IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 26, 2021, accepted April 20, 2021, date of publication April 27, 2021, date of current version January 28, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3075959

Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks

HUANGSHUI HU[1], YOUJIA HAN[1], MEIQIN YAO[1], AND XUE SONG[2]
[1]College of Computer Science and Engineering, Changchun University of Technology, Jilin 130012, China
[2]College of Artificial Intelligence, The Tourism College of Changchun University, Jilin 130618, China

Corresponding author: Youjia Han (364517162@qq.com)

This work was supported by the Science and Technology Development Project of Jilin Province under Grant 20200201009JC and Grant 20210201051GX.

ABSTRACT Due to the characteristics of limited resources and dynamic topology, wireless sensor networks (WSNs) are facing two major problems: security and energy consumption. Nowadays, the trust based solutions are feasible to cope with different bad behaviors of nodes, but there still exist a variety of attacks, high energy consumption and communication congestion between nodes. Therefore, this paper proposes a new trust based secure and energy efficient routing protocol (TBSEER) to solve these problems. TBSEER calculates the comprehensive trust value through adaptive direct trust value, indirect trust value and energy trust value, which can be resistant to black hole, selective forwarding, sinkhole and hello flood attacks. Moreover, the adaptive penalty mechanism and volatilization factor are used to fast identify the malicious nodes. In addition, the nodes only need to calculate the direct trust value, and the indirect trust value is obtained by the Sink, so as to further reduce the energy consumption caused by iterative calculations. Finally, the cluster heads find the safest multi-hop routes based on the comprehensive trust value, which can actively avoid wormhole attack. The simulation results show that the proposed TBSEER reduces network energy consumption, speeds up the identification of malicious nodes, as well as resists all common attacks.

INDEX TERMS Comprehensive trust value, direct trust value, indirect trust value, multi-hop route, WSNs.

I. INTRODUCTION

With the rapid development of Internet of Things, WSNs are more and more widely used in military, environmental monitoring, medical and industrial production, traffic control and other fields [1]–[3]. WSNs are composed of numerous sensor nodes, which collect data from the environment and send it to the Sink hop by hop [4]–[6]. Due to the characteristics of nodes, such as small size, limited memory, computing power and energy, the low energy consumption and low cost of nodes are the main aspects considered in the research and application [7]–[9]. In addition, WSNs are also deployed in the unattended and hostile environment, which makes them vulnerable to a variety of attacks [10], [11], [35]. Especially, there is no fixed topology in WSNs, and each node needs to have the function of routing to forward data. Therefore, the nodes are more vulnerable to various routing attacks [12]. How to defend against routing attacks from malicious nodes has become a hot topic in WSNs.

In order to guarantee the routing security of wireless sensor networks, many researchers have proposed kinds of secure routing protocols based on cryptography and authentication [13]–[16]. However, the security mechanism based on cryptography and identity verification is not appropriate to deal with improper behavior attacks of nodes [17], [18]. Because the premise of implementing these security mechanisms is that all nodes are cooperative and trustworthy, which is unrealistic for internal attacks on the network [19], [20]. Also, these mechanisms also require complex calculations and high memory capacity, which additionally leads to high energy consumption [21]. Therefore, the trust perception based security mechanisms have been proposed to solve the problems in the security mechanisms based on encryption and identity verification.

To defend against routing attacks in WSNs, especially internal attacks [36], the security mechanisms based on trust awareness have been verified to be effective. However, the traditional trust management system also has some problems. For example, when calculating the trust value for neighbor nodes like in references [10], [18], [20], nodes have frequent communication with neighbor nodes, resulting in

The associate editor coordinating the review of this manuscript and approving it for publication was Roberto C. Ambrosio.

information congestion, high energy consumption and long end-to-end delay. At the same time, the traditional trust management system like in references [9], [16], [33] only considers a single type of defense attacks and cannot quickly detect malicious nodes.

Therefore, in this paper, TBSEER are proposed to solve the above mentioned problems, and our main contributions can be summarized as follows:

1) Nodes use adaptive penalty coefficient and volatility factor with space and time constraints to calculate the direct trust value, so as to improve the accuracy of trust evaluation and the speed of identifying malicious nodes.

2) The Sink calculates the comprehensive trust value of the trusted neighbor nodes based on the direct trust value sent by the nodes, which reduces the information congestion and energy consumption caused by frequent communication with many neighbor nodes while calculating the indirect trust value.

3) By establishing inspector nodes to monitor the behaviors of member nodes and cluster heads in the clusters, a safe route can be selected from the multiple paths to actively avoid wormhole attacks from malicious nodes.

4) A new trust model and secure routing are constructed to improve the security of the network and enhance the ability to resist a variety of common attacks.

The remainder of the paper is organized as follows: Section II discusses the secure routing mechanisms proposed in the past. Section III presents the trust model of TBSEER. Section IV describes the secure routing protocol (TBSEER) based on the trust model in detail. Section V shows the simulation results, and verifies the performance of TBSEER. Section VI concludes this paper.

II. RELATED WORK

In reference [22], a secure hybrid routing protocol (SHRP) is proposed, which is based on the concepts of geography and layering. The whole SHRP process is divided into two stages: (i) clustering and cluster head selection, (ii) secure routing. First, SHRP uses a clustering algorithm to realize cluster planning. Then appropriate cluster heads are selected according to the center position, residual energy and mobility of nodes. Finally, secure routing mechanism uses symmetric and asymmetric cryptosystem to protect the security of packets in the transmission process, so as to resist eavesdropper, impersonation attack, replay attack and man-in-the-middle attack. Each cluster needs at least three nodes with GPS. Therefore, the implementation of the protocol requires a lot of computation and energy. Hybrid cryptography-based secure data communication scheme (HCBS) for wireless sensor networks is proposed in reference [23]. HCBS introduces elliptic curve cryptography (ECC) in key exchange and symmetric key cryptography in data encryption and MAC operations. However, the security needs to be improved, so a key management secure routing algorithm based on enhanced elliptic key cryptosystem (ECCSRA) is proposed in reference [24]. ECCSRA combines 512-bit ECC, Beta function, and Gamma function to prevent malicious users from using elliptic curve discrete logarithm to decrypt data when the secret key is unknown. In traditional elliptic curve-based encryption, the cyclic group used to form the secret key is formed by simple prime numbers. And ECCSRA uses Beta and Gamma functions to effectively generate secret keys, thereby improving network communication security. In reference [25], a secure end-to-end routing protocol is proposed, which has a special group key pre-distribution scheme. The protocol can provide authentication and key establishment at the same time, and can provide authentication to establish routing path and path key. The protocol uses path keys to remove the encryption and decryption of intermediate sensors, thereby protecting routing data and reducing the time required for intermediate sensors to process data. Specifically, reference [25] does not use multiple pairs of shared keys to repeatedly perform encryption and decryption on each link, but uses a unique end-to-end path key. In addition, the protocol has good performance in correctness, freshness of authentication response, freshness of communication key, forward secrecy of group key and backward secrecy of group key.

