WSN Network Node Malicious Intrusion Detection Method Based on Reputation Score

Junlin Zhang

School of Information Technology, Guangdong Technology College, Zhaoqing 526100, China
E-mail: junlin_zhang2610@163.com

Received 02 August 2022; Accepted 05 January 2023;
Publication 03 March 2023

Abstract

Wireless sensor network (WSN) is the Internet of Things by a large number of sensors in the external physical environment to obtain data information, and use wireless communication technology to provide users with information transmission services. At this stage, communication and security mechanisms are the main problems faced by WSN. This is because most of the existing sensors are powered by batteries with very limited energy, and most of them are deployed in an outdoor open environment, which is easy to be captured as a malicious node. Network attacks. However, the existing malicious node detection methods have shortcomings such as low efficiency, high energy consumption, and insufficient performance. Therefore, this paper proposes a WSN malicious node intrusion detection method based on genetic algorithm optimization of LEACH hierarchical routing protocol. Based on the optimization of the LEACH protocol by genetic algorithm, the method integrates the reputation evaluation mechanism, and screens and eliminates malicious

Journal of Cyber Security and Mobility, Vol. 12_1, 55–76.
doi: 10.13052/jcsm2245-1439.1213

nodes by calculating direct reputation, indirect reputation and comprehensive reputation, thereby ensuring the safe operation of WSN. The simulation results show that this method can effectively resist the attack of malicious nodes on WSN, and has obvious advantages over other methods.

Keywords: Intrusion detection, malicious node, reputation assessment, WSN.

1 Introduction

With the rapid progress of computer technology, wireless communication technology and sensor technology, the Internet of Things (IoT) has gradually been widely used in many fields [1]. An important condition for IoT operation is to establish a reliable perception system with the external physical environment, which is mainly achieved through WSN [2]. WSN contains a large number of sensor nodes. Through the sensing function of nodes, the information of external physical objects can be obtained, and wireless communication technology is used to realize information exchange between nodes and user-oriented information services [3]. The sensor nodes of WSN are generally deployed in an outdoor open environment and rely on battery power. Therefore, the data transmission efficiency and energy saving need to be improved. In addition, there are great security risks. In addition to external network attacks such as replay attacks and denial of service, there are also malicious node attacks from inside the network, which cause great harm to user information privacy and security [4]. Restricted by factors such as environment and energy consumption, the detection and defense of malicious nodes face great challenges, and it is extremely important to design an efficient and energy-saving malicious node detection method. To this end, the research introduces a reputation evaluation mechanism into the routing protocol based on genetic algorithm optimization, and judges malicious nodes and normal nodes according to the node's reputation score, so as to identify and eliminate malicious nodes and ensure the safe operation of WSN.

2 Related Works

The Internet of Things is a typical representative of the new generation of information technology, and its core technology is wireless sensor networks. Many other Internet of Things-related branches depend on the development

of WSN technology. Therefore, strengthening the research on WSN is of great significance to promote the development of the Internet of Things industry. At present, designing a high-efficiency and energy-saving WSN defense mechanism is an urgent problem to be solved, and many researchers have conducted in-depth discussions on it. Cryptography is a commonly used data protection technology in WSN, but it is difficult to resist attacks inside the network, and it needs to consume a lot of energy for a large number of calculations [5]. Trust management has shown good results in protecting WSN user privacy and information security, and can be used as an effective complement to cryptography. Therefore, many scholars design WSN defense mechanisms from the perspective of trust security [6]. Khan et al. used the trust model to calculate the trust value of nodes, and designed a WSN cluster head selection method based on biological inspiration and trust model. The simulation results show that the average trust value of cluster heads selected by this method is very high [7]. Nr et al. pointed out that the trust management method used in large-scale WSN is difficult to meet the requirements of security and reliability in practical applications. A new comprehensive trust estimation method is proposed to achieve effective trust estimation and malicious node identification. The experimental results show that the scheme has good performance in cost saving and malicious node detection [8]. Goyat et al. introduced a new trust mechanism into the LEACH protocol to judge the trust value and security of watermark nodes. The simulation results show that this method can effectively resist internal attacks and node tampering [9]. Liu et al. designed a secure positioning framework by using the trust mechanism. Based on the calculation of the trust degree of each node, the positioning is carried out, and the corresponding weights are dynamically updated. Simulation experiments show that this scheme is better than the existing algorithms in positioning accuracy, malicious detection efficiency and false detection rate have been significantly improved [10].

Nunoo-Mensah and others designed a real-time monitoring mechanism of trust behavior using game theory, and then conducted trust evaluation on this basis, and integrated the whole mechanism into the routing protocol. The simulation results show that the trust mechanism can effectively reduce energy consumption and improve the security protection efficiency compared with the traditional trust evaluation scheme [11]. Sajwan and others believe that the trust assessment methods in WSN can be divided into three types: social incentives, biological incentives and analytical methods, among which analytical methods (probability, fuzzy, etc.) are more important than the other two methods in the design of WSN trust assessment mechanism more

common [12]. Anwar adopted the Bayesian method to collect the direct and indirect trust values of nodes, and examined the correlation of historical data, thereby eliminating malicious nodes in the network. Compared with the previous scheme, the malicious node detection rate of this method was higher, with lower latency and higher network throughput [13]. Liu pointed out that the existing trust evaluation mechanism needs to be improved in terms of computing speed, energy saving and anti-cooperative attack. Therefore, a WSN trust computing scheme based on cross-validation is proposed. Theoretical and experimental analysis shows that this method can improve the computing speed. At the same time, it can effectively save energy, and can effectively resist the cooperative attack of malicious nodes [14]. Liu and Lu et al. introduced the secure boot model and BDRM in the routing protocol, and proposed a secure routing protocol integrating trust evaluation mechanism. The experimental results show that the protocol can effectively reduce packet loss while improving data transmission efficiency rate and energy consumption [15]. Jiang and others pointed out that the traditional trust mechanism is subject to the characteristics of the underwater environment, and for this purpose, an underwater WSN trust evaluation and update mechanism was designed using the C4.5 decision tree algorithm. The decision tree is trained by collecting trust evidence, and the reward and punishment factor is introduced to update the trust value in real time. In a dynamic environment, the malicious node detection and energy saving performance of this method are better than traditional algorithms [16].

