Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Secure routing protocol based on dynamic reputation and load balancing in wireless mesh networks

Xiaogang Yuan* and Yipiao Chen

Abstract

Aiming at the characteristics of dynamic topology change and vulnerability of wireless mesh networks (WMN), a secure routing protocol based on dynamic reputation and load balance (SRP-DRLB) is proposed to improve the routing security and load balance. By dynamically predicting of the reputation and traffic of the node in WMN, SRP-DRLB adopts edge weight strategy and node load idleness to avoid the competitive access of a large number of data packets to nodes with high reputation. SRP-DRLB dynamically adjusts routes according to the real-time status of network nodes' reputation and traffic, reducing the impact of malicious nodes on the network and the overload of high-reputation nodes, thus improving the identification rate of malicious nodes and node load balancing. Simulation results show that SRP-DRLB can effectively ensure the security of data transmission, and it has the advantages of improving the identification rate of malicious nodes, the success rate of packet transmission and avoiding network congestion.

Keywords: Wireless mesh networks, Secure routing, Reputation mechanism, Load balancing, Dynamic prediction

Introduction

WMN has become a widely used wideband multi-hop wireless network structure. Due to its advantages of low cost, fast networking, self-organization, high bandwidth, good compatibility and scalability, it is widely used in vehicle-mounted wireless monitoring, video conferencing, real-time management of road conditions, medical treatment and rescue in disaster areas, military communication, tactical command network and many other fields [1, 2].

Because of its multi-hop mode in information transmission and open wireless medium, WMN is more likely to be regarded as a target by network attackers. Because internal malicious nodes can be disguised by legitimate authorization, the traditional routing mechanism cannot accurately identify them in the routing process, resulting in a large amount of information destroyed in the routing process. Therefore, how to effectively identify malicious nodes and construct secure routing paths in the routing process has become a hot topic in the research of WMN secure routing mechanism. The security of routing protocol is closely related to the trust relationship between nodes. The trust relationship between nodes can describe and learn the behavior of nodes, enhance the security cooperation between nodes, and construct efficient and robust security routes. To improve the security of WMN, reputation-based schemes that predict the future behavior of nodes and identify suspicious nodes based on their past observations have been shown to be more resistant to attacks from internal nodes. However, the traditional trust-aware routing protocol has some limitations, mainly reflected in the calculation of node trust value is not accurate, and the cost of routing, transmission delay is large, which makes it difficult to ensure the security of multi-hop information transmission and load balance [3–5].

*Correspondence: xiaogang061218@163.com

School of Cyber Security, Gansu University of Political Science and Law, Lanzhou 730070, China

Using conventional trust mechanisms in [6] H. Lin et al. have proposed a secure routing protocol CR-HWMP (Hybrid Wireless Mesh Protocol based on Cross-layer Reputation Mechanism) based on cross-layer dynamic reputation mechanism that can realize privacy protection. It can resist internal attacks such as black hole and gray hole, realize privacy protection of user information, and improve the reliability and security of the network. A. Beheshtiasl et al.in [7] used fuzzy logic to obtain the reputation of routes, and a new algorithm is proposed to determine the optimal path with minimum error on the basis of reputation and security. H. Yang et al. in [8] have proposed a WMN secure routing mechanism SRMDR (Secure Routing Mechanism based on Dynamic Reputation) based on dynamic reputation. SRMDR integrates the historical comprehensive reputation of nodes and the current comprehensive reputation to calculate the dynamic reputation of nodes, determines the nodes whose dynamic reputation is less than the threshold as malicious nodes, and then establishes the secure routing path by combining the dynamic reputation mechanism and the routing mechanism. C. Wang et al. in [9] have proposed a wireless network reputation-aware secure routing method based on an improved genetic algorithm. With the goal of maximizing comprehensive reputation, minimizing network energy consumption and balancing load, the corresponding fitness function is constructed, so as to find the best routing path and achieve the goal of ensuring network security and balancing network load. The above secure routing protocols have many advantages, but also face the following disadvantages: (1) When routing protocols calculate the comprehensive reputation of routing nodes, the weighting coefficient of direct reputation and indirect reputation is set subjectively, so the comprehensive reputation of nodes may not be accurate enough. (2) The dynamic reputation of nodes is obtained by adding the current reputation and historical reputation of nodes, which makes the evaluation of the reputation of routing nodes lack of timeliness and dynamics. (3) A few nodes with high reputation are more heavily loaded than other nodes, which is prone to congestion, resulting in packet loss, increased end-to-end delay, and affected network performance.

The results of research in [10–13] show that the vertical prediction analysis of node reputation considering direct reputation, indirect reputation and historical reputation can improve the accuracy of reputation evaluation model. WMN node traffic has self-similar characteristics and can be used for traffic modeling and prediction, which is conducive to the realization of load balancing. Therefore, a secure routing protocol SRP-DRLB based on dynamic reputation and load balancing is proposed in this paper, which effectively improves the security and load balancing performance of WMN routing. The novelty and main contributions of this research includes:

(1) The Chebyshev neural network is used to dynamically predict the comprehensive reputation and traffic of the nodes, and the entropy weight method is used to fuse the direct trust value and the indirect trust value to calculate the comprehensive trust value, which improves the accuracy of the node trust evaluation model and node load.
(2) A new routing regulation factor, node security dynamic fitness, which is based on node dynamic trust and reputation and node load balancing, is designed to dynamically adjust the routing according to the real-time network situation.
(3) A secure routing mechanism SRP-DRLB is proposed based on edge weight, node reputation and load balance, which can dynamically select the forwarding path according to the edge weight, node trust value and load. Compared with the existing methods, this method can effectively alleviate network congestion and improve network efficiency while improving network security, and has high practical value.

