Security Optimization of Wireless Sensor Networks Based on Cloud Platform

https://doi.org/10.3991/ijoe.v14i02.8201

Rong Shi(✉)
Suzhou Institute of Industrial Technology, Suzhou, Jiangsu, China
rsrongshirs@126.com

Wang Xi
Suzhou Institute of Industrial Technology, Suzhou, Jiangsu, China
Soochow University, Suzhou, China

Abstract—In order to improve the security of wireless sensor network, the trust model of wireless sensor network based on cloud theory is established. The similarity comparison algorithm is introduced. Trust is expressed as a quantitative value. The new update function is designed to make the acquisition of trust more reasonable. In the research method and algorithm design, the wireless sensor network is different from the traditional network security. The balance problem of wireless sensor network security in algorithm computing strength and security intensity is studied. The results show that the trust model has good robustness. It can identify the malicious nodes accurately and quickly, and prevent the network from being destroyed. Therefore, the idea of cloud theory can effectively improve the security of the network.

Keywords—cloud platform, wireless sensor, network security optimization, cloud theory

1 Introduction

Wireless sensor network is a new information acquisition and processing technology. It combines the logical information world with the objective physical world. As a new type of technology, wireless sensor networks have shown broad application prospects in many fields, as stated in [1-2]. In general, it is deployed in harsh environments, unmanned areas or enemy positions. Therefore, the safety of wireless sensor networks has aroused great concern. It presents researchers with a large number of challenging topics, as stated in [3-4].

In recent years, with the rapid development of cloud platforms, sensor networks and cloud computing technologies are closely integrated. Cloud computing technology has greatly expanded the application space of sensor networks. It provides a new idea for solving many limitations of sensor networks, as stated in [5]. Based on traditional fuzzy mathematics and probability statistics, a cloud model is proposed, which is a fixed exchange model. It organically combines the fuzziness and randomness of

qualitative concepts in natural language. The introduction of cloud theory brings new research direction to the field of network security. Cloud similarity algorithm is proposed to expand the application of the cloud. It has a certain theoretical value and practical significance. However, due to the characteristics of the cloud, the calculation accuracy of the algorithm is not high, and the calculation is expensive. Its application is limited.

Based on cloud similarity algorithm, a trust model of wireless sensor networks based on cloud theory is established. Trust is expressed in quantitative values. The new update function is designed to make the acquisition of trust more reasonable. At the same time, the simulation experiment is set up to verify the validity of cloud theory in improving network security.

2 State of the art

With the rapid development of low-power micro sensor technology, embedded computing technology and integrated circuit technology, low-cost micro sensors are self-organized into networks through wireless links. Wireless sensor networks (WSN) are the product of the combination of three technologies, computing, communication and sensor. At present, it has become an active research branch in the field of computer science. The wireless sensor network is composed of random distribution, which integrates the wireless nodes of data acquisition, data processing and data communication module. Through the sensors built in the nodes, the environment and the information of the monitoring objects are monitored, perceived and collected in real time. By means of wireless communication and self-organizing multi hop network, information is sent to the end users, so that the physical world, computer world and human society can be effectively connected.

At present, with the continuous improvement and development of all aspects of wireless sensor networks, it is widely used in the military, commercial and civil fields of, as stated in [6-8]. In the military field, wireless sensor networks are composed of dense, low-cost, randomly distributed nodes. Self-organization and fault tolerance prevent it from crashing the entire system because of the damage done by some nodes in a malicious attack. This is incomparable to the traditional sensor technology. It is suitable for the harsh environment of the battlefield. In the battlefield, the commander often needs to know the situation of the troops, weaponry and military supplies in a timely and accurate way. The sensor will collect the corresponding information and send the data to the command post through the aggregation node, and then forward it to the command department. Finally, the data of each battlefield are fused to form a complete battlefield situation map. During the war, surveillance of the conflict areas and military sites is very important. By laying a network of sensors, it observes the enemy secretly and closely. The information of the battle is quickly collected. In the field of environment, wireless sensor networks provide convenience for field random data acquisition, such as tracking migration of migratory birds and insects, studying the impact of environmental change on crops, and monitoring the composition of ocean, air and soil. Several sensors are used in the ALERT system to monitor rainfall,

