Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9753851, 1 page
https://doi.org/10.1155/2023/9753851

Retraction

Retracted: A Secure Routing Protocol for Wireless Sensor Energy Network Based on Trust Management

Wireless Communications and Mobile Computing

Received 19 September 2023; Accepted 19 September 2023; Published 20 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] B. Yuan, "A Secure Routing Protocol for Wireless Sensor Energy Network Based on Trust Management," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5955543, 9 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5955543, 9 pages
https://doi.org/10.1155/2022/5955543

Research Article

A Secure Routing Protocol for Wireless Sensor Energy Network Based on Trust Management

Bingxia Yuan

Network and Information Center, Huizhou University, Huizhou, Guangdong 516007, China

Correspondence should be addressed to Bingxia Yuan; 201704429@stu.ncwu.edu.cn

Received 6 April 2022; Revised 4 May 2022; Accepted 9 May 2022; Published 29 May 2022

Academic Editor: Aruna K K

In order to enhance the ability of wireless sensor networks to resist various security threats and reduce the limitations caused by the characteristics of wireless sensor networks and sensor nodes, this paper proposes a secure routing protocol for wireless sensor networks based on trust management. Combined with the relevant parameters of wireless sensor network, the simulation experiment is carried out with MATLAB. Aiming at the trust management part of the wireless sensor network security protocol proposed in this paper, the malicious attack environment such as sensor node attributes is simulated to verify the resistance of this model to relevant malicious attacks. For the trust management-based wireless sensor network security routing protocol proposed in this paper, the model included in the protocol is compared to the existing security routing model, combining the characteristics of average simulation transmission, network life, and average routing update time. Experiments show that the model has better routing performance and has improved by an average of about 20%. We offer a new solution to solve the problem of wireless routing security.

1. Introduction

With the progress of science and technology and the rapid growth of human demand for information services, the application of wireless sensor network (WSN) has expanded rapidly in recent years. Wireless sensor network is an efficient, dynamic, and survivable wireless network established by a large number of intelligent wireless nodes or terminals in the wireless communication environment. Its communication depends on the cooperation between nodes rather than fixed infrastructure. Due to the flexibility of multihop networking and the open sharing of information, the security of information transmission has attracted extensive attention [1]. Trust aware routing protocol is not only an effective way to improve the security of WSN but also an important security guarantee for building a smart city in the future. However, in traditional trust aware routing protocols, a large amount of overhead caused by trust evaluation will seriously affect the network communication performance [2]. At the same time, wireless sensor networks are often placed in unsupervised or hostile environments and the subsequent security problems will also have a great impact on the data transmission of the network and greatly reduce the application value of wireless sensor networks [3]. The rapid development of short-range wireless multihop communication network technology continues to promote the construction of animal networking, cloud computing, social networks, and smart cities [4, 5]. In order to prevent wireless sensor networks from being attacked by malicious and selfish behavior, researchers have proposed many different types of secure routing protocols. However, existing security routing algorithms are often targeted at certain malicious or self-inflicted behavioral attacks [6, 7]. Figure 1 shows the wireless sensor security routing protocol. Wireless sensor network (WSN) is composed of self-distributed, self-organizing sensors in space, integrating wireless communication technology, embedded technology, sensor technology, and other cutting-edge technologies to monitor physical or environmental conditions, such as temperature, sound, and pressure, and transmit data to other places through the network through mutual cooperation between sensors. Because of its ability to be placed at will in harsh environments, its initial development was used in military fields, such as battlefield environment monitoring; today, such networks are

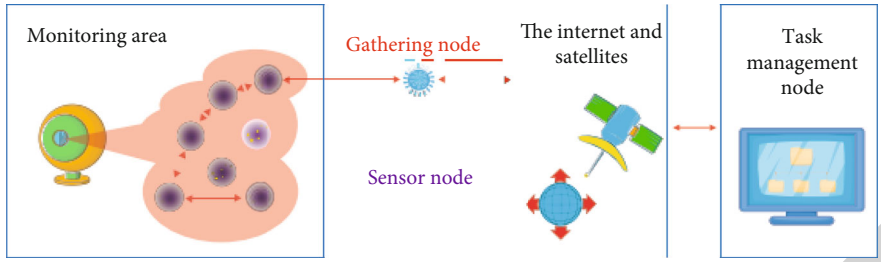

Figure 1: Secure routing protocol for wireless sensor networks.

used in many civilian fields, such as health monitoring, smart homes, and traffic control, disaster relief.

