Wireless Sensor Network Technology Based on Security Trust Evaluation Model

https://doi.org/10.3991/ijoe.v14i04.8590

Jinghua Zhu
Hunan Mechanical & Electrical Polytechnic, Changsha, China
7006612@qq.com

Abstract—Because the current research on wireless sensor networks is not thorough enough, with such shortcomings as lack of objectivity and insufficient accuracy of the trust evaluation model of network nodes, this paper proposes a trust evaluation model with multi-factor comprehensive consideration and Bayesian model, an improved trust evaluation model, by combining trust management mechanism, trust factor, fuzzy set and D-S evidence theory, solving factor singleness and imprecise evaluation in the original model. The simulation results show that the proposed model has good dynamic adaptability, higher detection rate and lower detection error rate, and it consumes less energy and improves the security of the network.

Keywords—Trust evaluation model, Multi-factor, Bayesian model, Wireless sensor

1 Introduction

With the advent of information age, people need more and more fine and extensive monitoring and precise transmission of environmental physical information through wireless sensors. The wireless sensors include sensors of temperature, humidity, gravity, pressure, lighting, etc., which make up the wireless sensor networks (WSN), which can monitor the data in real time and transmit it to the control center by wireless communication [1-2]. With such advantages as low cost, simple installation, small energy consumption and self-work, it greatly saves manpower, material resources and financial resources, and thus it has great application prospect in every field of national life and is considered as one of the most practical and scientific key technologies.

Because of the openness of the network system, it is easy to be threatened and attacked, so that its information is stolen and the network is destroyed. In addition, the system is often in an extremely harsh environment and is vulnerable to physical damage. These become the development bottlenecks of wireless sensor network system [3-5]. At present, there are two types of attacks: external attacks and internal attacks. With a high degree of concealment, Internal attacks are not easily resisted, and the resulting damage is even more powerful. The types of attacks common in wireless sensor networks are shown in Table 1.

Table 1. Common types of attack in wireless sensor networks

Attack name	Type	Means of realization	Consequence
Sniffing attack	External attack	Monitor the data message of adjacent nodes	Stealing network data message
Deception / replay attacks	External / internal attack	Forgery, tampering, and playback of network messages that do not exist	Destroy routing, increase network latency, cause data conflict
Selective forward attack	External / internal attack	Selective forwarding message	Cause important network data to be unable to reach the destination node
Sybil Attack	External / internal attack	Capture and clone other legitimate node identities	Misleading routing, monitoring data, stealing information, and providing false data
Sewerage attack	Internal attack	Using a compromise node to publish false routing information to attract network traffic	Destroy routing, cause network congestion
Wormhole attacks	Internal attack	Declaring false delay routing information to attract data and replay	Destroy the normal communication order of the network
DoS attack	External / internal attack	The congestion network takes up all the corresponding resources of the target node	Making the network or target node unable to respond to a legitimate service request
Tampering	External / internal attack	Before forwarding packets, malicious tampering of packet content	Legal packets cannot reach the destination node
Intelligent behavior attack	Internal attack	Using the compromise node to adjust the attack strength according to the network security policy	Malicious node detection that destroys the normal function of the network and evade the security mechanism

The traditional security mechanism based on encryption and authentication can only resist the attack from outside and cannot resist the attack from inside the network, so it can not satisfy the increasingly developing technology demand. Therefore, the trust management mechanism becomes the effective supplementary means of the traditional security mechanism. In that management mechanism, the node is evaluated and analyzed according to different characteristics, so as to ensure the transmission safety between the nodes, and thereby ensure the safety and reliability of the whole network. The researchers at home and abroad established various trust management models through different trust evaluation techniques (fuzzy logic, Bayesian theory, entropy theory, game theory, etc.), such as reputation-based model, position beacon information based on sensor network, reputation model based on agent, etc.) [6-8].

However, the topology of wireless sensor networks is in a dynamic state, the passive advantage limits the frequency of its evaluation, and the destruction of its performance by the harsh environment makes the trust management of wireless sensor networks difficult. Therefore, when designing the trust management mechanism of wireless sensor networks, it is necessary to meet the requirements of lightweight, adaptability, passivity and anti-attack. The trust management system architecture of typical wireless sensor network is shown in Figure 1.

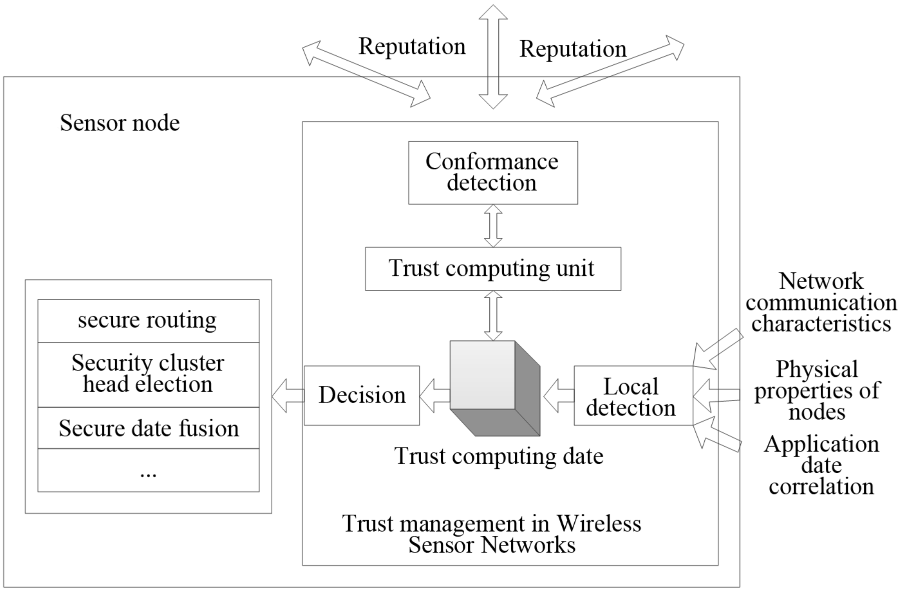
Reputation
Reputation
Sensor node
Conformance detection
Trust computing unit
secure routing
Security cluster head election
Secure date fusion
...
Decision
Local detection
Trust computing date
Network communication characteristics
Physical properties of nodes
Application date correlation
Trust management in Wireless Sensor Networks

