Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 6667100, 10 pages
https://doi.org/10.1155/2021/6667100

Research Article

Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks

Guiping Zheng,[1] **Bei Gong**,[1] **and Yu Zhang**[2]

[1]*Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China*
[2]*School of Information Science and Technology, Zhengzhou Normal University, Henan 450044, China*

Correspondence should be addressed to Yu Zhang; 20852192@qq.com

Received 7 November 2020; Revised 30 December 2020; Accepted 12 February 2021; Published 28 February 2021

Academic Editor: Zhuojun Duan

Wireless sensor network is a key technology in Internet of Things. However, due to the large number of sensor nodes and limited security capability, aging nodes and malicious nodes increase. In order to detect the untrusted nodes in the network quickly and effectively and ensure the reliable operation of the network, this paper proposes a dynamic network security mechanism. Firstly, the direct trust value of the node is established based on its behavior in the regional information interaction. Then, the comprehensive trust value is calculated according to the trust recommendation value and energy evaluation value of other high-trust nodes. Finally, node reliability and management nodes are updated periodically. Malicious nodes are detected and isolated according to the credibility to ensure the dynamic, safe, and reliable operation of the network. Simulation results and analysis show that the node trust value calculated by this mechanism can reflect its credibility truly and accurately. In terms of reliable network operation, the mechanism can effectively detect malicious nodes, with higher detection rate, avoid the risk of malicious nodes as management nodes, reduce the energy consumption of nodes, and also play a defensive role in DOS attacks in wireless sensor networks.

1. Introduction

Internet of Things (IoT) can be regarded as the third information technology revolution following the computer and the Internet [1, 2]. It connects massive device nodes through the Internet, enabling everything to be interconnected whenever and wherever. In recent years, the widespread applications of IoT have not only changed people's lifestyles but also have a certain impact on the original cultivation patterns. Wireless Sensor Network (WSN), as a key technology in IoT, is a network system composed of microsensor nodes through wireless communication, and it is also an important source of sensing data in IoT. WSNs have been widely used in various fields, including weather monitoring, medical care, military applications, and the study phenomena in places where people cannot easily reach [3–5]. Its development and application will also have far-reaching impact on various fields, so it is very essential to ensure the safe and reliable operation of WSNs.

While WSNs play a huge role in IoT, the security problems are even more severe due to the characteristics of the sensor network itself [6–9]. On one hand, nodes in WSNs are usually deployed in unattended environments, which makes nodes have great security risks, such as vulnerable to physical attacks, being captured by attackers, private information being extracted, being transformed into malicious nodes, and launching various attacks. On the other hand, due to the mobility and effectiveness of nodes, the network topology in WSNs will change dynamically, which makes it difficult to maintain the trust relationship between nodes. In addition, sensor nodes in WSNs are characterized by limited energy, weak computing and storage capacity, low power consumption, and intensive deployment, which leads to the security protection mechanism in traditional networks cannot function effectively in WSNs, making the security problems of WSNs more prominent. Therefore, it has important significance to research into security mechanisms of WSNs.

On account of the existing problems in WSNs, this paper puts forward a dynamic network security mechanism based on trust management. This mechanism is based on trusted networking and takes trust computing as the core. Based on trust measurements, it can effectively detect malicious nodes in the network so that the network can operate dynamically and reliably. Eventually, the proposed scheme was verified by experiments.

2. Related Work

In WSNs, there are many researches on the safe and reliable operation mechanism of the network, which are used to detect malicious nodes attacks. Zhang et al. [10] proposed a detection scheme based on watermarking technology to detect selective forwarding attacks, which can not only detect whether the routing node discards the data packet but also detect whether the data in the packet is tampered. However, the scheme has a large delay in extracting watermarks and is not suitable for large-scale networks. Xu [11] proposed a sensor network malicious node detection scheme based on double threshold. Each sensor node maintains the trust value of its neighbors to reflect their past behavior in decision-making. Two thresholds are used to reduce the false alarm rate and enhance the accuracy event area detection; thus, under the condition of without sacrificing normal node implementation to detect malicious nodes is more accurate. However, appropriate threshold selection problem is the difficulty of scheme. An adaptive security mechanism of on-demand access control is proposed by Mauro et al. [12] for multihop energy harvesting in WSNs. In this mechanism, nodes can use base stations to release their current security measures, which helps sending nodes select appropriate recipient nodes according to their security requirements. But it is possible to cause malicious nodes to launch malicious attacks by reducing network security measures.

Trust management, as one of the methods to effectively defend against network internal attacks and identify malicious nodes, has been widely used in WSNs, and many typical models also have been proposed by scholars at domestic and foreign. Aiming at the low accuracy and malicious recommendation of the IoT trust evaluation method, Xie et al. [13] proposed a dynamic trust evaluation method for IoT nodes. First of all, this method designed the node service quality persistence factor to represent the overall behavior of the node, then used the friend acquaintance degree to filter recommended nodes, and finally calculated the comprehensive trust degree based on information entropy. The method proposed in [13] can effectively reduce the impact of malicious recommendation behavior on trust evaluation, but the implementation process is complicated and computationally intensive. Objects in the Social Internet of Things (SIoT) [14, 15] interact with each other based on their social behavior, in which any object can be either a service provider or a service consumer. Jafarian et al. [16] compared the service query context with the previous query context of other reviewers based on a data mining model, taken into account indicators such as social similarity, service importance, and the residual energy of providers, and considered this issue to a three-dimensional space. They measured the value contribution of trust value by using a weighted method. But the definition of social boundary involved in this method is ambiguous, and it cannot accurately calculate social acquaintance, which is not applicable to IoT systems with complex social relationships. Lin et al. [17] proposed a perceptual network security connection model based on the characteristics of social networks. This model describes the inferred transfer, transmission, update, and changes in the dynamic environment of trust in the IoT from the perspective of sociology, but the model does not combine subjective and objective in the trust evaluation process, and the accuracy of node trust evaluation is deficient.