2. Literature Review

Although the wireless sensor network model based on trust management tends to mature and perfect over time, and many models take node attributes such as energy or data as the standard to evaluate direct trust, these literatures do not take into account the impact of node recommendation process and related data on direct trust. At the same time, in some models, by introducing time decay factor to give higher trust value and calculate weight to recent interactive data, on-off attacks can be detected and suppressed to a certain extent. However, with the complexity of attack frequency and attack intensity of malicious nodes, it is necessary to propose a new detection mechanism to deal with this threat [8, 9]. Trust management mechanism is becoming more and more popular in the field of wireless sensor network security. Some relevant literatures propose secure routing protocols based on trust mechanism to further improve the network performance. As the earliest known article applying trust management to wireless sensor network routing, it discusses how to make the best routing by using the routing trust value evaluated by the node and the corresponding routing data transmission overhead when there are multiple trusted secure routes between the source node and the sink node. However, with the increasing complexity of the basic routing protocol and security problems faced by wireless sensor networks, the requirements of the model proposed in this paper for establishing sufficient reliable routing in the network are not complete [10]. With the continuous popularization of various cluster head election mechanisms in wireless sensor networks, the continuous change of cluster head position has become one of the remarkable features in sensor networks. How to timely and effectively screen the nodes closer to the cluster head has also become an obstacle to the practical application of many trust-based secure routing protocols mentioned above. When establishing a secure data transmission route in combination with the trust management model, this paper does not introduce the specific location information of the source node or sink node and achieves the purpose of effective data transmission only through the accurate calculation of the trust value and the reasonable configuration of the routing protocol. At the same time, this kind of model rarely mentions the problem of how to update and maintain the established secure route in time, especially when the malicious node disguises as a normal node and joins the secure route to launch a malicious attack to interfere with or even destroy the normal communication between non adjacent nodes [11]. How to check this kind of malicious node in time has also become one of the key problems studied in this paper.

3. Research Methods

3.1. Integrated Secure Routing Model for Wireless Sensor Networks. In order to distinguish from some trust routing models that can only deal with some kinds of malicious attacks in the network, some comprehensive models that help to improve the data transmission security of wireless sensor networks are proposed. Compared with traditional models, these models have made great improvements in various malicious attacks against data routing and trust management. Combined with geographic routing principles, an environment trust sensing routing protocol ATSR is proposed. This protocol model has contributed to a more accurate assessment of nodes in a network, taking into account various factors, such as power and recommendations, but the model is based on the fact that all nodes know their geographic location information and are able to analyze location data of other nodes. On the basis of effective filtering, this presents a major challenge for sensor nodes with limited hardware conditions [12]. At the same time, by constantly promoting various mechanisms for selecting cluster heads in the wireless sensor network, the change of cluster head position has become a significant feature in wireless sensor networks. How to timely and effectively screen the nodes closer to the cluster head has also become an obstacle in the practical application of the model [13].

TSRI is a trust assumption and trust-based resource routing protocol. In this model protocol, when evaluating the trust value of neighbor nodes, any node only takes its packet forwarding accuracy as the evaluation standard and establishes a secure routing model that can be updated and maintained in time according to the trust value of nodes in the network. However, different from other protocol models based on trust mechanism, in this model, the trust recommendation from third-party nodes is not introduced into the calculation process as a factor of trust evaluation. Although these designs can effectively improve the network's resistance to a variety of malicious attacks, the model neglects to consider the possible attack means against the node energy in the network in the trust calculation. At the same time, when the malicious nodes in the network conspire with each other, the detection effect of the trust model

on malicious attacks decreases significantly [14, 15]. EDTM, an efficiently distributed trust model that takes into account three trust factors, such as node communication, power, and data, has contributed to wireless sensor networks in combating malicious attacks on communication data and trust management mechanisms. However, it focuses on establishing a stable trust management model and lacks more in-depth research on how to use the trust value evaluated between nodes to determine a reliable secure route. Therefore, the model lacks effective means to deal with the malicious attack on the route.

TSSRM, a trust aware secure routing mechanism protocol derived from TSRF, obtains the credibility of nodes by analyzing the energy consumption, mobility, and other factors of nodes. At the same time, combined with the QoS characteristics of routing, it explains the design idea, workflow process, and maintenance method of secure routing from source node to sink node. Compared with TSRF, TSSRM takes energy as an important reference for investigating the trust value of nodes, and the model includes a defense mechanism against on-off attacks, but it does not consider the adverse impact that the change of attack frequency may have on the network, and, like TSRF, it lacks the detection and investigation of mutual conspiracy between malicious nodes, so that the established secure route has no defense effect against collusive attacks and selfish attacks [16]. According to the above five comprehensive security routing models, the analysis of Table 1 shows the ability of these models to deal with various security threats. It can be seen from Table 1 that the five comprehensive models can deal with most attacks from malicious nodes. Except that the TSR does not introduce the recommendation of third-party nodes as the evaluation element of trust value, the models in the table have good resistance and detection effects on information tampering attacks and unfair evaluation attacks. At the same time, any comprehensive trust routing model is not enough to deal with all malicious attacks, especially when dealing with collusion attacks and selfish attacks. In addition, as the network environment becomes more complex, many smart malicious attackers can adjust the frequency of attacks to avoid detecting network security mechanisms. Obviously, these models do not have the ability to defend against malicious attacks with variable attack frequency [17].

