Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6657580, 10 pages
https://doi.org/10.1155/2021/6657580

Research Article

Construction of Trusted Routing Based on Trust Computation

Bei Gong, Jingxuan Zhu, and Yubo Wang

Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

Correspondence should be addressed to Yubo Wang; wangyubo@bjut.edu.cn

Received 24 December 2020; Revised 2 February 2021; Accepted 23 March 2021; Published 19 April 2021

Academic Editor: Xiao Zhang

In the field of applied IoT, a large number of wireless sensor devices are tasked with data production and collection, providing IoT subjects with a large amount of basic data to support top-level IoT applications. However, there is a considerable risk of being attacked on such sensor networks that are organized in a wireless form. These relatively independent network devices have extremely limited performance and lifetime, a problem that can be supplemented in a centralized network with base stations by relying on the performance of the core nodes of the network, but in a decentralized self-organizing network, they can have a serious adverse impact on the implementation of security solutions. Considering the fundamental nature of the data generated by such end devices in IoT application services, the protection of their security is also directly related to the quality of upper layer services provided. The main research result of this paper is the design of a trust routing scheme for self-organizing networks. The scheme is based on a comprehensive evaluation of data transmission rate, transmission delay, and other factors related to the operation status of the self-organized network and improves the efficiency of the overall work of the self-organized network by reducing the performance consumption of individual nodes of the self-organized network and balancing the network load.

1. Introduction

With the popularization and development of Internet technology, the old Internet infrastructure services gradually fail to meet the demand for Internet application services. As a form of network connection between network data and service devices, the deep connection to users and network devices and a wide range of application scenarios make Internet of Things (IoT) technology an important way to develop network services. And based on the development of mobile terminal technology, the field of IoT technology has gradually emerged as a new development direction represented by mobile Internet-built mobile IoT technology, with more emphasis on the flexibility of IoT devices in deployment, management, use, and other aspects. Therefore, mobile IoT technology has been developed by many Internet-developed countries as the next stage of important development goals and direction and to a large number of human and financial investment.

With the advancement of the technology and the application process, some new issues are emerging around mobile IoT. The dependence of the IoT on the Internet and the lack of basic security technologies make the overall security of the IoT a serious threat at the same time as the rapid development of the IoT application technology. This threat is reflected, on the one hand, in the fact that low-protection IoT terminal devices are more likely to be affected by network attacks, and on the other hand, when a large number of low-protection devices with network data transmission capabilities are controlled by a network attacker, the attacker can use this as a basis to further expand the threat of network attacks.

According to the predictions [1] made by Cisco, a leading provider of network equipment and services, regarding the data transmission during the operation of global networks, using 2018 statistics as a basis, Cisco believes that the number of data network users worldwide will increase 51% by 2023 from 3.9 billion in 2018, while there will be 29.3 billion network devices connected to the global Internet, in which the development of IoT technology has played an important role. In the forecast data, M2M devices [2], which are representative of IoT devices with services covering multiple

applications such as smart towns, smart grids, smart climate management, smart shopping, and smart picking, will account for more than 50% of the total network devices, making them a major component of global network connectivity. Such rapid network growth in the good direction will promote new concepts such as social IoT (SIoT) [3], which shares services over the Internet, while in the bad direction will lead to a rapid increase in attacks against network devices occurring in the network, with a 39% increase in DDoS attacks alone globally between 2018 and 2019 [1]. In 2016, the Mirai malware contaminated about 2.5 million endpoint devices and used them to carry out further network attacks [4]. A botnet malware attack called Dark Nexus, spanning China, Thailand, Brazil, South Korea, and Russia in a reverse proxy fashion, was also seen in April 2020 [5]. As a direct result of these problems, the applications built on the IoT infrastructure framework cannot guarantee the security and reliability of their application services. They also indirectly affect the reliable operation of other networks, as controlled IoT devices can be used to launch new network attacks. This risk poses a significant threat to IoT technologies, which rely on extensive data collection and remote interaction, with extremely high data transmission reliability requirements. This explosive growth accompanied by elevated industry risk requires effective countermeasures to be taken in order for mobile IoT application technology to achieve long-term growth [6].

In order to establish a secure and effective data transmission mechanism in the Internet of Things (IoT), which guarantees the security of data transmission while reducing the additional performance impact generated, this paper designs a wireless router establishment scheme based on distributed trust assessment. Firstly, a feasible data collection and trust assessment model is designed for the operating environment of the wireless self-organized network of IoT in order to realize the conversion from network state to quantitative trust assessment results. Then, based on the results of such a trust assessment, a set of route establishment schemes based on trust assessment is designed in combination with path length, transmission delay, and other metrics related to the network routing process. And a corresponding information maintenance mechanism to maintain and respond to network state changes is designed.

2. Related Work

Trust-based security is a new way of providing security without using cryptography approaches [7] and can effectively perform node anomaly behavior detection and overall network situational awareness tasks in an IoT environment. In terms of efficiency, avoiding or to some extent reducing the additional overhead in the execution of target devices for security through trusted security is also more suitable for use on IoT devices with limited resources. Trust in the field of wireless communication networks may be defined as the degree of reliability of other nodes performing actions [8, 9]. By evaluating this degree of reliability, it is possible to gain an understanding of the operation of each object in the network, and through the process of evaluating the trust, it is possible to obtain an assessment of the changes in the overall security situation of the network and to detect security events in the network. In the Internet of Things (IoT), which simultaneously has multiple characteristics of wireless transmission networks, social networks, and P2P networks [10], trust models are well suited to guide the overall operation of the network by describing its interactive behavior. For a self-organizing network at the end of the Internet of Things, the process can be described as some members acting socially to provide or request services from other members. A class of trust protocols such as [11–15] has emerged during research and development on self-organizing network security at the end of the Internet of Things (IoT). It is built on basic trusted security techniques, but the trust calculation process is complex and difficult to apply in sensor mobile self-organizing networks. And social network trust protocols such as [16–18] introduce social network relationships in trust management and enhance network security, but still fail to consider network operation efficiency well and lack countermeasures related to the spatial location change of sensing devices.