Fig. 1. WSN trust management architecture

2 Design of Trust Evaluation Model

In order to solve that problem that no relevant factors are considered in the traditional trust evaluation model, in combination with the uncertainty of trust management, a trust model of multi-factor comprehensive evaluation is proposed and is analyzed by using simulation experiment. In that model, the node trust calculation, the fuzzy partition and the fusion are carried out successively through the trust factor, the fuzzy set and the D-S evidence theory [9-11], with information security improvement in this paper.

2.1 Theoretical bases

Fuzzy classification. In order to make the trust measure of wireless sensor network nodes more effective, it is necessary to adopt multi-valued logic and consider different trust classes with different support. In this paper, the membership degree of fuzzy set theory is selected for quantitative analysis of trust. The following three variables are described as "untrusted" (subset T_1), "uncertain" (subset T_2) and "trusted" (subset T_3), with the membership functions established as u1 (t), u2 (t) and u2 (t = u1), the sum of which is 1 (u1 (t) + u2 (t) + u3 (t) = 1). Finally, the function is adjusted by experimental verification, as shown in Figure 2.

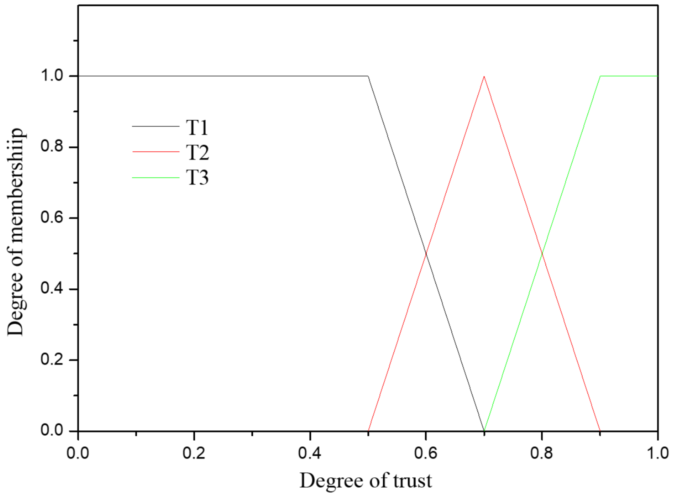

Fig. 2. Fuzzy classification of node trust

D-S evidence theory. D-S evidence theory is a theory of reasoning and calculation for evidence with inaccuracy and uncertainties. So, it can effectively solve the problem of computing uncertain information in trust evaluation. The formula of reliability function and likelihood function in its basic theory are as follows:

$$\begin{cases} m(\emptyset) = 0 \\ \sum_{A \subseteq 2^{\Omega}} m(A) = 1\,, A \neq \emptyset \end{cases} \tag{1}$$

$$Bel(A) = \sum_{B \subseteq A} m(B) = 1\,, \forall\, A \subseteq 2^{\Omega} \tag{2}$$

$$Pl(A) = 1 - Bel(\bar{A}), \;\; A \subseteq 2^{\Omega} \tag{3}$$

Identity-based public key cryptosystem. Identity-based public key cryptosystem is to bind personal identity information to public key. The trusted agency (CA) calculates the user's private key (private key =F (main key, public key)) through its own main key and public key, and securely and confidentially transmit it to the user, and the third-party organization and the directory to store public key or certificate are not needed. Compared with the certificate-based public key cryptosystem, the identity-based public key cryptosystem has the following advantages, as shown in Table 2.

Table 2. Comparison between certificate and identity based public key cryptosystem.

Comparison	Public key cryptosystem based on certificate	Identity based public key cryptosystem
Resource occupancy	Space for large storage of public key certificates	Saving storage resources
Authentication mechanism	More complex locks, public key certificates issued by CA are required and the legitimacy of the CA signature needs to be verified.	Simple, direct or evolving user identity information as a public key
Maintenance cost	A system that needs to maintain a user's public key directory	Only user information and system public parameters

2.2 Description of the trust evaluation model

Analysis of credibility factors. The premise of comprehensive evaluation of node trust is reasonable selection of trust metrics and analysis of credibility factors. The single trustworthiness factor evaluation system used in the current trust model cannot calculate the trust value of the node accurately and objectively, and the trustworthiness factors of multiple influence factors should be considered comprehensively, such as forwarding rate factor, integrity factor, consistency factor, and availability factor [12-14]. In addition to trustworthiness factors, there are network main task factor, network energy consumption factor and other influencing factor. Therefore, all trustworthiness factors are divided into network communication properties, node physical properties and application data security, and their trustworthiness factors (forwarding rate factor, integrity factor, availability factor) are defined.

Forwarding rate factor $\mathrm{FF}_{i,j}(\mathrm{t})$: Nodes in wireless sensor networks have limited energy, which needs to be relayed while sensing and transmitting data. Therefore, it is possible to analyze and judge whether the node is attacked or not by analyzing the data forwarding of the nodes. The forwarding rate factor function may be expressed as:

$$\mathrm{FF}_{i,j}(\mathrm{t}) = \frac{ACK_{i,j}(t)}{TP_{i,j}(t)} \tag{4}$$

Where, $ACK_{i,j}(t)$ is the number of feedback packets; $TP_{i,j}(t)$ is the number of packets to forward; i is evaluation node; and j is the node to be evaluated.