3.2. Trust Evaluation Method

3.2.1. Communication Trust Evaluation. Communication trust, as the most basic element to investigate the credibility of objective nodes in trust evaluation, is mainly evaluated according to the communication behavior of objective nodes observed by subjective nodes using watchdog mechanism, in order to use communication trust to detect black hole attacks and gray hole attacks that may be caused by objective nodes in time and effectively.

When calculating the communication trust of objective nodes, beta distribution is used as the calculation model. Since trust reflects the prediction of the subjective node on the possibility of normal communication between the objective node and the subjective node in the future based on the past behavior of the objective node, at the same time, in order to simplify the trust calculation process, the expectation of beta distribution is used to calculate the communication trust, as shown in

$$\mathrm{CT}_{i,j}^{t} = \frac{\mathrm{SCT}_{i,j}^{t} + 1}{\left(\mathrm{SCT}_{i,j}^{t} + 1\right) + \left(\mathrm{UCT}_{i,j}^{t} + 1\right)}, \tag{1}$$

where $\mathrm{CT}_{i,j}^{t}$ represents the communication trust value of subjective node i to objective node j in time t, while $\mathrm{SCT}_{i,j}^{t}$ and $\mathrm{UCT}_{i,j}^{t}$, respectively, represent the total number of successful and failed communications of j obtained from the communication trust measurement in time t.

3.2.2. Data Trust Assessment. In wireless sensor networks, malicious attacks against data security from compromise nodes can be divided into two categories. One is that compromise nodes forge data that is greatly different from or completely inconsistent with the actual situation they know, which affects the judgment of the sink node on the real situation of the sensor network. In addition, it is possible to introduce wrong data in data fusion and reduce the overall accuracy of data collection by the base station. The second is that the malicious node partially or completely replaces the contents of the data packet when forwarding the data packet from other nodes, which leads to data tampering attack. In particular, if the malicious node modifies the target node ID in the trusted routing discovery data packet to other malicious nodes, it may lead to slot attack. Beta distribution can be used to calculate data trust, which is the same as equation (1).

3.2.3. Energy Confidence Assessment. One of the most important characteristics of a wireless sensor is that the power directly determines the service life of the network. Therefore, some malicious attacks, such as energy loss attack, exhaust the energy of the captured node by making the captured node send invalid data endlessly. At the same time, abnormal energy consumption can also be used to detect whether a node has excessive power loss due to malicious attacks. The objective value of the trusted node is shown in the following:

$$\mathrm{ET}_{i,j}^{t} = \begin{cases} re^{t}(1 - \Delta p), & re^{t} \geq \varepsilon\ \Delta p \leq v, \\ 0, & re^{t} < \varepsilon\ \Delta p > v, \end{cases} \tag{2}$$

where $\mathrm{ET}_{i,j}^{t}$ represents the energy trust value of subjective node i to objective node j in time t; re^{t} is the residual energy rate; objective node energy rate change $\Delta p = |p_j^t - p_j^{t-1}|$; and v is the threshold.

3.2.4. Recommendation Trust Assessment. Recommendations from third-party nodes, as an important factor to assist subjective nodes to evaluate the trust of objective nodes, often become the target of malicious attacks such as unfair

Table 1: Comparison of ability of wireless sensor network security routing model to deal with various attacks.

		ATSR	TSR	TSRF	EDTM	TSSRM
For routing protocol	Black hole attack	√	√	√	×	√
	Grey hole attack	√	√	√	×	√
	Slot attack	×	√	√	×	√
	Information tampering attack	√	√	√	√	√
	Energy consumption attack	√	×	×	√	√
	On-off attack	√	×	√	√	√
	Contradictory behavior attack	×	×	√	√	√
For trust management	Unfair evaluation attack	√		√	√	√
	Collusion attack	×		×	×	×
	Selfish attack	√		×	×	×

evaluation attacks. When the models established in many literatures detect the possible hidden dangers in node recommendation, subjective nodes usually adopt negative strategies, that is, to remove the recommendation data that is quite different from most recommendations or their own direct evaluation results, which improves the accuracy of indirect trust value to a certain extent, but there is no further detection and punishment mechanism for suspicious nodes that provide inaccurate recommendation data. By introducing recommendation trust, we can realize the real-time adjustment of the trust value of the objective node as the recommendation node and effectively resist the selfish attack and collusion attack caused by the objective node. Calculate the recommended trust of the objective node, as shown in

