents the trust threshold value of route
(8) Add $(n_x, r(n_z, n_n))$ to $R^*_{Q_0}(n_x, n_n)$, $R^*_{Q_0}(n_x, n_n)$ represents the candidate set of the optimal route
(9) **end if**
(10) **end for**
(11) **if** $R^*_{Q_0}(n_x, n_n) = 0$
(12) n_x is removed out of the WSN
(13) **end if**
(14) **for** $j = 1; j < t; j++$
(15) $R^*_{Q_j}(n_x, n_n) = \oplus_{Q_j} r^*_{Q_{j-1}}(n_x, n_n)$, $r^*_{Q_{j-1}}(n_x, n_n) \subseteq R^*_{Q_{j-1}}(n_x, n_n)$
(16) **end for**
(17) **if** $R^*_{Q_t}(n_x, n_n) = 0$
(18) n_x is removed out of the WSN
(19) **else**
(20) Add n_x to N^*
(21) **return** $r^*_P(n_x, n_n)$, $r^*_P(n_x, n_n) \subseteq R^*_{Q_t}(n_x, n_n)$
(22) **end if**
(23) **end for**
(24) **end while**
(25) Process end

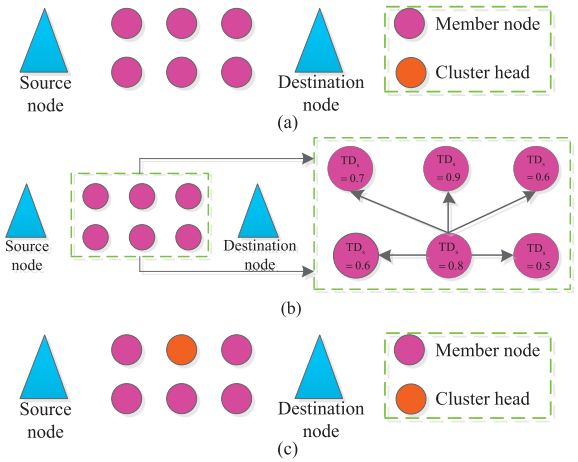

FIGURE 3. The choice process of cluster head.

Fig. 3 (b) shows the trust degree of each node in the model, where, the TD_s of neighbor nodes received by node with $TD_s = 0.8$ are 0.7, 0.9, 0.6, 0.6 and 0.5, respectively. It can be seen that the neighbor with high trust degree is the node whose TD_s is 0.9 by comparison, so the node with $TD_s = 0.8$ is associated with the node whose TD_s is 0.9 and becomes its member node. Considering the possible geographical overlap between clusters in the process of deployment, it is possible to select nodes with the highest TD_s in adjacent nodes as cluster head after finite comparisons, as shown in Fig. 3(c).

B. ROUTE CONSTRUCTION PROCESS

The network initialization is finished after determining the cluster head according to TD_s, then the transmission link need to be constructed. The establishment steps of TSSRM proposed in this paper is shown in Fig. 4.

S1. Node n_0 initializes the process of trust derivation and transmits the trust request packet TR to its neighbors (eg, node n_2) when it is ready to transmit message to node n_{11}. The trust request packet is expressed as $TR = \langle ei_{id}, ed_{id}, td(r)_{th}, ts, s, hl \rangle$, where ei_{id} and ed_{id} represent the identity of assessing node and assessed node, respectively. $td(r)_{th}$ denotes the threshold of route trust. ts denotes timestamp and s denotes the serial number of trust request packets. hl represents the hop counter of TR, hl is positive integer and decreases with the increasing of the number of forwarding. hl should not be set too large in order to reduce the flooding overhead caused by the trust transmission. In order to facilitate the description of the routing process, node n_0 is identified by ei_{id} and node n_2 is identified by ed_{id}. Node n_2 needs to check the freshness firstly after receiving the trust request packet, and the request will be abandoned if it is duplicate, otherwise, the request will be broadcasted to all the neighbor nodes of n_2.

