Received: 28 April 2020 | Revised: 11 July 2020 | Accepted: 3 August 2020

DOI: 10.4218/etrij.2020-0147

ORIGINAL ARTICLE

ETRI Journal WILEY

Trust-aware secure routing protocol for wireless sensor networks

Huangshui Hu[1] | **Youjia Han**[1] | **Hongzhi Wang**[2] | **Meiqin Yao**[1] | **Chuhang Wang**[3]

[1]College of Computer Science and Engineering, Changchun University of Technology, Chaoyang, China

[2]College of Computer Science and Engineering, Jilin University of Architecture and Technology, Changchun, China

[3]College of Computer Science and Technology, Changchun Normal University, Changchun, China

Correspondence
Hongzhi Wang, College of Computer Science and Engineering, Jilin University of Architecture and Technology, Changchun, China.
Email: 2814813541@qq.com

Funding information
"Thirteenth Five-Year" Science and Technology Project of Education Department of Jilin Province, Grant/Award Number: JJKH20181166KJ; Province Development and Reform Commission Project, Grant/Award Number: 2019C054-4

A trust-aware secure routing protocol (TSRP) for wireless sensor networks is proposed in this paper to defend against varieties of attacks. First, each node calculates the comprehensive trust values of its neighbors based on direct trust value, indirect trust value, volatilization factor, and residual energy to defend against black hole, selective forwarding, wormhole, hello flood, and sinkhole attacks. Second, any source node that needs to send data forwards a routing request packet to its neighbors in multi-path mode, and this continues until the sink at the end is reached. Finally, the sink finds the optimal path based on the path's comprehensive trust values, transmission distance, and hop count by analyzing the received packets. Simulation results show that TSRP has lower network latency, smaller packet loss rate, and lower average network energy consumption than ad hoc on-demand distance vector routing and trust based secure routing protocol.

KEYWORDS
Direct trust value, energy efficiency, indirect trust value, secure routing, trust-aware, wireless sensor networks

1 | INTRODUCTION

With the rapid development of the Internet of Things, wireless sensor networks (WSNs) are increasingly more widely used in military, environmental monitoring, medical care, industrial production, the smart city [1], traffic control, and other fields [2–7]. However, the limited computing power, storage capacity, energy, and other restrictions of the nodes influence the development of WSNs [8]. When randomly deployed in complex environments, WSNs are especially vulnerable to routing attacks from malicious nodes. Therefore, it is essential to establish new methods that can optimi ze security issues and reduce energy consumption in WSN [9], and studying secure routing protocols has become a popular topic for WSNs in the last decades [10].

Usually, encryption and authentication-based security mechanisms are used to defend against routing attacks from malicious nodes, which are unable to resist internal routing attacks because the attacker already has all the key and password information [11,12]. Moreover, complex calculations are needed for these mechanisms, consuming extra energy [13,14]. Hence, trust-aware–based security mechanisms have been proposed to solve the problems in encryption and authentication-based security mechanisms.

To ensure the security of WSNs, trust-based schemes have been proven to be more resistant to internal node attacks [15]. A trust-based scheme is helpful for predicting the future behavior of nodes according to past observations of them and for identifying an effective decision based on a suspicious node's behavior; this provides a new solution for the routing security

of WSNs. However, the traditional trust-aware–based routing protocols also have some drawbacks such as high energy consumption and few types of defendable attacks. In addition, the paths whose comprehensive trust value is based on hops may be inappropriate for data forwarding because the paths with a higher comprehensive trust value have more hops.

As mentioned above, the trust-aware secure routing protocol in WSN still faces the following major challenges:

(i) How to detect malicious nodes quickly: If the malicious nodes cannot be quickly found and excluded from the network, a large amount of data will be lost.
(ii) How to make the network resistant to multiple routing attacks: If the network can defend itself from only a few types of network attacks, the network will still face major security risks.
(iii) How to reduce the network energy consumption. One of the most important goals of WSNs is energy saving, which extends the network lifetime.

In this paper, a novel trust-aware secure routing protocol (TSRP) is proposed that considers not only the direct trust value between a node and its neighbors but also the indirect trust value decided by the common neighbors between the node and one of its neighbors. Moreover, volatilization factors are introduced to rapidly reduce the previously high trust value of malicious nodes to exclude them as early as possible. At the same time, a comprehensive trust value based on direct trust value, indirect trust value, and energy trust value is designed to defend against black-hole, selective forwarding, hello flood, and sinkhole attacks. Finally, according to the link quality and hops of the paths, the sink selects the optimal path with a high comprehensive trust value and few hops to avoid wormhole attacks. Simulations are presented to evaluate the performance of TSRP with respect to average residual energy, throughput, average end-to-end delay, average packet loss ratio, and average comprehensive trust value.

The rest of this paper is organized as follows: Section 2 presents the related work, and Section 3 provides the system model. The detail design of TSRP is described in Section 4. Simulations are given in Section 5. Finally, the paper is concluded in Section 6.