water level and soil moisture, and to predict the possibility of flash floods. In addition, the wireless sensor network can also accurately and timely forecast forest fire. Wireless sensor networks (WSN) can also be used in fine agriculture to monitor the pests in crops, the acidity of the upper soil, and the status of fertilization. On the medical side, the patient is equipped with a special purpose sensor node, such as heart rate and blood pressure monitoring equipment. Using wireless sensor networks, doctors can always understand the patient's condition. It is also possible to use wireless sensor networks to collect human physiological data for a long time. These data are very useful in the development of new drugs. The micro sensor nodes installed on the monitored objects will not bring too much inconvenience to human normal life. In commercial applications, wireless sensor networks also provide a lot of opportunities for them. At present, wireless sensor networks have been successfully applied to urban vehicle monitoring and tracking systems. A research institute in Germany has developed an auxiliary system for football referees, using wireless sensor network technology, to reduce the misjudgment rate of offside and goal in football matches. In addition, in many areas such as disaster rescue, warehouse management, interactive Museum, interactive toys, factory automation production line and so on, WSN will develop a new design and application mode.

In the application of commercial and military fields, security is the premise of application, such as bank protection network. In military deployments, sensor networks need to be protected from data collection, data storage, data transmission, and even the physical distribution of nodes, so that they cannot be understood by unrelated or enemy personnel. Otherwise, it can cause information leaks and decision errors. Obviously, for these applications, security issues can have catastrophic consequences if they cannot be solved. The characteristics of wireless sensor networks determine that it is very different from the traditional network security in the research methods and algorithm design. In algorithm computing strength and security strength, the proper balance is the main challenge of wireless sensor network security.

In summary, wireless sensor networks and traditional network security in the research methods and algorithm design is different. The balance problem of wireless sensor network security in algorithm computing strength and security strength must be solved. Based on cloud similarity algorithm, a trust model of wireless sensor networks based on cloud theory is established. Trust is expressed in quantitative values. The new update function is designed to make the acquisition of trust more reasonable. At the same time, simulation experiments are set up to verify the applicability of cloud theory in improving network security.

3 Methodology

3.1 The definition and characteristics of trust

In everyday life, trust decisions happen almost daily. Trust is a complex concept, which comes from social science. In information technology, trust can be defined as a

judgement of the reliability, safety, dependability and ability of entity behavior in a specific environment. The main features of trust are:

First, subjectivity. Trust is a judgment based on its own knowledge and experience. All trust is subjective in nature. Different entities may have different trusts for the same target entity.

Second, dynamic. Trust is related to time. It is based on a certain amount of time. Trust changes as time changes. This change is a process of slow rise and rapid drop.

Third, transitivity. Trust can be delivered. If entity A trusts B, B trusts C, B can recommend C to A, so that A trusts C.

Fourth, contextual relevance. Any one trust is associated with a certain content. With the change of context, an entity cannot immediately and clearly judge the impact of the change of the target entity, which brings difficulties to the study of trust.

The trust mechanism is the basis for the exchange, work and study of human beings in human society. The trust value can be gradually obtained through frequent contact between people. There is a gradual formation of trustworthy relationships between people, and it tends to listen to trusted beliefs from third parties about each other. Trust value one can be used as a key factor in judging human behavior in current complex social relations, and it can further guide the behaviors between people.

In wireless sensor networks, the cryptosystem based security system cannot effectively handle the attacks from the network and identify the malicious nodes. Therefore, the trust model, as an important supplement to this system, has come into being. Trust model has significant advantages in solving internal attacks in wireless sensor networks, identifying malicious nodes, selfish nodes, and improving system security and reliability. However, trust relationship is a very difficult and abstract mental cognition. When the trust relationship between entities cannot be clearly defined, it is unstable. Furthermore, the research on the trust model of wireless sensor networks is a very challenging task.

3.2 Calculation and updating of credibility

At present, although some of the corresponding trust models have been proposed, they are not ideal. In particular, trust is a qualitative concept. Its fuzziness is difficult to accurately describe and verify. Its subjectivity makes the trust of great randomness. The membership cloud model integrates the fuzziness, randomness and uncertainty of qualitative concept together, and realizes qualitative and quantitative transformation between concepts. It can provide valuable methods for trust research. In addition, the interval based cloud similarity comparison algorithm can effectively improve the accuracy and reduce the complexity of the computation. Therefore, the cloud theory is introduced into the security field of wireless sensor networks. A trust model based on cloud theory is proposed.