The internal attacks have not been considered in these methods mentioned above. Therefore, trust-based security mechanism is proposed to deal with different internal attacks. A multidimensional secure clustered routing (MSCR) based on binomial distribution is proposed in reference [34]. LTMS mainly includes the design of trust model and the selection of cluster heads. The trust model is composed of direct trust value and indirect trust value, which is used to select and update the cluster heads. In reference [26], a trust-based fuzzy implicit cross-layer protocol (TrufiX) is proposed. TrufiX uses multiple parameters extracted through information exchange between layers to mitigate the impact of network security threats. The proposed protocol consists of two fuzzy logic systems (FLS) in series. The first FLS considers distance, trust and response time to determine the appropriateness of nodes. The second FLS considers the fairness ratio, forwarding success rate and data transmission duration to determine the estimated trust of nodes. In reference [27], an energy-aware secure with routing trust (ESRT) scheme is proposed. The trust estimation mechanism of the scheme includes direct trust, indirect trust and expected positive probability of nodes. Then, ESRT selects a secure route according to trust, energy and hops. Unlike some previous schemes, ESRT does not care about the known geographic information and strict time synchronization. What's more, ESRT shows more flexibility in the case of heavy network load. But the premise of the proposed ESRT is that misbehaving nodes cannot collude with each other. In reality, the security performance of the scheme is not high. Therefore, reference [28] proposes a trust and energy aware secure routing protocol (TESRP) for WSNs. TESRP uses a distributed trust model to discover and isolate nodes with abnormal behavior. TESRP adopts a multi-facet routing strategy, which considers the trust value, residual energy and hops, and makes routing decisions simultaneously. However, in the routing phase, source nodes send RREQ packets and a large number of relay nodes forward RREQ packets, which may lead to information congestion and additional communication overhead. Reference [29] proposes another secure and trusted routing scheme. The scheme uses fuzzy logic to obtain the trust value of the route. Then, on the basis of considering trust and safety, the shortest path from source to destination is selected. For the routing problem, MDS-MAP algorithm is used to determine the optimal path with minimum error. In the trust management system, the scheme assumes that the destination nodes are a trusted entity. However, many malicious nodes can act as destination nodes to cheat legitimate nodes to send data to them. Therefore, reference [30] establishes a trust sensing-based secure routing mechanism (TSSRM) with lightweight characteristics and capabilities, which is still effective for malicious target nodes. TSSRM uses the semiring theory to find the optimized routes, which comprehensively considers the direct trust value, indirect trust value, incentive factor, energy trust and QoS index to construct the routing metric and select the optimal trusted route. However, TSSRM may cause high network delay and information congestion in large-scale WSNs. Therefore, reference [31] proposes a cluster-based secure routing algorithm, namely secured quality of service (QoS) aware energy efficient routing protocol (SQEER), to reduce network latency. The trust model of the SQEER uses an authentication technology and a key-based security mechanism to provide the trust score. Firstly, the trust model calculates the overall trust score by direct trust score and indirect trust score. Secondly, SQEER selects cluster heads according to QoS index and trust value to perform cluster-based secure routing. Finally, the final path is selected according to the path trust, energy and hops, which effectively realizes the security of routing. However, the implementation of SQEER includes the key security mechanism, which additionally increases the computational complexity for nodes. In order to reduce the burden of nodes, reference [32] proposes a security scheme for selfish nodes in WSNs. In this scheme, nodes are divided into three types: cluster head (CH), inspector node (IN) and member node (MN). If the IN finds some problems while listening to the transmission of the CH, it will be blacklisted and the MN within its range will be notified to stop forwarding data to the CH. However, if MN judges that it is intentional accusation of IN based on its own reputation system, MN can also reject IN's decision. At the same time, CH will also send random check request to IN to determine whether the status is normal for IN. In addition, CH does not participate in the election of IN to save energy. However, IN's geographic location isn't considered when electing IN. If IN is at the edge of the cluster, some MNs cannot be monitored. Therefore, in order to save energy and improve security, this paper proposes TBSEER whose historical trust value is volatilized under the volatilization factor and malicious behavior is punished under adaptive penalty coefficient, so as to improve the accuracy of the trust model. The direct trust value, indirect trust value

TABLE 1. Comparison of secure and trust-aware routing protocols.

Reference	Acronyms	Security model	Energy consideration	Network overhead cost	Applicability	Defense against internal attacks
[22]	SHRP	Symmetric and asymmetric cryptosystem	Yes	High	Limited	NO
[23]	HCBS	Hybrid Cryptography	No	High	Limited	NO
[24]	ECCSRA	The cyclic group based Elliptic curve cryptography	No	High	Limited	NO
[25]	--	Group key pre-distribution scheme	No	High	Limited	NO
[26]	TrufiX	Trust-based fuzzy implicit cross-layer	Yes	Moderate	Widespread	Yes
[27]	ESRT	Weighted sum of trust, energy, and hop counts	Yes	Moderate	Limited	Yes
[28]	TESRP	Weighted sum of trust, energy, and hop counts	Yes	Moderate	Limited	Yes
[29]	--	Trust&&fuzzy logic	Yes	Moderate	Widespread	Yes
[30]	TSRRM	Trust degree && QoS metrics	Yes	Moderate	Limited	Yes
[31]	SQEER	Trust model && authentication technique with a key	Yes	Moderate	Limited	Yes
[32]	--	Trust systems	Yes	Moderate	Widespread	Yes
[34]	MSCR	Trust management based on binomial distribution	Yes	Moderate	Limited	Yes
--	TBSEER	Adaptive trust and punishment mechanism && Active secure routing	Yes	Low	Widespread	Yes

and energy trust value are used to evaluate the comprehensive trust value, then the node's security is evaluated. Therefore, it can resist various attacks such as black hole, selective forwarding, sinkhole and hello flood attacks of malicious nodes. Consequently, the nodes with high security and high residual energy are selected as CHs according to the comprehensive trust value. Finally, according to the comprehensive trust value and transmission distance, the security of the routing paths is evaluated to find the best one that can actively defend against wormhole attack.

Table 1 provides the summary and comparison of the discussed schemes. Each scheme is evaluated in terms of related parameters such as design of security model, energy consideration, network overhead cost, applicability and defense against internal attacks.

III. TRUST MODEL

As in references [20], [37], [38], nodes identify malicious nodes by calculating trust values. How to improve the trust value of normal nodes and quickly reduce the trust value of malicious nodes is the key to protecting routing. Therefore, this paper uses the adaptive penalty coefficient to quickly reduce the trust value of malicious nodes, so as to achieve the purpose of quickly identifying malicious nodes and fast eliminating malicious nodes.

A. DIRECT TRUST VALUE

In order to establish a trust relationship between nodes, the behavior of the node must be converted into a value to indicate the degree of trust, which can be expressed as:

$$DT_{ij}^{t} = \gamma * HT_{ij}^{t} + (1 - \gamma) * (R_j + S_j)^t \tag{1}$$

where HT_{ij}^{t} represents the historical trust value of node i evaluated by node j after volatilization. The role of HT_{ij}^{t} is to further limit the role of historical trust values in the trust model. Node j may have a high level of trust before being captured as a malicious node.