Node security fitness

The resources of WMN nodes are limited. If there is a large demand for information processing in a short period of time or intrusion behaviors such as denial of service attacks, the load on nodes will increase rapidly, which will affect the routing of the entire network. In this paper, node security fitness is proposed by combining node comprehensive reputation with load, which can not only improve the security of network data transmission, but also avoid the transmission performance affected by high load on nodes with high reputation.

Reputation model

According to the complexity and variability of application environments, attack behavior and other factors of WMN, this paper uses the information entropy method to fuse the direct reputation and indirect reputation of nodes to form the comprehensive reputation degree, and improves the accuracy of the reputation evaluation model to judge the reputation degree of nodes.

Direct reputation

The direct reputation $DirR_{t:i\rightarrow j}$ represents the direct evaluation of node i on the reputation of node j at the current moment t. During the routing process, the data

packets sent by the node are transmitted to the neighbor node j by node i. Node i monitors the forwarding situation of node j while transmitting data packets. According to the monitoring results, the direct reputation of node j is calculated as $DirR_{t:i\to j}$ [8, 14]:

$$DirR_{t:i\to j} = Dirb_{t:i\to j} + 0.5 \times Diru_{t:i\to j} \tag{1}$$

$$Dirb_{t:i\to j} = \frac{s_{t:i\to j}}{(s_{t:i\to j} + f_{t:i\to j})L_{t:i\to j}} \tag{2}$$

$$Dird_{t:i\to j} = \frac{f_{t:i\to j}}{(s_{t:i\to j} + f_{t:i\to j})L_{t:i\to j}} \tag{3}$$

$$Diru_{t:i\to j} = 1 - Dirb_{t:i\to j} - Dird_{t:i\to j} \tag{4}$$

where, $s_{t:i\to j}$ is the number of successfully forwarded packets received by node j from node i, $f_{t:i\to j}$ is the number of discarded packets received by node j from node i, and $L_{t:i\to j}$ is the link quality of the wireless link between node i and node j.

$$L_{t:i\to j} = q_{t:i\to j} \cdot q_{t:i\to j} \tag{5}$$

$$q_t = \frac{k_{t:s}}{k_{t:e}} \tag{6}$$

where, $q_{t:j\to i}$ is the forward transmission rate of the wireless link between node i and node j, $q_{t:j\to i}$ is the reverse transmission rate of the wireless link between node i and node j, $k_{t:e}$ is the total number of data packets sent by the sending nodes at both ends of the wireless link in a transmission process, and $k_{t:s}$ is the total number of data packets received by the receiving nodes at both ends of a wireless link during a transmission.

Indirect reputation

When node i does not have enough historical interaction data to evaluate node j, node i initiates the indirect reputation calculation process to its neighbors. The trusted public neighbors of node i and node j are defined as $u_n = [u_1, u_2, u_3, \cdots, u_N]$, N is the number of trusted public nodes, and the indirect reputation of node i to node j is calculated from the direct reputation provided by their public neighbors as shown in Fig. 1. In the set of all public neighbor nodes, if the direct reputation of node i to node u_n is less than the threshold value, node u_n will be deleted from the public neighbor node. The value of the threshold in this paper is set as 0.6 [8, 15].

The higher the reputation of the trusted public node u_n is, the greater the proportion value of the recommendation opinion of node u_n in the final indirect reputation is. The corresponding weighting factor $W_{t:u_n}$ is as follows:

$$W_{t:u_n} = DirR_{t:i\to u_n} \Big/ \sum_{n=1}^{N} \left(DirR_{t:i\to u_n}\right) \tag{7}$$

where, $DirR_{t:i\to u_n}$ is the direct reputation of node i to node u_n.

The indirect reputation of node i to node j is as follows:

$$IndR_{t:i\to j} = \sum_{n=1}^{N} \left(W_{t:u_n} \cdot DirR_{t:u_n\to j}\right) = \frac{\sum_{n=1}^{N} \left(DirR_{t:i\to u_n} \times DirR_{t:u_n\to j}\right)}{\sum_{n=1}^{N} \left(DirR_{t:i\to u_n}\right)} \tag{8}$$

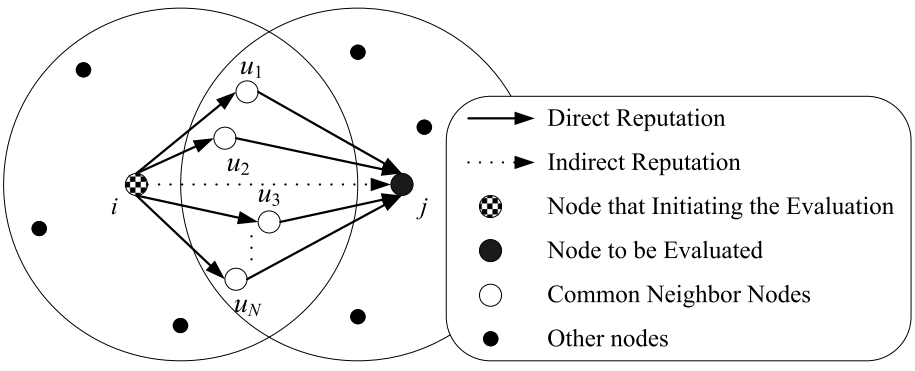

Fig. 1 Calculation of indirect reputation of node i to node j

where, $DirR_{t:u_n \to j}$ is the direct reputation of node u_n to node j.