S2. The neighbor nodes (n_1, n_3 and n_6) of node n_2 will send the trust reply to node n_0 through the reverse route after receiving the trust request packet. However, all the neighbor nodes that received the request will discard the request and no longer forward it if the value of hl in the trust request packet is decremented to zero.

S3. After obtaining the parameters provided by the neighbor nodes of node n_2, node n_0 will evaluate the trust status of node n_2 by combining direct trust, indirect trust and incentive factor. Then, node n_0 determines whether node n_2 can be as a relay node according to the constraint condition of trust route. Node n_0 can obtain a credible forwarding set (n_2, n_3) and send routing requests to the nodes in it according to the constructed trust calculation model.

S4. If there is an optimal route to node n_{11} in the credible node routing table, any intermediate credible node that

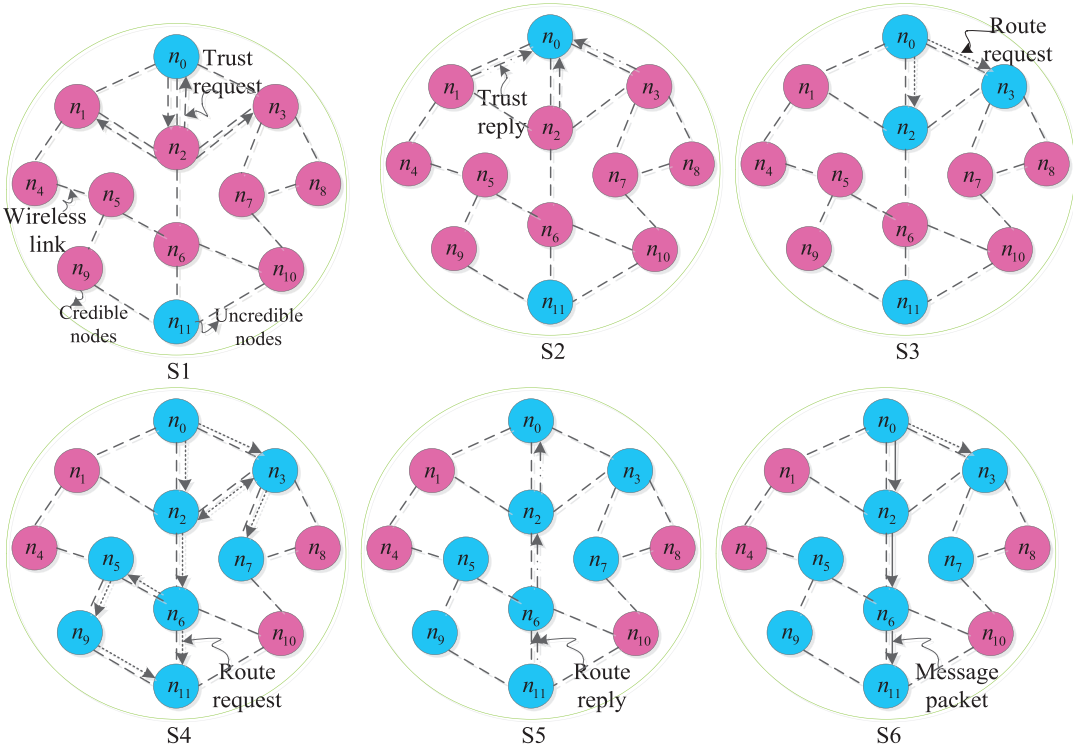

FIGURE 4. Routing process.

receives routing requests will send a reply to node n_0 so that the optimal route from n_0 to n_{11} can be obtained. In this case, go to S6. S1-3 will be repeated to find the next credible node if there is no optimal route to node n_{11} in the credible node routing table that received the routing requests.

S5. Node n_{11} will send a reply to node n_0 via the reverse route according to the routing algorithm in table 2 if it receives routing requests.