In terms of trusted route establishment, the security-aware ad hoc routing (SAR) [19] scheme designed by Sherchan et al. provides basic route discovery and route security for the route establishment problem in a wireless self-organizing network environment. It designed a node trust level management mechanism to evaluate the security of network nodes in the region. However, the complex computational process associated with secure schemes based on encryption and decryption algorithms can lead to degradation of internode transmission performance, which is unacceptable in sensor networks with relatively limited computational resources and energy.

The CENtralized Trust-based Efficient Routing (CENTERA) protocol [20] designed by Yi et al. uses authentication as the basis of trust and establishes a trust assessment for network nodes based on their forwarding situation. It performs the trust evaluation process and trust-based node state discrimination and malicious node quarantine through a base station designed in the solution. The trusted state of the node obtained from the forwarding case can be directly associated with the data forwarding process of routing, and the message and authentication computation, which is less expensive than the encryption and decryption computation, can also be used to protect the security of the message as it is propagated. However, the scheme's dependence on a base station prevents it from being directly applied to a self-organizing network of sensor devices. Also, such a centralized trust management model has a certain degree of lag in the feedback control process.

Based on existing research results related to trust models and trusted routing schemes, and taking into account the network situation of sensor self-organizing networks, this paper designs a routing scheme, including a self-organizing network trust assessment model, a trust-based routing scheme, and continuous maintenance of routing information. Compared with the above scheme, this proposal focuses on the application of trustworthy evaluation in distributed scenarios and the application of encryption algorithms in the network of IoT end devices

3. Trust Assessment Model

The design goal of the scheme is to address the problem of route security in sensor self-organizing networks. In the routing process, the core interaction is the transmission of data over the wireless medium, and the scheme divides this transmission process into two stages: route discovery and data relay. The route discovery stage is the network establishment stage, where devices exchange routing information several times to establish a basic data framework for the self-organizing network topology. In the data relay stage, the sensor dynamically carries out multiple relay node selection processes on multiple nonrepeating sensor devices according to the routing information established in the previous stage to complete the transmission of data from the source device to the destination device.

The trust assessment model in this scheme consists of three parts: trust model, trust data acquisition, and trust maintenance. The trust model describes the overall process of assessing the trustworthiness of a node, including a quantitative assessment of data related to the operational state of the network and a computational scheme for obtaining standard comprehensive trust assessment results based on the quantitative assessment. Trust data acquisition describes the way nodes acquire raw data in the trust assessment process, as well as the process of authenticating and assessing the trustworthiness of the data itself. Trust maintenance describes a scheme for maintaining the validity of a self-organized network trust state by controlling trust assessment behavior and responding to security events that occur during operation.

3.1. Trust Model. The design of the scheme's trust model is primarily used to describe the method by which nodes evaluate the process of data exchange between the network environments in which they are located, i.e., with other network nodes. In general, this evaluation process can be described as the evaluation and quantification of the data transmission rate, data transmission delay, and other parameters by a node in a self-organized network to calculate the comprehensive trust assessment value of other nodes in the same self-organized network.

In the specific design, the scheme uses a distributed trust assessment approach for the decentralized self-organized network of end devices. Suppose there are n network nodes p_1 to p_n in a self-organizing network M, a node p in a self-organizing network needs to autonomously complete a trust assessment of all other $n-1$ nodes, including the collection of network state data and the results of other node trust assessments.

3.1.1. Direct Trust Assessment. As part of the trust model, the direct trust assessment corresponds to the trust calculation based on the network state data described above; to complete this computational process, this paper designs a direct trust evaluation function $\mathrm{dta}(p)$ to quantify the network behavior of the target node. Suppose there are two network nodes A and B in a self-organizing network, and node A has to perform a direct trust assessment on node B. In this process, node A needs to obtain the following data: the list of network state parameters L_{ns}, the network state quantization evaluation function $\mathrm{qa}()$, and the network state evaluation weights $W_{\mathrm{ns}}.L_{\mathrm{ns}}[\mathrm{pno}, \mathrm{parno}]$ containing multidimensional operational state data collected by node A for other nodes. The function $\mathrm{qa}()$ describes the algorithm for quantitative evaluation of each dimension of data in $L_{\mathrm{ns}}.W_{\mathrm{ns}}[\mathrm{parno}]$ which contains the calculated weights of the results of the quantitative assessment of each state parameter in node A in the comprehensive trust assessment process. In summary, as an example of direct trust assessment of the m-dimension of node A on node B, the direct trust assessment function can be expressed as

$$\mathrm{DT} = \mathrm{dta}(p_{\mathrm{B}}) = \sum_{i=1}^{m} W_{\mathrm{ns}i}\mathrm{qa}\left(L_{\mathrm{ns}[\mathrm{B},i]}\right). \tag{1}$$

On this basis, it is only necessary to unify the dimensional composition of the network state parameter list and the network state quantization evaluation function within a self-organized network to obtain a relatively uniform standard of direct trust evaluation data to support the subsequent trust evaluation process.