Luo et al. [18] proposed a dynamic trust management system, which uses the hash algorithm to generate the unique identifier for nodes and uses the trust evaluation model based on the β density function to dynamically manage the trust value of each node. It can resist both external attacks and internal compromise attacks, but the model has large memory and energy costs and computational complexity. Bao and Chen et al. [19, 20] used collaborative filtering method to screen trust recommendation nodes and proposed a trust management model of IoT based on social relations. This model can improve the reliability of recommendation trust evaluation and enhance the ability of model to resist malicious recommendation behavior. However, in the process of direct trust evaluation, only the timeliness of trust is considered, which cannot accurately reflect the node behavior. A trust-based network security connection model suggested by Nguyen et al. [21], which is based on event-driven triggering trust refresh, extends trust definition and realizes data collection and analysis from multiple data sources. However, the dynamic adaptability of the model was insufficient. Chen et al. [22] raised a distributed adaptive filtering-based sensing network security connection model based on service-oriented architecture, which integrates dynamic direct trust and indirect trust to confirm the trust of nodes. On this basis, it guarantees the reliable operation of nodes, has good environmental adaptability, and fully considers the limited computing power of sensing nodes. However, the model lacks feedback control of nodes and cannot cope with malicious attacks well. Sathish et al. [23] improved the model proposed by Priayoheswari et al. [24] by introducing the proxy nodes and proposed an intelligent Beta reputation and dynamic trust evaluation model. The node credibility of the model was only evaluated by direct communication behavior. Although the energy consumption of trust calculation was reduced, the convergence rate of the model was reduced due to the lack of indirect trust evaluation process; thus, malicious nodes cannot be quickly identified.

To sum up, all kinds of current research schemes have their own characteristics (Table 1). Comparison of advantages and disadvantages of each scheme makes a comparative analysis of relevant work. The existing WSN dynamic adaptive security mechanism research has many deficiencies, which leads to the failure of existing WSN security mechanism to meet the needs of rapid development of WSNs. This paper proposes a dynamic adaptive security mechanism suitable for WSNs based on trust management. Firstly, it

Table 1: Comparison of advantages and disadvantages of each scheme.

Schemes	Advantages	Disadvantages
Detection scheme based on watermarking technology [10]	Effectively detect whether the data is discarded or tampered	The time delay of watermark extraction is large
Detection scheme of sensor network malicious nodes based on double threshold [11]	Reduce the false alarm rate and improve the accuracy of event area detection	The problem of threshold selection is the difficulty of this method
Adaptive security mechanism for on-demand access control [12]	Fully consider the security requirements of each node	May cause malicious nodes to launch malicious attacks using cuts in network security measures
A dynamic trust evaluation method for Internet of Things nodes [13]	Effectively reduce the influence of malicious recommendation behavior on trust evaluation	Complex implementation process and large amount of computation
Trust evaluation scheme based on data mining model in SIoT [16]	Comprehensively measure the value contribution of trust value assessment	The definition of social boundary is vague and cannot accurately calculate social familiarity
Perceived network security connection model [17]	Describe the changes of trust in various states from a sociological perspective	Without combining subjective and objective, the accuracy of node trust assessment is deficient
Dynamic trust management system [18]	To defend against external attacks but also to defend against internal compromise attacks	High memory and energy cost, high computational complexity
Trust management model of Internet of Things based on social relations [19, 20]	Improve the reliability of recommendation trust evaluation and enhance the ability of model against malicious recommendation behavior	Cannot accurately reflect node behavior
Trust-aware network security connection model [21]	Extending the definition of trust and realizing the function of data collection and analysis from multiple data sources	Lack of dynamic adaptability
Sensory network security connection model based on distributed adaptive filtering [22]	Good environmental adaptability, fully considering the computing ability of sensing nodes	Lack of feedback control to nodes, unable to resist malicious attacks perfectly
Intelligent Beta reputation and dynamic trust evaluation model [23, 24]	Reduce the energy consumption of trust computation	The convergence rate of the model is reduced, and the malicious nodes cannot be identified quickly

calculates the trust degree of sensor nodes in WSNs based on trust management model, then removes malicious nodes and selects management nodes based on trust degree, so as to make the network run dynamically and reliably.

3. Network Dynamic Security Adjustment Mechanism

The network dynamic adaptive adjustment mechanism proposed in this paper takes the trust computing model as the core, dynamically monitors the change of nodes in real time according to the trust degree of each node in the domain, and updates the network topology structure in time, thus ensuring the trusted operation of WSNs. The mechanism is described from three aspects: network model, trust evaluation model, and dynamic adaptive adjustment of WSNs.

3.1. Network Model Framework in WSNs. As shown in Figure 1, the network model in WSNs is mainly composed of four parts: ordinary nodes, domain management nodes, monitoring nodes, and base stations.