S6. The source node n_0 will send a packet to the destination node n_{11} via the constructed optimal route.

Considering that the direct trust derivation model mainly depends on its own detection system, which produces a little communication overhead. However, the indirect trust model is inseparable from the communication overhead since it involves the information interaction between recommended nodes. The TSSRM constructed in this paper only selects the suggestions provided by neighbor nodes of the evaluated node, which control the recommended range and reduce the communication overhead in the process of information transmission. In addition, the combination of direct trust, indirect trust and incentive factor can effectively detect the nodes which give up relay forwarding to save energy, so as to expel attack nodes or selfish nodes from the credible route quickly.

C. ROUTE MAINTENANCE METHODS

Route maintenance is used to handle the credible route repair caused by node movement or failure in WSN and the credible route update when new nodes are joined. Considering the credible route $n_0 \rightarrow n_2 \rightarrow n_6 \rightarrow n_{11}$ constructed in Fig. 4, the maintenance process of credible route can only be initiated from the upstream node at the beginning of the arrow to the downstream node at the end of the arrow. The upstream node of the failed link initiates route maintenance to obtain a new credible route to the destination node when any link in the route fails, for example $n_2 \nrightarrow n_6$. The direct trust degree of node n_6 for node n_2 will be updated immediately as every transaction occurs. If the change of the direct trust of node n_6 for node n_2 is greater than the trust update threshold value ε ($\triangle dt(n_2, n_6) > \varepsilon$), the node n_2 will evaluate the trust degree of node n_6, which is similar to S1-3 of TSSRM. Node n_2 will send routing update packets to source node n_0 via reverse route if it cannot find an alternative route to node n_6 or the trust degree of alternative route cannot meet the trust constraint conditions, and the optimal credible route will be reconstructed.

V. SIMULATION RESULTS AND PERFORMANCE EVALUATION

The performance of TSSRM is analyzed by NS2 in this paper. The simulation time is 500s; the malicious nodes can launch grayhole, tampering, on-off and bad mouthing attacks in the simulation. The basic routing protocol adopts GPSR, other defaults. All of the experiment parameters are shown in Table 3.

TABLE 3. Experiment parameters.

Parameters	Value
The type of sensor nodes	Normal node N, Malicious node M
Monitoring area	200 m×200 m
The number of sensor nodes	100
Communication distance	40m
Message internal	5s
Length of message	100B
Original trust degree	[0.5,1]
Distrust internal	[0,0.45]
Probability of error detected events	0.1
EB	1000J
E_{th}	400J
$P(a)$	0.01
$N(a)$	-0.1
ω_1, ω_2	0.90, 0.98
δ	0.15
$td(r)_{th}$	0.45

A. COMPUTATIONAL COST OF TSSRM

The computational cost of TSSRM is mainly focused on the calculation of trust degree. To analyze the computational complexity of trust degree, let *SA* denote the cost of scalar addition, *SS* denote the cost of scalar subtraction, *SM* denote the cost of scalar multiplication, and *SD* denote the cost of scalar division. In the process of calculating the trust degree of node, the computational cost of direct trust degree is $3SA + 2SM$, the computational cost of indirect trust degree is $SA + SM$, and the computational cost of incentive factor is $SA + SS + SD$. Thus, the total computational cost of trust degree C_{total} is:

$$C_{total} = 5SA + 3SM + SS + SD \tag{19}$$

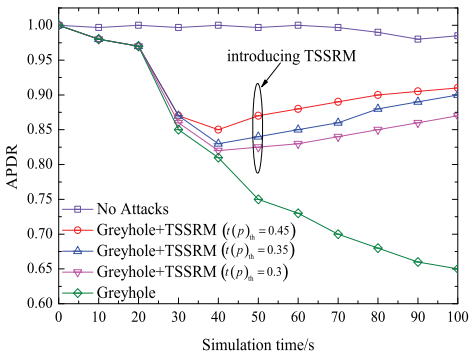

FIGURE 5. APDR under greyhole attack.