3.1.2. Indirect Trust Assessment. In the model, the indirect trust assessments correspond to the trust calculations based on the results of other node trust assessments above. In the process of trust assessment of nodes, due to differences in the level of interaction and spatial distribution between nodes, in a relatively large self-organized network, the data obtained by a node through direct data collection and the corresponding direct trust assessment results are only effective in reflecting the actual operational status of a small number of nodes. For other (typically spatially distant) nodes, the results of the trust assessment need to be corrected by indirect data. This indirect data can be raw network state data collected by other nodes or direct trust assessment results computed by other nodes that have not been corrected for indirect trust. Using raw data avoids inconsistencies in trust calculations due to differences in W_{ns} settings or dynamic adjustment of different nodes, but incurs a large additional data transfer overhead. In this paper, an indirect evaluation approach based on the results of trust calculations is chosen for the actual application scenario characteristics of the terminal self-organizing network.

Assuming that there are two network nodes A and B in a self-organized network, the following steps need to be taken in the process of indirect trust assessment of B by A. A first obtains direct trust assessment data DT from nodes other than itself and B. After getting DT, A needs to rely on the indirect trust correction function $\mathrm{itc}()$ according to the trustworthiness of the data source to correct the DT passed by the node. A simple $\mathrm{itc}()$ can be expressed as

$$\mathrm{itc}(\mathrm{DT}, T) = \frac{\mathrm{DT}_{i\mathrm{B}}T_{\mathrm{B}}}{\sum_{i}^{n-2}T_i}. \tag{2}$$

Also, node A needs to rely on the indirect trust validity function $\mathrm{itv}()$ to evaluate the data validity of the data source

node. For example, a simple itv() based on the distance of the network topology can be expressed in the following form:

$$\mathrm{itv}(\mathrm{DT}, p_i, p_{\mathrm{B}}) = \mathrm{DT}_{i\mathrm{B}}\mathrm{Dis}(i, \mathrm{B}), \tag{3}$$

where the result of $\mathrm{Dis}(i, \mathrm{B})$ is the value corresponding to the distance from i to B in the standardized vector of the inverse correlation dataset of topological distances. Although both itc() and itv() are used to calibrate the acquired DTs, itc() primarily deals with the node's level of trust, i.e., the effect of the node's past behavior on the validity of its DT data, while itv() is used to balance the computational bias of the data affected by the validity of the original data itself used by the source node to compute the direct trust. Together, the calculations of itc() and itv() determine the weight of the different sources of direct trust in the final indirect trust value. In summary, the function of indirect trust assessment of node A on node B in a self-organizing network containing n nodes is described as

$$\mathrm{IT} = \mathrm{ita}(p_{\mathrm{B}}) = \sum_{i=1}^{n-2} \mathrm{itv}(\mathrm{itc}(\mathrm{DT}_{i\mathrm{B}}, T_{\mathrm{B}}), p_i, p_{\mathrm{B}}). \tag{4}$$

The calculation of the indirect trust value reduces the large fluctuations of the trust assessment results within self-organized networks at low data traffic, while resisting some trust spoofing.

Composite trust calculation value of nodes $T_c = W_d\mathrm{DT} + W_i\mathrm{IT}$.

3.2. Trust Data Acquisition. The trust model, as an important basis for trust assessment, establishes uniform standards and methods for assessing trust and determines the mode of operation of the trust assessment. However, status data itself still remains an important factor in determining the validity of trust assessment results. The ability to obtain more valuable data during the operation of a self-organizing network determines the outcome of the trust assessment and the subsequent correctness of route establishment. The value referred to here includes attributes such as timeliness, truthfulness, and objectivity of the data. The present scheme therefore devises a number of methods in the trust data acquisition section to assess the above attributes in addition to methods for obtaining relevant data for trust assessment.

Since this paper focuses on the route establishment problem during data transmission, this scheme chooses wireless transmission as the main way for self-organizing nodes to obtain state data. The wireless data transmission process can be described simply as a node listening for data frames in the wireless medium, retaining the data to be processed and discarding other data frames. The scheme builds on this process by performing further analytical processing of data frames that should have been discarded to obtain basic network state data. The acquisition process can be described as follows. Suppose there are nodes A, B, and C in a self-organized network, and node A and node C need to complete data transmission through node B due to wireless data propagation distance limitation. In this process, the data transmitted by node A needs to pass through the A-B-C transmission path. In this scheme, when A sends a data frame X with destination address C to B, the data sending status $\mathrm{SS} = \{\mathrm{A}_s, \mathrm{A}_d, H, S, T_{\mathrm{send}}\}$ needs to be recorded, where A_s is the source address and A_d is the destination address, H is the data check value, and S is the data frame load size and stores each recorded SS in a data send status list L_{ss}. The state information used for trust assessment is thus obtained through maintenance of the L_{ss} in two main ways: one of them is the timeout record, where A deletes the timeout record and records it as a data transfer timeout event by scanning the L_{ss} at regular intervals and calculating the difference between the current time and T_{send} and comparing it with the preset timeout threshold T'. Its second is forwarding confirmation B, which operates normally during the usual data transfer, and should forward X to C after receiving X. Since the data is transmitted wirelessly, A, which is also in the transmission range of B, will receive an X from B as well. At this point, node A does not directly discard X but records the received information $\mathrm{RS} = \{\mathrm{A}_s, \mathrm{A}_d, H, S, T_{\mathrm{reci}}\}$ about X again. After completing the recording of the RS, A cross-referenced the RS with the SS in L_{ss}. If no corresponding entry is deleted, and if it exists, the difference between T_{reci} and T_{send} is recorded as the transmission delay for this data transfer. A successful data transfer event is recorded and the corresponding entry in L_{ss} is deleted.