Comprehensive reputation

Comprehensive reputation $ComR_{t:i \to j}$ refers to the comprehensive evaluation of the reputation of node j obtained from node i through direct and indirect means. This value is weighted and summed by direct and indirect reputation respectively, as shown in Eq. (9).

$$ComR_{t:i \to j} = \omega_{t:i \to j}^{Dir} \times DirR_{t:i \to j} + \omega_{t:i \to j}^{Ind} \times IndR_{t:i \to j} \tag{9}$$

where, $\omega_{t:i \to j}^{Dir}$ is the adaptive weight of direct reputation, and $\omega_{t:i \to j}^{Ind}$ is the adaptive weight of indirect reputation.

The proportion of direct reputation and indirect reputation in comprehensive reputation is different. In order to overcome the deficiency of subjective weight allocation and improve the accuracy of reputation evaluation, this paper uses information entropy to determine the weight of these two reputation degrees in the comprehensive reputation degree [16, 17].

$$\omega_{t:i \to j}^{Dir} = \frac{1 - \frac{H(DirR_{t:i \to j})}{\log_2 DirR_{t:i \to j}}}{\left[1 - \frac{H(DirR_{t:i \to j})}{\log_2 DirR_{t:i \to j}}\right] + \left[1 - \frac{H(IndR_{t:i \to j})}{\log_2 IndR_{t:i \to j}}\right]} \tag{10}$$

$$\omega_{t:i \to j}^{ind} = \frac{1 - \frac{H(IndR_{t:i \to j})}{\log_2 IndR_{t:i \to j}}}{\left[1 - \frac{H(DirR_{t:i \to j})}{\log_2 DirR_{t:i \to j}}\right] + \left[1 - \frac{H(IndR_{t:i \to j})}{\log_2 IndR_{t:i \to j}}\right]} \tag{11}$$

where, $H(DirR_{t:i \to j})$ is the information entropy of direct reputation, and $H(IndR_{t:i \to j})$ is the information entropy of indirect reputation. $H(DirR_{t:i \to j})$ reflects the average uncertainty of the reputation of node i to node j when the direct reputation degree of node i to node j is $DirR_{t:i \to j}$. $H(IndR_{t:i \to j})$ reflects the average uncertainty of the reputation of node i to node j when the indirect reputation degree of node i to node j is $IndR_{t:i \to j}$.

$$H(DirR_{t:i \to j}) = -DirR_{t:i \to j} \log_2 DirR_{t:i \to j} - (1 - DirR_{t:i \to j}) \log_2 (1 - DirR_{t:i \to j}) \tag{12}$$

$$H(IndR_{t:i \to j}) = -IndR_{t:i \to j} \log_2 IndR_{t:i \to j} - (1 - IndR_{t:i \to j}) \log_2 (1 - IndR_{t:i \to j}) \tag{13}$$

Idle degree of the load

Due to the limited resources of WMN nodes, packet loss is easy to occur, which affects the normal communication and even threatens security of the network. Therefore, a routing algorithm that is aware of node load is required to avoid high load on the node. This paper designs the idle degree of the node load $C_{t:j}$ to measure the load status of network nodes based on the traffic of the node. If there are multiple routes to the send the packet, the node adjusts the forwarding route according to the idle degree of the load on its neighbor nodes to prevent the normal forwarding work due to the heavy load on some nodes in the network [18, 19].

$$C_{t:j} = \begin{cases} 1 & 0 \le P_{t:j} < P_{j\min} \\ \frac{P_{j\max} - P_{t:j}}{P_{j\max} - P_{j\min}} & P_{j\min} \le P_{t:j} \le P_{j\max} \\ 0 & P_{j\max} \le P_{t:j} \end{cases} \tag{14}$$

where, $P_{t:j}$ is the current traffic of node j at time t, $P_{j\max}$ is the upper limit threshold of traffic of node j, and $P_{j\min}$ is the lower limit threshold of traffic of node j. When the value of $P_{t:j}$ is lower than the lower threshold, the idle degree of the load $C_{t:j} = 1$ indicates that the current resources of the node are sufficient and there is no need to adjust routes based on the load. When $P_{t:j}$ is between the upper threshold and lower threshold, the value of idle degree of the load $C_{t:j}$ is between 0 and 1. When $P_{t:j}$ is greater than the upper threshold, idle degree of the load $C_{t:j} = 0$, and the nodes and network links will become congested if the load on nodes continues to increase.