WSN is vulnerable to both internal and external security threats, and because of its complex and changeable operating environment and limitations in transmission power and node energy, the detection and defense of network attacks face great challenges. Traditional cryptography methods are difficult to resist the internal attacks of malicious nodes. In the existing research related to trust management, the constraints of the WSN operating environment have not been fully considered, and the processing capability of large-scale data needs to be improved, and machine learning algorithms are introduced. will increase the resource load. Therefore, the research uses the genetic algorithm to optimize the design of the WSN layered routing protocol to reduce network energy consumption and ensure the effect of intrusion detection, and then introduce a reputation evaluation mechanism into the protocol to effectively identify malicious nodes, resist internal network attacks, and improve WSN safety performance.

3 Design of WSN Intrusion Detection Method Using Reputation Evaluation Mechanism

3.1 WSN Energy-saving Routing Protocol Design

The energy of WSN data transmission nodes is limited. If the transmission process consumes a lot of energy, it will interfere with the normal operation of the network and affect the effect of the intrusion detection system [17]. Therefore, it is necessary to design a reasonable routing protocol to reduce the energy consumption of the data transmission process and ensure the performance of the WSN intrusion detection system. There are various defects in traditional routing protocols, and it is difficult to achieve the low energy consumption goal of WSN. Therefore, GA is used to improve the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol, and a hierarchical energy saving method is proposed. Routing Protocol. GA was originally generated from the simulation of population evolution in the natural environment, and has now become an optimization algorithm widely used in various fields [18]. GA is a global search algorithm that is easy to implement, has strong adaptability and high robustness, and its main process is shown in Figure 1.

The wireless communication energy consumption model adopts the first-order radio model, which mainly includes two ports of data transmission and data reception. The energy consumption of the sender when sending l bit data

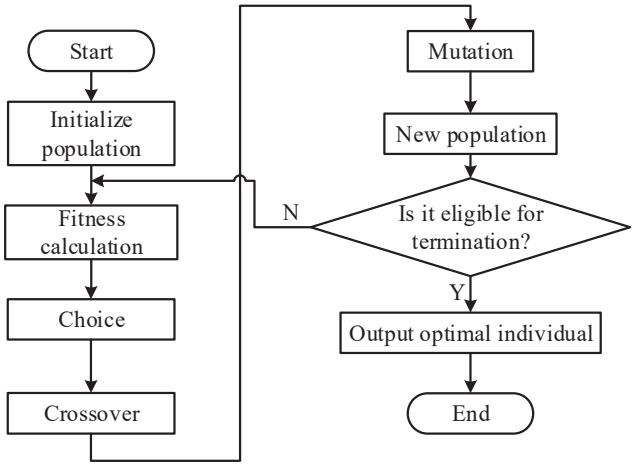

Figure 1 Flowchart of GA.

is $E_s(l,d)$ shown in formula (1).

$$E_s(l,d) = \begin{cases} lE_{elec} + ld_{fs}d^2 & d < D \\ lE_{elec} + ld_{mp}d^2 & d > D \\ D = \sqrt{\dfrac{d_{fs}}{d_{mp}}} \end{cases} \tag{1}$$

Formula (1), it E_{elec} represents the energy consumption value per 1 bit of data sent, represents the δ_{fs} constant of the free space model, represents the δ_{mp} constant of the multipath fading model, D represents the distance threshold of the two models, and d represents the distance between nodes. The energy consumption of the receiving end to receive l bit data is shown in formula (2).

$$\begin{cases} E_r(l) = lE_{elec} \\ E_p(l) = lE_{pa} \end{cases} \tag{2}$$

Formula (2), it $E_r(l)$ represents the energy consumption of receiving data, $E_p(l)$ represents the energy consumption of data aggregation, and E_{pa} represents the energy consumption value of each 1-bit data received by the cluster head. In the LEACH protocol, there is a problem that the random selection of cluster head nodes leads to excessive energy consumption. In order to solve this problem, combined with the genetic algorithm, the energy and position of the nodes are investigated when selecting the cluster head nodes, and the single-hop-multiple Hop combined transmission strategy. Firstly, a data transmission environment is assumed as follows: (1) a sensor is randomly distributed in a square area with a width of (3) The sending node can adjust the power according to the distance between the two ends, and the receiving node analyzes the position of the sending node according to the signal; (4) The sensor uses time division multiple access (Time division multiple access), TDMA) time slot adjustment working state; (5) The base station node is not limited. In the initial stage of the network, the LEACH algorithm traverses all sensor node information according to the base station node signal, and then sends it to the base station node, which saves all the information, and thus constructs a virtual network topology. The GA algorithm is introduced in the clustering stage, and three fitness functions are established according to the cluster head distribution, node distance and data transmission distance. The first part is the ratio of the mean residual energy of all nodes of the individual to the mean residual energy of surviving nodes,

as shown in formula (3).

$$f_1 = \frac{\frac{1}{H}\sum_{i=1}^{H} E_{CH(i)}^{n}}{\frac{1}{M}\left(\sum_{i=1}^{H} E_{CH}^{n}(i) + \sum_{j=1}^{M-H} E_{CM(j)}^{n}\right)} \tag{3}$$