2 | RELATED WORK

Many encryption-based schemes have been proposed in the last decades to not only prolong network lifetime but also guarantee network security. Kumaran and Ilango [16] proposed a hybrid offline and online encryption scheme that can realize both digital signature and encryption. Simulations show it can increase packet transmission rate and reduce communication collisions. Its drawbacks mainly include high computational complexity and ambiguous types of defensible attacks. Subsequently, in [17], a new encryption method based on elliptic curve cryptography (ECC) and homomorphic encryption was presented to ensure secure data transmission in clustering WSNs. The study specifically describes the attacks it can defend against such as hello flood, denial of service, and compromised cluster head attacks. However, this method leads to a high packet loss rate and long delay. In [18], the ECC algorithm was also used to generate binary strings for each sensor to form an unique 176 bit key to effectively defend against hello flood and selective forwarding attacks. Moreover, the packet loss rate and delay are also reduced. However, the residual energy of each node varies greatly when the algorithm runs 1000 rounds, which leads to unbalanced energy consumption. In [19], an improved protocol based on ECC was proposed to accelerate the authentication of multiuser message broadcasting. The protocol consists of four parts to realize the secure transmission of data: (a) system initialization; (b) user addition; (c) multiuser broadcast authentication; and (d) user revocation. In addition, it focuses on the improvement of the signature verification phase to reduce the computing cost of each node. The results show that the complexity and computational cost of the protocol are significantly reduced. However, none of the above encryption algorithms can effectively defend against attacks launched within the network.

Consequently, trust management-based secure routing protocols have been presented to solve the problems of the traditional encryption-based schemes. In [20], a trust-based drone energy-saving data acquisition scheme was proposed, which uses the quadratic optimization method of the drone path to find routing paths. Moreover, trust inference and evolve mechanisms are also utilized to identify the trust degree of the sensor node. Therefore, it can effectively find an optimized data collection trajectory and better balance the energy consumption of the network. In the beta reputation and direct trust (BRDT) model [21], the beta and direct trust model is used for secure communication in WSNs to reduce energy consumption. However, large overlapping areas of communication range among the cluster heads often lead to too many cluster heads, which wastes energy accordingly. In addition, the defendable attacks were not specified in BRDT. In [22], a secure routing protocol based on the trust levels of nodes called GradeTrust was proposed to defend against black-hole attacks. The packet delivery ratio is improved in GradeTrust, but only a black-hole attack can be defended against. Therefore, to defend against other kinds of attacks, a clustering-based secure routing protocol was proposed in [23]. First, the energy-efficient clustering algorithm is used to select cluster heads. Next, a trusted hardware module is adopted to encrypt the data during the operation of the network, which can effectively defend against many kinds of attacks such as data confidence and data integrity, and

compare node attacks. However, the cluster head nodes need to have permanent energy supply equipment, which leads to high requirements for the WSN layout. In [24], a trust-based energy-preserving multihop routing protocol was proposed, which is a hybrid of encryption and a trust management-based protocol. However, it does not calculate the indirect trust value, so some errors will occur when calculating the trust values of neighbor nodes. Therefore, a trust sensing secure routing mechanic was proposed in [25] based on semiring theory. It considers the direct trust calculation of nodes, indirect trust calculation of nodes, incentive factor, energy trust, and quality-of-service metrics to optimize secure routing paths. High computing power for the nodes is needed in [25]. Hence, to reduce the computational complexity of the nodes, a lightweight and quickly deployable trust–based secure routing protocol (TBSRP), which can detect and isolate the misbehaving nodes, was proposed in [26]. The protocol extends the route establishment process in ad hoc on-demand distance vector (AODV) routing [27] to select a reliable and effective path that includes all trusted nodes. The salient features of AODV include on-demand route finding, reduced control packet overhead, providing the latest routing information, broadcastingor unicasting routes at the same time, low storage cost, high scalability, and short connection establishment time [15]. Moreover, TBSRP uses a distributed trust model to identify malicious nodes dynamicallyto isolate them as early as possible. If the active path encounters a node with abnormal behavior, TBSRP can reroute the packet to an alternate routing path. The trust degree and hop number of nodes are used to select the most reliable and shortest routing path. However, it does not consider the energy of nodes while calculating the trust values, which may result in selecting nodes with high trust but low energy as the next hop.

3 | SYSTEM PRELIMINARIES

3.1 | Network model

A WSN with n nodes is considered to be randomly deployed over an L m × M m rectangular area of interest in this paper, and each node sends the information to the sink through one of its neighbors. The following assumptions are made to simplify the model.

- Each node and the sink are unmovable after deployment.
- Homogeneous nodes are considered and possess equal amount of initial energy; moreover, energy supplementation is impossible.
- Each node has a unique identifier number (ID).
- The distance between any pair of nodes or any node and the sink can be calculated based on the received signal strength.
- Radio links are symmetric.
- The sink knows the location information and ID of each node after deployment.

3.2 | Node trust model

The trust value of nodes is the basis of participating in secure routing cooperation, which means a node with a larger value is more likely to be selected as the relay node in the routing path. The direct trust value, indirect trust value, volatilization factor, and residual energy of a node are used to calculate the comprehensive trust value, and the node is considered to be untrustworthy if the comprehensive trust value is less than the preset threshold.

3.2.1 | Direct trust value

Based on the received and sent packets of its neighbors, a node can obtain its direct trust values with each neighbor, and the current direct trust value of node i with respect to its neighbor j can be formulated as

$$\mathrm{DT}_{ij}^{n} = \gamma * (\omega_1 R_t + \omega_2 S_t)^{n-1} + (1-\gamma) * (R_t + S_t)^{n}. \quad (1)$$

in which the former represents the historical trust value, and the latter represents the current trust value. Moreover, γ and $(1-\gamma)$ $(0 < \gamma < 1)$ are the weights for the historical and current trust values, respectively, which depend on the specific application of WSNs. Finally, R_t and S_t are the ratios of the number of sent and received packets to the total number of packets, respectively, which can be represented as follows.

$$R_t = \frac{\mathrm{receive\_message}_j}{\mathrm{message}_j}. \quad (2)$$

$$S_t = \frac{\mathrm{send\_message}_j}{\mathrm{message}_j}. \quad (3)$$

In addition, volatilization factors ω_1 and ω_2 are defined to rapidly exclude malicious nodes who have been transformed from normal nodes with high trust values so as to reduce a previously high trust value as soon as possible. This is represented as

$$\omega_1 = e^{-c_1 \ mod \ (T,\tau)}, \quad (4)$$

$$\omega_2 = e^{-c_2 \ mod \ (T,\tau)}, \quad (5)$$

where T is the current time of the network, and τ is the time threshold. In addition, c_1 and c_2 are factors used to adjust the speed of the change in trust value. To avoid misclassifying

some legitimate nodes, such as those at remote locations, who do not participate in sending and forwarding packets for a long time, mod(T, τ) is introduced to ensure that the historical trust value is not too small, and the volatilization factor decays periodically in a certain range. In addition, the values of τ, c_1, and c_2 are application-specific.