The first stage: the calculation of credibility

After the nodes are deployed in the network, each node begins to carry out the data transmission. At the same time, the node monitors some of the behavior attributes of the neighbor nodes in each time period. The information is stored in a matrix. After n time periods, the behavior attribute monitoring matrix of node i on node j is (1):

$$Xij = \begin{vmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{11} & x_{12} & \cdots & x_{1n} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{vmatrix} \tag{1}$$

Among them, the number of rows m is the number of attributes. The number of columns n is the number of time periods experienced.

When node i evaluates the credibility of j, it also needs to obtain the trustworthiness of j from other neighbor nodes, so the credibility obtained is indirect credibility. A schematic diagram of indirect credibility is shown in Figure 1.

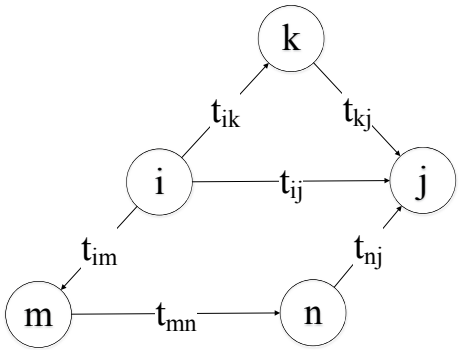

Fig. 1. A schematic diagram of indirect credibility

As shown in Figure 1, if nodes k and m are neighbor nodes that interact with node i, the i requests the two to pass on their credibility to the node j. Among them, k and j have a direct interaction, and m and j have no history of interaction. m neighbor nodes n and j have an interaction history. Therefore, m first obtains the credibility of j from n, and then gives this credibility to node i. In this example, the credibility of access to node i is expressed as formula (2):

$$t_{i,j}^{indirect} = t_{i,k}^{direct} \times t_{k,j}^{direct} + t_{i,m}^{direct} \times \left(t_{m,n}^{direct} \times t_{n,j}^{direct} \right) \tag{2}$$

The total trustworthiness can be obtained by adding the direct trust and the indirect trust weight as formula (3):

$$t_{i,j} = \omega_1 \times t_{i,j}^{direct} + \omega_2 \times t_{i,j}^{direct} \left(0 < \omega_1, \omega_2 < 1, \omega_1 + \omega_2 = 1 \right) \tag{3}$$

The second stage: renewal of credibility

After a reliability calculation, the node i keeps the credibility of the node j. After a period of interaction, the node i calculates the credibility of the j again. The credibility needs to be updated at this point. Update function is $t_{new}=\omega t_1+(1-\omega)\ t_2$, $0<\omega<1$. t_1 is the credibility of the previous one. t_2 is the credibility of the calculation. ω is a time attenuation factor. t_{new} is between the two. When $\omega<0.5$, the credibility of historical records accounts for less weight. The process of updating reliability with time attenuation is formed. It is in line with people's understanding of trust.

After a series of collation, the update function is obtained (4):

$$t_{new}=\begin{cases}\left[(n+\omega-1)t_1+(1-\omega)t_2\right]/n, & t_1\geq t_2\\ (1-m+m\omega)t_1+m(1-\omega)t_2, & t_1>t_2\end{cases} \tag{4}$$

The values of n and m can be set according to specific needs.

3.3 The basis for judging the reliability of nodes

Before the robustness of the trust model is detected, the cloud model can detect the abnormal behavior. The behavior attribute is used as the basis of the evaluation of the trust model. Cloud models can monitor behavior rules:

First, message conflict rules. The number of conflicts should be kept in a reasonable range. Too much conflict may be a collision attack for malicious nodes to disturb the channel. If there is no message conflict for a long time, it is possible to attack the black hole to attract the normal node to send data to it.

Second, retransmit rules. The number of nodes that allow the normal node to retransmit the last packet should be within a reasonable range. Otherwise, it may deplete the normal node energy of malicious nodes or the black hole attack launched by malicious nodes, attracting normal nodes.

Third, data information rules. Between the adjacent nodes, the data content of the communication should have the similarity, and the numerical deviation will be in a reasonable range. The large deviation of numerical value is likely to use the selective forward attack to tamper the data information for the malicious nodes.