Therefore, in order to accelerate the reduction of the trust value of node j, the volatilization factor λ is introduced to reduce the effect of the historical trust value. The expression formula of historical trust value is given as:

$$HT_{ij}^{t} = \lambda(DT_{ij}^{t-1} + HT_{ij}^{t-1}) \tag{2}$$

where λ controls the influence of the historical trust value on the current direct trust value. The larger the value of λ, the greater the influence of the historical trust value on the direct trust value.

$$R_j = \frac{\theta * receive\_message_j - rejection_j}{message_j} \tag{3}$$

$$S_j = \frac{\theta * send\_message_j - un\_send_j}{message_j} \tag{4}$$

where $(R_j + S_j)^t$ represents the trust value in the current state, γ and $(1 - \gamma)$ respectively represent the weight of the trust value after the historical trust value volatilized and the trust value in the current state. $0 < \gamma < 1$, and the value depends on the specific WSNs. $receive\_message_j$ indicates that node i monitors the number of data packets received by node j, and $send\_message_j$ indicates that node i monitors the number of data packets sent by node j. $message_j$ represents the total number of data packets received and sent by the monitored node j. $rejection_j$ and un_send_j respectively represent the number of data packets that node j refuses to receive and refuse to send. Considering the importance of quickly identifying malicious nodes, we define an adaptive penalty coefficient θ expressed as:

$$\begin{aligned} \theta &= \frac{-a_1}{1 + e^{-a_2 * AC_j + a_3}} + 1 \\ AC_j &= \frac{AB_j}{NB_j} \end{aligned} \tag{5}$$

where AB_j and NB_j respectively represent the abnormal behavior and normal behavior of node j. a_1, a_2, and a_3 are the adjustable parameter of the adaptive penalty coefficient. If node j is captured as a malicious node, its proportion of abnormal behaviors AC_j will increase suddenly. Therefore, under the action of AC_j, the penalty coefficient θ will adaptively decrease, resulting in a rapid decrease in the direct trust value of malicious nodes. In this paper, it is more appropriate to set a_1, a_2, and a_3 to 0.9, 10 and 4 respectively. The change curve of the adaptive penalty coefficient is shown in Fig. 1.

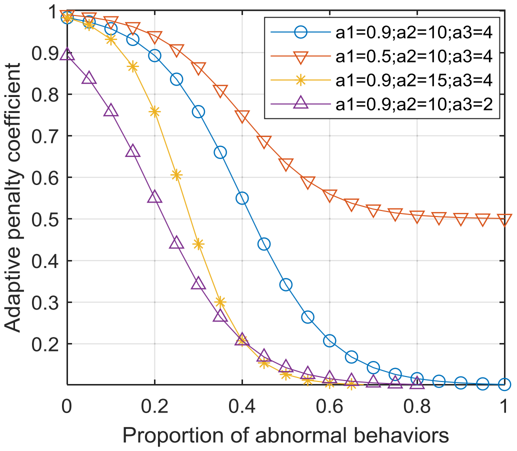


FIGURE 1. Adaptive penalty coefficient under different parameters.

B. INDIRECT TRUST VALUE

In the traditional scheme, calculating the indirect trust value requires a large amount of communication energy and may also cause information congestion. This is because before node i calculates the indirect trust value of node j, it must ask the public trusted neighbor node u for the direct trust value of node j.

As shown in Fig. 2, the public trusted neighbor node u is a member of B_h, $B_h = [B_1, B_2, B_3, \cdots, B_q]$, $u \in B_h$.

Therefore, in order to avoid the transmission of a large amount of query information between nodes, this paper

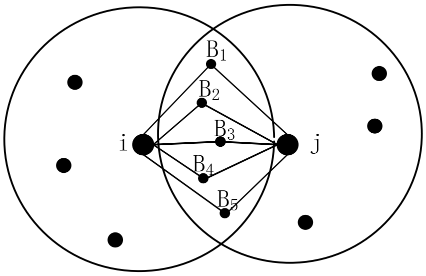


FIGURE 2. **The public trusted neighbor nodes.**

adopts a centralized computing mode to reduce the burden on nodes. The indirect trust value of all nodes is calculated by the Sink, and each node only needs to attach the direct trust value to the neighbor node in the data packet, and then send it to the Sink, so there will be no extra energy consumption.

In order to evaluate the trust value of node j accurately, node i needs to know the direct trust value that the third node u evaluates node j. The calculation formula of indirect trust value that node i evaluates node j is expressed as follows:

$$IT_{ij}^{t} = \frac{1}{q}\sum_{u\in B_h}^{q}(DT_{iu}^{t} * DT_{uj}^{t}) \tag{6}$$

where, q is the number of public trusted neighbor nodes, DT_{iu}^{t} is the direct trust value that node i evaluates node u; DT_{uj}^{t} represents the direct trust value that node u evaluates node j.

C. ENERGY TRUST VALUE

In the network, there may be a situation where the trust value of a node is high but its remaining energy is low, which makes the node die prematurely, thereby affecting the structure and energy consumption of the entire network. Therefore, in order to save network overhead and balance the energy consumption of nodes, this paper considers the remaining energy of the node when calculating the trust value of the node.

$$E\_receive_j = l * E_{elec} \tag{7}$$

$$E\_send_j = \begin{cases} l * E_{elec} + l * \varepsilon_{fs} * d^2, & d < d_0 \\ l * E_{elec} + l * \varepsilon_{mp} * d^4, & d \geq d_0 \end{cases} \tag{8}$$

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

where E_{elec} is the radio frequency energy consumption coefficient of the nodes, and l is the size of messages and data packets. The initial energy of node j is expressed by E_0 and the remaining energy is expressed by RE_j which is shown as:

$$RE_j = E_0 - E\_receive_j - E\_send_j \tag{10}$$

When the residual energy of node j is greater than or equal to the threshold, node j is considered to be capable of participating in the cooperation, otherwise, no matter how high the trust value of the node, it cannot participate in the information transmission. Therefore, the energy trust value of node j is:

$$E_j = \frac{RE_j}{E_0} \tag{11}$$

D. COMPREHENSIVE TRUST VALUE

The comprehensive trust value is composed of three aspects: direct trust value, indirect trust value and energy trust value. It represents the trust level of the nodes. The higher the comprehensive trust value of the nodes, the higher the trust level. If node i evaluates that the comprehensive trust value of node j is lower than the threshold CT_{th}, then node i considers node j to be a malicious node, and excludes this malicious node from the network, prohibiting it from participating in any network activities. Therefore, the comprehensive trust value of node i to node j is expressed as follows:

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

where, η_1, η_2 and η_3 are the weights of direct trust value, indirect trust value and energy trust value, respectively, $\eta_1 + \eta_2 + \eta_3 = 1$. The comprehensive trust value CT_{ij}^{t} satisfies [0, 1].

IV. SECURE ROUTING DESIGN

In this section, we will describe the secure routing in our proposed TBSEER scheme in detail.

A. NETWORK MODEL

Before elaborating on the design of secure routing, we would like to make certain assumptions about the basic model of the network, including:

(i) Sensor nodes are randomly deployed in the network to detect the surrounding environment.

(ii) Each sensor node has the same initial energy, computing power and storage capacity, and is static.

(iii) The Sink is static and has unlimited resources.

(iv) After node deployment, the Sink knows the unique identifier (ID) and location information of each node.

The network is composed of clusters of different sizes, and each cluster is composed of three kinds of nodes, namely member nodes (MNs), cluster heads (CHs) and inspector nodes (INs). CHs undertake the task of data forwarding within and between clusters. In the absence of security measures, malicious nodes become CHs will cause more damage to the network than members nodes. Therefore, CHs must be assumed by the nodes with high energy and high trust value. MNs attach the direct trust value for the neighbor nodes and their energy to the detected data and send it to the CHs, and CHs forward the data packets to the Sink in a multi-hop way. The Sink calculates the comprehensive trust value of the nodes according to the received direct trust value and residual energy. Thereafter, the new comprehensive trust values are sent back to the nodes. Therefore, it avoids the phenomenon of high communication times, high energy consumption and information congestion when the traditional trust model collects the trust value of third-party nodes for neighbors. IN is responsible for monitoring the change of signal strength of nodes in the cluster, and the purpose is to detect whether it is captured as malicious nodes with wormhole attack. Therefore, IN is selected by the corresponding CH, close to itself and has high trust value.