$$\mathrm{RT}_{i,j}^{t} = \frac{\mathrm{SRT}_{i,j}^{t} + 1}{\left(\mathrm{SRT}_{i,j}^{t} + 1\right) + \left(\mathrm{URT}_{i,j}^{t} + 1\right)}, \tag{3}$$

where $\mathrm{RT}_{i,j}^{t}$ represents the recommended trust value of subjective node i to objective node j in time t, while $\mathrm{SRT}_{i,j}^{t}$ and $\mathrm{URT}_{i,j}^{t}$, respectively, represent the total number of successful and failed communications of j measured by the recommended trust measure in time t [18–20].

4. Result Analysis

4.1. Experiment and Analysis of Trust Management Model in Multiple Attacks. MATLAB is used as the simulation program to simulate the proposed trust management model based on node multiattribute. At the same time, combined with various malicious attacks, the trust management model in the trust-based wireless sensor network integrated security routing protocol is compared to analyze the effectiveness of the proposed model in resisting malicious attacks, as shown in Figure 2. In the experiment, a comprehensive attacker including all attacks is introduced to analyze and compare the response ability of the proposed trust management model and other models.

Synthesizing all the malicious attacks that may exist in wireless sensor networks mentioned above, simulate the network environment with great security threats. In this experiment, the probability of malicious attacks launched by malicious nodes against communication, data, energy, and recommended four node attributes is 25%, respectively. At the same time, malicious nodes can also affect the normal trust evaluation process of the network through collusion, contradictory behavior, and on-off attacks. Figure 2 shows the change curve of the average packet transmission rate of the network with the increase of the proportion of malicious attacks of malicious nodes in the total communication behavior of the network. It can be seen from the figure that compared with other trust management models, due to the introduction of sliding time window, the possible malicious behaviors in each time unit can be accurately recorded, and the attack frequency detection mechanism is used as an auxiliary [21, 22]. When the proportion of malicious attacks increased to 50%, although most malicious nodes were removed from the secure route, some undetected malicious nodes continued to launch contradictory behaviors or collusive attacks that could not be effectively detected. The routing trust value evaluation is seriously disturbed, and the average packet transmission rate is reduced to the extent that the network communication is blocked. Due to the means to deal with all the above malicious attacks, the average packet transmission rate of the model remains at a high level, which proves that the model still has good security in the severe network environment of dealing with a combination of multiple malicious attacks.

4.2. Simulation Experiment and Analysis. The secure routing model of multiattribute wireless sensor networks based on trust management is compared with three secure routing

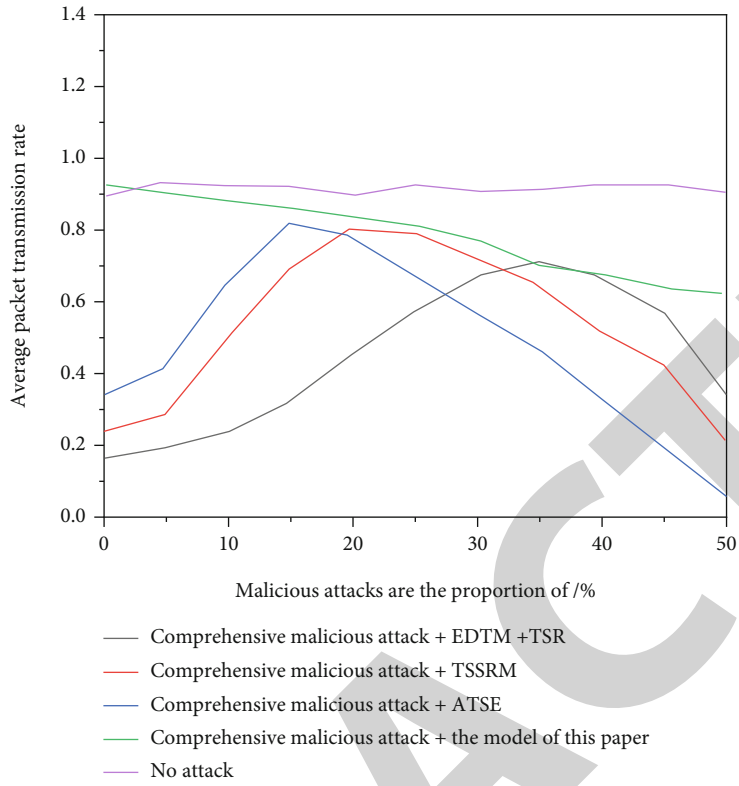

Figure 2: Performance of various malicious attacks combined with various trust management models in the environment.