Formula (3), H represents the total number of cluster head nodes, $f_2 = -$ represents the number of surviving nodes, $CH(i)$ represents n the cluster head node of the first round, and its residual energy is $E_{CH(i)}^{n}$, $CM(j)$ represents n the ordinary node of the first round, and its residual energy is $E_{CM(j)}^{n}$. The second part is the ratio of the distance between the cluster head node and the distance between the cluster head node and the common node, as shown in formula (4).

$$f_2 = \frac{\sum_{i=1,j=1,i\neq j}^{H} d(CH_i, CH_j)}{\sum_{i=1}^{M-H} d(CH_i, CH_i)} \tag{4}$$

Formula (4), it $d(CH_i, CH_j)$ represents the distance between the cluster head node and the distance between the $d(CH_i, CH_i)$ cluster head node and the common nodes in the cluster. The third part is the data transmission delay determined by the data transmission distance, as shown in formula (5).

$$f_3 = \max(n_i + 1) \quad i = 1, 2, 3, \ldots, H \tag{5}$$

Formula (5), it n_i represents i the number of nodes in the cluster. The calculation function of the fitness obtained by the three-part weighted calculation is shown in formula (6).

$$F = \gamma_1 f_1 + \gamma_2 f_2 + \gamma_3 f_3 \tag{6}$$

Formula (6), γ_1, γ_2, γ_3 represent the corresponding weight coefficients of each part, and $\gamma_1 + \gamma_2 + \gamma_3 = 1$. After the fitness value is calculated according to the function, the "roulette" method is used for selection operation to generate a new genetic population. Under the "roulette" method, the fitness value of an individual $Gp(ind)$ has a direct impact on its genetic probability, as shown in formula (7).

$$Gp(ind) = \frac{F_j}{\sum_{j=1}^{C} F_j} \tag{7}$$

Formula (7), it F_j represents $Gp(ind)$ the fitness of the individual and C represents the size of the population. After selecting genetic individuals, the

method of single-point crossover is used to randomly determine the crossover point of chromosomes, and the genes on both sides of the crossover point are exchanged, and the crossover probability is P_c [19]. Then, the chromosome is mutated to generate new genetic individuals. The main method is to invert a random gene according to the probability, which is expressed as the exchange of cluster head nodes and non-cluster head nodes. In the final stage of clustering, all nodes are called members of a cluster, and each cluster head allocates time division multiple access time slots. At this stage, the cluster head node judges its own identity according to the id, and then broadcasts its own information. The ordinary node will receive the signal broadcast by the cluster head node, and analyze the signal strength and distance respectively, and join the optimal clustering based on this. After clustering, the information transmission within the cluster is completed, and then the information transmission between different clusters is carried out. This process of the traditional LEACH protocol adopts a single-hop method. The distance between some clusters is too large, which leads to excessive energy consumption, which leads to death. The number of nodes increases [20]. Therefore, the use of multi-hop mode for information transmission between clusters with a long distance can effectively reduce energy consumption. The cluster head node selects the backup path node according to the distance between the adjacent cluster head and the base station node, and the distance is greater than the removal criterion. The selection criterion is $f(CH_i)$ shown in formula (8).

$$f(CH_i) = \alpha_1 \frac{E_{CH_i}}{E'} + \alpha_2 \left(1 - \frac{M_{CH_i}}{\sum_{h=1}^{H} M_{CH_i}}\right) + \alpha_3 \frac{d(CH_j, BS)^2}{d(CH_j, CH_i)^2 + d(CH_j, BS)^2} \tag{8}$$

Formula (8), α_1, α_2, α_3 represent the corresponding weights, and $\alpha_1 + \alpha_2 + \alpha_3 = 1$ the values are all non-zero positive real numbers less than 1, M_{CH_i} representing the number of surviving nodes in $B(\ )$ the cluster in this round, representing the CH_i number of clusters, E' representing the energy value of the node before data transmission, which CH_j indicates the starting cluster head node of data transmission. The node with the largest value according to formula (8) is selected as the node for the next hop, thereby determining the optimal path to the base station node, and realizing the data transmission oriented to the base station.

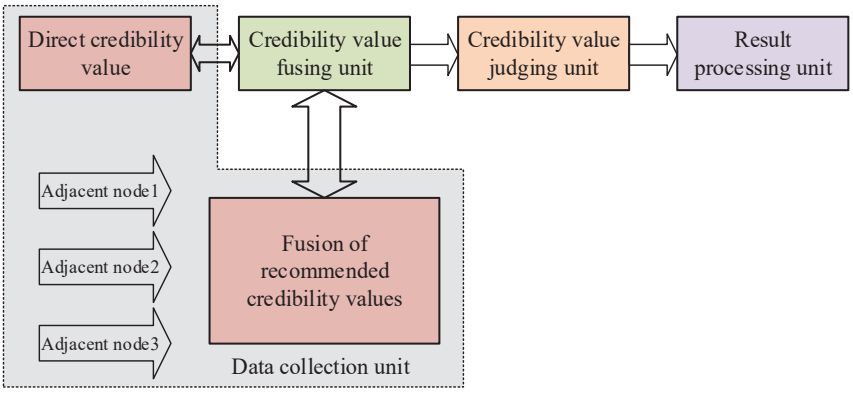

Figure 2 Structure of reputation mechanism.

3.2 Design of WSN Node Reputation Evaluation Mechanism

In order to strengthen the security of WSN, a reputation mechanism is introduced into the routing protocol for improvement, and the malicious nodes can be effectively identified by deleting nodes with low reputation points. Calculating the reputation score of a node through reputation evaluation is the key to the reputation mechanism. This process is divided into two aspects: direct evaluation and indirect evaluation. The main method is to observe and judge the behavior of the node to be evaluated during communication. its credibility. The existing WSN reputation mechanism structure usually includes four units: data collection, reputation integration, reputation judgment and result processing, as shown in Figure 2.