Security fitness model

According to the comprehensive reputation and the idle degree of the load on the node, the security fitness $F_{t:i \to j}$ of the node is calculated as follows:

$$F_{t:i \to j} = ComR_{t:i \to j} \cdot C_{t:j} \tag{15}$$

The security fitness of the node includes the comprehensive reputation and load, which can be used as the basis of route selection to avoid the situation that nodes with high reputation are accessed by a large number of packets. The higher the security fitness value of a node is, the higher the priority of the node is when selecting a route [20, 21].

Dynamic fitness of node basedon prediction of reputation and traffic

reputation and traffic of the node in WMN is predictable. Chebyshev neural network is a kind of neural network based on Chebyshev orthogonal polynomials, which has excellent approximation performance. The orthogonality of basis functions ensures that the neural network can solve the weights at the nodes of polynomials quickly,

which can better meet the demand of prediction of the reputation and traffic of the node in WMN.

Rrediction of reputation and traffic based on Chebyshev neural network

Chebyshev neural network consists of an input layer, a hidden layer and an output layer. The excitation function of its hidden neurons is Chebyshev orthogonal polynomial [22]. The network operation is shown in Fig. 2. Input layer is $x = (x_1, x_2, \cdots, x_n)^T$. The hidden layers is $H_k = T_k(x_k)$, and $T_k(x) = \cos(k \arccos x)$ are Chebyshev polynomials of the first kind. The output layer is $y = (y_1, y_2, \cdots, y_n)^T$, and $y_i = \sum_{k=1}^{K} \omega_k T_k(x_i)$. The gradient descent method is used to modify the weights of the network training.

The prediction of comprehensive reputation and traffic of WMN nodes takes the current comprehensive reputation $ComR_{t:i\to j}$ and traffic $P_{t:j}$ as the input of Chebyshev neural network, and the output of the network is the predicted value of comprehensive reputation $ComR^{pre}_{t+1:i\to j}$ and traffic $P^{pre}_{t+1:j}$ at the next time.

$$ComR^{pre}_{t+1:i\to j} = \sum_{n=1}^{N} \omega_n T_n(ComR_{t:i\to j}) \tag{16}$$

$$P^{pre}_{t+1:i\to j} = \sum_{m=1}^{M} \omega_m T_m(P_{t:i\to j}) \tag{17}$$

Dynamic security fitness of nodes

According to the predicted value of comprehensive reputation $ComR^{pre}_{t+1:i\to j}$ and traffic $P^{pre}_{t+1:j}$ at the next time, the predicted value of security fitness $F^{pre}_{t+1:i\to j}$ of node j at the next time is as follows:

$$F^{pre}_{t+1:i\to j} = ComR^{pre}_{t+1:i\to j} \cdot C_{t+1:j} \tag{18}$$

The dynamic security fitness of node j $DynF_{t:i\to j}$ is as follows:

$$DynF_{t:i\to j} = \gamma F_{t:i\to j} + (1-\gamma) F^{pre}_{t+1:i\to j} \tag{19}$$

where, γ is the weight factor used to distinguish the node security fitness at the current time and the predicted value of node security fitness at the next time. γ needs to meet the requirements of $0 < \gamma < 1$, and $\gamma = 0.5$ is used in this paper.

Secure routing mechanism based on edge weight anddynamic security fitness of the node

The shortest path routing policy causes the central node with a large degree and multiple shortest paths to be accessed by a large number of packets, which easily causes the congestion of the network [23, 24]. In this paper, the static characteristics and dynamic characteristics of WMN are integrated, and the security routing mechanism is adopted to select forwarding paths according to the edge weights and dynamic security fitness of nodes in the network, which can improve the security of the network while reducing the congestion of the network and improving efficiency of the network.

Determination of optimalpath based on edge weight

The routing strategy based on edge weight assigns weight to the edges connected by the "central node" to reduce the probability of these edges being accessed. This method can effectively reduce the congestion of the network and improve the Efficiency of transmission. The selection of the optimal path is determined by the following equation [25]:

$$Q[P(i\to r):\alpha,\beta] = \min \sum_{s=i}^{r-1} \left\{\min[(1-DynF_{t:s\to s+1}),(1-DynF_{t:s+1\to s+2})]\right\}^{\alpha} \cdot \left\{\max[(1-DynF_{t:s\to s+1}),(1-DynF_{t:s+1\to s+2})]\right\}^{\beta} \tag{20}$$

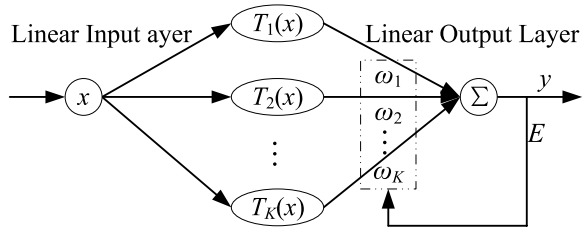

Fig. 2 Single-input Chebyshev neural network model

where, node i is the source node of data packets, and node r is the destination node of data packets. x_s and $x_s + 1$ are the two nodes associated with an edge. $k(x_s)$ is the degree value of node x_s. The value range of the adjustable parameters are $0 \le \alpha \le 0.9$ and $0 \le \beta \le 1$, and $\alpha = 0.5$ and $\beta = 0.7$ are adopted in this paper.