3.2.2 | Indirect trust value

The indirect trust value of node i to node j is based on the trust relationship provided by the third-party node. As shown in Figure 1, node B_i is a third-party trusted node. Node i is the trust evaluator, node j is the evaluation target, and node B_i is the recommender of node i. Here, $B_i \in B_h = \{B_1, B_2, \ldots, B_m\}$ (m is the number of the common trusted nodes), and B_h is the set of public trusted neighbor nodes of node i and node j. The indirect trust value of node i to node j is shown as below.

$$\mathrm{IT}_{ij}^{n} = \frac{1}{m} \sum_{B_i \in B_h} \left(\mathrm{DT}_{iB_i}^{n} * \mathrm{DT}_{B_i j}^{n} \right), \tag{6}$$

where $\mathrm{DT}_{iB_i}^{n}$ is the direct trust value of node i to B_i, and $\mathrm{DT}_{B_i j}^{n}$ is the direct trust value of node B_i to j, where node B_i is any public trusted neighbor of i and j. Node B_i will be removed from the set of public trusted neighbors if the trust value of node i to B_i is less than threshold Th^n. In addition, the value of Th^n is set to .

3.2.3 | Energy trust value

The same energy consumption model used in [28] is used in this paper. When a node j receives and transmits l bit data over distance d, the consumed energy of receiving and sending is

$$E\_\mathrm{receive}_j = l * E_{\mathrm{elec}}, \tag{7}$$

$$E\_\mathrm{send}_j = \begin{cases} l * E_{\mathrm{elec}} + l * \varepsilon_{\mathrm{fs}} * d^2 \; d < d_0 \\ l * E_{\mathrm{elec}} + l * \varepsilon_{\mathrm{mp}} * d^4 \; d \geq d_0 \end{cases}, \tag{8}$$

$$d_0 = \sqrt{\varepsilon_{\mathrm{fs}} / \varepsilon_{\mathrm{mp}}}, \tag{9}$$

where E_{elec} denotes the energy/bits consumed by the transmitter electronics, $\varepsilon_{\mathrm{fs}}$ represents the energy consumption for a free space model, and $\varepsilon_{\mathrm{mp}}$ represents the energy consumption for a multipath fading model. Additionally, d_0 is the threshold value for an amplifier to adjust its power.

Let the initial energy of j be E_0. Then, the remaining energy RE_j is

$$\mathrm{RE}_j = E_0 - E\_\mathrm{receive}_j - E\_\mathrm{send}_j. \tag{10}$$

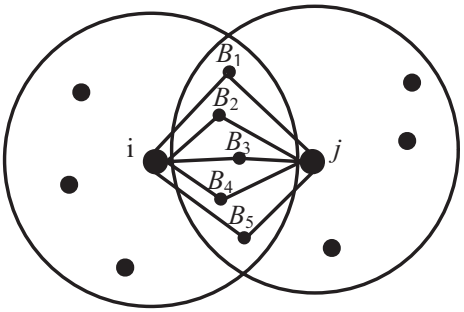

FIGURE 1 Common nodes of nodes i and j

Only when the residual energy RE_j of j is greater than or equal to threshold E_{th} can node j participate in the operation of TSPR, and then the energy trust value of j is

$$E_j = \frac{\mathrm{RE}_j}{E_0}. \tag{11}$$

3.2.4 | Comprehensive trust value

Considering security and energy consumption, the comprehensive trust value of node i to j is formulated as follows:

$$CT_{ij}^{n} = \eta_1 * DT_{ij}^{n} + \eta_2 * IT_{ij}^{n} + \eta_3 * E_j, \tag{12}$$

where η_1, η_2, and η_3 are the weights of the direct, indirect, and energy trust values, respectively, which satisfy $\eta_1 + \eta_2 + \eta_3 = 1$. Moreover, the values of η_1, η_2, and η_3 are 0.34, 0.4, and 0.26, respectively, in this study.

As can be seen from the above description, malicious nodes launching black-hole attacks, which make the values of S_t quickly become close to zero, will be excluded from the network because their comprehensive trust values drop sharply with the rapid reduction in their previous trust values under the action of the volatilization factors. In addition, the values of R_t drop sharply to zero when the malicious nodes launch hello flood attacks, and then, they are excluded because of their low comprehensive trust values. For the same reason, the selective forwarding and sinkhole attacks can be defended against because of their effects on the comprehensive trust value through the volatilization factors S_t and R_t.

4 | PROPOSED PROTOCOL

TSRP consists of two phases, namely routing establishment and routing maintenance. Routing establishment in TSRP is an extension of AODV, which extends the route request (RREQ) and route replies (RREP). Moreover, the node ID, comprehensive trust value, residual energy, and hops are added in RREP.