Ordinary nodes are used for data sensing and collection, so as to conduct information interaction between nodes, and evaluate and calculate direct and indirect local trust according to the interaction results.

Domain management nodes are high-trust nodes selected from ordinary nodes, which are mainly used to maintain the credibility of nodes within the domain, ensure that the nodes in the region are in a secure and reliable environment, calculate the comprehensive trust of each node, isolate malicious nodes in time, and communicate directly with the base station.

Monitoring nodes not only have the same function as the domain management nodes but also need to monitor the behavior of the domain management nodes. If the management nodes behave abnormally, they will directly send reports to the base stations. Each region contains two monitoring nodes, whose comprehensive trust value is second only to the domain management node in this region.

Base stations are used to select the domain management nodes and update the domain management nodes timely according to the reports from monitoring nodes. In this paper, it is assumed that the base stations are completely credible.

3.2. Trust Evaluation Model. The trust assessment framework proposed in this paper is shown in Figure 2. The trust degree of nodes is firstly calculated by the local trust degree between

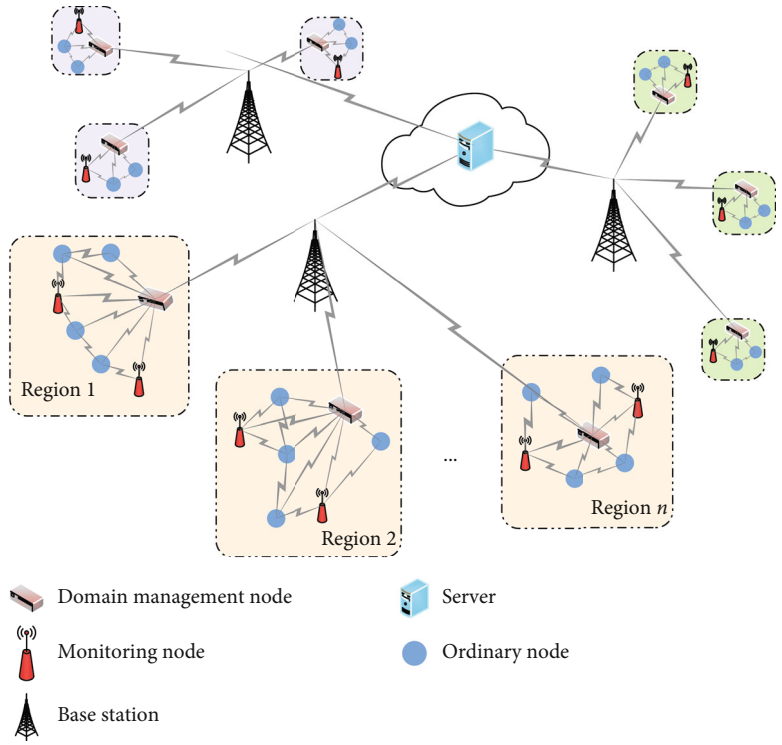


Figure 1: WSN node deployment architecture.

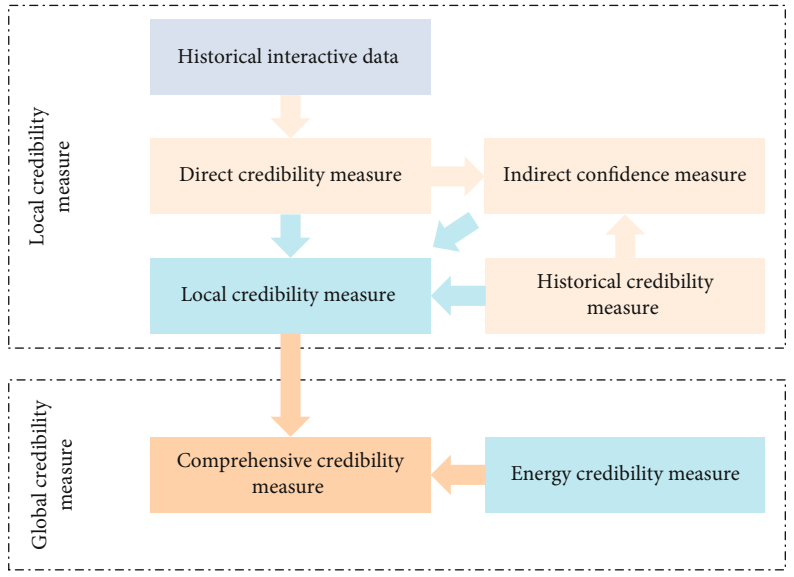


Figure 2: Trust assessment architecture.

the nodes in the domain, and then, the comprehensive trust degree of those nodes is calculated by domain management nodes. Improve the credibility of nodes, this paper sets the automatic update time ΔT, so as to calculate the trust degree of nodes regularly. In the following description, only the calculation process within one detection time ΔT is only described.

3.2.1. Related Definitions and Initialization. The calculation of nodes trust is the core of this mechanism. Trust is the ability to believe that a node has reliable and safe behavior in a certain context. Trust value is a quantitative representation of the trust ability of a node, and its size determines the credibility of the node. In this paper, the trust value range of node is [0,1], where 0 means that the node belongs to a completely untrusted node, and 1 means that the node is completely trusted. In the initial stage, the trust value of all nodes is initialized in this paper, and the value is 0.5. Domain management nodes and monitoring nodes are served by nodes with strong computing power and high energy.