Fourth, the rule of routing hops. In a wormhole attack, two malicious nodes cooperate with each other, which covers the actual distance. In the normal node, the transmission through the wormhole has fewer hops and lower delay. Therefore, the hop number of nodes should be kept in a reasonable range.

The above four attribute rules require a reasonable scope as a qualification. The formation is most reasonable at the peak, and the distance from the peak is more likely to be a malicious attack. Such features conform to the attributes of the cloud representation. Therefore, the above attribute rules can be used as the trust cloud to judge the reliability of the node.

3.4 Setting of experimental environment and experimental parameters

The MATLAB simulation platform is adopted and implemented in M language. In the experiment, the network model is as follows:

200 sensor nodes are randomly deployed in a 100 * 100 square area, and the converging node is located at the upper left corner of the region. Both the sensor nodes and the aggregation nodes are static, that is, the movement of position no longer occurs after deployment. All nodes are isomorphic. They have the same physical structure unit and energy, and have data fusion function.

The experiment will use the real data collected by 54 Mica2Dot sensor nodes. These data are collected every 30 seconds, including humidity, temperature, light and voltage. In these data, the temperature values are screened separately, and the noise value obeying the normal distribution is added to simulate the data value of the abnormal sensor nodes.

The experimental data are collected every 30 seconds. In this experiment, a reliability calculation is carried out every 10 minutes, that is, each calculation contains 20 data as the research domain of the cloud model.

First, the parameters in the trust model are set. After the statistical analysis of the global data, the trust base cloud of the temperature is obtained. The similarity between the cloud of every 20 temperature dates and the trust base cloud is more than 0.6. Therefore, the credibility of the threshold value is set to 0.6. In addition, the weights ω_1 and ω_2 of direct trust and indirect trust in the model are 0.8 and 0.2, respectively. The time attenuation factor of the update function ω is 0.3. The values of n and m in the update function are now discussed. Here, the m is set to 1, and the value of n is studied. A large segment of data in the data is used as the domain of research. The effect of the reliability on the updated function is observed in the case of n taking different values.

When n=4, As the normal set of data is too slow, the reliability value becomes unbelievable. There is a false judgment. Therefore, the n value in the case of greater than or equal to 4 has a greater impact on the credibility distortion, which is easy to lead to misjudgment. When n=3, In the period from 3 to 5, the calculated reliability is only up to 0.05, even if it rises for three periods of time. The small rise in the range is not conducive to the improvement of the "enthusiasm" of the nodes. Therefore, in this experimental environment, the n value is 2, that is, the increase is changed to the original 1/2. The influence of rising coefficient n on reliability is shown in Figure 2.

4 Result Analysis and Discussion

4.1 Comparison of two data reliability calculations by CTM

After determining the parameters, the anti-attack test of CTM is carried out. The reliability curve of the normal data and malicious data is calculated by CTM, as shown in Figure 3.

Although the reliability of the normal data calculated by the CTM has some fluctuations, the fluctuation range is not large. It is stable and greater than the threshold.