B. CLUSTER HEAD ELECTION

First, each node broadcasts the ID of the neighbor with the largest comprehensive trust value. Secondly, after receiving the packets, the neighbor node checks whether packets matches its ID. If it matches, the number of times it is elected will be increased by one ($Elected\_num = Elected\_num+1$). Finally, each node broadcasts a packet with *Elected_num*, and the node with the highest *Elected_num* serves as CH.

C. INSPECTOR NODE ELECTION

INs are responsible for monitoring the signal strength in the cluster to further reduce the loss caused by MNs or CHs being captured as malicious nodes. In order to avoid the situation that INs in reference [32] can not detect the signal strength of all nodes in the cluster, this paper selects the node with close distance to CH, high energy and high trust value as IN. The formula for CH to select IN is given as:

$$p_{IN} = CT_{ij}^{t} * e^{-d_{toCH}} \tag{13}$$

$$d_{toCH} = \frac{d_{toch} - d_{tochmin}}{d_{tochmax} - d_{tochmin}} \tag{14}$$

where d_{toCH} represents the normalization of the distance between MNs. d_{toch} is the distance from the node to its own CH. $d_{tochmin}$ And $d_{tochmax}$ are the minimum and maximum distances from the MNs in the cluster to its own CH, respectively.

(a) INs monitoring MNs: After INs are selected, INs monitor the MNs in the cluster according to the inequality shown in Eq. (15), so as to quickly find the wormhole attacks initiated by malicious nodes.

$$\left| RD_j = \sqrt{\sum_{j=1}^{cn} \left(RSSI_j - \overline{RSSI}\right)^2 / cn} \right| \leq \zeta \tag{15}$$

where $RSSI_j$ is the received signal strength of node j in the cluster detected by the INs, cn is the number of MNs in the cluster, and $\overline{RSSI}$ is the average value of the received signal strength of all MNs in the cluster. Therefore, as long as a malicious node initiates a wormhole attack, it can be detected by judging whether its RSSI deviates from the normal range.

(b) INs monitoring CHs: If CHs are captured as malicious nodes, the damage to the network will be huge. Especially wormhole attack is not easily detectable. Therefore, it is essential and important to prevent malicious CHs from launching wormhole attacks. In order to detect wormhole attack as early as possible, the Sink can actively avoid wormhole attacks according to Eq. (16) to protect the network to the greatest extent.

$$P_r = \sum_{\substack{i=1 \\ j=i+1}}^{chn} \frac{R^{*} CT_{CH_iCH_j}^{t}}{d_{CH_i\_CH_j}} \tag{16}$$

where $CT_{CH_iCH_j}^{t}$ is the comprehensive trust value for CH_i to evaluate the next hop CH_j, R is the maximum communication radius of CHs, and $d_{CH_iCH_j}$ is the distance between CH_i and next hop CH_j.

In order to ensure that INs are normal, CHs will randomly send a check packet to INs. If INs reply to CHs, CHs notify the MNs in the cluster to maintain the high trust value of INs. If INs do not reply to the CHs, CHs re-select INs and inform MNs in the cluster of the ID of the new INs, and the old INs will no longer play a monitoring role.

D. NEXT HOP CLUSTER HEAD ELECTION

In order to improve the efficiency and security of the network, we entrust the Sink with unlimited resources to undertake the task of selecting a secure route. Using the P_r value can avoid wormhole attacks and reduce the energy consumption of nodes in the transmission process. The steps of the proposed work are as follows:

Step1: The source CH_i sends a request packet to preselect CHs for the next hop (CH_{i+1}, CH_{i+4}, CH_{i+6} in Fig. 3).

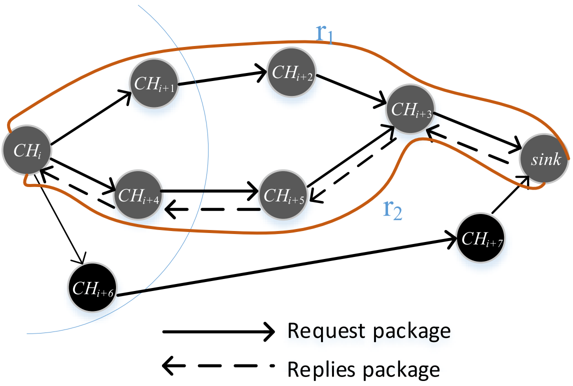


FIGURE 3. The process of secure path selection.

Step2: Preselect CHs to add its ID information to the request packet after receiving the request packet. Then they continue to send request packets to its next hop preselected CHs (CH_{i+2}, CH_{i+5}, CH_{i+7} in Fig. 3). And so on until the Sink.

Step3: After receiving request packets from multiple paths (such as paths r_1 and r_2), the Sink calculates each path's P_r value according to formula (16). Then the Sink selects the path with the maximum value as the best route (such as path r_2), and sends the determination packet along this path in reverse.

Step4: After the source CH_i receives the confirmation packet from the Sink, it stores the optimal route in the trusted routing table (it is an array of variable size, which depends on the number of intermediate nodes in the route).

Therefore, the TBSEER actively avoids malicious nodes (as shown in CH_{i+6}, CH_{i+7}) and improves the speed of detecting wormhole attack.

E. TRUST VALUE UPDATE

The calculation and update of the trust value are the foundation and focus of the trust model. Different from the previous trust-based secure routing protocols, the indirect trust value of this protocol is handled by the Sink instead of collecting a large number of direct trust values from neighbor nodes. Therefore, this protocol avoids a lot of communication overhead and alleviates the congestion between nodes when updating the trust values.

Specific updating steps are described as follows.

Step 1: MNs monitor the normal and abnormal behaviors of the neighbor nodes, and use formula (1) to evaluate the direct trust values of the neighbor nodes.

Step 2: After CHs, INs and routes are determined, the network begins to enter the stable communication stage like LEACH.

Step 3: when entering the last time slot of the stable phase, MNs attach the direct trust values of the evaluated neighbor nodes and their remaining energy to the data packet.

Step 4: MNs send packets to their CHs, and then CHs send them to the Sink in a multi-hop manner. Finally, the Sink calculates the indirect trust value and the comprehensive trust value according to the direct trust value.

Step 5: The Sink sends the calculated comprehensive trust value to each CH by multicast, and CHs forward it to MNs after receiving it. So that the node can update the comprehensive trust value for neighbors.

However, in step 3, the Sink may receive some malicious evaluation from malicious nodes evaluating neighbor nodes. Therefore, in order to ensure the accuracy of calculating the CT_{ij}^{t} value, the Sink will first evaluate the credibility of each node's DT_{ij}^{t} value and filter out the abnormal direct trust value.

The credibility of the direct trust value that public neighbor node k evaluates node j is expressed as follows:

$$\partial_k = \frac{\sum_{u=1}^{q} \left| DT_{uj}^{t} - DT_{kj} \right|}{q} \tag{17}$$

If the value of ∂_k is larger, the direct trust value provided by node k is more likely to be malicious from malicious nodes. Therefore, the credibility threshold is set to filter out the direct trust value of $\partial_k > \partial_0$. The credibility threshold ∂_0 is the predetermined value associated with the particular network environment and information.