For another part of the data, such as the routing information of neighboring nodes and the transmission bandwidth of the data link, limitations due to issues such as network transmission efficiency cannot be obtained through active condition monitoring or operational testing. However, if their data changes are used as some kind of security event triggering mechanism, an incident response mechanism can be reached despite the inability to identify the specific source of the problem. On this premise, it is only necessary to establish a secure information sharing mechanism within the self-organized network and use signature authentication for key information, where the signature authentication only needs to ensure security in a short period of time due to the high timeliness of the state information; in the event of a security incident, information can be shared and cross-referenced to identify the problem and then traced back to the source of the problem based on data signatures.

3.3. Trust Maintenance. The scheme uses a dual event- and time-driven trust update model. In the general mode, the trust value is updated periodically based on the results of statistical analysis of data and historical data within a certain period of time, and at the same time, a number of self-organized network management events will trigger the trust update, in order to respond effectively in the event of relatively specific network security events.

Time-driven periodic trust updates in the scheme are used as a routine maintenance method for the self-organized network trust status, and their main task is to assess the impact of recent network behavior of self-organizing equipment within a specific time frame and in accordance with the design requirements. The main assessment functions include the following: Node Trust Update

Periodic Function uc(), Node Trust Update Function tu(), and parameter selection functions for trust updates. uc() describes the process of calculating the trust update cycle UC and, to some extent, reflects the effective time of the current trust state. The calculation needs to correlate the current overall trust, the raw data, and the previous update interval. The function is described as follows: $\mathrm{UC} = \mathrm{uc}(T_{\mathrm{cur}}, T_{\mathrm{his}}, \mathrm{UC}) = W_T(T_{\mathrm{cur}} - T_{\mathrm{his}})/\mathrm{UC} + \mathrm{UC}_b$. Adjust the size of the trust update interval based on trust trends to balance the overhead caused by trust updates with the corresponding delays. The Node Trust Update Function focuses on the relationship between the current trust value and the historical trust value. Based on the trust update interval, the effective time of the historical trust value can be used as its impact weight on the current trust state when calculating a new trust value to avoid sharp fluctuations in the trust value. Trust assessment results

$$T = \mathrm{tu}(\mathrm{HD}, T_n) = W_{\mathrm{h}} \sum_{i=1}^{\mathrm{len}} \frac{\mathrm{UC}_i T_i}{\mathrm{UC}_t} + W_n T_n. \tag{5}$$

W_h and W_i are the weights of the historical trust value and the current trust value, respectively. The historical trust value HD consists of several sets of historical trust value records and a composite value for the corresponding update interval. Here, the update interval is not the actual update interval time but a calculated value maintained by the trust update module in relation to the actual update interval. This computed value gradually decreases with each trust update event until it falls below a preset threshold and is removed from the computed sequence.

The scheme also includes a trust update mechanism with security event triggers on top of the periodic updates. As mentioned in the periodic update, the scheme designs correlation functions for reducing the additional overhead caused by large fluctuations in trust during system operation, but this also reduces the responsiveness of the model. Due to slower trust changes, it may take longer to dispose of anomalous behavior nodes when they appear in the system. In order to reduce such occurrences, there is a need to establish additional trust renewal mechanisms that are triggered by unforeseen events. The scheme monitors both communication changes and trust threshold events in its implementation.

Communication change monitoring is achieved by monitoring changes in data traffic. As the data production side, the self-organizing gateway will receive relatively stable data uploads from all other nodes in the self-organizing network during the effective operation of the self-organizing network. Therefore, when a gateway node finds that a sensor node has not uploaded data for a long period of time, there is a high probability that the node data transmission will be interrupted or the node will go offline in the network. The program responds in the following ways. First, it will confirm whether the target node is out of the current self-organized network by collecting direct route information for each node and stop responding if the node is normally offline. Otherwise, data transfer tests will be conducted between the target node and the gateway node to find transmission breakpoints and adjust their trust state as well as the data records in the associated node.

Trust threshold events are initiated by each node itself. For a node based on the preset node direct trust thresholds, when the node is found to exist in the operation of a section of the direct trust, the calculation value is lower than the preset value (including the direct trust caused by the communication changes in monitoring the decline in trust) for a number of parameters and data related to trust calculations, including W_d, W_i, and other trust weights and calculated values in HD to be corrected, and triggers a trust update.

4. Route Establishment

4.1. Routing Algorithm. The routing establishment process in this scheme takes the comprehensive trust value output from the trust model as the main parameter, and each sensor node within the self-organized network takes its own direct route as the information basis. The scope of the routing table is gradually extended by exchanging routing information between nodes several times and eventually reaching full reachability with the internal self-organizing network.