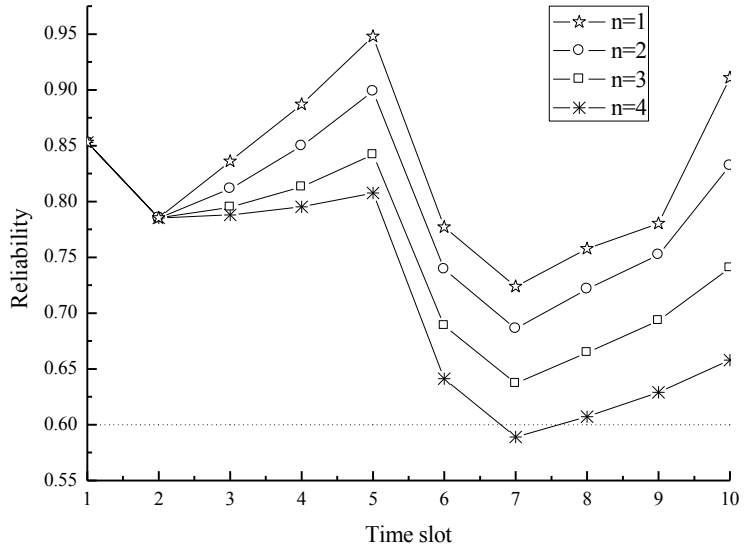

Fig. 2. The influence of rising coefficient n on reliability

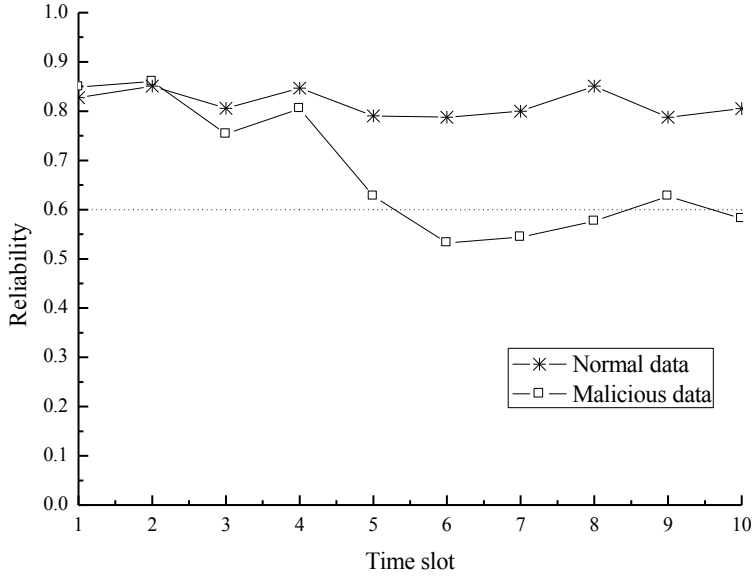

Fig. 3. Comparison of two data reliability calculations by CTM

The data of malicious nodes fluctuate greatly, and the damage behavior is found. In the calculation of the sixth degree of credibility, it is judged by CTM as a malicious node. Since then, the malicious nodes try to hide their behavior and be accepted by the network by improving their credibility. However, when it reaches a threshold, the node has been isolated by the network. Therefore, the trust model designed in this paper is effective and reasonable, and the algorithm is stable.

4.2 The influence of evil mouth attack on CTM reliability calculation

Evil mouth attack is a common type of attack in the trust model. In the process of obtaining indirect credibility, its neighbor nodes are malicious nodes. The node maliciously destroys the other nodes, and the reliability of the transfer is very low. Its purpose is to make the node believe that the normal node to be calculated is a malicious node. The influence of evil mouth attack on CTM reliability is shown in Figure 4.

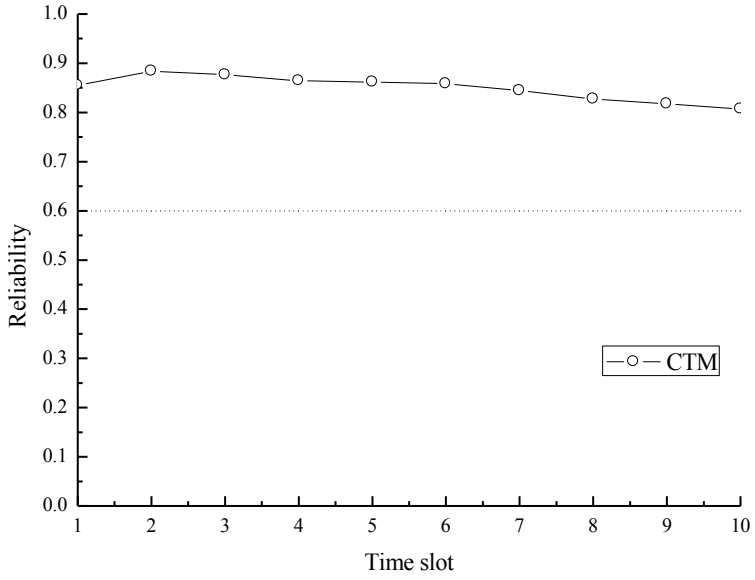

Fig. 4. The influence of evil mouth attack on CTM reliability

In the process of reliability integration, the direct credibility of node computing occupies a large proportion. When dealing with the evil mouth attack, the credibility is reduced, but the decrease is very small. It has little effect on the low destruction of normal nodes. Therefore, the evil mouth attack is suppressed, which shows the robustness of the CTM.