V. SIMULATION RESULTS AND PERFORMANCE EVALUATION

In this section, the performance of TBSEER is analyzed by MATLAB and compared with TSSRM and TESRP. The simulation time is based on round, and the malicious nodes can launch black hole, selective forwarding, sinkhole, hello flood and wormhole attacks in the simulations. When the network runs to the 100th round, the malicious nodes successfully invade the network and launch attacks. The experimental parameters are listed in Table 2.

TABLE 2. Simulation parameters.

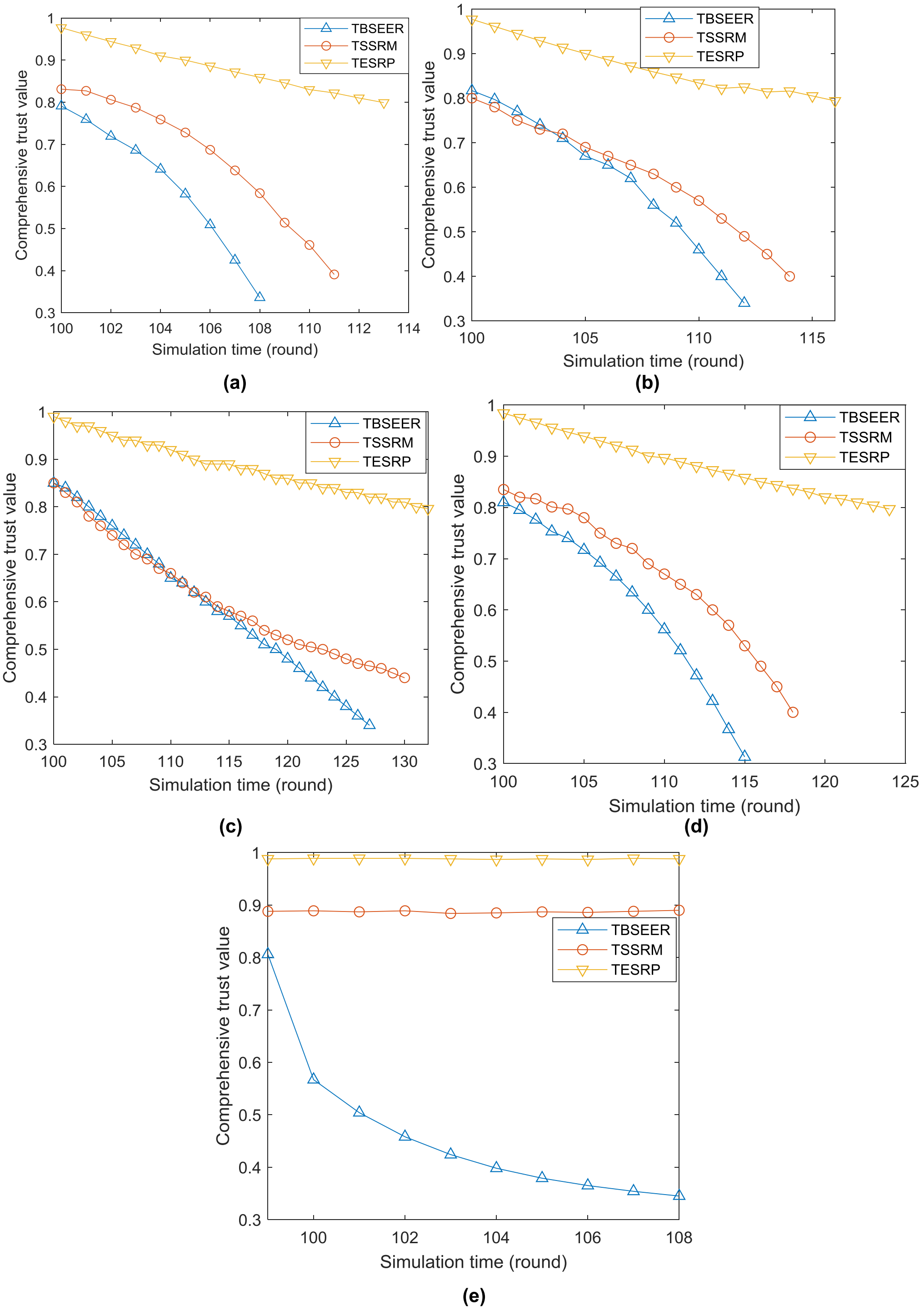
Parameter	Value
Initial energy of the node	1J
Control packet size	400 bits
Data packet size	4,000 bits
Number of nodes	100
Area	100m*100m
Initial trust value	0.5
CT_{th}	0.35
η_1、η_2、η_3	{0.33 , 0.33 , 0.33}
λ	0.5
d_0	87 m
γ	0.5

A. COMPREHENSIVE TRUST VALUE OF MALICIOUS NODES UNDER ATTACK

The comprehensive trust value represents the security of nodes. As long as the comprehensive trust value is lower than the threshold, the nodes are malicious. Fig. 4 shows the change of comprehensive trust value of malicious nodes under different malicious attacks. In order to verify the security of TBSEER, TSSRM and TESRP, 5% of malicious nodes are injected into WSNs in 100 rounds to launch black hole, selective forwarding, sinkhole and hello flood attacks, respectively.

When the network runs to the 100th round, 5% of malicious nodes launch black hole attacks, and the comprehensive trust value of TBSEER, TSSRM and TESRP decreases as the network runs. It can be seen from Fig. 4(a) that the comprehensive trust value of TBSEER decreases the fastest, and it only takes 8 rounds to fight against malicious nodes to exclude them from the network. This shows that the security mechanism in TBSEE is the most effective. Compared with TSSRM and TESRP, the performance of TBSEER against black hole attack is increased by 37.5% and 62.5%, respectively.

Compared with black hole attack, selective forwarding attack is more difficult to identify. Because selective forwarding attacks will randomly drop important packets, which increases the difficulty of identification. Fig. 4 (b) shows the ability that three security mechanisms resist malicious nodes when they launch selective forwarding attacks. It can be seen from Fig. 4(b) that TBSEER takes 13 rounds to counter the selective forwarding attacks before it can be excluded from the network. Compared with TSSRM and TESRP, the per-



(a)

(b)

(c)

(d)

(e)

FIGURE 4. (a) changes of comprehensive trust value of malicious nodes with black hole attack. (b) Changes of comprehensive trust value of malicious nodes with selective forwarding attack. (c) changes of comprehensive trust value of malicious nodes with sinkhole attack. (d) changes of comprehensive trust value of malicious nodes with hello flood attack. (e) changes of comprehensive trust value of malicious nodes with wormhole attack.

formance of TBSEER against selective forwarding attacks increased by 15.38% and 30.77%, respectively.

The principle of sinkhole attacks is that malicious nodes broadcast that the control packet contains one hop arrival information to the network, which attracts the surrounding nodes to send a large number of packets to them, and furthermore selectively discard the packets. In order to reduce the damage of this attack for the network and speed up the malicious nodes to be recognized by others, TBSEER introduces an adaptive penalty coefficient, which makes the more times of malicious behavior, the stronger the penalty effect, and quickly reduces the trust value of malicious nodes. It can be seen from Fig. 4(c) that TBSEER takes 28 rounds to counter the sinkhole attacks before it can be excluded from the network. Compared with TSSRM and TESRP, the performance of TBSEER against selective forwarding attack increases by 11.11% and 18.52%, respectively.