4.1 | Routing establishment

Any node in the network can broadcast a RREQ message to initiate the process of routing establishment, so the sink could receive multiple RREQs, whose number equal the number of link tables, denoted by link_list = {link_1, link_2, …, link_r}, where r is the number of links. In addition, link i in the link table is composed of the source node and all the relay nodes, which can be represented by link = {node_1, node_2, …, node_k}, where k is the number of nodes in the link, link ∈ link_list. The optimal link is selected from the link table by the sink according to the link quality, which is described as follows:

$$\text{link\_qua} = \sum_{i=1,j=i+1}^{k} \text{CT}_{ij}^{n} \Big/ \text{dis}, \tag{13}$$

where dis is the transmission distance of the link, which can be formulated as follows:

$$\text{dis} = \sum_{i=2}^{k} \left(\sqrt{(\text{node}_i - \text{node}_{i-1})^2}/R \right). \tag{14}$$

It can be seen from (13) if there is a wormhole attack, the distance between two malicious nodes will be very long, which inevitably produces a large dis value to reduce the link quality, and the malicious nodes are excluded from the link. Here, R is the communication radius of the node.

Furthermore, considering the delay of the link, TSRP defines another link quality indicator PV, which is expressed as

$$\text{PV} = \lambda * \left(\sum_{i=1,\, j=i+1}^{k} \text{CT}_{ij}^{n} \Big/ \text{dis} \right) + (1-\lambda) * \text{jump}^{-1}, \tag{15}$$

where jump is the number of hops in the link, and λ and $1-\lambda$ are the weight coefficients of the link quality and link delay, respectively. The PVs are ordered for the link_list from largest to smallest to build the routing table PV_List = {PV_1, PV_2, … , PV_r} , and then, PV_1 is the optimal routing path.

The detailed routing establishment process is described as follows:

1. Any source node i initiates the routing establishment process by broadcasting RREQ to its neighbors that have a comprehensive trust value higher than threshold PV_{th}. After receiving the RREQ, each neighbor checks whether its distance from the sink is less than the distance between node i and the sink. If it is, go to step 2, as shown for nodes 2, 3, 5, and 8 in Figure 2. Otherwise, discard RREQ, as shown for node m.
2. Each selected neighbor, as shown for nodes 2, 3, 5, and 8 in Figure 2, checks whether its residual energy is lower than the preset threshold. If it is, discard RREQ, otherwise go to step 3.
3. Each selected neighbor, as shown for nodes 3, 5, and 8 adds its ID, comprehensive trust value, residual energy, and hops jump = jump + 1 to RREQ and multicasts RREQ.
4. The nodes receiving RREQ check their distance to the sink and residual energy as in steps 1 and 2, and the inappropriate nodes discard RREQ, as shown for node 4 in Figure 2. Moreover, each selected node checks all its received RREQs, and if the source ID is the same, it only broadcasts the RREQ with the shortest distance and the smallest number of hops so as to avoid a routing loop, until the sink receives the RREQs
5. The sink also may receive one or more RREQs such as r_1 and r_2 in Figure 2. It then calculates the PV of each path, sorts them from largest to smallest, and stores the results in link_list. Selecting the first path from link_list, the sink sends an RREP along this path in reverse until source node i is reached.
6. Once the comprehensive trust value or the residual energy of a node in the path is lower than the threshold (as shown for node 10 in Figure 2), the node will send an RERR to the sink along the path to notify the sink of its unreliability. Hence, the sinkselects the second path from link_list to send the RREP again, until the most trusted routing path is found.
7. After receiving the RREP, the source node i transmits data along this path; moreover, the nodes and the surrounding nodes along this path update their comprehensive trust values in a certain period T_t.

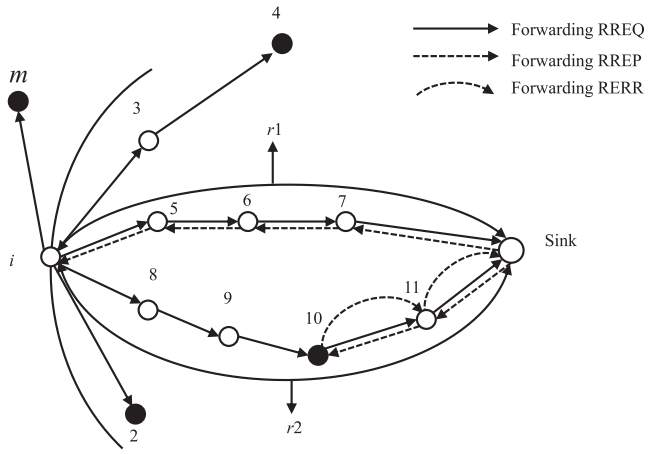

FIGURE 2 Routing establishment

4.2 | Routing maintenance

During the data transmission, the previous path will no longer be trusted once the comprehensive trust value or the