B. EFFECT OF ATTACKS ON TSSRM

Fig. 5 and Fig. 6 show the average packet delivery rate (APDR) in the case of grayhole attack which drops 50% packets and tampering attack, respectively. By comparing the different environment (the environment without attack, the attacked environment without using TSSRM and the attacked environment using TSSRM with different threshold), it can be seen that grayhole attack and tampering attack launched by malicious nodes will decrease the APDR. TSSRM can improve the APDR effectively, and the higher

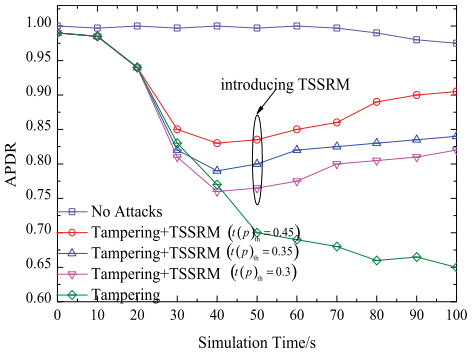

FIGURE 6. APDR under tampering attack.

the threshold sets, the more obvious the improved effect is. However, setting much higher threshold will improve the trust standard, thereby reducing the number of credible nodes and links, which may cause the set of credible link to be empty. Therefore, the threshold of route trust needs to be selected according to the size of deployment and the node density appropriately.

The common trust mechanisms and detection algorithms are difficult to handle on-off attack and bad mouthing attack effectively. Since TSSRM combines behavior with energy and introduces SEDTF in the process of constructing comprehensive trust degree, it can effectively identify the above attack behaviors, as shown in Fig. 7 and Fig. 8. And w represents the proportion of malicious nodes.

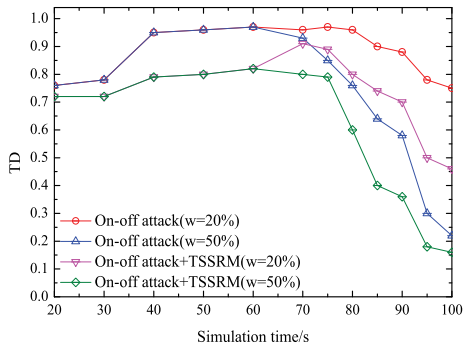

FIGURE 7. TD under on-off attack.

Fig. 7 shows that the trust degree (TD) usually increases with time if there is no abnormal phenomenon (from 20s to 70s). But the trust degree will decline when the malicious nodes activate on-off attack (from 70s to 100s). When the SEDTF is utilized for TSSRM to handle on-off attacks, as time goes on, the more accurate the judgment for the trust of malicious node is, the higher the accuracy of trust evaluation is, because the SEDTF makes that bad behavior will be memorized for a longer time than good behavior. For instance, the trust degree of malicious nodes without SEDTF is 0.58, while the value measured by TSSRM is 0.36 (the proportion of malicious nodes is 50% at 90s).

Fig.8 shows that the inconsistent examine mechanism (IEM) can resist bad mouthing attack effectively.

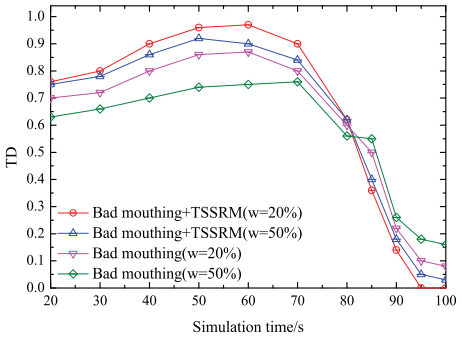

FIGURE 8. TD under bad mouthing attack.