3.2.2. Local Credibility Measure. Local trust is the result of mutual evaluation between interdomain nodes, which is mainly composed of direct credibility measure and indirect credibility measure.

(1) Direct Credibility Measure. The direct trust value is that the evaluation nodes combine the historical direct interaction data to predict the possible behavior of the evaluated nodes in the future. Trust evaluation method based on Bayesian can effectively reduce the complexity of trust calculation and energy consumption. In this method, if the number of successful and unsuccessful interactions between nodes N_i and N_j is u and v, respectively, the interaction results between nodes N_i and N_j obey Beta distribution. Therefore, the mathematical expectation $E(\text{beta}(p \mid u, v))$ of the Beta probability density function $\text{beta}(p \mid u, v)$ is obtained as the direct trust value D_{ij}, which is taken by (1).

$$D_{ij} = E(\text{beta}(p \mid u, v)) = \frac{u + \mathbf{1}}{u + v + \mathbf{2}}. \tag{1}$$

(2) Indirect Credibility Measure. Although direct trust is directly detected between nodes through information interaction, if the degree of interaction between two nodes is not enough or affected by channels or malicious nodes attack, the direct trust cannot measure the credibility of nodes. Therefore, this paper uses recommendation trust to make the prediction of nodes trust more accurate.

The recommended trust value of evaluating node N_i to evaluated node N_j needs to be obtained from node N_k, where N_k belongs to N_j's neighbor nodes set $\text{Ne}(N_j)$. In the IoT environment, node distribution is relatively dense, which leads to a large number of neighbor nodes. If each neighbor node makes recommendations, the network energy consumption will be accelerated, and the risk of bad-mouthing attack with higher or lower reputation may be faced. Therefore, this paper selects a set $\text{PNe}(N_j)$, a subset of $\text{setNe}(N_j)$, to calculate the recommended trust value for node N_j. The process of determining the partial neighbor node set $\text{PNe}(N_j)$ is as follows:

(a) The evaluation node N_i requests the domain management node to request the n nodes with the highest global trust degree in the set $\text{Ne}(N_j)$ as the recommended nodes, and the global trust degree of these nodes must not be lower than the recommended trust threshold δ_0

(b) After receiving the set $\text{PNe}(N_j)$ from the domain management node, node N_i sends a trust recommendation delivery request to the nodes in $\text{PNe}(N_j)$. Node N_k in set $\text{PNe}(N_j)$ receives the request and then sends D_{kj} to node N_i, where D_{kj} represents the direct trust from node N_k to N_j, according to (2) calculate the recommended trust RT_{ij}^k of the neighbor nodes N_k to N_k

$$\text{RT}_{ij}^k = \text{LT}_{ik}^{\text{old}} * D_{kj}, \tag{2}$$

where $\text{LT}_{ik}^{\text{old}}$ represents the historical local trust of nodes N_i to N_k. Therefore, node N_i calculates the final recommendation trust RT_{ij} based on the recommendation value of each node to node N_j in set $\text{PNe}(N_j)$. Since each neighbor node has different trust degree at node N_i, it is necessary to give certain weights to the recommendation trust value of each node. In this paper, according to (3), the weight w_k of the recommendation trust of node N_k in the indirect trust value is calculated, where $|\text{PNe}(N_j)|$ represents the total number of nodes in the set. Then, according to (4), the recommended trust RT_{ij} from nodes N_i to N_j is calculated.

$$w_k = \frac{\text{RT}_{ij}^k}{\sum_{l=\mathbf{1}}^{|\text{PNe}(N_j)|} \text{RT}_{ij}^l}, \tag{3}$$

$$\text{RT}_{ij} = \sum_{k=\mathbf{1}}^{|\text{PNe}(N_j)|} w_k * \text{LT}_{ik}^{\text{old}} * D_{kj}. \tag{4}$$

(3) Local Trust Synthesis and Update. After the evaluation node N_i passes the above process, the direct trust degree D_{ij} and the recommended trust degree RT_{ij} for the evaluated node N_j can be obtained. The evaluation node N_i first calculates the local trust degree $\text{LT}_{ij}^{\text{new}}$ within ΔT according to (5), then combines the local trust degree $\text{LT}_{ij}^{\text{old}}$ in the previous ΔT , and finally updates the local trust degree LT_{ij} according to (6). This process needs to measure the proportion of D_{ij} and $\text{LT}_{ij}^{\text{old}}$, where η_0 and η_1 are the measuring factors, and their values are set according to the specific environment.

$$\text{LT}_{ij}^{\text{new}} = \eta_{\mathbf{0}} D_{ij} + (\mathbf{1} - \eta_{\mathbf{0}})\text{RT}_{ij}, \tag{5}$$

$$\text{LT}_{ij} = \eta_{\mathbf{1}} \text{LT}_{ij}^{\text{old}} + (\mathbf{1} - \eta_{\mathbf{1}})\text{LT}_{ij}^{\text{new}}. \tag{6}$$

3.2.3. Global Credibility Measure. Global credibility measurement is mainly about calculating comprehensive trust. In the calculation of comprehensive trust, the energy state of the nodes needs to be considered in order to eliminate the influence of energy changes. It is known from Section 3.1 that each region has a domain management node and two monitoring nodes. For the convenience of description, this article uses G_x to represent the domain management node of area x, and the two monitoring nodes of G_x represent by $G_x^{M_1}$ and $G_x^{M_2}$. G_x, $G_x^{M_1}$, and $G_x^{M_2}$ will receive the local trust matrix $M(x)$ as shown in (7), where $m(m = |G_x|)$ represents the total number of nodes in the region x.