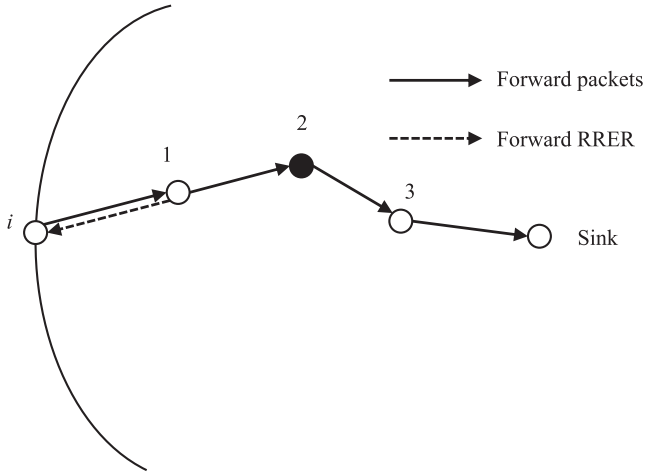

FIGURE 3 Routing maintenance

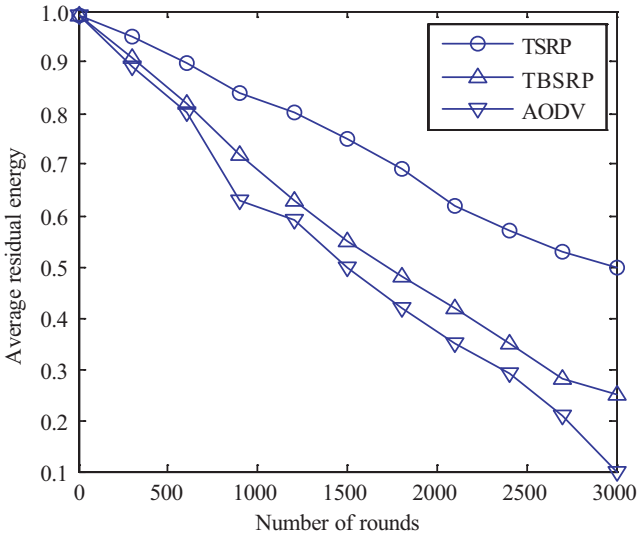

FIGURE 4 Comparison of the average residual energy

residual energy of any node in the path is lower than a threshold, which is called *E* node, as shown for node 2 in Figure 3. Subsequently, routing maintenance is started. The *E* node sends a RERR to source node *i* along the reverse route. Once node *i* receives the RERR, it runs the routing establishment again, as described in Section 4.1.

5 | SIMULATIONS AND ANALYSIS

The performance of our proposed TSRP was evaluated via MATLAB and compared with AODV and TBSRP. In this evaluation, 100 nodes were randomly deployed over a 100 m × 100 m square monitoring area with a communication radius of 30 m. The number of malicious nodes accounted for 10% of all nodes in this network. Malicious nodes could launch wormhole, black-hole, selective forwarding, sinkhole, and hello flood attacks on the network. Among them, each kind of attack accounted for 2% of the malicious nodes. In addition, malicious nodes with selective forwarding attacks randomly dropped 60% to 80% of the packets. Other simulation parameters are shown in Table 1.

TABLE 1 Simulation parameters

Parameter	Value
Initial energy of the node	1J
Control packet size	400 bits
Data packet size	4000 bits
Initial trust value	0.5
CT_{th}	0.35
c_1	0.04
c_2	0.03
d_0	87 m

5.1 | Average residual energy

First, the average residual energy of the network, which is the average value of the residual energy of all the surviving nodes, was tested. Figure 4 compares the average residual energy for the case of five malicious nodes in the network.

IT can be seen in Figure 4 that the average residual energy of AODV drops sharply to 0.16 J because of the absence of a defensive measure; therefore, the malicious nodes deteriorate the structure of the network and lead to uneven energy consumption. For TBSRP with a security scheme, its average residual energy decreases gradually to 0.3 J. However, the average residual energy is only reduced to 0.5728 J for TSRP because each node selects the nodes with larger comprehensive trust values and more residual energy as its next hop nodes, so the energy consumption is more balanced than that of AODV and TBSRP.

5.2 | Average end-to-end delay

Second, the average end-to-end delay was evaluated and the results are compared in Figure 5. With the increase in malicious nodes, the average end-to-end delay for all algorithms increases. In AODV, the packet loss rate increases rapidly with the increase in malicious nodes because there is no defensive measure. Once packet loss occurs, the node needs to establish reconnection and retransmit the packets, which undoubtedly increases the end-to-end delay. For TBSRP and TSRP, the average end-to-end delay slowly increases with the increase in malicious nodes because of their adopted security mechanisms. However, the delay of TSRP is significantly lower than that of TBSRP. As Figure 5 shows, the end-to-end