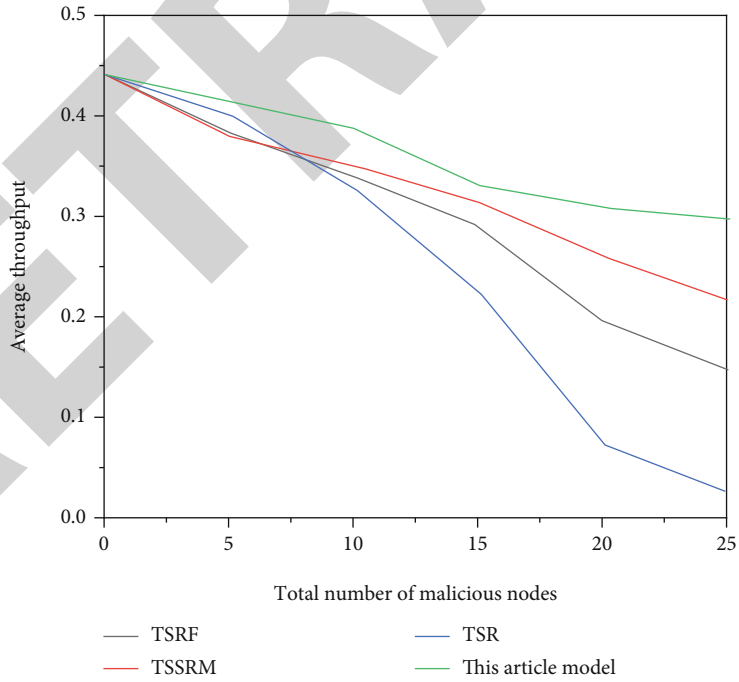

Figure 3: Comparison of average end-to-end data transmission delay of each model.

models: TSRI, TSRF, and TSSRM. At the same time, combined with the evaluation of the overall routing performance, energy consumption, and routing maintenance function, simulation validation is performed when the number of malicious nodes in the network changes. To verify the packet transmission efficiency of the secure routing model, each model is evaluated through the concept of average network throughput. Average bandwidth refers to the average number of packets transmitted per second from the source node to the absorber node for each route in the network.

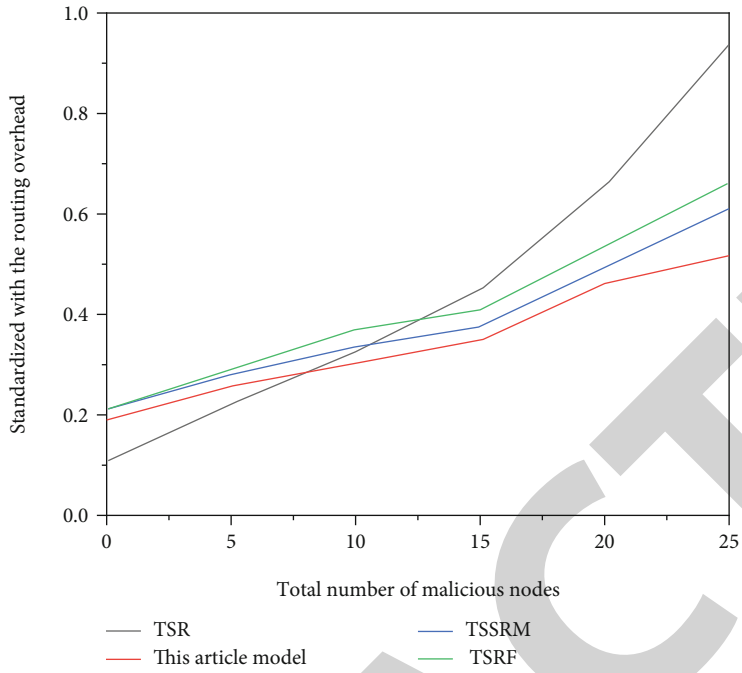

Figure 4: Comparison of standardized routing overhead of each model.