$$M(x) = \begin{bmatrix} \text{LT}_{\mathbf{11}} & \text{LT}_{\mathbf{12}} & \cdots & \text{LT}_{\mathbf{1}m} \\ \text{LT}_{\mathbf{21}} & \text{LT}_{\mathbf{22}} & \cdots & \text{LT}_{\mathbf{2}m} \\ \vdots & \vdots & \ddots & \vdots \\ \text{LT}_{m\mathbf{1}} & \text{LT}_{m\mathbf{2}} & \cdots & \text{LT}_{mm} \end{bmatrix}. \tag{7}$$

For node N_j, by searching for elements greater than zero in the $M(x)$'s column vector, denoted by the set S_j, then obtain the average value $\bar{T}_j$ from (8), and obtain the energy trust ET_j of node N_j from (9); finally, calculate the comprehensive trust degree T_j of node N_j according to (10), where E_j^{now} represents the current energy value of node N_j, E_j^{start} represents the initial energy value of node N_j, and η_2 represents the weight factor.

$$\bar{T}_j = \frac{\mathbf{1}}{|S_j|} \sum_{\mathrm{LT}_{ij} \in S_j} \mathrm{LT}_{ij}, \tag{8}$$

$$\mathrm{ET}_j = \frac{E_j^{\mathrm{now}}}{E_j^{\mathrm{start}}}, \tag{9}$$

$$T_j = \eta_2 \bar{T}_j + (\mathbf{1} - \eta_2)\mathrm{ET}_j. \tag{10}$$

3.3. Dynamic Adaptive Adjustment of WSNs. Based on the trust calculation, the base station can clearly grasp the status of all the sensing nodes in the region, so as to better use computing resources and communication resources from a global perspective and realize the adaptive adjustment of WSNs. Next, the dynamic network security adjustment mechanism will be studied from the selection and update of domain management nodes and the isolation of malicious nodes.

3.3.1. Domain Management Node Selection and Update. The process of selecting and updating domain management nodes is shown in Figure 3. The specific process is as follows:

(i) Domain management node G_x and monitoring nodes $G_x^{M_1}$ and $G_x^{M_2}$ obtain their respective comprehensive trust lists by calculation, which are, respectively, recorded as L_1, L_2, and L_3 and then sent them to the base station

(ii) After receiving L_1, L_2, and L_3, the base station selects the trust value with the highest number of occurrence as the final trust value of the node according to the three comprehensive trust values of each node

(iii) After the base station gets the final trust list L containing each node, it needs to timely update the comprehensive trust values of G_x, $G_x^{M_1}$, and $G_x^{M_2}$. Firstly, the similarity θ_i between L and L_i is calculated according to (11). Then, the similarity θ_i is judged. If it is 1, then the comprehensive trust value remains unchanged; otherwise, the comprehensive trust value will be reduced to $(1 - \theta_i)$ times of the original

$$\theta_i = \frac{\mathbf{1}}{m} \sum_{j=\mathbf{1}}^{m} \left(L^i == L_i^j ? \mathbf{1} : \mathbf{0} \right). \tag{11}$$

(iv) The base station sets the trust threshold δ_1. If the comprehensive trust of domain management node or monitoring node is lower than δ_1, the three nodes with the highest trust degree in the domain need to be reselected as the new domain management node G_x and monitoring node $G_x^{M_1}$ and $G_x^{M_2}$. The base station will send the final trust list L to the updated G_x, $G_x^{M_1}$, and $G_x^{M_2}$ as the comprehensive trust of each node in the domain

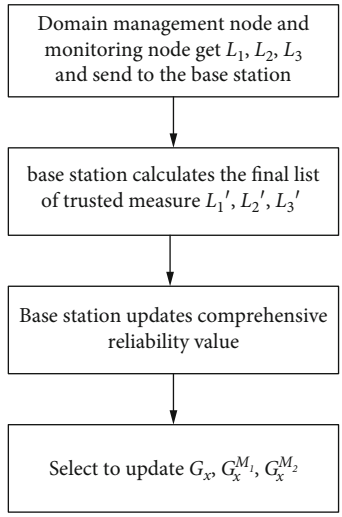


Figure 3: Domain management node selection and update process.