The research uses the representative of Bayes decision theory, beta distribution, to construct the WSN reputation mechanism model. Its probability density function and its expectation are shown in formula (9) [21].

$$\begin{cases} B(p|\eta,\iota) = \dfrac{\Gamma(\eta+\iota)}{\Gamma(\eta)\cdot\Gamma(\iota)} p^{\mu-1}(1-p)^{\iota-1} \quad 0 \le p \le 1 \\ E(p) = \dfrac{\eta}{\eta+\iota} \\ \eta = n_s + 1 \\ \iota = n_f + 1 \end{cases} \tag{9}$$

Formula (9), if $\eta < 1$, then $p \neq 0$; if $\iota < 1$, then $p \neq 1$; n_s represents the number of successful node communications, and n_f represents the number of node communications failures. Each node does not interact with all other

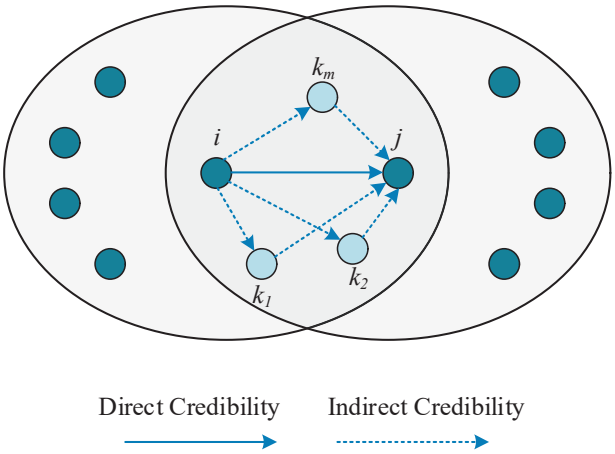

Figure 3 Credibility evaluation mechanism.

nodes. Each node only needs to evaluate the reputation of its neighboring interacting nodes, and then build a complete reputation network, so that each node can obtain the reputation of all other nodes. The evaluation mechanism is shown in Figure 3.

Firstly, the reputation of the node is directly evaluated. According to the formula (9), the direct reputation score of the node relative to the node is calculated as $Dt(i,j)$ shown in the formula (10).

$$Dt(i,j) = \frac{\eta_{ij} + 1}{\eta_{ij} + \iota_{ij} + 2} \tag{10}$$

In formula (10), it η_{ij} represents i the number of successful communication between the node ι_{ij} and the node j and j the number of failures in the communication between the node and the node i. In the actual transmission of data, factors such as WSN network congestion or failure will also have a negative impact on data communication, which will affect the reputation of nodes lower than the actual situation, resulting in normal nodes being mistakenly detected as malicious nodes. To avoid this situation, an adjustment factor is introduced as shown in formula (11).

$$a = \frac{n_{invasion}}{n_{all}} \tag{11}$$

Formula (11), it $n_{invasion}$ represents the number of node interaction failures due to attacks, and n_{all} represents the total number of node interaction failures, thereby improving the evaluation method of direct reputation.

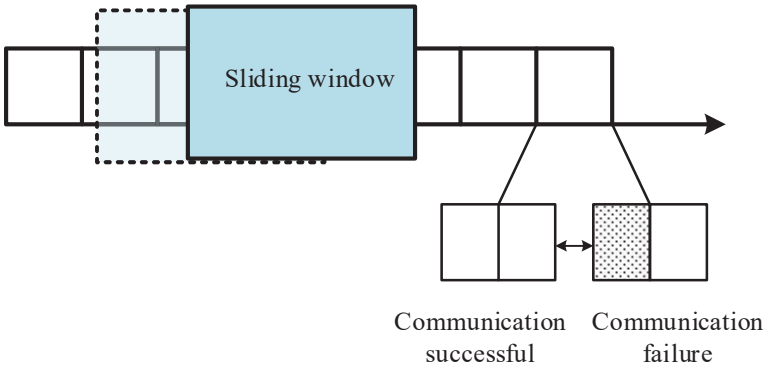

Figure 4 Principle of sliding window method.

The direct reputation degree calculated according to the single-round communication state between nodes cannot reflect the actual reputation of the node, and it is necessary to add the investigation of the historical communication state. For this reason, the window method is used to improve the evaluation of direct reputation, as shown in Figure 4.

Assuming that there are a total p of j interactive rounds, q the i number of interactions in each round is k

$$\begin{cases} \eta_k(i,j) = \sum_{h=k-p+1}^{k} (\varphi_h \cdot \eta_h(i,j)) \\ \iota_k(i,j) = \sum_{h=k-p+1}^{k} (\varphi_h \cdot \iota_h(i,j)) \end{cases} \tag{12}$$

Formula (12), it $\eta_k(i,j)$ represents the number of successful communications between the $\iota_k(i,j)$ nodes i in j the first k round, the number of times of communication failures between the φ_h nodes in i the first k round, and j the weight of the total amount of data transmission in the round. In addition, malicious nodes may adopt delayed attack methods to obtain higher reputation points in the early stage, thereby evading the detection of the system, which needs to improve the difficulty of obtaining reputation. Therefore h, $Dt_h(i,j)$ the weight is defined as $\varphi_h = 1 - Dt_h(i,j)$: Reputation points. The improved direct reputation score calculation is shown in formula (13).

$$Dt(i,j) = \frac{\eta_{ij}^k + 1}{\eta_{ij}^k + \iota_{ij}^k + 2} \tag{13}$$

In order to avoid the joint misleading of reputation evaluation by malicious nodes, the indirect reputation score needs to be calculated by the adjacent nodes shared by the nodes, and its calculation is shown in formula (14).

$$\begin{cases} It(i,j) = \sum_{k=1}^{s} \varphi_k \cdot Rt_k(i,j) \\ Rt_k(i,j) = Dt(i,k) \times Dt(k,j) \\ \varphi_{k=} \dfrac{Dt(i,k)}{\sum_{k=1}^{s} Dt(i,k)} \end{cases} \tag{14}$$