Self-organized networks are described in the scheme as a graphical data structure $G = (V, E, W)$. The routing model $G' = (V, E_R, T)$, which is built on top of the network topology, is a directed graph belonging to G. V is the set of points of G', a collection of nodes in a self-organizing network, $p_1 \cdots p_n \in V$. E_R is the edge set of G', which is every single-hop routing path in the routing model $R(a, b) \in E_R$, $a \in V, b \in V, a \neq b$. T is the edge weight of G', which is the path selection weight computed in the routing model based on node trust, path state, and so on. On this basis, a trusted route path can be described by an ordered set of nodes $L_N = [p_1, p_2, \cdots, p_n]$ between the starting node and the target node. The process of establishing such a trusted routing path is based on the calculation and selection of the path selection weights T. The calculation of T has been described in the trust model in Section 3. Each node needs a route score R_s, which is calculated by combining the T, route distance, and other factors of the path nodes, as the basis for route selection. The route scoring function rsc() is as follows: $R_s = \mathrm{rsc}(T, L, D) = w_t T + w_L L + w_d D$. It can be seen that R_s is calculated from the weighted sum of node trust value T, route distance score L, and transmission delay score D. The routing distance and transmission delay are statistical quantities that require a scoring function such as $L = (R_l w + w^2)/R_l$ to unify with the T numerical standard. The calculation weights w_t, w_L, w_d need to be set according to the needs of the route calculation process. Higher values of w_t increase the sensitivity of the route establishment process to changes in self-organized network security conditions and maintain good data transmission quality. A higher value of w_L can reduce the number of forwardings per unit of data in a self-organized network, which helps to reduce the overall data transmission overhead in the network and extend the effective running time. And for w_d, this scheme already includes an evaluation of the transmission delay in the

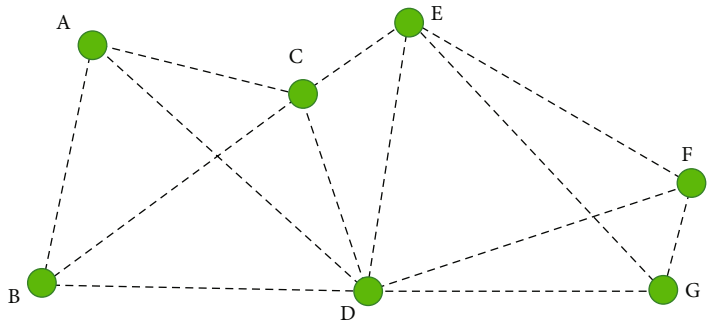

Figure 1: Network topology.

calculation of T. Here, w_d is added only as a run parameter that is closely associated with the routing process, in order to reduce the coupling of the dynamic configuration of the route selection and trust evaluation process and to increase the flexibility of the scheme configuration. w_d can be set to a lower value if there are no special requirements for data transmission delay.

4.2. Route Establishment Process. The route establishment process described in this paper proceeds on the basis of a hypothetical network topology. Suppose there are 7 nodes in the self-organized network, and the network topology is shown in Figure 1. Assume that the self-organized network has been running for some time and that each node in the network has the list of self-organized nodes and the computed trust list. At this point, node A in the network is sending data to node F. The route selection process is described as follows:

(1) A finds out if there is a route entry to F in the list of existing routes and selects the path with the best route score to send if the corresponding route entry exists. If it does not exist, A needs to send a route establishment request rer to its neighbor nodes (i.e., all nodes that can establish a direct route). The rer includes the necessary data such as source node A and destination node F, and the transmission path is shown in Figure 2.

(2) The node receiving the rer responds to the request and looks up the route entry to node F in the local route list. If present, it sends the corresponding route entry to the rer source and ends the response. If not, it sends the rer in the same manner as in (1). Note that nodes responding to rer need to avoid responding repeatedly to the same source node and destination node rer to avoid possible routing loop problems. Figure 3 shows the response of the rer sent by node C.

(3) After the node receives a response from a neighbor node, it needs to perform the following calculations: let A be the sending node of rer and B be the responding node. First, A obtains a comprehensive trust assessment T_B of B from the trust data and then uses the path length of the route entry R of B as the path trust weight and combines the route trust value in R with T_B to obtain the route trust value T for A through B to F. The new route distance and delay are also calculated accordingly. Finally, node A calculates the route score through B to F based on the newly acquired T, L, and D.

(4) When node A receives all of the rer response data, it records the route path with the route score and selects the route entry with the high route score as the path to send data to F to complete the route establishment, as shown in Figure 4. Further screening conditions may need to be established during the selection process to improve the quality of network data transmission. As in this scheme, if the allowable lower limit of the route trust value is set, this route path is directly discarded when the T-value of the existing route entry is below a preset threshold to avoid the security risk associated with a low-trust path.

4.3. Route Maintenance during Data Transmission. Once the route list is established, the node already has the ability to complete the data transfer, but as with the trust evaluation process, the node's route list is also time-sensitive. Therefore, a route maintenance and update mechanism is necessary to maintain the trusted state of the route. Route maintenance in this scheme relies on the triggering of routing-related state changes, specifically trust state changes, route path changes, and relay node state changes.

4.3.1. Trust State Changes. Trust state changes are routing updates that result after a periodic or event-triggered change in a node's trust value. In this case, the node needs to correct the current route list based on the new trust data for the route's trust value and composite score and reselect the preferred route.

4.3.2. Route Path Changes. Route path changes are routing updates that result when a node's direct route changes, where the change can be a direct route change due to a neighbor node going offline or a route change due to path blocking triggered by a trust value below a threshold.