Integrity factor ($\mathrm{IF}_{i,j}(\mathrm{t})$): When the data packet is sent to the next node, the source node will monitor whether the data packet is tampered or not and whether it is forwarded completely within a certain period of time, which ensures that the integrity and correctness of the data is not tampered with. The integrity factor function can be expressed as:

$$\mathrm{IF}_{i,j}(\mathrm{t}) = \frac{IP_{i,j}(t)}{FP_{i,j}(t)} \tag{5}$$

Where, $IP_{i,j}(t)$ is the number of completely and correctly forwarded packets and $FP_{i,j}(t)$ is the number of packets to forward.

Availability factor ($\mathrm{AF}_{i,j}(\mathrm{t})$): The node cannot be used due to the interference of the network channel and the extremely harsh environment, so it is necessary to prove the evaluated node by sending and inspecting data packet. The availability factor calculation formula can be expressed as:

$$\mathrm{AF}_{i,j}(\mathrm{t}) = \frac{ACK_{i,j}(t)}{ACK_{i,j}(t)+NACK_{i,j}(t)} \tag{6}$$

Where, $ACK_{i,j}(t)$ is the number of responded packets and $\mathrm{N}ACK_{i,j}(t)$ is the number of un-responded packets.

2.3 Experimental simulation and performance analysis

The trust model is simulated and compared with the model RFSN and the model TMS. The experimental parameters are set as shown in Table 3.

Table 3. Experimental parameters

Parameter	Data
Packet loss rate and tamper rate	70-100%
Trust update cycle /τ	10s
Adaptive time factor / (β_s, β_l)	0.3, 0.8
Threshold of node trust classification / (θ, δ)	0.3, 0.09
Simulation area	100*100
Number of nodes	100
Node radius	30
Packet size	100

Only when the trust model has good dynamic adaptability, can the attack behavior of nodes be recognized in time and accurately. Figure 3 shows the variation of the direct trust value under ON-OFF attack. It can be seen from the figure that the basic confidence function m ({T}) of the node-trusted proposition gradually increases, the basic confidence function m ({T, -T}) of the node-state uncertainty proposition gradually decreases, and the basic confidence function of the node-untrusted proposition always is 0. When a malicious attack is launched, the trust that slowly accumulates decreases rapidly. Therefore, it is particularly important to timely identify and eliminate malicious attacks.

When the indirect trust values are considered, a bad - facing attack can easily occur. The trust model is analyzed and compared with the RFSN model and the TMS model respectively for two cases such as a malicious node discrediting a normal node and a malicious node advocating other malicious nodes, and the results are shown in Figures 4 and 5.

As can be seen from Figure 4, when a malicious node discredits a normal node, the RFSN model is the least influenced, followed by the proposed trust model, and the TMS model is the greatest influenced, which shows that the proposed model can be improved in the aspects of comprehensiveness and objectivity. However, it can be seen from Figure 7 that the RFSN model cannot resist the advocacy of the malicious node to the accomplice, but the proposed model has good resistance. This is mainly because the proposed trust model considers both direct trust and indirect trust, and the value of node trust is more objective and accurate.

In order to further analyze the safety of the model, the three models are analyzed and compared with respect to the detection rate, with the results shown in Figure 6. It can be seen from the figure that the proposed model is obviously superior to the other two models, which is because the proposed model introduces the concept of fuzzy set and quantizes the subjective trust; the weights of direct trust and indirect trust are modified; and trust value is comprehensively considered in Dempster.