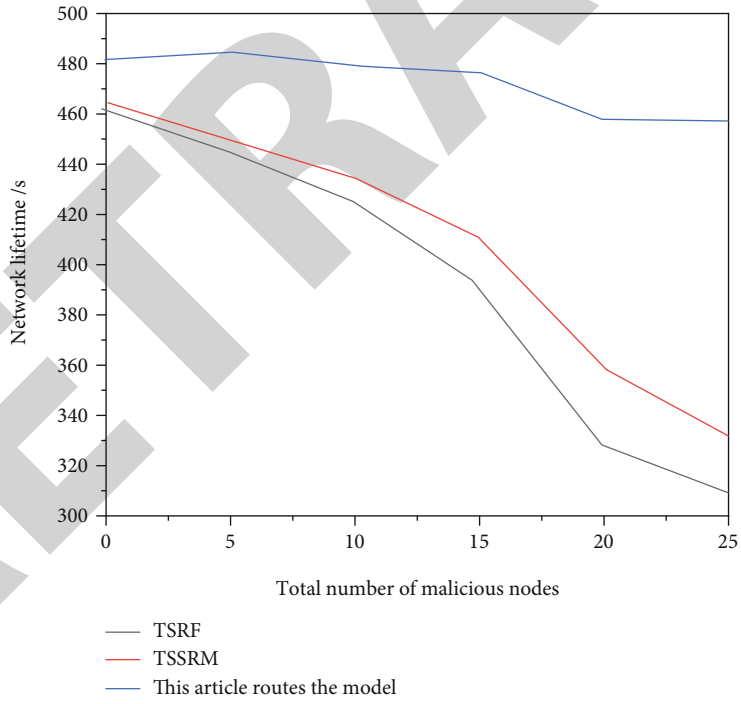

Figure 5: Comparison of network life of each model.

As can be seen in Figure 3, the average throughput of each model is set to the same level in the absence of malicious nodes in the network. Firstly, because the impact of many attack methods such as energy loss attack and contradictory behavior attack on network trust evaluation is not considered in the design process of TSR model, therefore, as the number of malicious nodes increases, its average throughput decreases rapidly, and the model almost completely fails when the total number of malicious nodes in the network reaches 25 [23]. At the same time, the model proposed in this paper performs better than other comparison models in terms of network throughput. This is because this model adopts the method of comprehensive trust evaluation and cooperates with appropriate secure route detection mechanism to make the secure route established between end-to-end more reliable. In addition, because TSSRM model and

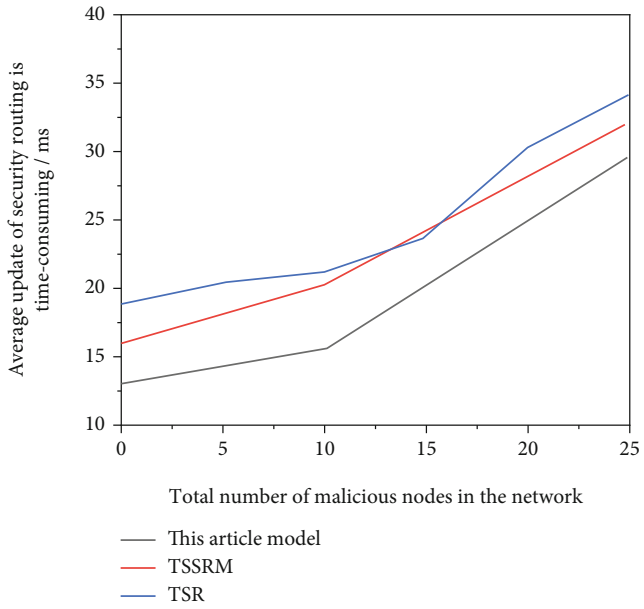

Figure 6: Comparison of average update security routing time of each model.

TSRF model ignore the punishment of selfish nodes that do not participate in trust recommendation, when the launching probability of selfish attack increases with the total number of malicious nodes, the network throughput also decreases to a certain extent.

By introducing an average transmission delay between the ends to test the efficiency and quality of the secure routing installed in the network, the average delay between transmissions represents the average time taken to transfer data from the source node to the target node.

To evaluate the difference between the proposed model and the comparative model in the cost of node control (see Figure 4), the concept of standardized routing overhead is introduced into the simulation experiment. The standard routing increment is the ratio of the number of control packets transmitted through nodes in the network to the number of data packets sent to create secure routes. This can be seen in Figure 4, and when the number of malicious nodes in the network is 0, the TSR model has the lowest routing overhead among the four comparison models. This is because the trust evaluation model of TSR does not include the trust recommendation process between nodes, so the transmission number of control packets is greatly reduced [24, 25]. As the number of malicious nodes in a network increases, the security routing model proposed in this paper is based on a wireless sensor network security routing model based on trust management, TSSRM and TSRF models proposed in this paper are more stable in routing overhead. In addition, the security routing model proposed in this paper adopts standby routing strategy and more optimized routing method than TSSRM and TSRF models, so the network using this routing model can maintain a high-quality path that requires less data retransmission and meets the requirements of high reliability and less hops.