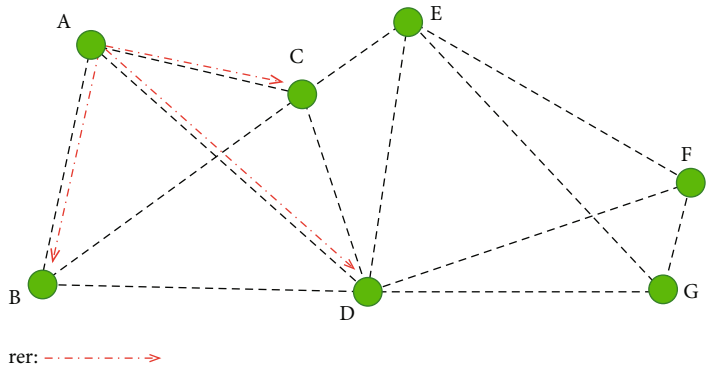

Figure 2: rer transmission path.

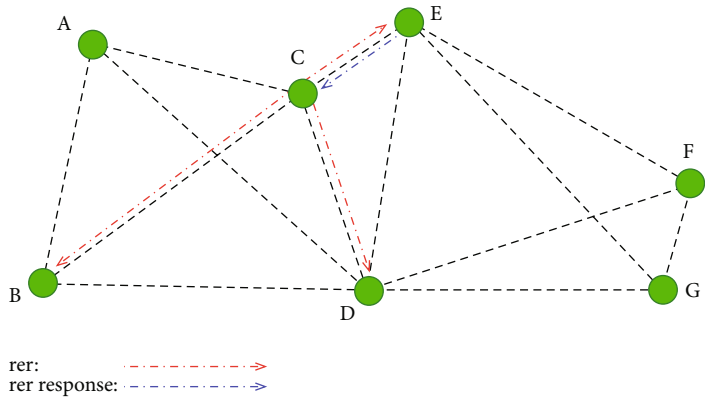

Figure 3: rer response.

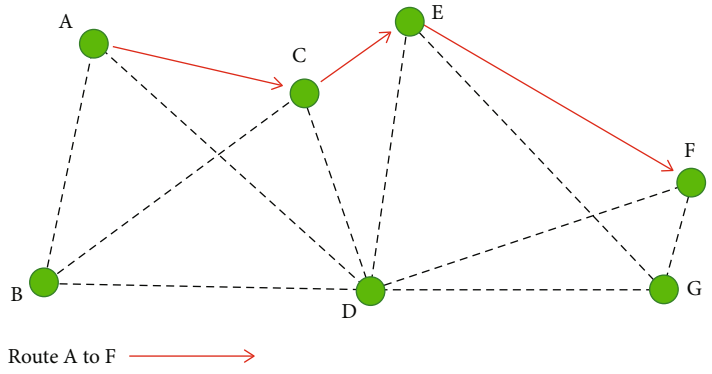

Figure 4: Route path.

4.3.3. Relay Node State Changes. Relay node state changes are the routing updates that result from changes in the routing list of a relay node. After a node within the self-organized network (set this node to A) updates its route list, A broadcasts this route change to its neighbor nodes. If the node B that receives the information meets the following conditions, the routing table contains the route through A and when other alternative routes exist in the routing table. B needs to recalculate the route scores for routes passing through A and update the routing table if a route entry priority change occurs.

5. Performance

In this section, the actual performance of the proposed scheme is tested, including the execution of the model under different parameters and the performance of the model against different forms of network attacks. The experimental environment and data settings other than those described within this section are based on the results of runs of other associated experiments in the laboratory, and a detailed description of these is of little relevance to the main content of this paper and can be considered as initial run parameters

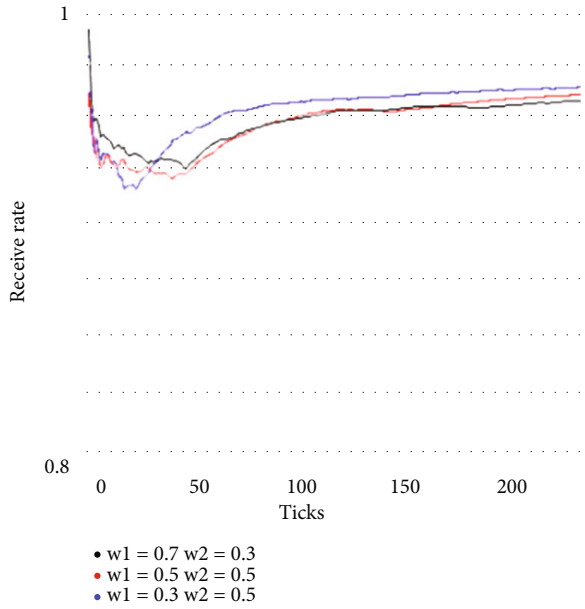

Figure 5: Different W_d and W_i.

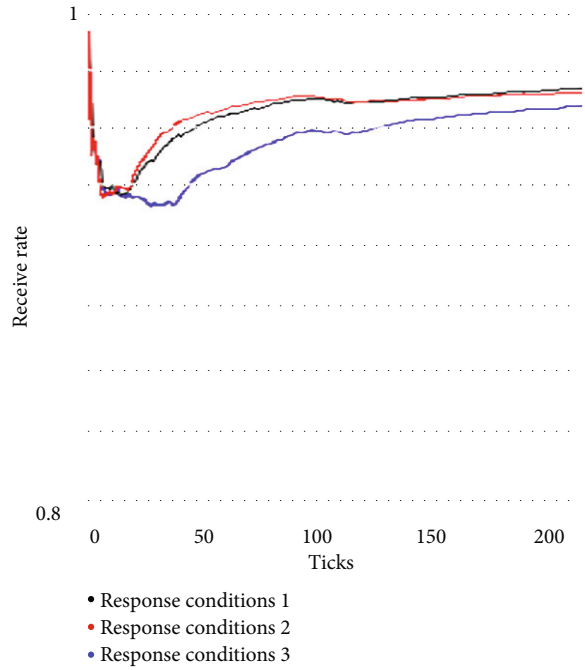

Figure 6: Different response conditions.