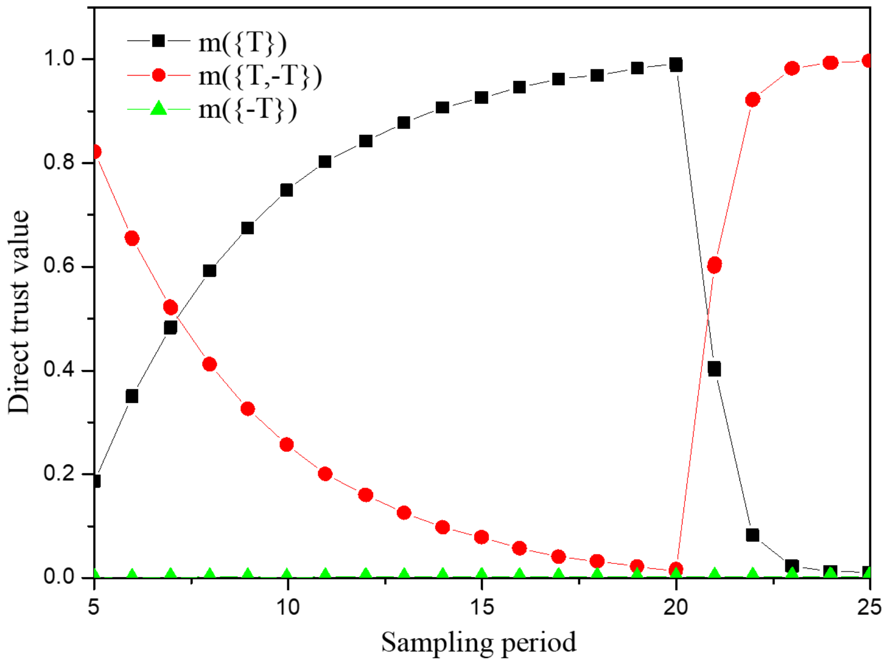

Fig. 3. Change of direct trust value under ON-OFF attack

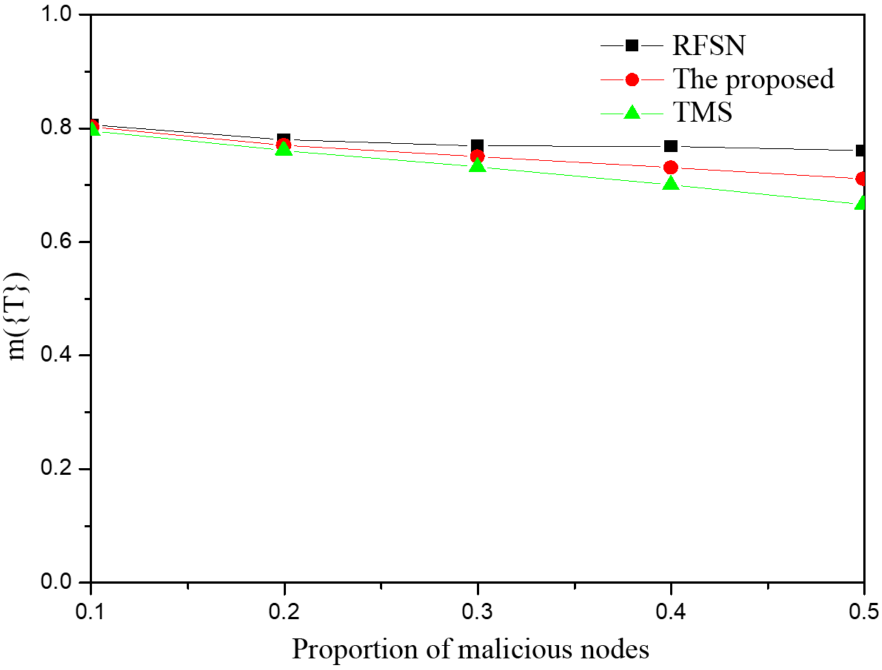

Fig. 4. Malicious nodes discrediting normal nodes

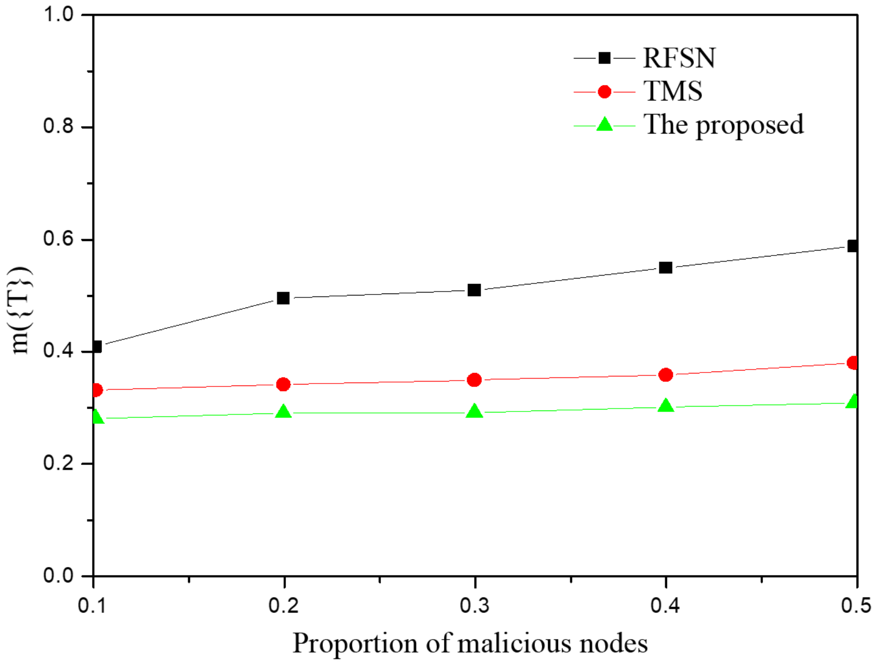

Fig. 5. Malicious nodes advocating malicious nodes

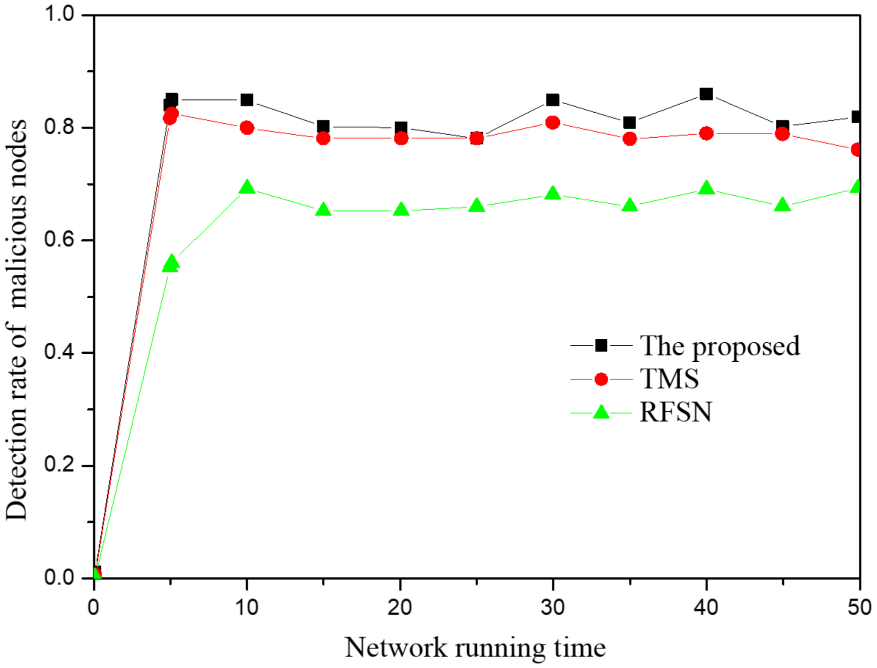

Fig. 6. Detection rate of malicious nodes

3 Implementation of Improved Bayesian Distributed Trust Evaluation Model

On the basis of the above, the typical Bayesian trust evaluation model is improved, mainly by modifying the abnormal attenuation factor, updating the sliding window and adaptive forgetting factor, and using the direct trust value reliability to judge the demand of indirect trust. Based on weight allocation of information entropy, the improved model is verified and analyzed by simulation.