The energy consumption of each model is analyzed by comparing the network lifetime of the three energy-constrained safe routing models of Figure 5 nodes, including TSSRM, TSRF, and the routing model. Figure 5 shows that if the network has a small number of malicious nodes, the network life of the secure routing model proposed in this document is about 470 seconds. As the number of harmful knots increases, they tend to reconcile with each other, the standby routing mechanism in the routing protocol gradually fails, and the periodic feedback from the sink node begins to play a role, which leads to a slight decline in the network life curve when the total number of malicious nodes reaches 20. At the same time, in the network using TSSRM and TSRF, it is not enough to deal with the collusion from malicious nodes and potential attackers who may adopt changeable attack strategies. Therefore, if the total number of malicious nodes in the network continues to increase, the service life of the network using both models tends to decrease significantly. This confirms that the safe routing model proposed in this document is more energy efficient.

Some safety route models, including the route model in this document, will update the route in a timely manner at the request of the intermediate node, in the event of a malfunction on a specified safe route and affecting the normal operation of the current route, compare the routing model in this paper with TSR and TSSRM (TSSRM is consistent with the secure routing maintenance model adopted by TSRF) models that introduce secure routing maintenance, and analyze the time required to reestablish a secure and reliable route when the source node or sink node receives the route update notification caused by a malicious node. As shown in Figure 6, when the number of malicious nodes in the network is small, the source node using this model will directly call the standby secure route stored in memory to replace the current secure route, so it has a faster route update speed than other models. As the number of malicious nodes in the network increases, a feedback mechanism is being introduced to receive information from the sink from time to time and the source node applying the model in this paper can indirectly judge that the malicious nodes in the route are one or more according to the type of route update notification received, so as to adopt the strategy of using standby route or refinding new route, which can effectively save the time required to update the secure route. Therefore, compared with the TSR model of secure routing update by sink nodes or TSSRM with relatively simple malicious node feedback mechanism, this model has greater advantages in timeliness and rapidity of secure routing update.

5. Conclusion

With the continuous popularization of wireless sensor network technology, wireless sensors are more and more used in different occasions. However, due to the limitations brought by the characteristics of sensors and the uncertainty of the application environment, the security of wireless sensor networks has increasingly become a hot issue in this field. In fact, whether applied in harsh and turbulent military battlefield or arranged in good and stable deep mountain

jungle, in order to make the sensor nodes play the function of detecting and transmitting data normally, the primary premise is to ensure that the wireless sensor network is free from the interference and destruction of various malicious attacks. In addition, in order to deal with many security problems in the process of node trust evaluation caused by the widespread application of trust management mechanism in wireless sensor networks, it is necessary to propose a secure routing model that can comprehensively improve the network's resistance to various attacks. After a comprehensive analysis of the research status of secure routing models for wireless sensor networks based on trust management at home and abroad, combined with the shortcomings of the existing models in the process of node trust evaluation, the potential security risks that malicious nodes using changeable attack strategies may bring to the network, and the lack of effective secure routing update methods in the existing models, this paper gives the corresponding views. The research results and main contributions obtained focus on the following points:

(1) Firstly, the malicious attacks in wireless sensor networks are divided into two categories: routing and trust management. Then, the defense ability of the existing trust-based secure routing model for various malicious attacks is compared. When proposing the routing model, this paper focuses on all possible security threats and verifies the comprehensiveness of the proposed model in defending against malicious attacks by means of simulation experiments

(2) In the trust-based multiattribute secure routing model proposed in this paper, the trusted routing between the origin node and the sink node is established based on the trust value obtained from the comprehensive evaluation of communication, data, energy, and recommendation. Among them, different attribute measures are adopted for each node attribute to enhance the accuracy of the calculation of the corresponding attribute trust value and the ability to deal with malicious attacks on the corresponding attribute. In particular, the introduction of recommendation attribute greatly reduces the possible adverse effects of selfish attacks on the network and all kinds of unfair recommendations

(3) In the trust-based multiattribute secure routing model proposed in this paper, the model performs better than other comparative models in terms of network throughput, average end-to-end data transmission delay, model standardized routing overhead, model network life, and average time-consuming of updating secure routing

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that she has no competing interests.

References

[1] H. R. Shaukat, F. Hashim, M. A. Shaukat, and K. Ali Alezabi, "Hybrid multi-level detection and mitigation of clone attacks in mobile wireless sensor network (MWSN)," *Sensors*, vol. 20, no. 8, p. 2283, 2020.

[2] R. Ahmed, Y. Chen, and B. Hassan, "Optimal spectrum sensing in mimo-based cognitive radio wireless sensor network (CR-WSN) using glrt with noise uncertainty at low SNR," *AEU - International Journal of Electronics and Communications*, vol. 136, no. 4, article 153741, 2021.

[3] W. Gui, Q. Lu, M. Su, and F. Pan, "Wireless sensor network fault sensor recognition algorithm based on MM∗ diagnostic model," *Access*, vol. 8, pp. 127084–127093, 2020.