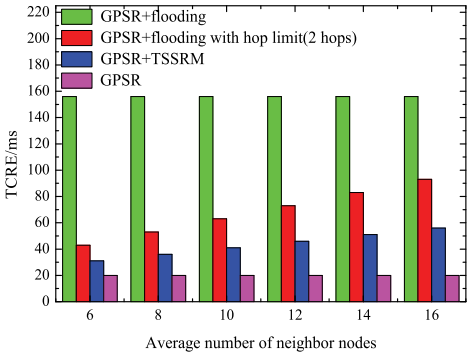

FIGURE 10. Time consumption on routing establishment.

The bad mouthing attacker provides positive/negative suggestions about normal/malicious behavior. Thus, trust degree is much lower when evaluating normal nodes' behavior (from 20s to 70s) under bad mouthing attack, vice versa. However, the trust degree will increase when the behavior of normal node is evaluated with the assistance of IEM, since the IEM can filter out most of the false suggestions and improve the accuracy of trust assessment. For instance, the trust degree of normal node is 0.58 without IEM, while the value measured by TSSRM is 0.97 (the proportion of malicious nodes is 20% at 60s).

C. EFFECTIVENESS AND SECURITY OF TSSRM

In order to maintain the generality, the efficiency and security of TSSRM is evaluated on the basis of BAR [39] and GPSR protocol.

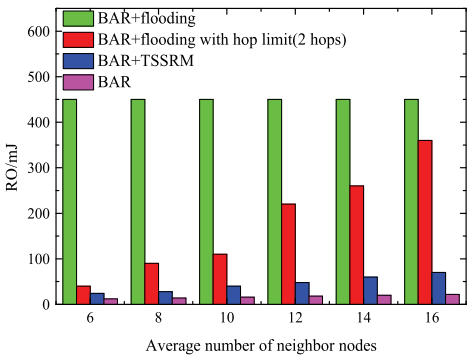

FIGURE 9. Routing overhead.

The routing overhead (RO) of TSSRM in the environments with different network density is shown in Fig. 9. Flooding mechanism is the most effective mechanism to improve the successful rate of route establishment. However, the control information in the process of broadcasting and replaying often leads to much energy consumption. TSSRM can reduce the RO significantly under the premise of ensuring the successful rate of transmission, since it adopts the efficient trust calculation model. The simulation results show that TSSRM will save 80.55% of the RO compared with flooding with 2-hop limit when the number of neighbors is 16, which is similar to BAR which does not use any flooding and security mechanism. Therefore, TSSRM can reduce the energy consumption under the condition of ensuring the successful rate of transmission. The time consumption of routing establishment (TCRE) among different schemes is shown in Fig. 10. In contrast, TSSRM needs to verify the trust degree of node before establishing the routing, so it takes slightly longer time than the GPSR which establishes the routing directly, but the time consumption of TSSRM is much lower than other mechanisms. Specifically, TSSRM can save 39.78% of the time for establishing secure and credible routing compared with the flooding with 2-hop limit when the number of neighbors is 16.

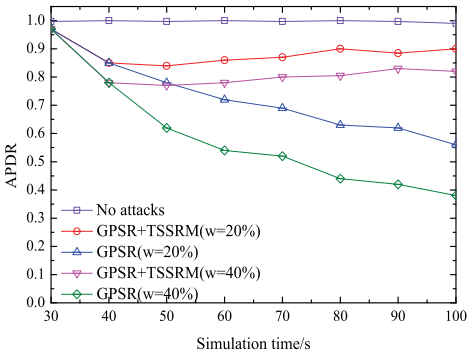

FIGURE 11. The impact of malicious nodes.

Assuming that malicious nodes initiate grayhole, tampering, on-off, and bad mouthing attacks (from 30s) to verify the security of TSSRM in the network. The probability of each attack is 25%. Fig. 11 shows that the APDR increases by about 40% by introducing TSSRM into the existing routing protocols. For example, the APDR has increased from 56% to 90% by introducing TSSRM to existing routing protocol (GPSR) when the proportion of malicious node is 20% at 100s, and the APDR change from 38% to 82% when the proportion of malicious nodes is 40% at 100s.