3.1 Model algorithm flow

This model is mainly to observe and count the normal and abnormal behavior of nodes, and judge in cooperation with the behavior recommended by the third party, which is only started when the direct trust level is insufficient, so that the energy consumption of the node can be reduced, and the detailed algorithm flow is shown in Figure 7.

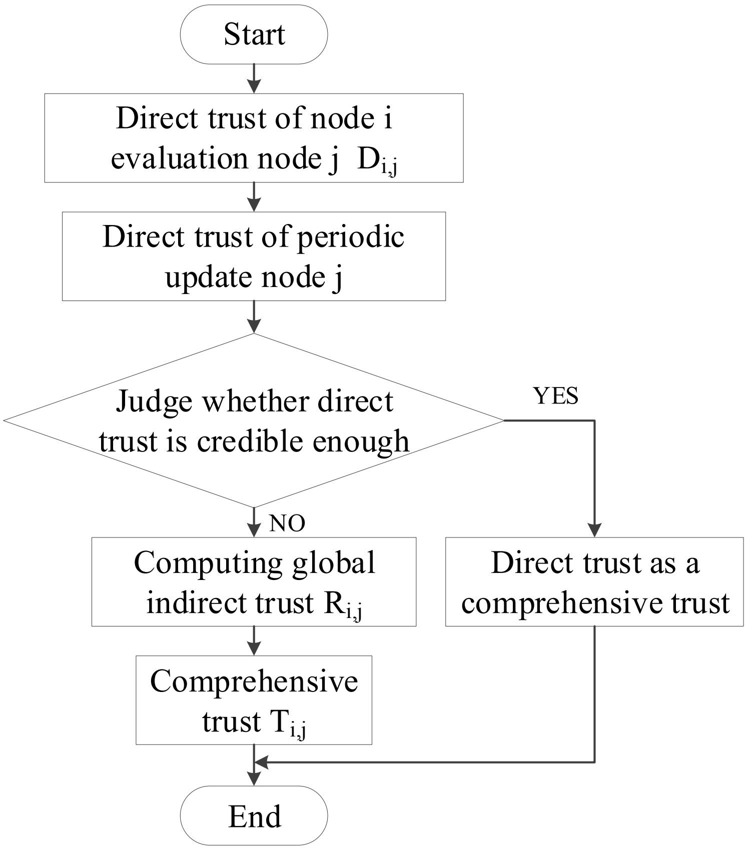
Start
Direct trust of node i evaluation node j $D_{i,j}$
Direct trust of periodic update node j
Judge whether direct trust is credible enough
YES
NO
Computing global indirect trust $R_{i,j}$
Direct trust as a comprehensive trust
Comprehensive trust $T_{i,j}$
End

Fig. 7. Flow chart of improved algorithm

3.2 Simulation experiment and analysis of results

The improved trust model is simulated and compared with the literature (Denko, M.K., et al, 2011). The experimental parameters are set as shown in Table 4.

Table 4. Simulation parameters

Parameter	Data
Forwarding rate	[0.9,1.0]
Initial energy of node E_{init}	0.5J
Transmission and reception of energy consumption E_{elec}	50nJ/bit
Amplifier power consumption ε_{amp}	10pJ/bit/m^2
Simulation area	100*100
Number of nodes	100
Number of malicious nodes	0-20%
Node radius	30
Packet size	100

Trust value of nodes. Firstly, the node trust value with the change of the sampling period is analyzed, and the trend is shown in Figure 8. It can be seen from the figure that the trust value of normal node gradually increases and the trust value of malicious node gradually decreases, which indicates that normal node and malicious node can be effectively identified and detected in the area of experiment simulation.

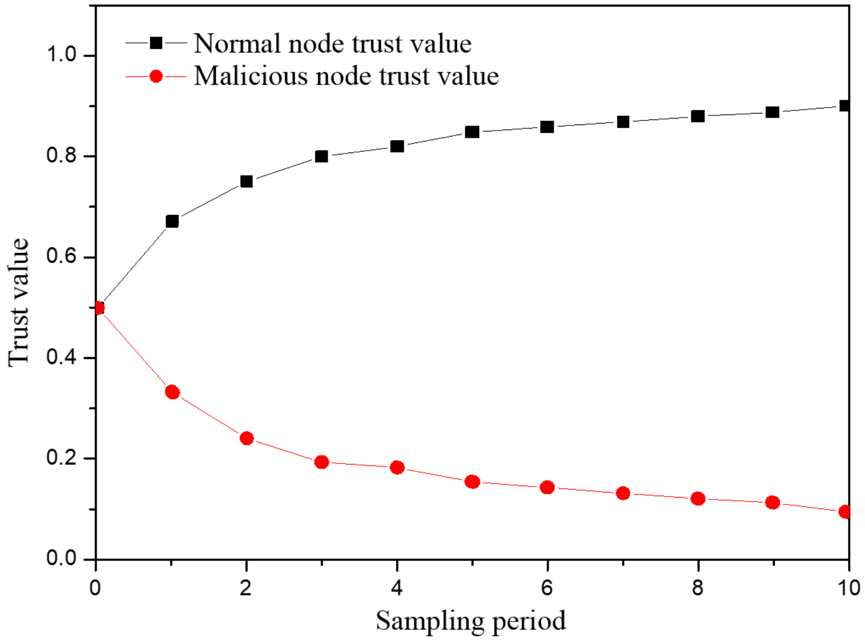

Fig. 8. Trend of node trust change

Confidence level. In order to investigate the rationality of this confidence level, the improved model is compared with the model in the literature (Denko, M.K., et al, 2011), and the results are shown in Figure 9. It can be seen from the figure that the direct trust value and the confidence level of the direct trust in the literature are basically the same, but the confidence level of the direct trust in the improved model tends to increase as the number of node interactions increases. Therefore, compared with the model in the literature, the improved model can recognize the confidence level of nodes with the same trust value and distinguish nodes more effectively.