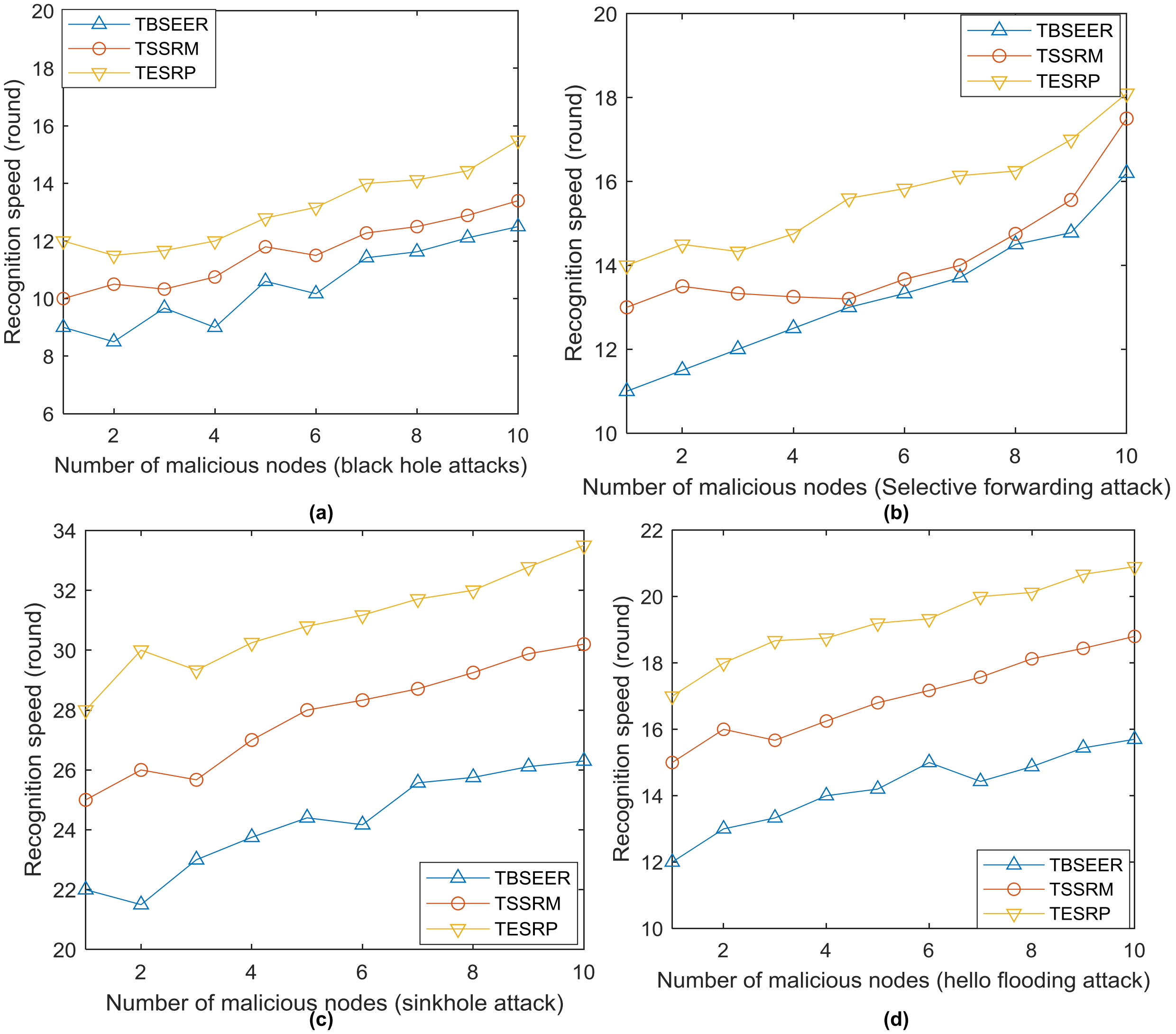
Next, we verify the performance of three trust based security schemes under the hello flood attack. As shown in Fig. 4(d), under the resistance of TBSEER, the comprehensive trust value of malicious nodes drops below the threshold the fastest, so the security of TBSEER is optimal. Compared with TSSRM and TESRP, the performance that TBSEER against hello flood attacks has increased by 20% and 60%, respectively.

Finally, we verify the ability of TBSEER, TSSRM and TESRP to resist wormhole attack. As can be seen from Fig. 4(e), the comprehensive trust values of malicious nodes for TSSRM and TESRP are not reduced. It shows that under the protection mechanism of TSSRM and TESRP, the trust that the result of malicious nodes being evaluated by the network is still very high, and the wormhole attack initiated by malicious nodes cannot be detected. However, when 2% of malicious nodes launch wormhole attacks, TBSEER only needs 8 rounds to exclude them from the network.

B. IDENTIFICATION SPEED

How to improve the speed that Malicious nodes identified by network is one of the focuses of many researchers. Fig. 5 shows the average identification speed that three trust based security schemes to identify malicious nodes with the increase of malicious nodes in the network.

Firstly, we verify the capability that TBSEER resists black hole attacks under different number of malicious nodes. It can be seen from Fig. 5(a) that the more black hole attacks, the more rounds are needed to identify malicious nodes.



(a)

(b)

(c)

(d)

FIGURE 5. (a) The average speed at which malicious nodes are identified under black hole attack. (b) The average speed at which malicious nodes are identified under selective forwarding attacks. (c) The average speed at which malicious nodes are identified under sinkhole attacks. (d) The average speed at which malicious nodes are identified under hello flood attacks.

In addition, the average identification speed of TBSEER is faster than TSSRM and TESRP, because the trust value of malicious nodes decreases rapidly under the effect of S_j, volatilization factor and adaptive penalty coefficient.

Secondly, we verify the capability that TBSEER resists selective forwarding attacks under different number of malicious nodes. As can be seen from Fig. 5 (b), the average identification speed of TBSEER is 6.97% and 18.1% faster than TSSRM and TESRP, respectively.

Then, we verify the capability that TBSEER resists sinkhole attacks under different number of malicious nodes. Due to the joint action of S_j, R_j, volatilization factor and adaptive penalty coefficient, the trust level of malicious nodes decreases rapidly. As can be seen from Fig. 5 (c), the average identification speed of TBSEER is 14.63% and 27.62% faster than TSSRM and TESRP, respectively.

Finally, we verify the capability that TBSEER resists hello flood attacks under different number of malicious nodes. As can be seen from Fig. 5 (d), the average identification speed of TBSEER is 19.62% and 35.69% faster than TSSRM and TESRP, respectively. This is because R_{j}, volatilization factor and adaptive penalty coefficient work together to accelerate the speed that malicious nodes identified by the network.

C. PACKET LOSS RATE

The packet loss rate refers to the ratio of the number of data packets not received by the sink to the data packets sent by the node.

As can be seen from Fig. 6, as the number of malicious nodes in the network increases, a large amount of data flows to malicious nodes, so the packet loss rate of the network increases gradually. However, TBSEER's trust model designs the adaptive penalty coefficient, which makes the more malicious behaviors, the stronger the penalty effect. In addition, the volatilization factor is introduced to reduce the high trust value of the node just captured as malicious. Therefore, the speed at which malicious nodes are identified becomes faster, and the packet loss rate of the network is the slowest. The results show that compared with TSSRM and TESRP, the packet loss rate of TBSEER is reduced by 19.4% and 47.83%, respectively.