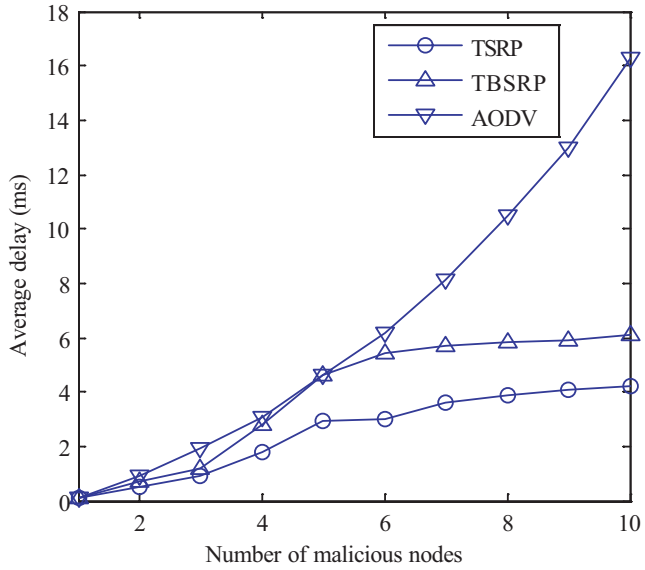

FIGURE 5 Comparison of the average end-to-end delay

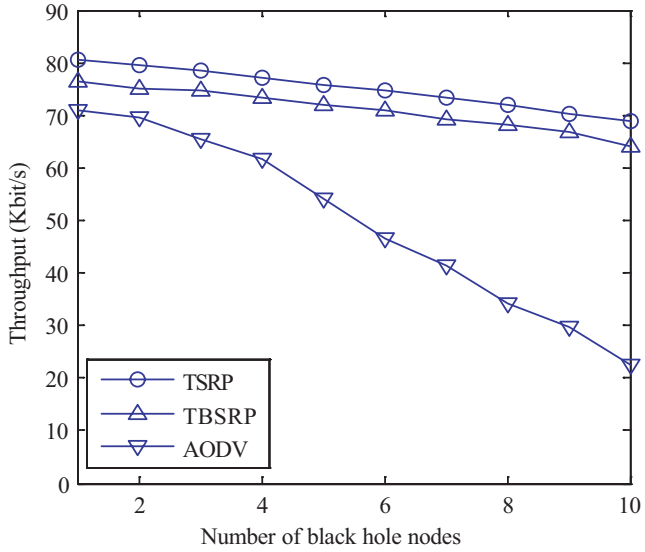

FIGURE 6 Comparison of the network throughput

delay for TBSRP is 6.11 ms whereas that of TSRP is 4.23 ms when the number of malicious nodes is 10. The main reason is that TSRP selects not only more secure paths but also paths with fewer hops to transmit data than does TBSRP.

5.3 | Throughput

Third, as shown in Figure 6, the throughput of the network decreases as the number of black-hole nodes increases, because the increase in black-hole nodes disrupts network routing and the loss of a large number of packets leads to a reduction in throughput. Because the AODV protocol does not have any protection measures, the network throughput is rapidly reduced from 70.82 kbit/s to 22.48 kbit/s. The TBSRP and TSRP protocols use a trust model to protect the routing security of the network and enhance the stability of the network routing. Therefore, the downward trend in TBSRP and TSRP agreements is relatively flat. In contrast to TBSRP, TSRP considers the influence of historical trust value on the node's comprehensive trust value and defines a volatilization factor to enhance the accuracy of trust evaluation, thereby increasing the speed of malicious node recognition. In addition, the sink selects the safest route from many routes to reduce the possibility of malicious nodes becoming relay nodes. Therefore, the throughput level of TSRP is better than that of the TBSRP protocol.

5.4 | Average packet loss rate

Finally, the average packet loss rate is given in Figure 7, which is the ratio of the difference between the number of the packets sent by the source node and the number of the packets received by the sink to the number of the packets sent by the source node. The average packet loss rate for AODV increases rapidly with the increase in rounds because of its absence of a security scheme. At the same time, the packet loss rates of TSRP and TBSRP increase first and then decrease. Furthermore, the packet loss rate of TSRP starts to decline after 2100 rounds, but that of TBSRP declines after 2400 rounds, which means TSRP excludes malicious nodes from the network faster than does TBSRP. Accordingly, the average packet loss rate of TSRP is 2.23% higher than that of TBSRP.