Formula (14), s represents the number of adjacent nodes in common, $Rt_k(i,j)$ represents the node – k to-node j recommendation reputation score, φ_k represents k the weight of the node's recommended reputation score, $Dt(i,k)$ represents the node – i to-node k direct reputation score, and (k,j) represents the node – k to-node j direct reputation score. After obtaining the direct credit score and indirect credit score, the comprehensive credit score can be calculated. In order to avoid excessive calculation, the credibility of the direct credit score is first evaluated. The confidence coefficient of the direct reputation score in the confidence λ interval is set as, and its calculation is $(Dt(i,j) - \sigma, Dt(i,j) + \sigma)$ shown in formula (15).

$$\lambda = \frac{\int_{Dt(i,j)-\sigma}^{Dt(i,j)+\sigma} \omega^{\eta_{ij}^{-1}(1-\omega)^{\iota_{ij}^{-1}}} d\omega}{\int_{0}^{1} \omega^{\eta_{ij}^{-1}(1-\omega)^{\iota_{ij}^{-1}}} d\omega} \tag{15}$$

Confidence coefficient threshold is set as λ', if $\lambda > \lambda'$, the direct credit score can be equivalent to the comprehensive credit score; if $\lambda < \lambda'$, the indirect credit score is calculated, and the comprehensive credit score is calculated according to the weighted value ϕ, as $Ct(i,j)$ shown in formula (16).

$$Ct(i,j) = \rho = Dt(i,j) \cdot \phi + It(i,j) \cdot (1 - \phi) \tag{16}$$

The final credit score calculation process is shown in Figure 5.

The above reputation evaluation mechanism is introduced into the initial stage and the clustering stage of the WSN routing protocol. In the initial stage, each node evaluates its reputation according to the interaction behavior of adjacent nodes, and transmits the information to the base station node, from which the base station obtains the reputation of all nodes and builds a

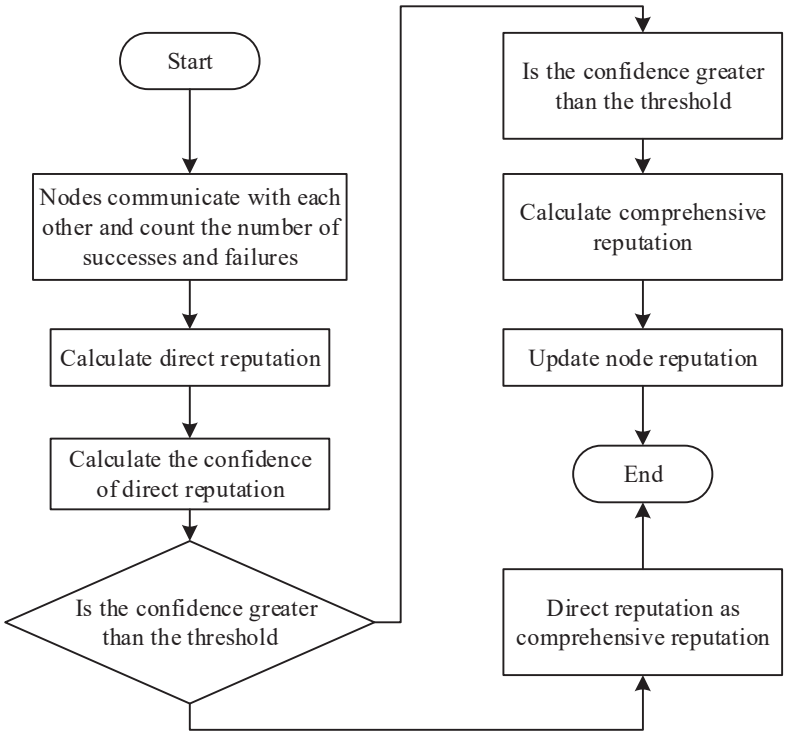

Figure 5 Flow chart of reputation calculation.

complete reputation network. At this stage, the reputation evaluation mechanism mainly compares the reputation score of each node with the reputation threshold (0.5), realizes the preliminary identification and exclusion of a small number of malicious nodes, and broadcasts the malicious node id through the base station, so that the data is only in the remaining normal transfer between nodes. In the clustering stage, it is mainly divided into two parts: cluster head selection and inter-cluster transmission, reputation evaluation and corresponding malicious node detection. On the one hand, the reputation score is used as a part of the GA fitness function, so as to integrate the reputation evaluation mechanism in the cluster head selection stage, and the fitness calculation at this time is shown in formula (17).

$$F = \alpha f_1 + \beta f_2 + \gamma f_3 + \lambda \cdot Ct \tag{17}$$

In formula (17), α, β, γ, λ represent weight coefficients. On the other hand, the reputation score is used as an additional weight for the selection of

alternate path nodes, so as to integrate the reputation evaluation mechanism in the inter-cluster transmission stage, reducing the probability of data transmission to malicious nodes. From this, the new standby path node selection criterion is obtained as shown in formula (18).

$$f(CH_i) = \alpha_1 \frac{E_{CH_i}}{E'} + \alpha_2 \left(1 - \frac{M_{CH_i}}{\sum_{h=1}^{H} M_{CH_i}}\right) + \alpha_3 \frac{d(CH_j, BS)^2}{d(CH_j, CH_i)^2 + d(CH_j, BS)^2} + \alpha_4 \cdot Ct \quad (18)$$

4 Performance Analysis of WSN Intrusion Detection Method Using Reputation Evaluation Mechanism

4.1 WSN Routing Protocol Simulation Analysis

The superiority of the performance of the LEACH multi-layer routing protocol improved by GA (GA-LEACH), it is compared with traditional LEACH, improved LEACH based on K_means (K-LEACH) and improved LEACH with angular clustering (C-LEACH) protocol for simulation comparison. The simulation platform is as follows, CPU: Intel ® CoreTMi7-8750H, 2.2GHz CPU frequency, Windows10 operating system. Python 3.9 is easy to operate and can focus on solving problems; It can be compatible with many platforms to avoid incompatibility when encountering other languages; Its standard library is very large and can handle various tasks, so Python 3.9 is selected as the simulation program. The simulation environment is Python 3.9, the simulation scene is a 100 m $\times$ 100 m WSN, 100 sensor nodes are randomly deployed in the scene, the base station node is located at (50, 50), the initial energy of the node is 1J, and the energy consumption of the transceiver unit is 50 nJ/b, is 10 pJ/b/m^2, the data packet is 1000 bit, and the population size is 20, which are 0.4, 0.4, and 0.2, respectively, the crossover rate is 0.7, and the mutation rate is 0.01. Figure 6 shows the variation of the network residual energy of each protocol.