4.3 The influence of the update function on the reliability calculation

A renewal function with slow ascending and descending property is designed in credibility updating. It can identify earlier when nodes have malicious behaviors, and reduce the damage of malicious nodes to the network. In the experiment, the reliability of the data sent by the same group of malicious nodes is calculated. When n=l, the extent of the rise and decline of credibility is the same, that is, the original update function. After the ninth update, the credibility is below the threshold. It is judged to be a malicious node. After the tenth update, the malicious node disguised its behavior. The reliability value is above the threshold value. Malicious nodes are accepted by the

network. When n=2, the CTM model adopts the slow rise and fast drop update function. After the sixth update, the value of the credibility is close to the threshold. After eighth and ninth updates, the node has been identified as a malicious node. It is too late to try to disguise its behavior. Even if the credibility increased after the tenth update, the threshold was not reached. The CTM model can quickly and effectively identify and contain malicious nodes. It is isolated from the network as early as possible, thereby reducing the damage to the network. The influence of the update function on the reliability calculation is shown in Figure 5.

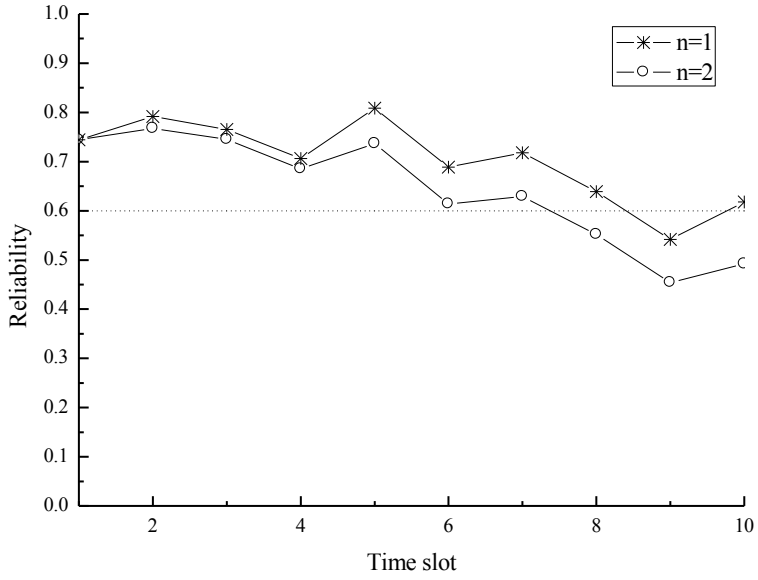

Fig. 5. The influence of the update function on the reliability calculation

4.4 Comparison of the reliability of CTM calculation in two cases

In a complex sensor network environment, the accidental error of the node often occurs. A good trust model should have a certain fault tolerance, which separates the accidental error from the malicious behavior area, and makes the calculation more accurate. The error of the normal node is incidental. Even if this is a mistake, it does not affect the next action. There is no connection between the two acts. Malicious nodes have destructive behavior in the network. The behavior of malicious nodes is sometimes good and sometimes bad. The intention is to carry out an attack on the premise of maintaining a high degree of trust. Some malicious nodes can implement a high degree of trust through good behavior for a period of time and implement attacks. This attack takes advantage of the dynamic characteristics of trust, and achieves the attack effect through the inconsistency in the time domain. Comparison of the reliability of CTM calculation in two cases is shown in Figure 6.