Trust based source routing protocol (TSR) [40] can kick out untrusted nodes so as to obtain credible information forwarding routing and resist attacks from malicious nodes. In TSR, the source node can establish multiple loopless routes to the destination node during the route discovery process, and each route has an evaluation vector consisting of hop count and route trust. The destination node will select the

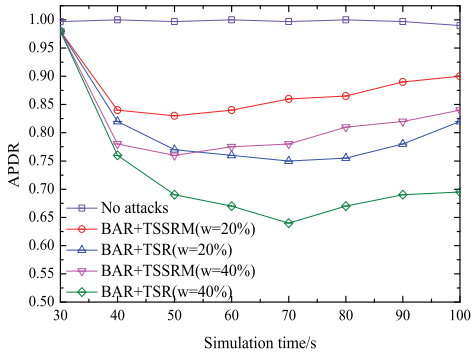

FIGURE 12. The impact of indirect trust.

shortest one as the forwarding routing. But TSR only considers direct trust. Since it is almost impossible to detect the behavior of each node exactly in real conditions, the error probability of detection is set as 0.1. Fig. 12 shows that the APDR will reduce significantly when malicious nodes initiate attacks in WSN (from 30s). TSSRM can increase the APDR by about 10% compared with TSR, since it considers direct trust, indirect trust and incentive factor, which can resist error detection effectively.

VI. CONCLUSION

WSN is an important part of modern communication systems, and trust sensing routing protocol for WSN is an effective way to improve security, therefore, the study of trust sensing routing protocol is very important. This paper presents a trust sensing based secure routing mechanism to handle common network attacks. An optimized routing algorithm is proposed by using semiring theory, which considers the trust degree and other QoS metrics. Simulation results show that TSSRM can reduce the routing overhead and improve the reliability of data transmission compared with the traditional trust mechanism. Future research will design a distributed intrusion detection system for WSN, which may provide a new way for the research of trust degree and ubiquitous routing.

REFERENCES

[1] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with energy harvesting nodes in fading wireless channels: Optimal policies," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1732–1743, Sep. 2011.

[2] N. Marlon, C. Jose, A. B. Campelo, O. Rafael, V. C. Juan, and J. S. Juan, "Active low intrusion hybrid monitor for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 23927–23952, 2015.

[3] G. Ottman, A. Bhatt, H. Hofmann, and G. Lesieutre, "Adaptive piezoelectric energy harvesting circuit for wireless, remote power supply," *IEEE Trans. Power Electron.*, vol. 17, no. 5, pp. 669–676, Sep. 2002.

[4] A. K. A. Mohammad and S. Gadadhar, "Enhancing cooperation in MANET using neighborhood compressive sensing model," *Egyptian Informat. J.*, vol. 6, no. 1, pp. 1–15, 2016.

[5] G. G. Uttam and D. Raja, "SDRP: Secure and dynamic routing protocol for mobile ad-hoc networks," *IET Netw.*, vol. 3, no. 2, pp. 235–243, 2014.

[6] W. K. K. Chin and K. L. A. Yau, "Trust and reputation scheme for clustering in cognitive radio networks," in *Proc. Int. Conf. Frontiers Commun., Netw. Appl. (ICFCNA)*, Kuala Lumpur, Malaysia, Nov. 2014, pp. 1–6.

[7] Y. Gao, H. W. Chris, J. J. Duan, and J. R. Chou, "A novel energy-aware distributed clustering algorithm for heterogeneous wireless sensor networks in the mobile environment," *Sensors*, vol. 15, no. 10, pp. 31108–31124, 2015.

[8] J.-G. Choi and S. Bahk, "Cell-throughput analysis of the proportional fair scheduler in the single-cell environment," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 766–778, Mar. 2007.