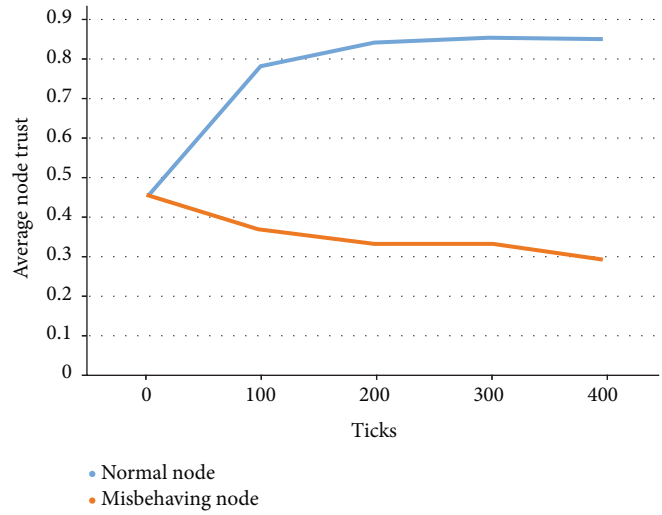

Figure 7: Message alteration attacks.

set randomly within a certain range, with no significant effect on the experimental results.

Figure 5 shows the effect of direct and indirect trust on the change in the overall receive rate of the network during the composite trust calculation process. w1 and w2 correspond to the direct trust value weights W_d and indirect trust value weights W_i, respectively, in the trust model when calculating T_c. Based on the analysis of the changing patterns of the receive rate curves under different parameter configurations, it can be concluded that the higher the direct trust value weights the faster the corresponding rate of composite trust, but the slower trust propagation will lead to a lower rate of its long-term receive rate increase, holding all other parameters constant. The higher the indirect trust value, the faster the trust spreads, but a more severe reduction in receive rate may occur in the short term.

Figure 6 shows the trend of network data transmission rates for different response conditions. The response conditions are of a relatively simple threshold type, where the three curves correspond to the overall data transmission rate from within the group network at threshold values of 0.4, 0.3, and 0.25. By comparison, it can be intuitively understood that the higher the threshold, the more likely the security response is to be triggered, which also makes the node faster to respond to unexpected security events accordingly. The lower the threshold, the more difficult it is to trigger a security response and the slower the node's corresponding response to unexpected security events. However, it should be noted that if we take the curve of Response conditions 2 as a reference, the corresponding curve of Response conditions 3 is not much different from Response conditions 2 in speed compared with Response conditions 1, but the number of emergency responses triggered by Response conditions 3 is much higher than that triggered by Response conditions 2 because it is closer to the initial value of the node trust, which means that Response conditions 3 have paid a lot of computing cost but have no actual effect compared with Response conditions 2. Therefore, it can be understood that the response condition setting needs to be adjusted according to the basic operation of the network, and too high or too low of the trigger conditions will cause the efficiency and stability of the network to decline.

Figure 7 shows the trend of trust changes when the scheme responds to message alteration attacks, where the vertical coordinate is the mean of the composite trust value for the corresponding type of node in the self-organized network and the horizontal coordinate is the time passed since the attack occurred in the self-organized network. From the change of the two lines corresponding to the normal node

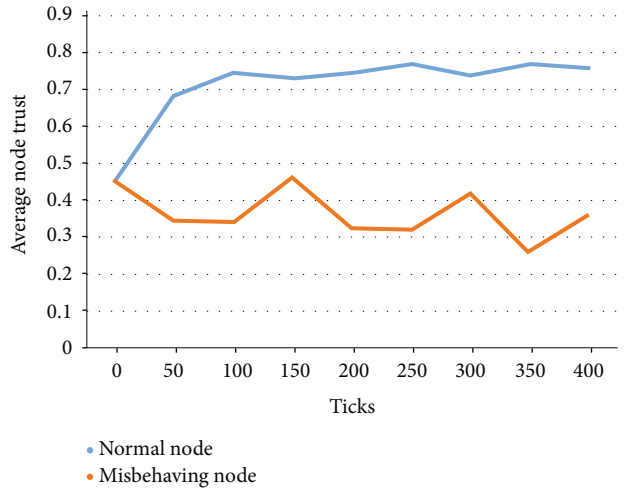

Figure 8: Badmouth attack.