As can be seen from Figure 6, the LEACH protocol has the fastest network energy consumption, which is exhausted within the iteration round of 600; while the GA-LEACH protocol has the slowest network energy consumption, which is exhausted when the iteration round is about 1800. The network energy consumption of the K-LEACH and C-LEACH protocols is slower than that of LEACH to varying degrees, but still significantly faster

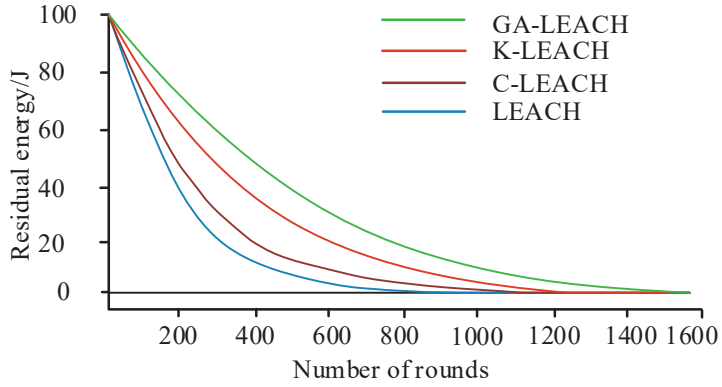

Figure 6 Network residual energy change.

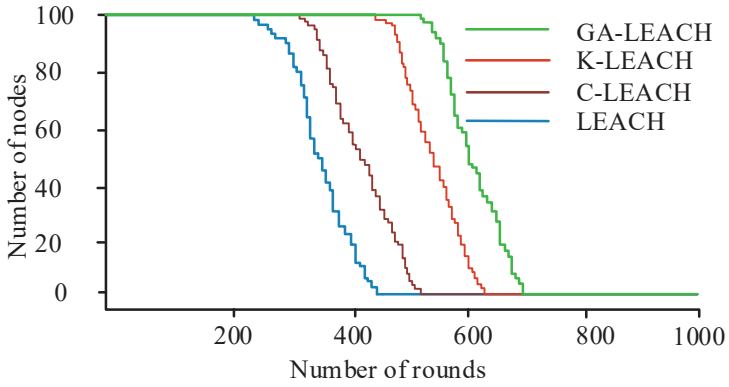

Figure 7 Changes in the number of surviving nodes.

than that of GA-LEACH. Therefore, in the same network operating environment, the network energy consumption speed of GA-LEACH protocol is the slowest, the remaining energy is significantly higher than that of LEACH, K-LEACH and C-LEACH protocols, and the energy saving effect is much higher than that of the traditional LEACH protocol before the improvement. promote. And the change of the number of network surviving nodes of each protocol is shown in Figure 7.

From Figure 7 that the number of surviving nodes in the network of the LEACH protocol starts to decrease significantly when the iteration is about 220 rounds, and all nodes die when the iteration is about 480 rounds; while the network surviving nodes of the GA-LEACH protocol are in the iteration about 510 rounds. Compared with the LEACH before the improvement, the

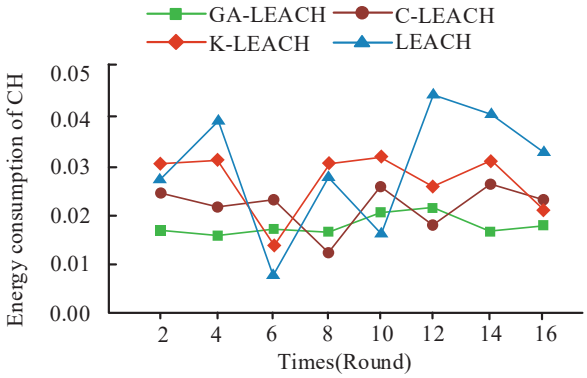

Figure 8 Energy consumption of cluster head.

network node survival time of the GA-LEACH protocol increased by 40.12%; the nodes of the K-LEACH and C-LEACH protocols survived Compared with LEACH, the situation has improved to a certain extent, but there is a certain gap compared with GA-LEACH. Therefore, when a certain iteration round is reached, the number of surviving nodes in the network of each protocol has a significant downward trend, and the decline time point of the GA-LEACH protocol is significantly later than that of the LEACH, K-LEACH and C-LEACH protocols, and in the number of surviving nodes in the whole iterative process is more than that of LEACH, K-LEACH and C-LEACH protocols. Figure 8 shows the energy consumption of the cluster head in a single round in the network of each protocol.

It can be seen from Figure 8 that the energy consumption of the cluster head of the GA-LEACH protocol is the lowest overall, and the fluctuation is small, and the trend is stable; while the energy consumption of the cluster head of the LEACH protocol is obviously high and extremely unstable; the K-LEACH and C-LEACH protocols Compared with LEACH, the energy consumption of the cluster head of GA-LEACH has a certain improvement, but the improvement effect has a certain gap compared with GA-LEACH. It can be seen that the performance of the GA-LEACH protocol is better than that of the LEACH, K-LEACH and C-LEACH protocols in terms of the remaining energy of the network, the number of surviving nodes in the network, and the energy consumption of the cluster head, and it is greatly improved compared with the previous ones. Therefore, the use of GA-LEACH protocol WSN can achieve high-efficiency and energy-saving information transmission, and also provides good conditions for the effective operation of the intrusion detection system.