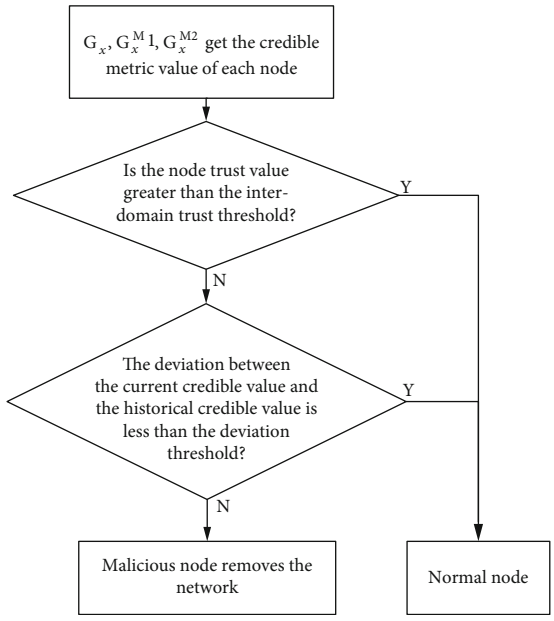


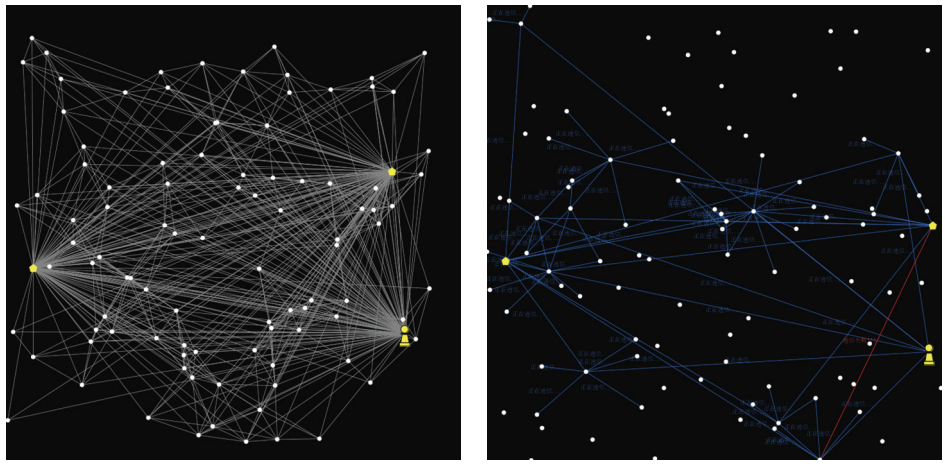
Figure 4: Malicious node detection process.

3.3.2. Malicious Node Detection. Over time, nodes may be attacked or damaged naturally, so malicious nodes need to be removed in a timely manner. Figure 4 shows the malicious node detection process.

After receiving the node information sent from the base station, G_x, $G_x^{M_1}$, and $G_x^{M_2}$ first determine whether the comprehensive trust value of each node is lower than the

Table 2: Some parameters of simulation experiment.

Parameter	Values
Simulation area size	100 m*100 m
Number of nodes	100
Energy consumption for data transmission and reception	25 nJ/bit
Normal node initial energy	1 J
Manage node and monitor node initial energy	5 J
Packet size	40 bit
Wireless communication radius	15 m
Packet forwarding rate	Random number between [0.9,1]
Initial confidence	0.5



(a) Node distribution diagram (b) Node communication diagram

Figure 5: Simulation effect of the experiment.

interdomain trust threshold δ_2. If lower than, it indicates that the node is insufficient in energy or is a malicious node. Otherwise, it is further detected whether the deviation of the current comprehensive trust value and the historical comprehensive trust value of the node are smaller than the deviation threshold δ_3. If the deviation is less than δ_3, it is a normal node. If it is greater than δ_3, it can be divided into two situations: first, the current comprehensive trust value minus historical comprehensive trust value is greater than δ_3, indicating that the trust value of the node has been greatly increased, and it can be determined that the node has disguised behavior; second, if the historical comprehensive trust value minus the current comprehensive trust value is greater than δ_3, it indicates that the trust value of the node has been significantly reduced, and the node can be determined to be energy deficient or become a compromise node.

In addition, domain management node G_x can recognize DOS attacks when information is exchanged between nodes. According to the actual environment of region x, set the threshold δ_4 of interdomain node interaction within the detection period. If the total number of interactions between nodes N_i and N_j exceeds δ_4, it indicates that the interactions between nodes N_i and N_j are too frequently, and it is highly likely that malicious DOS attacks will occur. Then, the behaviors of nodes N_i and N_j should be observed to further determine whether it is a malicious node and then remove them from the network.

4. Simulation Experiment and Safety Analysis

4.1. The Simulation Results. In order to better verify the detection efficiency and energy consumption of this mechanism for malicious nodes, NetLogo is used to simulate the proposed mechanism in this paper. Since the simulation calculation process of each region is consistent, only one region is simulated. Some parameters of the simulation experiment are shown in Table 2.

Figure 5 shows the effect diagram of simulation using NetLogo. The figure on the left shows the initial network state. If the nodes can communicate with each other, they are indicated by connecting lines in the initial network state. The right figure represents the communication state at a certain moment, in which the lines represent the communication between nodes, the successful communication between nodes is represented by blue, and the failure is represented by red.

Firstly, in the trust calculation section, by analyzing the comprehensive trust value of all nodes, the comprehensive trust value curve of malicious nodes and the normal nodes in Figure 6 can be obtained. As can be seen from Figure 6,

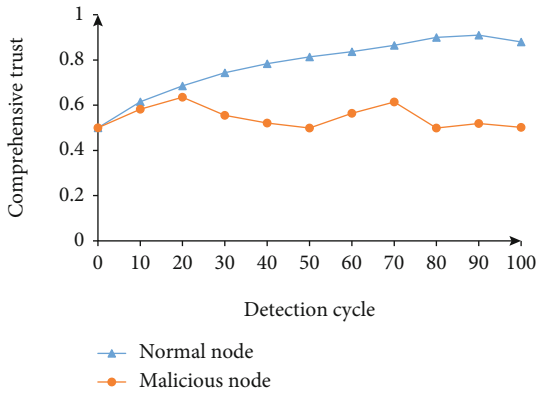


Figure 6: Curve of comprehensive trust change.

the normal node comprehensive trust value appears gradually rising trend, but with an increasing number of detection cycle, ordinary node comprehensive trust value will decline. This is because with the increase of detection cycle, the energy of nodes is limited, which leads to the gradual increase of the influence of the energy trust of nodes on the comprehensive trust. However, there is no regularity in the change in the overall trust of malicious nodes. Because malicious nodes do not know their comprehensive trust, it is possible to launch attacks at any time. But overall, the trust of malicious nodes will be far smaller than the normal nodes as the detection cycle changes.