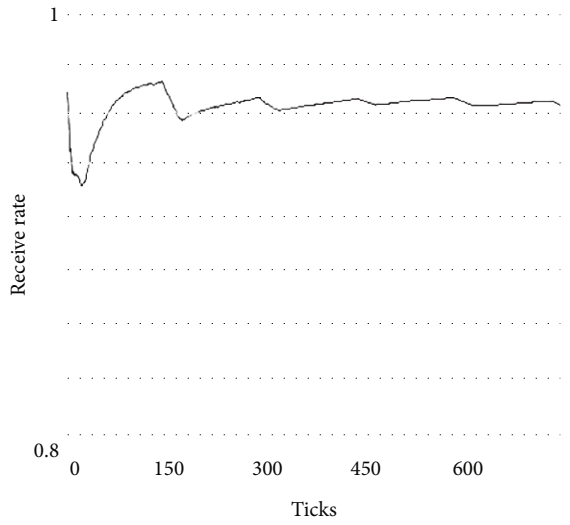

Figure 9: On-off attack.

and the misbehaving node, we can see that after the misbehaving node in a self-organized network attacks and affects the data transmission in the network, the trust evaluation of other nodes in the self-organized network decreases rapidly, which is significantly different from the trust value of other normal nodes.

Figure 8 shows the trend of trust changes in the program's response to the badmouth attack. The model's trust assessment produces large fluctuations when there are misbehaving nodes in the self-organizing network that provide erroneous trust data. However, through the handling of the trust model in the scheme, this trust fluctuation does not affect the distinction between misbehaving nodes and normal nodes when the number of misbehaving nodes in the network is not dominant.

Figure 9 shows the trend in the receipt rate of the program in response to an on-off attack, where the vertical coordinate is the receive rate of the overall data from the self-organized network and the horizontal coordinate is the time since the attack occurred. The misbehaving node periodically changes its own behavior, causing confusion in the node trust assessment process. It can be seen that the network's receive rate drops within a short period of time after an attack is developed but then rises rapidly when other nodes respond accordingly. This makes low-frequency attacks have less impact on the overall operation of the network, while high-frequency attacks are distinguished as misbehaving nodes and isolated, thus limiting the effectiveness of on-off attacks.

6. Conclusion

In sensor self-organized networks, the lack of high-performance base station nodes and the performance limitations of each network node make it impossible to effectively implement information security techniques that rely on encryption and signatures. It is necessary to provide security to the sensor nodes with minimal reliance on encryption and decryption operations. The trust-based trusted routing scheme designed in this paper establishes a more comprehensive and effective trust evaluation system within the self-organizing network through distributed trust evaluation. In terms of energy consumption, the distributed trust evaluation and the passive data collection approach share the consumption of trust computation among the self-organizing network nodes while reducing the additional overhead incurred in the trust evaluation phase. And the mode of adjusting the path selection based on node energy consumption also partially achieves load balancing of data transmission among the self-organizing network nodes. And the effectiveness of the attack form of trust spoofing is reduced by an integrated trust computation with multiple trust sources. The trust and routing distance based routing scheme allows self-organizing networks to efficiently perform the discovery and isolation process on misbehaving nodes completely autonomously, achieving automatic response and effective disposal of multiple forms of network attacks. Nevertheless, the lightweight design of this solution provides limited protection against Blackhole, Sybil, and other forms of attacks on the sensor self-organizing network.

Data Availability

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Project under grant 2019YFB2102303.

References

[1] "Cisco annual internet report (2018–2023) white paper," https://www.cisco.com/c/en/us/solutions/collateral/executive-

perspectives/annual-internet-report/white-paper-c11-741490.html.

[2] R. Mehta, J. Sahni, and K. Khanna, "Internet of things: vision, applications and challenges," *Procedia Computer Science*, vol. 132, pp. 1263–1269, 2018.

[3] A.-S. K. Pathan, Z. M. Fadlullah, S. Choudhury, and M. Guerroumi, "Internet of things for smart living," *Wireless Networks*, 2019.

[4] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of things: evolution and technologies from a security perspective," *Sustainable Cities and Society*, vol. 54, 2020.

[5] The Hacker News, "Dark Nexus: a new emerging IoT botnet malware spotted in the wild," April 2020, https://thehackernews.com/2020/04/darnexus-iot-ddos-botnet.html.

[6] G. J. Chen, *Mobile Internet of Things: Business Model and Case Analysis and Practical Application*, Post & Telecom Press, China, 2016.

[7] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 131–140, 2008.

[8] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communication Surveys and Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[9] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[10] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of things systems," *Computer Communications*, vol. 97, pp. 1–14, 2017.

[11] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[12] F. Li and J. Wu, "Uncertainty modeling and reduction in MANETs," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 1035–1048, 2010.

[13] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: a multi-dimensional trust management approach," in *2010 Eleventh International Conference on Mobile Data Management*, pp. 85–94, Kansas City, USA, 2010.

[14] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, pp. 1238–1246, Phoenix, AZ, USA, 2008.

[15] P. B. Velloso, R. P. Laufer, D. de O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172–185, 2010.

[16] S. Adali, R. Escriva, M. K. Goldberg et al., "Measuring behavioral trust in social networks," in *2010 IEEE International Conference on Intelligence and Security Informatics*, pp. 150–152, Vancouver, BC, Canada, 2010.

[17] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, pp. 418–424, Boston, MA, USA, 2011.

[18] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Computing Survey*, vol. 45, no. 4, 2013.

[19] S. Yi, P. Naldurg, and R. Kravets, "A security-aware routing protocol for wireless ad hoc networks," in *Stochastic Analysis in Discrete and Continuous Settings*, Springer, 2002.

[20] A. Tajeddine, A. Kayssi, A. Chehab, I. Elhajj, and W. Itani, "CENTERA: a centralized trust-based efficient routing protocol with authentication for wireless sensor networks," *Sensors*, vol. 15, no. 2, pp. 3299–3333, 2015.