[4] W. Chen and X. Wang, "Coal mine safety intelligent monitoring based on wireless sensor network," *IEEE Sensors Journal*, vol. PP(99), pp. 1–1, 2020.

[5] R. H. Dong, H. H. Yan, and Q. Y. Zhang, "An intrusion detection model for wireless sensor network based on information gain ratio and bagging algorithm," *International Journal of Network Security*, vol. 22, no. 2, pp. 218–230, 2020.

[6] W. He, F. Lu, J. Chen, R. Yi, and Y. Zhang, "A kernel-based node localization in anisotropic wireless sensor network," *Scientific Programming*, vol. 2021, 8 pages, 2021.

[7] S. Chauhan, M. Singh, and A. K. Aggarwal, "Cluster head selection in heterogeneous wireless sensor network using a new evolutionary algorithm," *Wireless Personal Communications*, vol. 119, no. 1, pp. 585–616, 2021.

[8] N. Barthwal and S. K. Verma, "An optimized routing algorithm for enhancing scalability of wireless sensor network," *Wireless Personal Communications*, vol. 117, no. 3, pp. 2359–2382, 2021.

[9] M. Prabha, S. S. Darly, and B. J. Rabi, "A novel approach of hierarchical compressive sensing in wireless sensor network using block tri-diagonal matrix clustering," *Computer Communications*, vol. 168, no. 2, pp. 54–64, 2021.

[10] Y. M. Raghavendra and U. B. Mahadevaswamy, "Energy efficient intra cluster gateway optimal placement in wireless sensor network," *Wireless Personal Communications*, vol. 119, no. 2, pp. 1009–1028, 2021.

[11] V. K. Quy, V. H. Nam, D. M. Linh, N. T. Ban, and N. D. Han, "A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in iot networks," *Wireless Personal Communications*, vol. 120, no. 1, pp. 49–62, 2021.

[12] V. Patil and S. Deshpande, "Design of FPGA soft core based WSN node using customization paradigm," *Wireless Personal Communications*, vol. 122, no. 1, pp. 783–805, 2022.

[13] C. G. Krishnan, A. H. Nishan, S. Gomathi, and G. A. Swaminathan, "Energy and trust management framework for MANET using clustering algorithm," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1267–1281, 2022.

[14] S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, and D. Draheim, "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sensors Journal*, vol. 21, no. 6, pp. 8716–8733, 2021.

[15] K. A. Awan, I. U. Din, A. Almogren, and H. Almajed, "Agri-trust-a trust management approach for smart agriculture in

cloud-based internet of agriculture things," *Sensors*, vol. 20, no. 21, p. 6174, 2020.

[16] H. Xia and W. Yang, "Security access solution of cloud services for trusted mobile terminals based on TrustZone," *International Journal of Network Security*, vol. 22, no. 2, pp. 201–211, 2020.

[17] J. Zhang, "Interaction design research based on large data rule mining and blockchain communication technology," *Soft Computing*, vol. 24, no. 21, pp. 16593–16604, 2020.

[18] X. Meng and G. Zhang, "Truetrust: a feedback-based trust management model without filtering feedbacks in P2P networks," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 175–189, 2020.

[19] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. - PP(99), pp. 1–14, 2020.

[20] R. Huang, P. Yan, and X. Yang, "Knowledge map visualization of technology hotspots and development trends in China's textile manufacturing industry," *IET Collaborative Intelligent Manufacturing*, vol. 3, no. 3, pp. 243–251, 2021.

[21] M. Raj, P. Manimegalai, P. Ajay, and J. Amose, "Lipid data acquisition for devices treatment of coronary diseases health stuff on the internet of medical things," *Journal of Physics: Conference Series*, vol. 1937, p. 012038, 2021.

[22] A. Sharma and R. Kumar, "Risk-energy aware service level agreement assessment for computing quickest path in computer networks," *International Journal of Reliability and Safety*, vol. 13, no. 1/2, p. 96, 2019.

[23] M. Bradha, N. Balakrishnan, A. Suvitha et al., "Experimental, computational analysis of Butein and Lanceoletin for natural dye-sensitized solar cells and stabilizing efficiency by IoT," *Evironment, Development and Sustainability*, vol. 24, no. 6, pp. 8807–8822, 2022.

[24] F. Almuzaini, S. Alromaih, A. Althnian, and H. A. Kurdi, "Whatstrust: a trust management system for whatsapp," *Electronics*, vol. 9, no. 12, p. 2190, 2020.

[25] J. Zhang, J. Sang, K. Xu, S. Wu, and J. Yu, "Robust captchas towards malicious OCR," *IEEE Transactions on Multimedia*, vol. PP(99), pp. 2575–2587, 2020.