Then, different proportion of malicious nodes is deployed in the network, as shown in Figure 7, and the detection rate changes of malicious nodes in 10, 20, and 40 cycles are compared, respectively. It can be seen from the horizontal direction that the detection rate will decrease as the number of malicious nodes increases, because the increase in malicious nodes will affect the accuracy of trust value and thus affect the judgment of nodes to some extent. Vertically, the longer the detection cycle, the higher the detection rate will be. This is because as the detection cycle increases, the malicious nodes will gradually be isolated, and the comprehensive trust generated by the interaction will become more and more accurate, which is conducive to the detection of malicious nodes. Overall, when malicious nodes are lower than 20%, the average detection rate of this paper is higher than 75%. This mechanism can detect and isolate malicious nodes quickly and effectively.

Finally, since sensor nodes are resource-constrained, it is necessary to analyze the energy consumption of nodes. Figure 8 shows that as the number of malicious nodes increases, the total energy consumption in the network increases gradually. At the same time, it can be seen that compared with [13], the scheme in this paper reduces the network energy consumption and the aging rate of nodes.

4.2. Security Analysis. In this paper, the recommendation trust value of all neighbor nodes is not used in the calculation of recommendation trust, but the set of high-trust neighbor nodes is screened out. This method can effectively exclude the malicious recommendation behavior of neighbor nodes and avoid bad-mouthing attack.

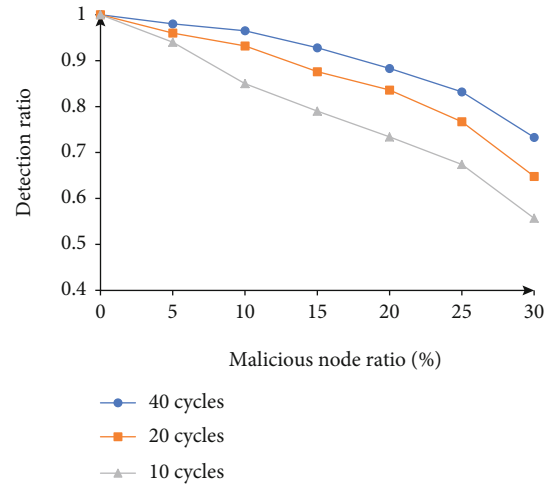


Figure 7: Detection rate of malicious nodes.

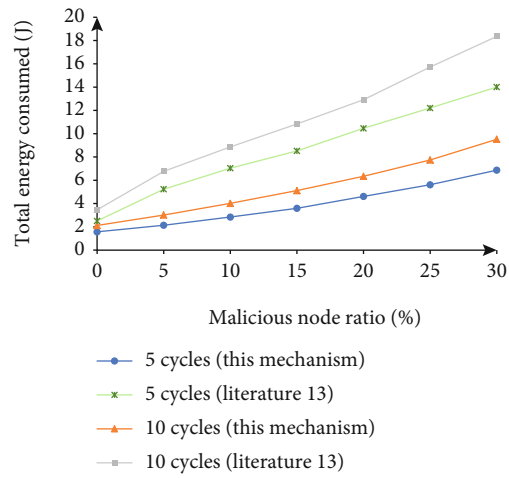


Figure 8: Total network energy consumption.

Domain management nodes play a role in managing other common nodes in the region. If a domain management node is attacked as a compromise node to launch a malicious attack, the trust value of all nodes cannot be measured, and the region falls into an extremely insecure situation. In this paper, monitoring nodes are set up to observe the behavior of the domain management node at any time and report it to the base station in time. The base station will verify the reported content. If true, the credibility of domain management node will be reduced, and the domain management node will be replaced with a node with higher trust. In addition, monitoring nodes have the same computing tasks as domain management nodes. If the base station detects that their behavior is abnormal, the domain management node and the monitoring node are replaced with new nodes in time. This method can effectively deal with the risk of domain management node being attacked.

In the traditional trust management mechanism, there is a risk of disguised attack, that is, when malicious nodes find their trust value is lower than other nodes, they will suspend the attack behavior, improve their trust value in a short term

through good performance, or change the identity and rejoin the network. In this paper, the comprehensive trust degree of nodes is only stored in the management node, the monitoring nodes, and the base station. Malicious nodes are not clear about themselves trust degree, so the masking behavior of malicious nodes is effectively avoided.

5. Conclusion

The key of network dynamic trusted operation is to identify and isolate malicious nodes to ensure their trusted operation. This paper proposes a network security mechanism based on trust management to deal with the threats faced by WSNs. Based on the trusted access of nodes, this mechanism firstly calculates the local trust degree of nodes according to existing interaction behavior and further obtains the comprehensive trust degree of nodes that can reflect the trust degree of nodes. In network management, the selection and updating of domain management nodes and detection of malicious nodes are carried out according to the comprehensive trust degree of nodes. Through simulation experiment analysis, the node's comprehensive trust can accurately reflect their behavior, detect and isolate malicious nodes in time, and effectively guarantee the trusted and reliable operation of WSNs.