4.2 Performance Analysis of Node Reputation Evaluation Security Mechanism

In order to verify the performance of the malicious node detection method based on reputation evaluation mechanism (REM-MD), it is compared with the reputation threshold model (BRSN) and the routing protocol without the reputation evaluation mechanism (Original) in the simulation environment. The influence of network performance indicators under each method is investigated when the number of intrusion nodes increases. The main indicators include network throughput, network life cycle and network routing overhead. Figure 9 shows the change of network throughput of WSN using each method when malicious nodes increase.

It can be found in Figure 9 that when the malicious node is 0, the network throughput of each method is relatively high, and the gap is small, and as the number of malicious nodes gradually increases, the network throughput of each method gradually decreases. The downward trend of Original is the most obvious, and the downward trend of BRSN is slightly slower than that of Original. When the number of malicious nodes increases to 12, the network throughput of original drops by 31.8%, and the network throughput of BRSN drops by 21.2%. Network throughput dropped slowly, dropping only 6.1% when the number of malicious nodes increased to 12. Figure 10 shows the changes of the network life cycle of WSN under each method when malicious nodes increase.

It can be seen from Figure 10 that when the number of malicious nodes is small, the network lifetime of REM-MD is longer than that of BRSN, but slightly shorter than that of Original. The additional energy consumption generated by the mechanism is related, but the energy consumption is lower

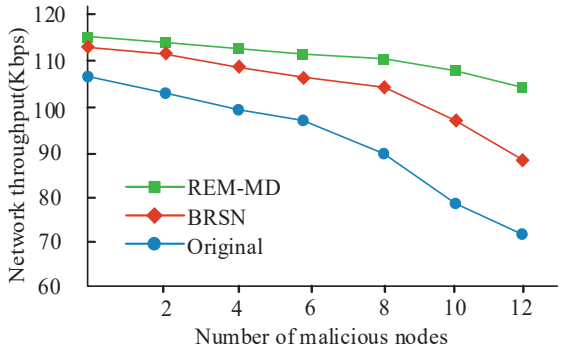

Figure 9 Impact of malicious nodes on network throughput.

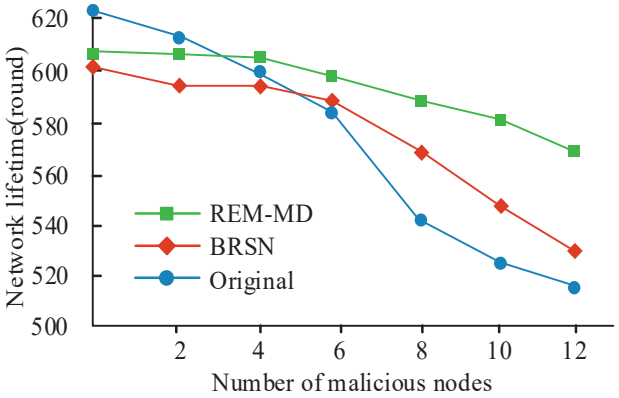

Figure 10 Influence of malicious nodes on network lifetime.

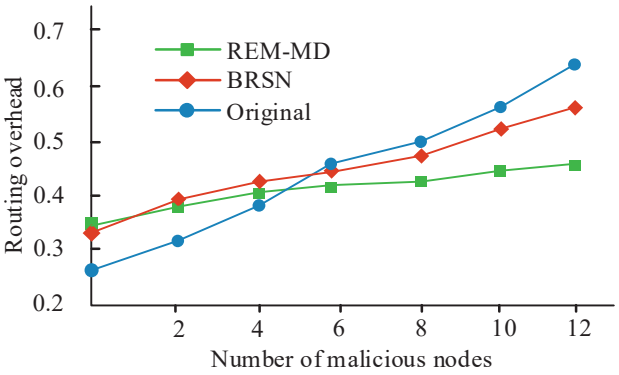

Figure 11 Impact of malicious nodes on routing overhead.

than that of BRSN. With the increase in the number of malicious nodes, the network life cycle under each method is shortened to varying degrees. Among them, the shortening trend of Original and BRSN is more obvious. When the number of malicious nodes increases to 12, it shortens by 16.7% and 11.8% respectively. %, the network lifetime of REM-MD was shortened by only 6.8%. Figure 11 shows the change of routing overhead of WSN of each method when malicious nodes increase.

According to Figure 11, when the number of malicious nodes is low, the routing overheads of REM-MD and BRSN are similar, and both are slightly higher than Original, which is related to the additional communication overhead generated by the malicious node detection mechanism. When the number of malicious nodes gradually increases, the routing overhead of

original increases significantly and exceeds that of REM-MD and BRSN. The routing overhead of BRSN also increases more significantly than that of REM-MD. However, the routing overhead of REM-MD increases the slowest, and with the increase of the number of malicious nodes, the effect of REM-MD to save overhead becomes more and more obvious. To sum up, the performance of WSN using REM-MD is better than that of Original and BRSN in terms of network throughput, network life cycle and routing overhead, and can effectively resist the impact of malicious node attacks on WSN.