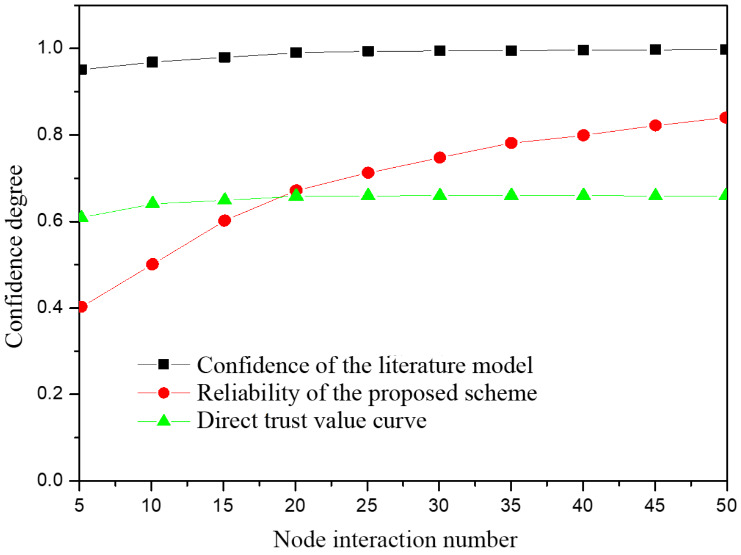

Fig. 9. The tendency of confidence to change under different number of interactions

Detection rate and detection error rate. In order to identify malicious nodes in wireless sensor networks, trust quantization is performed on the nodes, and two indexes of detection rate and detection error rate are formed. The improved model is compared with the model without abnormal attenuation factor and the model in the literature [15], and the analytic results are shown in Figures 10 and 11.

As can be seen from Figure 10, the detection rate of malicious nodes in all three models decreases as the proportion of malicious nodes increases. Among them, the model in the literature [15] is the fastest, followed by the model without abnormal attenuation factor, and the improved model is relatively stable.

This is because only good reputation is considered in the model of trust fusion in literature, and the improved model makes use of information entropy and abnormal attenuation factor to compare and measure the information, so the detection rate is the highest.

As can be seen from Figure 11, the detection error rate of the three models for malicious nodes increases with the increase in the proportion of malicious nodes. However, the improved model has the smallest increase amplitude and the lowest detection error rate, which is because the abnormal attenuation factor eliminates the change of node trust due to abnormal behavior and realizes higher detection rate and lower detection error rate.

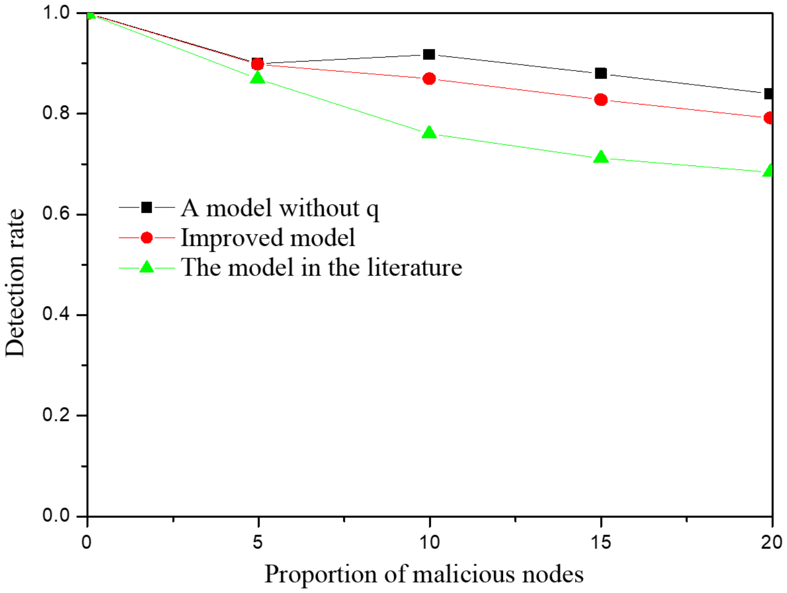

Fig. 10. Contrast diagram of detection rate

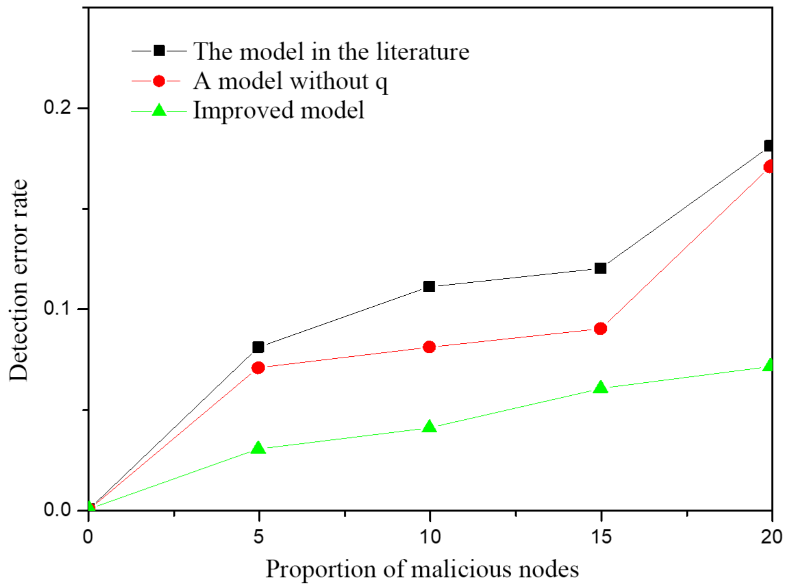

Fig. 11. Comparison diagram of detection error rate

Influence of anomaly attenuation factors. In order to further study the influence of the attenuation factor on the detection rate and the detection error rate, it is verified by many experiments with the results shown in Figure 12.