Network congestion evaluation index $H(R)$ is as follows:

$$H(R) = \lim_{t\to\infty} \frac{W(t)}{Rt} \tag{21}$$

where, $W(t)$ is the total number of existing packets in the network at time t, and R is the number of newly generated data packets per unit time.

If H is approximately 0, it indicates that packets can be timely digested after entering the network, and there is no congestion in the network. If $H > 0$ is selected, data packets cannot be digested in time and the network is congested. Therefore, there is a critical value R_c. When $R < R_c$, the packet can be digested in time, H is approximately 0, the network is in a stable state, and the network transmission efficiency is high. When $R > R_c$, packets cannot be digested in time, network congestion occurs, the average transmission time increases, and the network transmission efficiency is low.

Establishment of route

Step1: Source node i initiates the establishment process of the route and broadcasts the RREQ (Route Request).

Step2: When any neighbor node j receives RREQ, the next options are as follows: (1) If node j is a malicious node, it will directly agree to be the next-hop forwarding node and return an Accept message to node i, and then go to Step6. (2) If j is a trusted node, it first determines whether its current idle degree fo the load $C_{t:j}$ meets the requirements. If it can't meets the requirements, RREQ will be ignored. If it meets the requirements, and then go to Step3. During route establishment, the idle threshold of the load is set to 0.1.

Step3: Neighbor node j queries the direct reputation $DirR_{t:j\to i}$ of node i from the local reputation database, and the next options are as follows: (1) If $DirR_{t:j\to i}$ exists and $DirR_{t:j\to i}$ is less than the security threshold, node j determines that node i is a malicious node, ignores RREQ, and broadcasts information throughout the network. (2) If $DirR_{t:j\to i}$ is equal to or greater than the security threshold, it is judged that node i is a trusted node, return Accept message to i, and go to step6. (3) If the $DirR_{t:j\to i}$ does not exist, initiate the indirect reputation calculation process and go to Step4. During route establishment, the threshold of node comprehensive reputation is set to 0.6.

Step4: Node j broadcasts a request to its neighbor nodes for information about inquiring about reputation and asks for recommendation information about reputation of node j. After receiving the reputation query information, any common neighbor node m of node i and node j inquires the local reputation database and feeds back the query result to the node. Node i will sort out the recommendation information received from all neighboring nodes, calculate the indirect reputation $IndR_{t:j\to i}$ of node j, and go to Step5.

Step5: According to the calculation result of indirect reputation, node j determines whether node i is a malicious node by performing a comprehensive reputation calculation and the management process of malicious nodes. The next options are as follows: (1) If node i is a malicious node, node j will impose forced isolation on i, ignore RREQ, and record the calculation result of the comprehensive reputation of node i. (2) If node i is a secure node, node j sends an accept message to node i to agree to provide the service, and go to Step6.

Step6: When node i receives the Accept message, node i executes Step4 to judge whether node j is a malicious node and decide whether to accept node j as a forwarding node. The next options are as follows:(1) If node j is judged to be a malicious node, node i will punish node j or force node j to be isolated, ignore RREQ, and record the calculation result of comprehensive reputation of node j; (2) If node j is judged to be a trusted node and node j is accepted as a forwarding node, go to Step7.

Step7: Node j receives the notification that the source node i agrees to act as a forwarding node, generates a new RREQ, and broadcasts the new RREQ in the network to continue the route establishment process.

Step8: Run Step1 to Step7 repeatedly until the route that meets the conditions is found. If there are multiple paths that all meet requirements, perform the following steps to select the optimal path:

(1) Chebyshev neural network is used to predict the comprehensive reputation $ComR^{pre}_{t+1:i\to j}$ and traffic $P^{pre}_{t+1:j}$ of the nodes in the route at the next time.
(2) The dynamic security fitness $DynF_{t:i\to j}$ of each node in all routes is calculated.
(3) According to Eq. (20), the path selection method based on edge weight strategy is used to determine the optimal route.

Maintenance of route

During data transmission, the predicted values of comprehensive reputation $ComR^{pre}_{t+1:i\to j}$ and load idleness of nodes $C_{t+1:j}$ in the path are regularly detected, and the threshold for starting route adjustment is set to 0.6 and 0.05.

(1) All the nodes in the route regularly check their predicted value of the composite reputation and idle degree of the load. If any parameter is lower than the threshold, the node will can't transmit data. The node sends the information about the route maintenance along the path to inform source node i that the path is unreliable and needs to restart the route establishment path.
(2) All the nodes in the route regularly calculate the comprehensive reputation and load idle value of the

last-hop node and next-hop node. If all parameters are greater than the threshold, the transmission of the data continues. If any parameter is smaller than the threshold, the system stops the transmission of the data and sends the information about route maintenance to the source node.

(3) After receiving the route maintenance information, the source node first broadcasts to all nodes to record and isolate the newly discovered malicious nodes, and then initiates the route establishment process again to establish a new secure route path.

Simulation

In order to verify the performance of SRP-DRLB, it was simulated and tested in MATLAB environment, and was compared with CR-HWMP proposed in [6] and SRMDR proposed in [8].