[9] K. B. Sourav and M. K. Pabitra, "SIR: A secure and intelligent routing protocol for vehicular ad hoc network," *IET Netw.*, vol. 4, no. 6, pp. 185–194, 2015.

[10] E. Adel, K. Abdellatif, and E. Mohammed, "A new trust model to secure routing protocols against DoS attacks in MANETs," in *Proc. 10th Int. Conf. Intell. Syst. Theories Appl. (SITA)*, Taipei, Taiwan, Oct. 2015, pp. 1–6.

[11] J.-M. Chang, T. Po-Chun, W. G. Isaac, C. C. Han, and C. F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Syst. J.*, vol. 9, no. 6, pp. 65–75, Jun. 2015.

[12] P. G. Fernando, M. C. A. Rossana, T. O. Carina, and J. N. Souza, "EPMOSt: An energy-efficient passive monitoring system for wireless sensor networks," *Sensors*, vol. 14, no. 3, pp. 10804–10828, 2015.

[13] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.

[14] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, to be published.

[15] Z. Liu, X. Yang, P. Zhao, and W. Yu, "On energy-balanced backpressure routing mechanisms for stochastic energy harvesting wireless sensor networks," *Int. J. Distrib. Sensor Netw. (IJDSN)*, vol. 12, no. 8, pp. 1–9, 2016.

[16] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2471–2481, Jun. 2009.

[17] Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 2013–2027, Sep. 2016.

[18] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks," *Ad Hoc Netw.*, vol. 19, no. 6, pp. 142–155, 2014.

[19] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method," *Int. J. Netw. Secur.*, vol. 5, no. 9, pp. 14–21, 2007.

[20] D. Zhu, X. Yang, W. Yu, and X. Fu, "Network coding vs. Traditional routing in adversarial wireless networks," *Int. J. Ad Hoc Netw.*, vol. 20, no. 2, pp. 119–131, 2014.

[21] P. Zhao, X. Yang, W. Yu, and X. Fu, "A loose virtual clustering based routing for power heterogeneous MANETs," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2290–2302, Sep. 2013.

[22] W. Yu and J. Lee, "Efficient energy sensitive routing protocols in mobile ad-hoc networks," in *Proc. Process. Int. Conf. Wireless Netw.*, Shanghai, China, Jun. 2002, pp. 3–9.

[23] R. Morsi, D. S. Michalopoulos, and R. Schober, "Multiuser scheduling schemes for simultaneous wireless information and power transfer over fading channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 1950–1964, Apr. 2015.

[24] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.

[25] B. Paramasivan, M. J. V. Prakash, and M. Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks," *J. Commun. Netw.*, vol. 17, no. 1, pp. 75–83, Feb. 2015.

[26] I. Krikidis, S. Timotheou, S. Nikolaou, and G. Zheng, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 16424–16450, Nov. 2014.

[27] A. Vosoughi, R. C. Joseph, and A. Marshall, "Trust-aware consensus-inspired distributed cooperative spectrum sensing for cognitive radio ad hoc networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 2, no. 3, pp. 24–37, Sep. 2016.

[28] A. Cornejo, S. Viqar, and J. L. Welch, "Reliable neighbor discovery for mobile ad hoc networks," *Ad Hoc Netw.*, vol. 12, no. 6, pp. 259–277, 2014.

[29] Y. Sun, Z. Han, and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE J. Mag.*, vol. 46, no. 2, pp. 112–119, Feb. 2008.

[30] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electron. Notes Theor. Comput. Sci.*, vol. 197, no. 2, pp. 131–140, 2008.