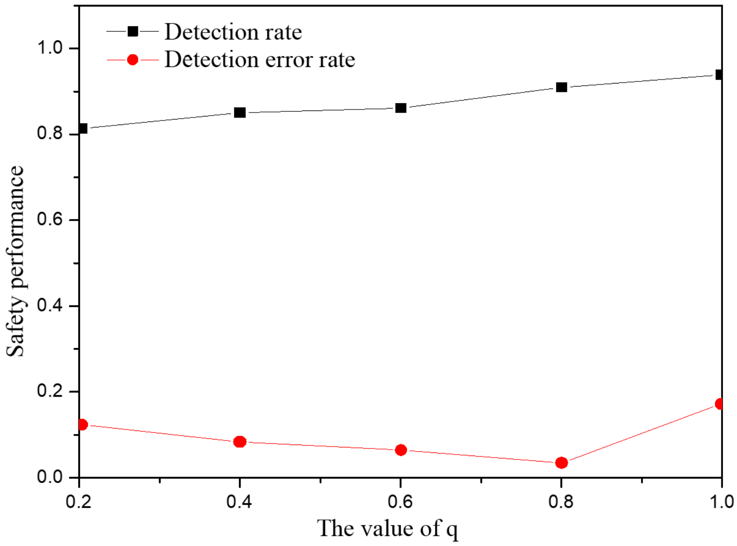

Fig. 12. The effect of abnormal attenuation factor on detection rate and detection error rate

As can be seen from Figure 12, as the abnormal attenuation factor increases, the detection rate gradually increases, and the detection error rate decreases first and then increases. This is because when the abnormal attenuation factor is lower, some malicious nodes cannot be recognized, while when the abnormal attenuation factor is higher, the abnormal nodes with non-intrusion factors are considered as malicious nodes. Therefore, it is necessary to take the value of the abnormal attenuation factor according to the specific environments. In this paper, when the abnormal attenuation factor is 0.8, the security performance of the network is the best.

Analysis of the energy consumption. At different ratios of malicious nodes, the energy consumption of the network is analyzed and compared with the results of the RFSN model. The results are shown in Figures 13 and 14.

As can be seen from Figure 13, as the simulation cycle progresses, the energy of the entire network tends to decrease. However, the energy consumption of the improved model is smaller than that of RFSN model. And as the proportion of malicious nodes increases, the energy of the entire network decreases.

As can be seen from Figure 14, when the simulation ends, as the proportion of malicious nodes increases, the energy remaining in the network gradually decreases, but is greater than the energy remaining in the RFSN model. This is because when the confidence level of direct trust is lower than its threshold, the calculation of indirect trust is started, which greatly saves the energy of the network and improves the usage time of the network.