The parameters of the simulation model are set as follows: The scene area is 1000 m × 1000 m. There are 100 nodes, and the communication radius of nodes is 200 m. The number of malicious nodes is 30, and the security threshold of node reputation is 0.6. Malicious nodes can launch wormhole attacks, black hole attacks, selective forwarding and Hell flooding attacks on the network. The data stream generated by the node is a fixed bit stream, the data rate is 11Mbps, and the packet size is 1 KB. There are 20% high-load nodes in the node. The simulation time is 100 s, and the simulation results are the average data obtained through 20 simulations.

Identification rate of malicious nodes

Identification rate of malicious nodes refers to the probability and accuracy of the identification of malicious node. In Fig. 3, the change of malicious node identification rate of the three routing mechanisms over time is compared, and the ability of different routing mechanisms to accurately identify malicious nodes can be analyzed. As can be seen from the simulation results, SRP-DRLB adopts Chebyshev neural network to dynamically predict the comprehensive reputation of nodes, so it can identify malicious nodes faster than SRMDR and CR-HWMP at the initial stage of the experiment. With the increase of time, the identification rate of malicious nodes of the three mechanisms gradually increases, and the final recognition rate is around 90%. Because SRP-DRLB uses information entropy to fuse direct reputation and indirect reputation to obtain comprehensive reputation, the node evaluation has better real-time performance and accuracy. The final identification rate of malicious nodes of SRP-DRLB is slightly higher than that of the other two routes.

False positiverate of malicious nodes

False positive rate of malicious nodes refers to the probability of misdiagnosing a normal node as a malicious node. Figure 4 compares the malicious node false positive rate of the three routes in the presence of malicious node attacks. The malicious node false positive rate of the three routes increases with the increase of the proportion of malicious nodes. Because the SRP-DRLB adopts Chebyshev neural network to dynamically predict the comprehensive reputation of nodes, it can be more accurate and speed up the evaluation of node reputation, make a prospective evaluation of node reliability, and can effectively and accurately identify malicious nodes. According to the simulation results, the false positive rate of malicious nodes of SRP-DRLB is 1% and 3% lower than that of SRMDR and CR-HWMP,