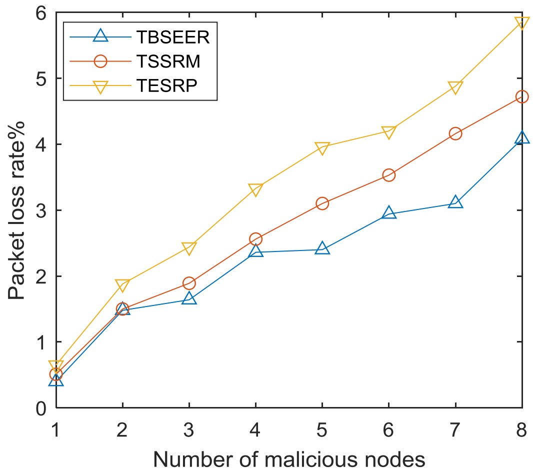


FIGURE 6. **Packet loss rate.**

D. AVERAGE END TO END DELAY

Fig. 7 shows that the average end-to-end delay increases as the number of malicious nodes increases. Due to the frequent packet loss in the scenario, the upper layer of the transmission protocol needs to wait for the establishment of the link and the packet re-transmission between nodes, which leads to the increase of the delay. When the number of malicious nodes in TBSEER increases, due to excessive packet loss, the routing stability decreases sharply, which increases the delay of the packet to destination. Although both TSSRM and TESRP adopt a trust evaluation model, neither TSSRM nor TESRP considers the influence that volatilization factor evaporates historical trust value and penalty coefficient punishes malicious behavior. Therefore, TBSEER has lower latency than TSSRM and TESRP, and the average latency is reduced by 6.74% and 18.31%, respectively.

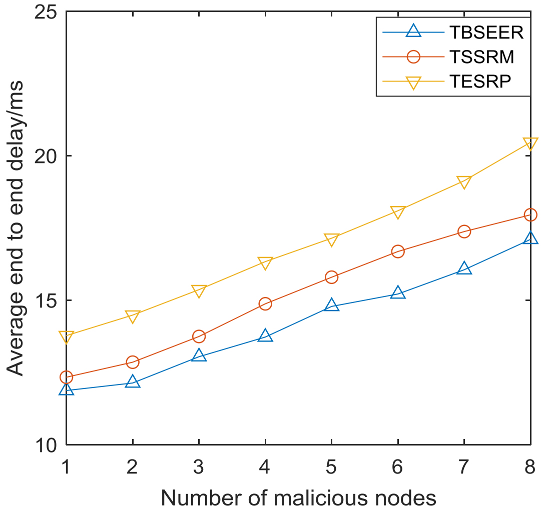


FIGURE 7. **Average end to end delay.**

E. ENERGY CONSUMPTION ON CALCULATING INDIRECT TRUST VALUE

In the trust model, the direct trust value provided by the third-party nodes participates in node updating and calculating the indirect trust value of neighbors. Therefore, the trust model has produced a certain communication cost.

Fig. 8 shows the node's communication energy to calculate the indirect trust value in different environments. Because TBSEER uses the Sink with unlimited energy and powerful functions to update and calculate the indirect trust value, the Sink shares the burden of the nodes and saves the energy of the nodes. In addition, the energy consumption of nodes increases with the number of nodes in the network. However, the performance of TBSEER is still better than TSSRM.

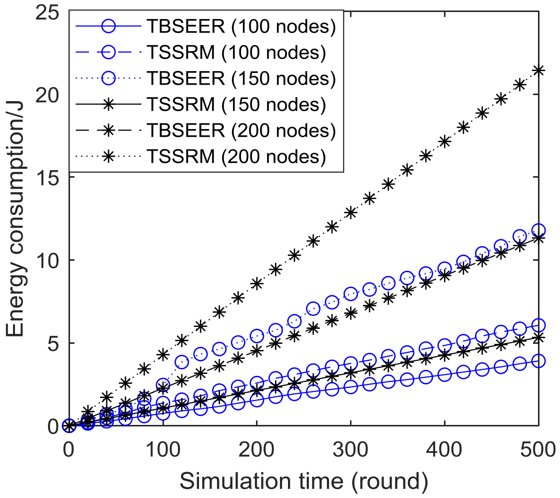


FIGURE 8. Energy consumption on calculating indirect trust value.

VI. CONCLUSION

It is of great significance to provide secure and energy-saving routing paths in resource-constrained wireless sensor networks. This paper proposes a new trust based secure and energy efficient routing protocol TBSEER to deal with various common network attacks. The target of TBSEER is to improve the security of the network as much as possible while saving the network energy consumption. TBSEER presents a new trust model, which considers the influence of the volatilization factor and adaptive penalty coefficient. It can accelerate the identification speed of malicious nodes and effectively identify black hole, selective forwarding, sinkhole and hello flood attacks. In addition, the nodes find a safe and energy-saving route based on the trust model in a multi-path search method, which actively avoids wormhole attack. The simulation results show that compared with the traditional trust based mechanisms, TBSEER can reduce routing overhead and improve data transmission reliability.

TABLE 3. Definition of Acronyms.

Acronyms	Definition
WSNs	wireless sensor networks
TBSEER	a trust based secure and energy efficient routing protocol
SHRP	a secure hybrid routing protocol
HCBS	Hybrid cryptography-based secure data communication scheme
ECCSRA	ECC based Secure Routing Algorithm
ECC	elliptic curve cryptography
MAC	Media access control
LTMS	a lightweight trust management scheme
TrufiX	Trust-based fuzzy implicit cross-layer protocol
FLS	fuzzy logic systems
ESRT	an energy-aware secure with routing trust scheme
TESRP	a trust and energy aware secure routing protocol
RREQ	route request packet
MDS-MAP	Multidimensional scaling-map
TSSRM	a trust sensing based secure routing mechanism
QoS	quality of service
SQEER	Secured QoS aware Energy Efcient Routing
CH	cluster head
IN	inspector node
MN	member node
ID	identifier
RSSI	Received Signal Strength Indication

All the acronyms mentioned in this paper are listed in Table 3.

REFERENCES

[1] B. P. Laxmi and A. Chilambuchelvan, "GSR: Geographic secured routing using SHA-3 algorithm for node and message authentication in wireless sensor networks," *Future Gener. Comput. Syst.*, vol. 76, pp. 98–105, Nov. 2017.

[2] A. Alromih, M. Al-Rodhaan, and Y. Tian, "A randomized watermarking technique for detecting malicious data injection attacks in heterogeneous wireless sensor networks for Internet of Things applications," *Sensors*, vol. 18, no. 12, p. 4346, Dec. 2018.

[3] H. K. D. Sarma, A. Kar, and R. Mall, "A hierarchical and role based secure routing protocol for mobile wireless sensor networks," *Wireless Pers. Commun.*, vol. 90, no. 3, pp. 1067–1103, Jun. 2016.

[4] A. Rachedi and A. Hasnaoui, "Advanced quality of services with security integration in wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 15, no. 6, pp. 1106–1116, Apr. 2015.

[5] G. D. Devanagavi, N. Nalini, and R. C. Biradar, "Secured routing in wireless sensor networks using fault-free and trusted nodes," *Int. J. Commun. Syst.*, vol. 29, no. 1, pp. 170–193, Jan. 2016.

[6] K. Selvakumar, L. Sairamesh, and A. Kannan, "An intelligent energy aware secured algorithm for routing in wireless sensor networks," *Wireless Pers. Commun.*, vol. 96, no. 3, pp. 4781–4798, Oct. 2017.

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

[8] Y. Wang, M. Zhang, and W. Shu, "An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 145, Dec. 2018.