5 Conclusion

With the development and popularization of wireless communication technology and IoT, the application of WSN has become more and more extensive, and the security defense problems exposed by it is limited by the existing technology and operating environment, which has also attracted the attention of a large number of scholars. Due to the insufficiency of traditional network security defense methods and malicious node detection methods, it is imminent to propose a new effective defense method for WSN. In order to realize the efficient and energy-saving malicious node detection, the existing LEACH routing protocol is optimized by using the GA algorithm, and then a WSN node reputation evaluation mechanism is proposed, which is integrated into the preparation and clustering stages of the improved protocol. Therefore, by calculating the direct reputation and indirect reputation, the comprehensive reputation score of the node is obtained, the credibility of the node is judged, and the malicious node with low reputation score is eliminated. In the simulation experiment, the effect of the improved protocol is first verified. The results show that the energy saving effect of GA-LEACH is obvious, which provides a good foundation for the reputation evaluation mechanism. In the performance simulation verification of the reputation evaluation mechanism, the negative impact of malicious nodes on the network throughput, network life cycle and routing overhead of the WSN with the reputation evaluation mechanism is significantly suppressed, and the effect is better than the reputation threshold model and the reputation evaluation without adding the reputation evaluation mechanism. The routing protocol of the mechanism has been significantly improved. Therefore, the malicious node intrusion detection method proposed in this study can effectively resist the network internal attacks of malicious nodes, and malicious node detection methods for more attack methods need to be further explored.

Fundings

The research is supported by: Characteristic innovation projects (NATURAL SCIENCES) of Guangdong Provincial Department of education in 2017: Mobile cloud storage security research and application (fund No. 2017ktscx205); Higher education teaching reform project of Guangdong Provincial Department of education in 2018: Promoting the connotation construction and development of computer specialty with professional evaluation and professional certification as the starting point (fund No. 661).

References

[1] Eugene S, Thanassis T, Wendy H. Analytics for the Internet of Things: A Survey. ACM Computing Surveys, 2018, 51(4):1–36.

[2] Maxim C, Sherali Z, Zubair B, et al. Internet of Things Forensics: The Need, Process Models, and Open Issues. IT Professional, 2018, 20(3):40–49.

[3] Tai WL, Chang YF, Hou PL. Security Analysis of a Three-factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments. International Journal of Network Security, 2019, 21(6):1014–1020.

[4] Hajiheidari S, Wakil K, Badri M, et al. Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks, 2019, 160(SEP.4):165–191.

[5] Souissi I, Ben Azzouna N, Ben Said L. A Multi-Level Study of Information Trust Models in WSN-assisted IoT. Computer Networks, 2019, 151(MAR.14):12–30.

[6] Gaber T, Abdelwahab S, Elhoseny M, et al. Trust-based Secure Clustering in WSN-based Intelligent Transportation Systems. Computer Networks, 2018, 146 (DECa9):151–158.

[7] Khan T, Singh K, Le HS, et al. A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks. IEEE Access, 2019, PP(99):1–1.

[8] Nr A, Hgbcd E, Sba F. Improvement of Watermarking-LEACH Algorithm Based on Trust for Wireless Sensor Networks. Procedia Computer Science, 2019, 159(C):803–813.

[9] Goyat R, Kumar G, Alazab M, et al. A secure localization scheme based on trust assessment for WSNs using blockchain technology. Future Generation Computer Systems, 2021(12):221–231.

[10] Liu Y, Lu Y, Sheng L, et al. A Dynamic Behavior Monitoring Game Based Trust Evaluation Scheme for Clustering in Wireless Sensor Networks. IEEE Access, 2018, PP(99):1–1.

[11] Nunoo-Mensah H, Boateng KO, Gadze JD. The adoption of socio- and bio-inspired algorithms for trust models in wireless sensor networks: A survey. International journal of communication systems, 2018, 31(6):e3444.1–e3444.18.

[12] Sajwan M, Gosain D, Sharma AK. CAMP: cluster aided multi-path routing protocol for wireless sensor networks. Wireless Networks, 2019, 25(5):2603–2620.

[13] Anwar RW, Zainal A, Outay F, et al. BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks. Future generation computer systems, 2019, 96(JUL.):605–616.

[14] Liu C, Li X. Fast, Resource-Saving, and Anti-Collaborative Attack Trust Computing Scheme Based on Cross-Validation for Clustered Wireless Sensor Networks. Sensors (Basel, Switzerland), 2020, 20(6):1–25.

[15] Lv Y, Liu K, Zhang D, et al. A Secure Routing Protocol Based on Reputation Mechanism. International Journal of Network Security, 2018, 20(5):862–871.

[16] Jiang J, Zhu X, Han G, et al. A Dynamic Trust Evaluation and Update Mechanism based on C4.5 Decision Tree in Underwater Wireless Sensor Networks. IEEE Transactions on Vehicular Technology, 2020, PP(99):1–1.

[17] Cheour R, Jmal MW, Abid M. New combined method for low energy consumption in Wireless Sensor Network applications. Simulation, 2018, 94(10):873–885.

[18] Gong DW, Jing S, Miao Z. A Set-Based Genetic Algorithm for Interval Many-Objective Optimization Problems. IEEE Transactions on Evolutionary Computation, 2018, 22(99):47–60.

[19] Sun, Zhang, Zheng, et al. Multi-Sensor Data Fusion Algorithm Based on Trust Degree and Improved Genetics. Sensors, 2019, 19(9):1–25.

[20] Yamazaki S, Ohuchi K. Performance Analysis of Total Power Consumption in Linear Multi-hop Networks. Wireless Personal Communications: An International Journal, 2018, 100(8):337–349.

[21] Hu C, Fan W, Du JX, et al. A novel statistical approach for clustering positive data based on finite inverted Beta-Liouville mixture models. Neurocomputing, 2019, 333(MAR.14):110–123.

Biography

Junlin Zhang obtained his master's degree in engineering from South China Agricultural University (2004). At present, he is working as an associate professor in the School of Information Technology of Guangdong Technology College. He is also a member of the Professional Committee of Teaching Quality Management of Guangdong Private Higher Education Institutions. He has published articles in more than 10 well-known peer-reviewed journals and conference minutes. His areas of interest include computer network security, Internet of Things technology, software technology and higher education management.