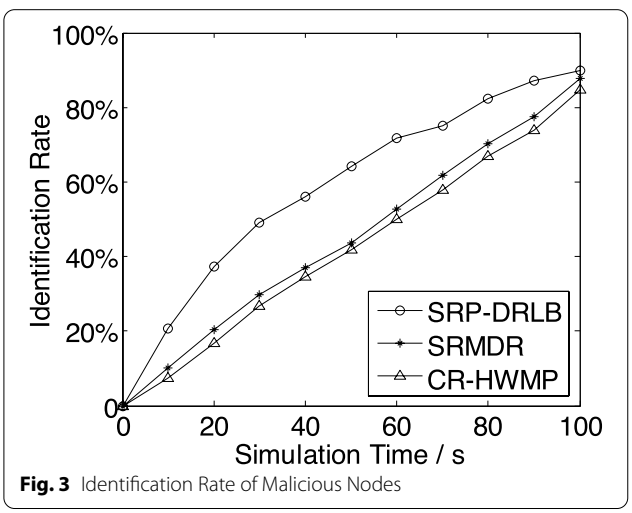

Fig. 3 Identification Rate of Malicious Nodes

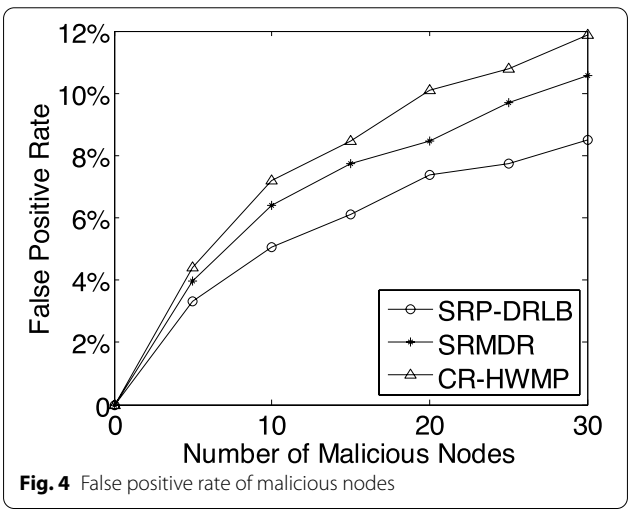

Fig. 4 False positive rate of malicious nodes

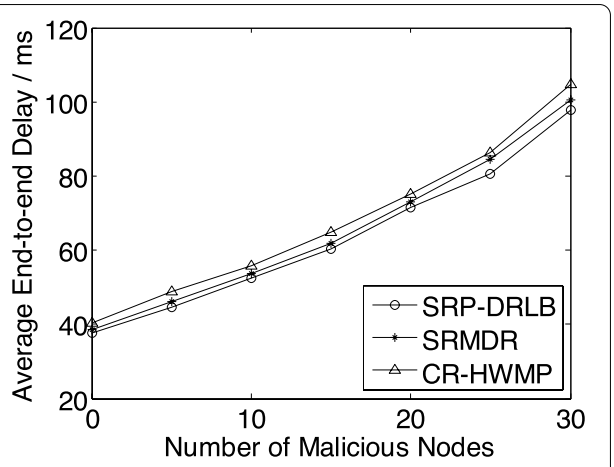

Fig. 5 Average End-to-end Delay

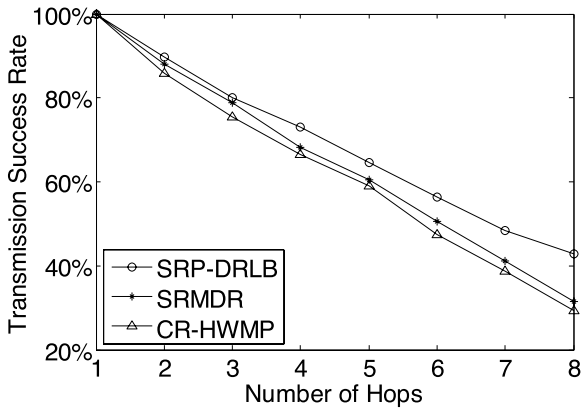

Fig. 7 Transmission success rate when the high-load router reaches 90% load

respectively. SRP-DRLB has the lowest false positive rate of malicious nodes and has certain advantages over the other two routes.

Average end-to-end delay

Average end-to-end delay refers to the average time it takes for a packet to be transmitted from the source node to the destination node. The simulation results in Fig. 5 compare the changes of the average end-to-end delay of the three routing mechanisms with the increase of malicious nodes. The SRP-DRLB and SRMDR mechanisms should have a high identification rate of malicious nodes and a relatively slow increase in average end-to-end delay. Although SRP-DRLB needs to predict nodes and traffic and calculate node security fitness, the computation overhead increases, but SRP-DRLB can choose more secure and load-balanced routes, avoiding congestion of nodes with high reputation. Therefore, the average end-to-end delay of SRP-DRLB is slightly lower than that of SRMDR, and is significantly lower than that of CR-HWMP by about 6 ms.

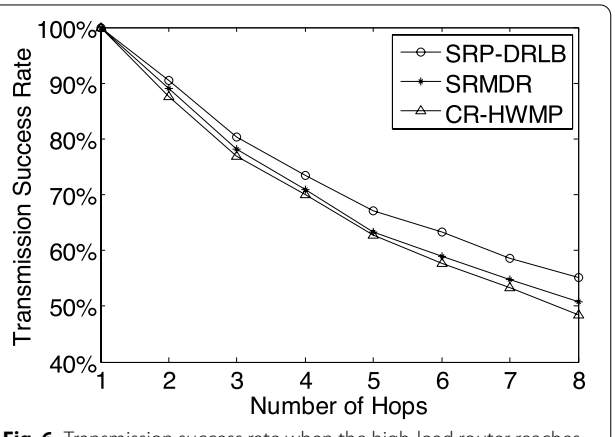

Fig. 6 Transmission success rate when the high-load router reaches 60% load

Success rate of transmission packet

The success rate of packet transmission refers to the success rate of packet transmission from the source node to the destination node, which reflects the adaptation of the routing algorithm to the current network. Figures 6 and 7 respectively show the experimental results of packet transmission success rate when the high-load routes of the three routing mechanisms reach 60% and 90% load. When the route load reaches 60%, the packet transmission success rate of SRP-DRLB is 5% and 6% higher than that of SRMDR and CR-HWMP. When the route load reaches 90%, the packet transmission success rate of SRP-DRLB is 9% and 11% higher than that of SRMDR and CR-HWMP. SRP-DRLB performs better than SRMDR and CR-HWMP in the success rate of packet transmission, especially with the increase of router load and route hops, SRP-DRLB has more obvious advantages in the success rate of data transmission. The reasons are as follows: (1) SRP-DRLB adopts the traffic prediction and load awareness mechanism to judge whether the current node is suitable for forwarding node by the load idleness, so that the node with relatively low load can be selected as the forwarding node as far as possible. (2) SRP-DRLB uses the edge weight policy to select routes, which can prevent the nodes with high reputation from being accessed by a large number of packets and help avoid network congestion and high packet loss rate; In addition, because the network load is relatively balanced, SRP-DRLB can improve the success rate of packet transmission and the security of the whole network.

Conclusion

In this paper, the secure routing mechanism of WMN is studied and a secure routing protocol is proposed based on dynamic reputation and load balancing. SRP-DRLB uses Chebyshev neural network to predict the comprehensive reputation and traffic of nodes, which speeds up the identification of malicious nodes and the establishment of routes, and realizes the load balancing of nodes with high reputation. The simulation results show that SRP-DRLB achieves certain improvement in the identification rate of malicious nodes, misjudgment rate of malicious nodes, and end-to-end delay. SRP-DRLB has obvious advantages in avoiding network congestion and improving the success rate of packet transmission, and improves the node quality and data security in the routing process. In the future work, methods to reduce the time cost of SRP-DRLB and improve the speed of removing malicious nodes will be studied to further improve the operation efficiency and security of SRP-DRLB.