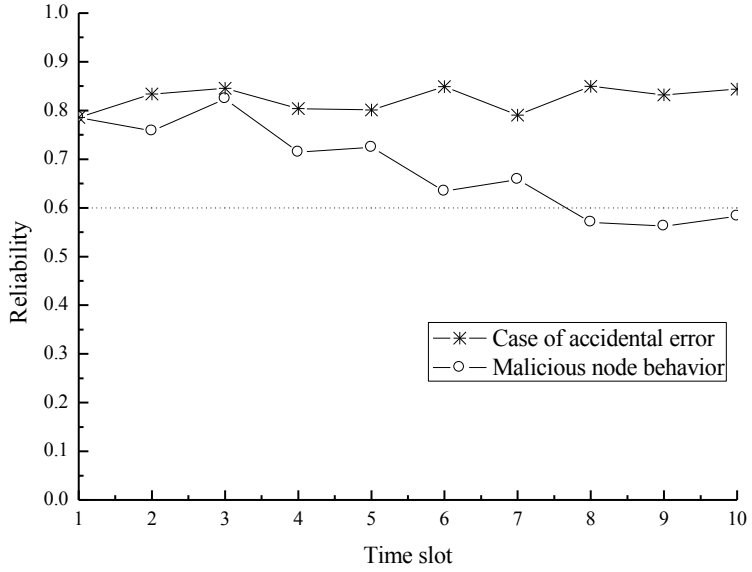

Fig. 6. Comparison of the reliability of CTM calculation in two cases

Figure 6 compares the reliability of CTM in the occurrence of accidental and malicious behavior. In case of a node accidental error, though there is a fluctuation in the calculation of credibility, the overall change is not large. The credibility of the malicious nodes calculated by CTM has a downward step phenomenon. After a malicious act, it tries to disguise identity through a small amount of normal behavior. However, under the update mechanism, the ultimate credibility is below the threshold. The identity of a malicious node is identified and isolated from the network.

5 Conclusions

Based on the current research status of wireless sensor network security technology at home and abroad, the security optimization of the cloud platform in wireless sensor networks is studied. On the basis of similarity comparison algorithm, a trust model based on cloud theory is established. The node constructs the trust cloud of the neighbor nodes and calculates the similarity between the node and the trust base cloud. In the process of updating reliability, on the basis of the original update function, the character of "slow rise and fast drop" is achieved by reducing the rise range. The simulation experiments show that the model has good robustness. It can quickly and accurately identify the malicious nodes in the network to prevent the network from being destroyed. The research of wireless sensor network security technology is a frontier technology topic in the field of network. Cloud theory is introduced into wireless sensor networks. The experiment shows that the idea of cloud theory can effectively improve the security of the network.

6 Acknowledgement

This paper was supported by National Natural Science Foundation of China (No 61702351), China Postdoctoral Science Foundation (No.172985), Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No. 17KJB520036), Jiangsu Planned Projects for Postdoctoral Research Funds (No. 1701172B), and Application Foundation Research of Suzhou of China (No. SYG201653).

7 References

[1] Chen, J., & Huang, L. (2013). A fault-resilient method for wireless sensor networks in pervasive computing.Sensor Letters,11.5: 853-861. https://doi.org/10.1166/sl.2013.2655

[2] Chung, W. Y., Yu, P. S., & Huang, C. J. (2013). Cloud computing system based on wireless sensor network.Computer Science and Information Systems,877-880.

[3] El-Emary, I. M. M., Husain, K. Q., & Alyoubi, B. A. (2012). Security issues of wireless sensor networks in various applications.International Journal of Academic Research,4: 317-328. https://doi.org/10.7813/2075-4124.2012/4-6/A.45

[4] Ma, J. (2016). Security issues of wireless sensor networks based on target tracking.International Journal of Online Engineering, 12: 97. https://doi.org/10.3991/ijoe.v12i10.6211

[5] Othman, S. B., Trad, A., & Youssef, H. (2014). Security architecture for at-home medical care using Wireless Sensor Network.Wireless Communications and Mobile Computing Conference,304-309. https://doi.org/10.1109/IWCMC.2014.6906374

[6] Roy, S., & Nene, M. J. (2015). A security framework for military application on infrastructure based wireless sensor network.IEEE International Conference on Research in Computational Intelligence and Communication Networks,369-376. https://doi.org/10.1109/ICRCICN.2015.7434266

[7] Xu, W., Yang, Z., & Wang, X. (2015). A technical and business perspective on wireless sensor network for manufacturing execution system.Mathematical Problems in Engineering,1-15. https://doi.org/10.1155/2015/267195

[8] Yu, C., Yao, D., Yang, L. T., & Jin, H. (2017). Energy conservation in progressive decentralized single-hop wireless sensor networks for pervasive computing environment. IEEE Systems Journal,11: 823-834. https://doi.org/10.1109/JSYST.2014.2339311

8 Authors

Rong Shi is with the School of Software and Services Outsourcing, Suzhou Institute of Industrial Technology, Suzhou 215011, Jiangsu, China.

Wang Xi is with the School of Software and Services Outsourcing, Suzhou Institute of Industrial Technology, Suzhou 215011, Jiangsu, China, and the School of Computer Science and Technology, Soochow University, Suzhou 215006, China

Article submitted 16 October 2017. Resubmitted by the authors 29 November 2017. Final acceptance 05 February 2018. Final version published as submitted by the authors.