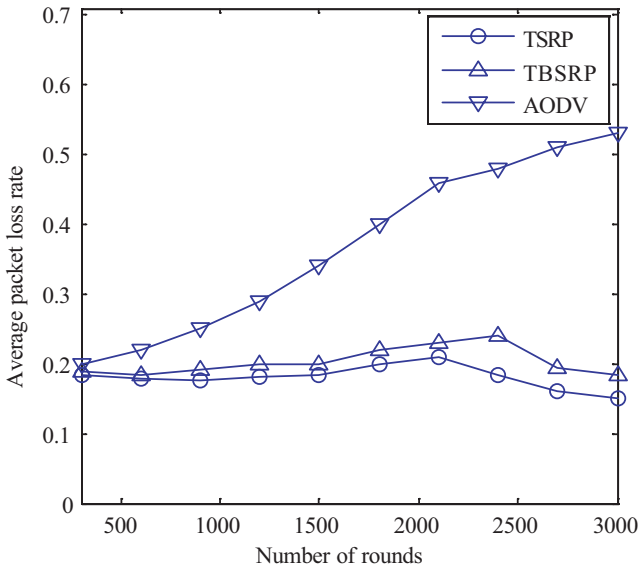

FIGURE 7 Comparison of the average packet loss rate

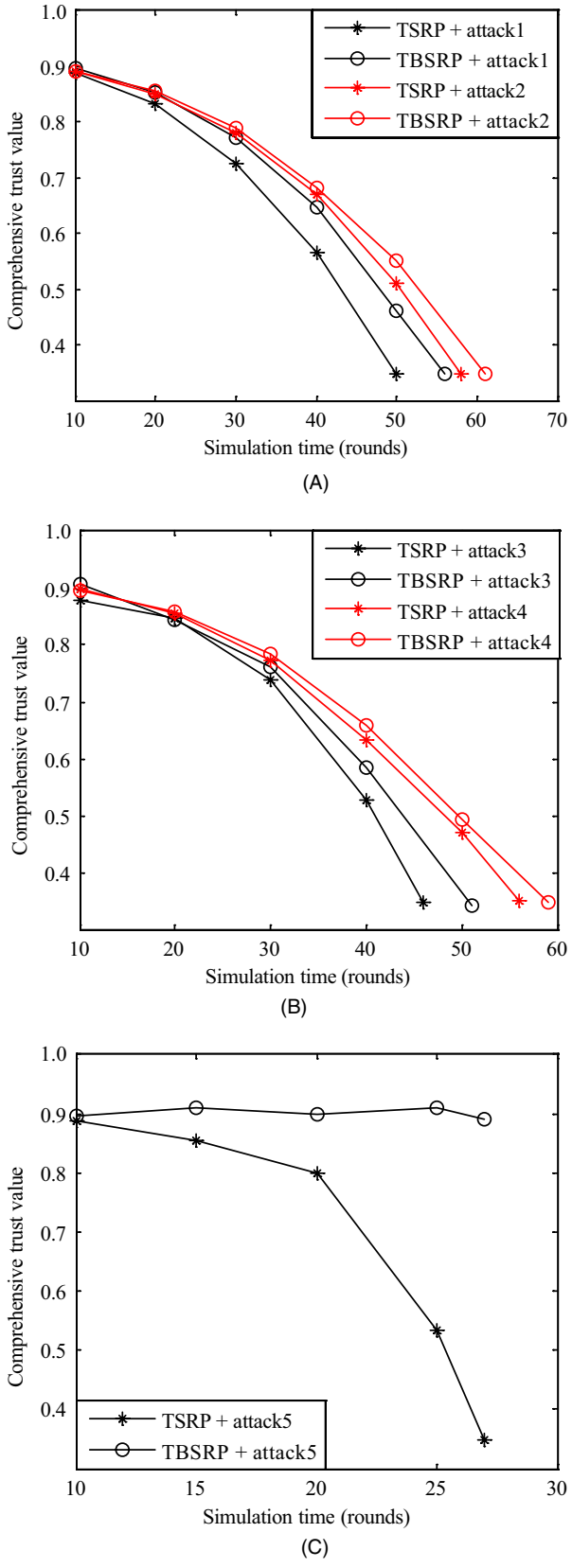

FIGURE 8 Comparison of the average comprehensive trust value: (A) trust models under black-hole and hello flood attacks, (B) trust models under sinkhole and selective forwarding attacks, and (C) trust models under wormhole attacks

5.5 | Average comprehensive trust value under different attacks

The comprehensive trust value of a node represents the security level of the node. A higher comprehensive trust value indicates stronger security. Figure 8 shows the change in the malicious nodes' average comprehensive trust value under different attacks, where attack1, attack2, attack3, attack4, and attack5 represent black-hole, hello flood, sinkhole, selective forwarding, and wormhole attacks, respectively. The proportion of malicious nodes performing each attack is 2%. Figure 8 shows that the average comprehensive trust value of malicious nodes is decreasing. The network determines a node to be a malicious node when its comprehensive trust value drops below 0.35.

As can be seen in Figure 8A and B, the speeds at which TSRP detects black-hole, hello flood, sinkhole, and selective forwarding attacks are 12%, 5%, 10%, and 5.3% higher than the values of TBSRP, respectively. This is because TSRP takes into account the role of historical trust values and volatilization factors when calculating direct trust values so that the trust value of malicious nodes quickly decreases. As Figure 8C shows, when faced with a wormhole attack, TBSRP is powerless, but TSRP can quickly filter out malicious nodes that launch wormhole attacks because in TSRP, the sink calculates the link quality to exclude a link involved in the wormhole attack from the network in the routing establishment phase. Thus, TSRP can quickly reduce its trust value when faced with malicious attacks and exclude it from the network so it can no longer participate in any network behavior.

6 | CONCLUSION

Because of the dynamic and unpredictably changing behavior of nodes, reliable and energy-efficient data transmission is a challenging task. Therefore, this paper proposed a trust-aware secure routing protocol: TSRP. TSRP uses the direct trust value, indirect trust value, volatilization factor, and residual energy to comprehensively calculate the node's comprehensive trust value to resist black-hole, selective forwarding, hello flood, and sinkhole attacks, Next, the sink selects an optimal routing path with high security and few hops to resist wormhole attacks and simultaneously reduce the energy consumption of the optimal path search and data transmission. The simulation results show that TSRP successfully completed the task of secure and energy-saving data transmission. Moreover, TSRP is superior to AODV and TBSRP in terms of energy efficiency, packet loss rate, throughput, average end-to-end delay, and average comprehensive trust value.

CONFLICTS OF INTEREST

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ORCID

Youjia Han https://orcid.org/0000-0003-2154-3234
Meiqin Yao https://orcid.org/0000-0003-4302-550X