Abbreviations

WMN: Wireless Mesh Networks; SRP-DRLB: Secure Routing Protocol based on Dynamic Reputation and Load Balancing; SRMDR: Secure Routing Mechanism based on Dynamic Reputation; CR-HWMP: Hybrid Wireless Mesh Protocol based on Cross-layer Reputation Mechanism; RREQ: Route Request.

Authors' contributions

All authors participated in the study of system models and computational theory, and drafted the manuscript. The specific contributions are as follows: Xiaogang Yuan studied and established the dynamic security fitness of nodes and security routing mechanism, and carried out simulation; Yipiao Chen carried out theoretical research on the reputation model and traffic prediction. The authors read and approved the final manuscript.

Funding

The research is supported by Young Doctor Foundation of Education Department of Gansu Province(2022QB-132).

Availability of data and materials

The authors declare that all the data supporting the findings of this study are available within the article.

Declarations

Competing interests

The authors declare no conflict of interest.

Received: 16 August 2022 Accepted: 11 October 2022
Published online: 05 November 2022

References

1. Yan Z, Gautam S (2022) A Wireless Mesh Opportunistic Network Routing Algorithm Based on Trust Relationships. IEEE Access 10:4786–4793
2. Sun Z, Wu P (2019) Research on IWSN Secure Routing Based on Trust Evaluation Model. Chin J Sensors Actuators 32(6):858–865
3. Mittal M, Iwendi C (2019) A Survey on Energy-Aware Wireless Sensor Routing Protocols. EAI Endorsed Transactions on Energy Web 24(6)e5
4. Zhang Q, Ren X (2022) Trust-based reliable transmission routing protocol for wireless sensor network. App Res Comput 39(5):1514–1518
5. Hu H, Han Y, Yao M (2022) Trust based secure and energy efficient routingprotocol for wireless sensor networks. IEEE Access 10:10585–10596
6. Lin H, Ma J (2014) Cross layer reputation mechanism based secure routing protocol for WMN. J Xidian Univ 41(1):116–123
7. Beheshtiasl A, Ghaffari A (2019) Secure and trust-aware routing scheme in wireless sensornetworks. Wireless Pers Commun 107(4):1799–1814
8. Yang H, Han Y (2019) Wireless Mesh network secure routing mechanism based on dynamic reputation. J Commun 40(4):195–201
9. Wang C, Wang X, Hu H, Zhao H, Han Y (2021) Secure clustering routing protocol based onimproved GA and trust-aware for wireless sensor networks. J Jilin Univ (Science Edition) 1237–1244
10. Zeng M, Jiang H, Wang X, Liu W (2013) Reputation evaluating model and security routing protocol of wireless sensor networks based on grey Markov model. App Res Comput 30(12):3758–3761
11. Liu Y, Liu N, Li X, Ji Q (2017) Load balancing routing protocol based on traffic prediction for wireless mesh networks. Computer Science 44(1):109–112
12. Iwendi C, Zhang Z, Du X (2018) ACO based key management routing mechanism for WSN security and data collection. IEEE Int Conf Industrial Technol (ICIT) 2018:1935–1939
13. Chen D, Qiu H, Zhu K, Wang Q, Zhu J (2021) An inter-domain routing reputation model based on autonomous domain collaboration. SCTENTTA STNTCA Inform 51(9):1540–1558
14. Han Y, Hu H, Yao M (2021) A trust-aware secure routing protocol for wireless sensor networks. Comput Eng 47(09):145–152
15. Han Y, Hu H, Guo Y (2022) Energy-aware and trust-based secure routing protocolfor wireless sensor networks using adaptive genetic algorithm. IEEE Access 10:11538–11550
16. Zhang G, Yang Y, Zhang D, Li J (2019) Secure routing mechanism based on trust against packetdropping attack in internet of things. Comp Sci 46(6):153–161
17. Pann L, Tao Y, Xu X, Wang J (2019) A secure clustering routing protocol based ontrust and balancing energy consumption. J Beijing Univ Posts Telecommun 42(3):29–36
18. Bi M, Ju Y, Hou R (2019) Environmentally-adaptive secure routing protocol for satellite networks. J Xidian Univ 47(1):66–72
19. Wang C, Liu X, Hu H (2020) Energy-efficient and load-balanced clustering routing protocol for wireless sensor networks using a chaotic genetic algorithm. IEEE Access 8:158082–158096
20. Yan D, Tao L, Gao J, Li L (2013) Research on space network secure routing algorithm. Spacecraft Eng 22(5):80–84
21. Wu C, You X, Lyu T (2018) Research on multipath secure routing based on confidence degree. J Northeast Normal Univ 50(4):66–72
22. Liang J, Sun W, Xiao N, Chen W, Guo Z (2020) Intelligent routing strategy for software-defined satellite network based on Chebyshev neural network. J Nat Uni Defense Technol 42(5):23–30
23. Wang J, Liu J, Zhang F (2021) Heterogeneous clustering routing protocol based on energy and trust. Computer Engineering and Design 42(4):927–933
24. Su F, Du K (2020) Trust based energy efficient opportunistic routing algorithm in wireless sensor networks. Comput Sci 47(2):300–305
25. Xu J, Li H, Wang JA, Zhao H (2015) Research on routing strategy based on edge weight and node load. J Northeastern Univ 36(12):1691–1695

Publisher's Note