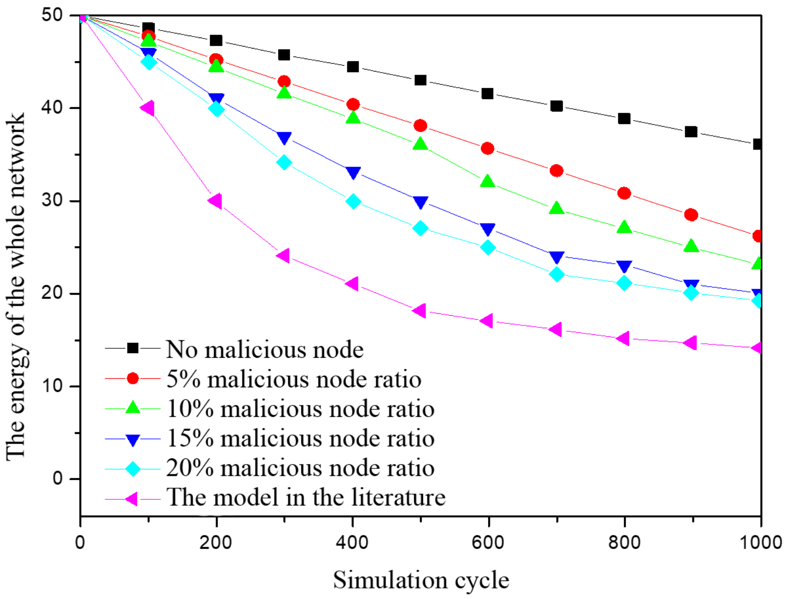

Fig. 13. Network energy consumption contrast diagram

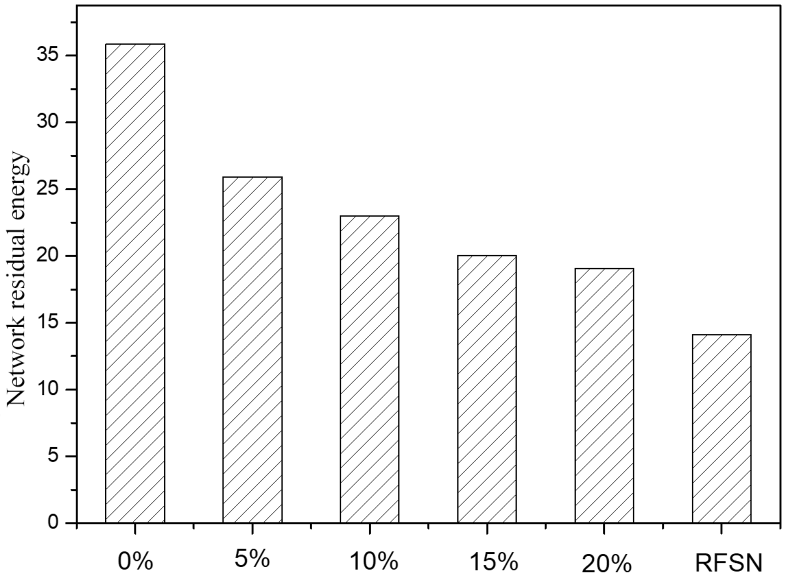

Fig. 14. Analysis of network residual capacity after 1,000 rounds

4 Conclusions

With the development of Internet of Things and artificial intelligence technology, the demand of wireless sensor network technology is increasing. At present, the research on wireless sensor networks is not thorough enough, and the objectivity and accuracy of trust evaluation model for network nodes are not enough. Based on this, this paper proposes a trust evaluation model with multi-factor comprehensive consideration and Bayesian model, an improved trust evaluation model, which solves the problems of factor singleness and imprecise evaluation in the original model, realizes the dynamic adaptability of the model, improves the network security performance and reduces the network energy consumption.

1. A trust model of multi-factor comprehensive evaluation is proposed. The node trust calculation, fuzzy division and fusion are carried out by means of trust factor, fuzzy set and D-S evidence theory, with the information security improved.
2. This paper proposes an improved model based on Bayesian theory, which is modified by abnormal attenuation factor, and updated by sliding window and adaptive forgetting factor, and the demand of indirect trust is judged by the confidence level of direct trust value, with allocated weights according to information entropy.
3. Experimental validation and analysis of the model show that the proposed model has good dynamic adaptability, higher detection rate, lower detection error rate, and less consumption of network energy, and better network security.

5 References

[1] Singh, J. (2015). Security issues in wireless sensor networks (wsn). Lecture Notes in Engineering & Computer Science, 2170(1): 40-40.

[2] Govindan, K., & Mohapatra, P. (2012). Trust computations and trust dynamics in mobile adhoc networks: a survey. IEEE Communications Surveys & Tutorials, 14(2): 279-298. https://doi.org/10.1109/SURV.2011.042711.00083

[3] Mármol, F. G., & Pérez, G. M. (2012). Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network & Computer Applications, 35(3): 934-941. https://doi.org/10.1016/j.jnca.2011.03.028

[4] Chen, I. R., Guo, J., Bao, F., & Cho, J. H. (2014). Trust management in mobile ad hoc networks for bias minimization and application performance maximization. Ad Hoc Networks, 19: 59-74. https://doi.org/10.1016/j.adhoc.2014.02.005

[5] Komathy, K., & Narayanasamy, P. (2008). Trust-based evolutionary game model assisting aodv routing against selfishness. Journal of Network & Computer Applications, 31(4): 446-471. https://doi.org/10.1016/j.jnca.2008.02.002

[6] Duan, J., Gao, D., Yang, D., Foh, C. H., & Chen, H. H. (2017). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for iot applications. IEEE Internet of Things Journal, 1(1): 58-69. https://doi.org/10.1109/JIOT.2014.2314132

[7] Yu, H., Shen, Z., Miao, C., Leung, C., & Niyato, D. (2010). A survey of trust and reputation management systems in wireless communications. Proceedings of the IEEE, 98(10): 1755-1772. https://doi.org/10.1109/JPROC.2010.2059690

[8] Bao, F., Chen, I. R., Chang, M. J., & Cho, J. H. (2012). Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Transactions on Network & Service Management, 9(2): 169-183. https://doi.org/10.1109/TCOMM.2012.031912.110179

[9] Li, X., Zhou, F., & Du, J. (2013). Ldts: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE Transactions on Information Forensics & Security, 8(6): 924-935. https://doi.org/10.1109/TIFS.2013.2240299

[10] Tajeddine, A., Kayssi, A., Chehab, A., Elhajj, I., & Itani, W. (2015). Centera: a centralized trust-based efficient routing protocol with authentication for wireless sensor networks†. Sensors (Basel, Switzerland), 15(2): 3299-3333. https://doi.org/10.3390/s150203299

[11] Duan, J., Gao, D., Foh, C. H., & Zhang, H. (2013). Tc-bac: a trust and centrality degree based access control model in wireless sensor networks. Ad Hoc Networks, 11(8): 2675-2692. https://doi.org/10.1016/j.adhoc.2013.05.005

[12] Ishmanov, F., Malik, A. S., Begalov, B., & Begalov, B. (2015). Trust management system in wireless sensor networks: design considerations and research challenges. Transactions on Emerging Telecommunications Technologies, 26(2): 107-130. https://doi.org/10.1002/ett.2674

[13] Jadidoleslamy, H. (2015). Tms‐hcw: a trust management system in hierarchical clustered wireless sensor networks. Security & Communication Networks, 8(18): 4110-4122. https://doi.org/10.1002/sec.1327

[14] Qi, J., Yong, T. L., & Zhong, C. (2008). Trust management in wireless sensor networks. Journal of Software, 19(7): 1716-1730. https://doi.org/10.3724/SP.J.1001.2008.01716

[15] Denko, M. K., Sun, T., & Woungang, I. (2011). Trust management in ubiquitous computing: a bayesian approach. Computer Communications, 34(3): 398-406. https://doi.org/10.1016/j.comcom.2010.01.023

6 Author

Jinghua Zhu is with the Hunan Mechanical & Electrical Polytechnic, Changsha 410000, China, she is mainly focused on research direction intelligent algorithm and computer application technology, electronic commerce. Teachers from Hunan Mechanical and Electrical Polytechnic have published more than ten papers on electronic commerce and computer application technology. (E-mail: 7006612@qq.com)

Article submitted 16 October 2017. Resubmitted by the authors 29 November 2017. Final acceptance 23 February 2018. Final version published as submitted by the author.