[9] W. A. Aliady and S. A. Al-Ahmadi, "Energy preserving secure measure against wormhole attack in wireless sensor networks," *IEEE Access*, vol. 7, pp. 84132–84141, 2019.

[10] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. K. Nehemiah, and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks," *Wireless Pers. Commun.*, vol. 105, no. 4, pp. 1475–1490, Feb. 2019.

[11] G. Rajeshkumar and K. R. Valluvan, "An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network," *Wireless Pers. Commun.*, vol. 94, no. 4, pp. 1993–2007, Jun. 2017.

[12] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure routing protocol based on multi-objective Ant-colony-optimization for wireless sensor networks," *Appl. Soft Comput.*, vol. 77, pp. 366–375, Apr. 2019.

[13] Q. Yang, X. Zhu, H. Fu, and X. Che, "Survey of security technologies on wireless sensor networks," *J. Sensors*, vol. 2015, pp. 1–9, Dec. 2015.

[14] V. T. Kesavan and S. Radhakrishnan, "Cluster based secure dynamic keying technique for heterogeneous mobile wireless sensor networks," *China Commun.*, vol. 13, no. 6, pp. 178–194, Jun. 2016.

[15] T. A. Alghamdi, "Secure and energy efficient path optimization technique in wireless sensor networks using DH method," *IEEE Access*, vol. 6, pp. 53576–53582, 2018.

[16] B. E. Bilgin and S. Baktir, "A light-weight solution for blackhole attacks in wireless sensor networks," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 27, no. 4, pp. 2557–2570, Jul. 2019.

[17] A. Saidi, K. Benahmed, and N. Seddiki, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks," *Ad Hoc Netw.*, vol. 106, Sep. 2020, Art. no. 102215, doi: 10.1016/j.adhoc.2020.102215.

[18] Z. Hong, Q. Shao, X. Liao, and R. Beyah, "A secure routing protocol with regional partitioned clustering and beta trust management in smart home," *Wireless Netw.*, vol. 25, no. 7, pp. 3805–3823, Oct. 2019.

[19] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Netw.*, vol. 26, pp. 1–14, Sep. 2019.

[20] R. I. Sajan and J. Jasper, "Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network," *Int. J. Commun. Syst.*, vol. 33, no. 8, p. e4341, May 2020.

[21] M. Mathapati, T. S. Kumaran, A. Muruganandham, and M. Mathivanan, "Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network," *J. Ambient Intell. Humanized Comput.*, Jun. 2020, doi: 10.1007/s12652-020-02169-7.

[22] B. Muthusenthil and H. Kim, "SHRP—Secure hybrid routing protocol over hierarchical wireless sensor networks," *Int. J. Comput. Commun. Control*, vol. 12, no. 6, pp. 854–870, Dec. 2017.

[23] F. Mezrag, S. Bitam, and A. Mellouk, "Secure routing in cluster-based wireless sensor networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8254138.

[24] S. Viswanathan and A. Kannan, "Elliptic key cryptography with beta gamma functions for secure routing in wireless sensor networks," *Wireless Netw.*, vol. 25, no. 8, pp. 4903–4914, Nov. 2019.

[25] L. Harn, C.-F. Hsu, O. Ruan, and M.-Y. Zhang, "Novel design of secure end-to-end routing protocol in wireless sensor networks," *IEEE Sensors J.*, vol. 16, no. 6, pp. 1779–1785, Mar. 2016.

[26] I. A. Umar, Z. M. Hanapi, A. Sali, and Z. A. Zulkarnain, "TruFiX: A configurable trust-based cross-layer protocol for wireless sensor networks," *IEEE Access*, vol. 5, pp. 2550–2562, 2017.

[27] A. Ahmed, K. A. Bakar, M. I. Channa, A. W. Khan, and K. Haseeb, "Energy-aware and secure routing with trust for disaster response wireless sensor network," *Peer Peer Netw. Appl.*, vol. 10, no. 1, pp. 216–237, Jan. 2017.

[28] A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan, "A secure routing protocol with trust and energy awareness for wireless sensor network," *Mobile Netw. Appl.*, vol. 21, no. 2, pp. 272–285, Jan. 2016.

[29] A. Beheshtiasl and A. Ghaffari, "Secure and trust-aware routing scheme in wireless sensor networks," *Wireless Pers. Commun.*, vol. 107, no. 4, pp. 1799–1814, Apr. 2019.

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

[31] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS aware trust based routing algorithm for wireless sensor networks," *Wireless Pers. Commun.*, vol. 110, no. 4, pp. 1637–1658, Feb. 2020.

[32] Z. Ishaq, S. Park, and Y. Yoo, "A security framework for cluster-based wireless sensor networks against the selfishness problem," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–11, Jul. 2018.

[33] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.

[34] W. Fang, W. Zhang, W. Chen, J. Liu, Y. Ni, and Y. Yang, "MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–20, Jan. 2021.

[35] X. Yu, F. Li, T. Li, N. Wu, H. Wang, and H. Zhou, "Trust-based secure directed diffusion routing protocol in WSN," *J. Ambient Intell. Humanized Comput.*, vol. 2020, no. 5, pp. 1–13, Nov. 2020.

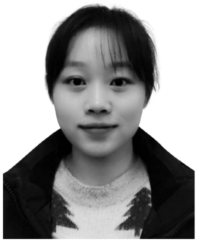
[36] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, "Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks," *IEEE Trans. Eng. Manag.*, vol. 68, no. 1, pp. 170–182, Feb. 2021.

[37] A. Saidi, K. Benahmed, and N. Seddiki, "Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks," *Ad Hoc Netw.*, vol. 106, no. C, pp. 1–59, Sep. 2020.

[38] K. Thangaramya, K. Kulothungan, S. I. Gandhi, M. Selvi, S. V. N. S. Kumar, and K. Arputharaj, "Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN," *Soft Comput.*, vol. 24, no. 21, pp. 16483–16497, Nov. 2020.

HUANGSHUI HU received the B.Eng. degree in computer application from the Changchun University of Science and Technology (currently, Jilin University), Changchun, China, in 1999, and the M.S. and Ph.D. degrees in engineering from Jilin University, Changchun, in 2005 and 2012, respectively. From 2005 to 2008, he worked as a Research and the Development Manager with Changchun Lianxin Technology Company Ltd., Changchun. From 2008 to 2013, he worked as a Technical Director of Jilin Omnidirectional Technology Company Ltd., Changchun. Since 2015, he has been with the Department of Computer Science and Engineering, Changchun University of Technology, where he is currently working as a Professor. His main research interests include topology control in wireless sensor networks and multifunction vehicle bus networks.

YOUJIA HAN received the B.Eng. degree from the Anhui Wenda University of Information Engineering, Hefei, China, in 2018. He is currently pursuing the M.S. degree with the Changchun University of Technology, Changchun, China. His main research interest includes wireless sensor networks security.



MEIQIN YAO received the B.Eng. degree from the Anhui Wenda University of Information Engineering, Hefei, China, in 2018. She is currently pursuing the master's degree with the Changchun University of Technology, Chuangchun, China. Her main research interest includes wireless sensor networks.

XUE SONG received the B.Eng. degree in computer applications from the Jilin Normal University of Engineering and Technology, Changchun, China, in 2017, and the M.S. degree in education from Changchun Normal University, in 2020. Since 2020, she has been working with the School of Artificial Intelligence, School of Tourism, Changchun University. Her main research interests include the Internet of Things and virtual reality technology.