REFERENCES

1. Y. Ren et al., *A trust-based minimum cost and quality aware data collection scheme in P2P network*, Peer-to-Peer Netw. Appl. **13** (2020), 2300–2323, doi: https://doi.org/10.1007/s12083-020-00898-2
2. Y. Liu et al., *ActiveTrust: Secure and trustable routing in wireless sensor networks*, IEEE Trans. Inf. Forensics Secur. **11** (2016), 2013–2027.
3. H. Lazrag, R. Saadane, D. Aboutajdine, *A game theoretic approach for optimal and secure routing in WSN*, in Proc. Int. Afro-Eur. Conf. Industrial Adv. (Marrakesh, Morocco), Nov. 2016, pp. 218–228.
4. Y. M. Zhou and L. Y. Li, *A trust-aware and location-based secure routing protocol for WSN*, Appl. Mechan. Mater. **373–375** (2013), 1931–1934.
5. M. Al-Shalabi et al., *Energy efficient multi-hop path in wireless sensor networks using an enhanced genetic algorithm*, Inf. Sci. **500** (2019), 259–273.
6. M. Elhoseny et al., *Optimizing K-coverage of mobile WSNs*, Expert Syst. Appl. **92** (2018), 142–153.
7. Z. Sun et al., *Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks*, Appl. Soft Comput. **77** (2019), 366–375.
8. M. Selvi et al., *An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks*, Wirel. Pers. Commun. **105** (2019), 1475–1490.
9. T. Li et al., *Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things*, Trans Emerging Telecommun. Technol. (2020), e3956, https://doi.org/10.1002/ett.3956.
10. L. Yao, F. X. Gao, and L. Cong, *Research on static game theory based secure routing algorithm in WSN*, Appl. Mechan. Mater. **571–572** (2014), 1030–1036.
11. G. Zhang et al., *Using trust to establish a secure routing model in cognitive radio network*, PLoS One **10** (2015), no. 9, e0139326, doi: https://doi.org/10.1371/journal.pone.0139326
12. P. Gong, T. M. Chen, and Q. Xu, *ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks*, J. Sensors **2015** (2015), 1–10.
13. O. Alfarraj, A. A. Alzubi, and A. Tolba, *Trust-based neighbor selection using activation function for secure routing in wireless sensor networks*, J. Ambient Intell. Humanized Comput. (2018), 1–11, doi: https://doi.org/10.1007/s12652-018-0885-1.
14. G. Dhand and S. S. Tyagi, *SMEER: Secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks*, Wirel. Pers. Commun. **105** (2019), 17–35.
15. Ahmed et al., *Energy-aware and secure routing with trust for disaster response wireless sensor network*, Peer-to-peer Netw. Applicat. **10** (2017), 216–237.
16. U. S. Kumaran and P. Ilango, *Secure authentication and integrity techniques for randomized secured routing in WSN*, Wirel. Netw. **21** (2015), 443–451.
17. M. Elhoseny et al., *A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption*, J. King Saud Univ.-Comput. Inf. Sci. Archive **28** (2016), 262–275.
18. M. Elhoseny et al., *An energy efficient encryption method for secure dynamic WSN*, Secur. Commun. Netw. **9** (2016), 2024–2031.
19. H. Bashirpour et al., *An improved digital signature protocol to multi-user broadcast authentication based on elliptic curve cryptography in wireless sensor networks (WSNs)*, Math. Comput. Appl. **23** (2018), 1–15.
20. B. Jiang et al., *Trust based energy efficient data collection with unmanned aerial vehicle in edge network*, Trans. Emerging Telecommun. Technol. (2020), e3942, doi: https://doi.org/10.1002/ett.3942.
21. B. Priayoheswari et al., *Beta reputation and direct trust model for secure communication in wireless sensor networks*, in Proc. Int. Conf. Inf. Analytics (Pondicherry, India), Aug. 2016, 73:1–11, doi: https://doi.org/10.1145/2980258.2980413
22. D. Airehrour, J. Gutierrez, and S. K. Ray, *Gradetrust: A secure trust based routing protocol for MANETs*, in Proc. Int. Telecommun. Netw. Appl. Conf. (Sydney, Australia), Nov. 2015. pp. 65–70.
23. T. Wang et al., *A trusted and energy efficient approach for cluster-based wireless sensor networks*, Int. J. Distrib. Sensor Netw. **12** (2016), 1–13.
24. S. Raza et al., *Trust based energy preserving routing protocol in multi-hop WSN*, in Networked Systems, vol. 9466, Springer, Cham, Switzerland, 2015, pp. 518–523, doi: https://doi.org/10.1007/978-3-319-26850-7_42
25. D. Qin et al., *Research on trust sensing based secure routing mechanism for wireless sensor network*, Int. Conf. Commun. **5** (2017), 9599–9609.
26. A. Ahmed et al., *Countering node misbehavior attacks using trust based secure routing protocol*, TELKOMNIKA Telecommun. Comput. Electron. Contr. **13** (2015), 260–268.
27. E. Perkins and E. M. Royer, *Ad-hoc on-demand distance vector routing*, in Proc. IEEE Workshop Mobile Comput. Syst. Appl. (New Orleans, LA, USA), Feb. 1999, pp. 90–100, doi: https://doi.org/10.1109/MCSA.1999.749281.
28. W. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, *Energy-efficient communication protocol for wireless microsensor networks*, in Proc. Annu. Hawaii Int. Conf. Syst. Sci. (Maui, HI, USA), Jan. 2000, pp. 3005–3014.

AUTHOR BIOGRAPHIES

Huangshui Hu received his BEng degree in computer applications from Changchun University of Science and Technology (now Jilin University), Changchun, China, in 1999, and his MS and PhD degrees in engineering from Jilin University, Changchun, China, in 2005 and 2012, respectively. From 2005 to 2008, he worked as a research and development manager at Changchun Lianxin Technology Co., Ltd, Changchun, China. From 2008 to 2013, he worked as a technical director of Jilin Omnidirectional Technology Co., Ltd, Changchun, China. Since 2015, he has been with the Department of Computer Science and Engineering, Changchun University of Technology, Changchun, China, where he is now as a professor. His main research interests are topology control in wireless sensor networks and multifunction vehicle bus networks.

Youjia Han received his BEng degree from Anhui Wenda University of Information Engineering, Hefei, China, in 2018. He is now studying for an MS degree at the Changchun University of Technology, Changchun, China. His main research interest is wireless sensor network security.

Hongzhi Wang received his BEng degree in computer applications from Tianjin University of Communication and Electronic System, Tianjin, China, in 1983, and his MS and PhD degrees in engineering from Jilin University, Changchun, China, in 1993 and 2000, respectively. From July 1983 to 2006, he worked at the College of Computer Science and Engineering, Changchun University of Technology, Changchun, China. Since 2018, he has been with the College of Computer Science and Engineering, Jilin University of Architecture and Technology, Changchun, China, where he is now a professor. His main research interests are topology control in wireless sensor networks and multifunction vehicle bus networks.

Meiqin Yao received her BEng degree from Anhui Wenda University of Information Engineering, Hefei, China, in 2018. She is currently studying for a master's degree at Changchun University of Technology, Changchun, China. Her main research interest is wireless sensor networks.

Chuhang Wang received her BEng degree in computer applications from Jilin University, Changchun, China, in 1999 and her MS degree in software engineering from Jilin University, Changchun, China, in 2005. She worked in the network center of Changchun Normal University, Changchun, China, from 2005 to 2011. Since 2005, she has been with the Department of Computer Science and Technology, Changchun Normal University, where she is now an assistant professor. Her main research interests are wireless sensor networks and real-time embedded systems.