Data Availability

No data were used to support this study.

Conflicts of Interest

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

Acknowledgments

This research was supported by the National Key R&D Program of China (2019YFB2102303), the National Natural Science Foundation of China (61971014), and the 2020 Henan Key Research and Development Project (202102310522).

References

[1] S. B. Shen and C. Lin, "Opportunities and challenges in study of Internet of Things," *Journal of Software*, vol. 8, pp. 1621–1624, 2014.

[2] H. Kaur and R. Kumar, "A survey on Internet of Things (IoT): layer-specific, domain-specific and industry-defined architectures," *Advances in Computational Intelligence and Communication Technology*, vol. 1086, pp. 265–275, 2021.

[3] R. Krishnan, "Mobile application for emergency navigation during disaster using wireless sensor network," *Advances in Wireless Communications and Networks*, vol. 4, no. 1, p. 1, 2018.

[4] N. Brinis and L. A. Saidane, "Context aware wireless sensor network suitable for precision agriculture," *Wireless Sensor Network.*, vol. 8, no. 1, pp. 1–12, 2016.

[5] G. Ramesh and R. Nivedha, "Micro climate monitoring-web application using wireless sensor network," *International Journal of Science and Research (IJSR)*, vol. 5, no. 4, pp. 104–106, 2016.

[6] J. Furtak, Z. Zielinski, and J. Chudzikiewicz, "Security techniques for the WSN link layer within military IoT," in *IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 233–238, Reston, VA, USA, 2016.

[7] D. Pandita, R. K. Malik, and Department of ECE, Geeta Engineering College, Panipat Kurukshetra University, Kurukshetra, Haryana, India, "A survey on clustered and energy efficient routing protocols for wireless sensor networks," *International Journal of Trend in Scientific Research and Development*, vol. Volume-2, no. Issue-6, pp. 1026–1030, 2018.

[8] W. L. Wu, N. X. Xiong, and C. X. Wu, "Improved clustering algorithm based on energy consumption in wireless sensor networks," *The Institution of Engineering and Technology*, vol. 6, no. 3, pp. 47–53, 2017.

[9] J.-Y. Yu, E. Lee, S.-R. Oh, Y.-D. Seo, and Y.-G. Kim, "A survey on security requirements for WSNs: focusing on the characteristics related to security," *IEEE Access*, vol. 8, pp. 45304–45324, 2020.

[10] D. Y. Zhang, C. Xu, and S. Lin, "Detecting selective forwarding attacks in WSNs using watermark," *International Conference on Wireless Communications and Signal Processing (WCSP)*, vol. 2011, pp. 1–4, 2011.

[11] C. J. Xu, *Research on detection scheme of malicious nodes and abnormal data in wireless sensor network [Ph.D. thesis]*, Nanjing University of Posts and Telecommunications, 2020.

[12] A. D. Mauro, X. Fafoutis, and N. Dragoni, "Adaptive security in ODMAC for multihop energy harvesting wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 3, 2015.

[13] L. X. Xie and R. X. Wei, "Dynamic trust evaluation method for IoT nodes," *Journal of Computer Applications*, vol. 39, no. 9, pp. 2597–2603, 2019.

[14] A. U. Rehman, R. A. Naqvi, A. Rehman, A. Paul, M. T. Sadiq, and D. Hussain, "A trustworthy SIoT aware mechanism as an enabler for citizen services in smart cities," *Electronics*, vol. 9, no. 6, p. 918, 2020.

[15] K. C. Chung and S. W.-J. Liang, "An empirical study of social network activities via social Internet of Things (SIoT)," *IEEE Access*, vol. 8, pp. 48652–48659, 2020.

[16] B. Jafarian, N. Yazdani, and M. S. Haghighi, "Discrimination-aware trust management for Social Internet of Things," *Computer Networks*, vol. 178, p. 107254, 2020.

[17] Z. T. Lin and L. Dong, "Clarifying trust in Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering.*, vol. 30, no. 2, pp. 234–248, 2018.

[18] W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks," *Security and Communication Networks.*, vol. 9, no. 7, pp. 613–621, 2016.

[19] F. Y. Bao and R. Chen, "Trust management for the Internet of Things and its application to service composition," World of Wireless, Mobile & Multimedia Networks IEEE, 2012.

[20] I. R. Chen, F. Bao, and J. Guo, "Trust-based service management for Social Internet of Things systems," *IEEE Transactions on Dependable and Secure Computing.*, vol. 13, no. 6, pp. 684–696, 2016.

[21] H. L. Nguyen, O. J. Lee, J. E. Jung, J. Park, T. W. Um, and H. W. Lee, "Event-driven trust refreshment on ambient services," *IEEE Access.*, vol. 5, pp. 4664–4670, 2017.

[22] I. R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2017.

[23] S. Sathish, A. Ayyasamy, and M. Archana, "An intelligent beta reputation and dynamic trust model for secure communication in wireless networks," *Industry Interactive Innovations in Science, Engineering and Technology (I3SET)*, vol. 11, pp. 395–402, 2017.

[24] B. Priayoheswari, K. Kulothungan, and A. Kannan, "Beta reputation and direct trust model for secure communication in wireless sensor networks," in *Proceedings of the International Conference on Informatics and Analytics*, New York, NY, USA, 2016.