[31] E. Cho, S. A. Myers, and J. Leskovec, "Friendship and mobility: User movement in location-based social networks," in *Proc. ACM SIGKDD*, Oct. 2011, pp. 8–10.
[32] J. Q. Ma, Y. P. Zhong, and S. Y. Zhang, "Frequency-hopping based secure schemes in sensornets," in *Proc. 5th Int. Conf. Comput. Inf. Technol. (CIT)*, Shanghai, China, Sep. 2015, pp. 459–463.
[33] R. Jay, V. Sunil, and G. Chirag, "Securing VANET by preventing attacker node using watchdog and Bayesian network theory," *Procedia Comput. Sci.*, vol. 79, no. 12, pp. 649–656, 2016.
[34] M. C. Zhang, C. Q. Xu, J. F. Guan, Q. T. Wu, R. J. Zheng, and H. K. Zhang, "B-iTRF: A novel bio-inspired trusted routing framework for wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 2242–2247.
[35] G. Lu, "Design and implement of intrusion detection system in network security," M.S. thesis, Northeast Petroleum Univ., Daqing, HL, China, 2003.
[36] P. F. Xu, Z. G. Chen, and X. H. Deng, *Research On Neighboring Graphs Based Topology Control In Wireless Sensor Networks*. Beijing, China: Publishing House Electronics Industry, 2006, pp. 13–17.
[37] Y. L. Sun, W. Yu, and Z. Han, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–315, Feb. 2006.
[38] J. F. Tian, X. Y. Chen, and T. Liu, "Trust evaluation model based on semiring," *Comput. Eng. Appl.*, vol. 44, no. 15, pp. 88–91, 2008.
[39] M. E. Mahmoud and X. Shen, "Trust-based and energy-aware incentive routing protocol for multi-hop wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Budapest, Hungary, Jun. 2008, pp. 88–91.
[40] H. Xia, Z. Jia, X. Li, L. Ju, and E. H. M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Netw.*, vol. 11, no. 7, pp. 2096–2114, 2013.

DANYANG QIN received the B.Sc. degree in communication engineering and the M.Sc. and Ph.D. degrees in information and communication system from the Harbin Institute of Technology, in 2006, 2008, and 2011, respectively. She is currently a Post-Doctoral Fellow with the Electronic Science and Technology Post-Doctoral Research Center and an Associated Professor with Heilongjiang University. Her current researches include wireless sensor network, wireless multihop routing and ubiquitous sensing.

SONGXIANG YANG received the bachelor's degree in communication engineering from Heilongjiang University in 2015. He is a Post-Graduate Fellow with the School of Electronics Engineering, Heilongjiang University. He has been a member of the Advance Ubiquitous Networking Communication Team. His current research is the key technologies in wireless sensor network.

SHUANG JIA received the bachelor's degree in communication engineering from Heilongjiang University in 2014. She is a Post-Graduate Fellow with the School of Electronics Engineering, Heilongjiang University. She has been a member of the Advance Ubiquitous Networking Communication Team. Her current research is the key technologies in wireless sensor network.

YAN ZHANG received the bachelor's degree in communication engineering from Heilongjiang University in 2016. She is a Post-Graduate Fellow with the School of Electronics Engineering, Heilongjiang University. She has been a member of the Advance Ubiquitous Networking Communication Team. Her current research is the key technologies in wireless sensor network.

JINGYA MA received the bachelor's degree in communication engineering from Heilongjiang University in 2015. She is a Post-Graduate Fellow with the School of Electronics Engineering, Heilongjiang University. She has been a member of the Advance Ubiquitous Networking Communication Team. Her current research is the key technologies in wireless sensor network.

QUN DING received the B.Sc. degree from the Department of Physics, Heilongjiang University, and the M.Sc. and Ph.D. degree in instrument science and technology from the Harbin Institute of Technology, in 1997 and 2007, respectively. She is a Professor/Doctoral Supervisor, and the Dean of Electronic Engineering College, Heilongjiang University, the Director of the key lab of electronic engineering high universities, and the institute of communications in Heilongjiang Province. Her current researches include security and communication privacy, wireless network technology.