Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 3, March 2019, pp. 949-958
DOI: 10.23940/ijpe.19.03.p24.949958

Random Unite Authentication for Multiple Nodes in Wireless Sensor Networks

Fan Zhang*

Zhengzhou Institute of Technology, Zhengzhou, 450000, China

Abstract

In a wireless sensor network, authentication of multiple nodes can effectively reduce the overhead of node communication and improve the security of wireless sensor network operation. However, when the node was authenticated by existing methods, the positional information of the node was easily exposed, resulting in a high calculation repetition rate and increased consumption of node communication. A random unite authentication method based on RSA and trusted nodes was proposed. The multi-node authentication model of the RSA method was used to effectively authenticate other nodes in the wireless sensor network. The node trust degree was introduced, and the node authentication key was updated by the identity-based and bilinear theory. After the trust reputation management based on the Beta distribution node was used to calculate the trust degree of the node, it was verified whether the trust degree of the communication node was trustworthy to the node; the verification result was identified. Finally, the method of combining symmetric cryptography with node information authentication code was used to implement trusted node authentication in wireless sensor networks. Experiments showed that the authentication node results of this mechanism were stable, which overcame the shortcomings of low stability of multi-node authentication results in the current method.

Keywords: wireless sensor network; multiple nodes; random; unite authentication; RSA

(Submitted on November 5, 2018; Revised on December 3, 2018; Accepted on January 2, 2019)

1. Introduction

A wireless sensor network is a distributed sensor network whose end is a sensor that can sense and inspect the outside world [1]. It is a multi-hop mobile ad hoc network composed of a large number of sensor nodes. It is generally arranged in areas where people are not easily reachable in harsh environments and unmanned areas. It has the advantages of low cost, fast deployment and strong fault tolerance [2]. It can be widely used in defence military, environmental monitoring, field investigation, anti-terrorism relief and other fields. Although it has broad application prospects, security issues have always been a constraint to its development. Due to the low power consumption of sensor nodes, and its energy, computing and storage capabilities are very limited. How to design a multi-node random unite authentication method for wireless sensor networks of various scales and different application scenarios has become an important research topic in the case of the unique working mode of wireless sensor networks and limited sensor node resources [3]. The security threat is mainly caused by the low cost of the wireless sensor network, the low power consumption of the sensor node, the low speed of computing network load, and the small storage space. The environment of open applications and the performance of limited nodes make the network vulnerable to attack, which leads to the design of wireless network security mechanisms in a harsh environment.

If we want to improve the environment of wireless network security mechanism design, node authentication is an important method for wireless sensor network operation security area research. Node random authentication can effectively suppress attacks generated outside the network [4]. At present, there are some achievements in wireless sensor network node authentication, but the existing methods have the problems of high energy consumption of the network and high communication overhead of the wireless sensor network. To this end, this paper studies the multi-node random unite

* Corresponding author.
E-mail address: coolzf@163.com

authentication method of wireless sensor networks. In the wireless sensor network node authentication scheme proposed by Huang et al., the node trust degree was calculated by the security action coefficient and the frequency of interaction to prevent the abnormal node from disguising as a normal node [5]. It can make the node trust degree related to the behaviour of the current node, and avoid the node obtaining higher trust degree after fewer transaction times. When authenticating a sensor network node, the node identity, smart card, and password were combined. After the trusted node trusts, the trusted node and the user were authenticated by the node, and the trusted sensor node and the user and the gateway node were mutually authenticated. Now, the network user can replace the password at will. However, this method also had problems such as the user forgetting the password and low password security level.

Therefore, this paper proposed a multi-node random unite authentication method in wireless sensor networks. The method initialized the wireless sensor network and utilized the multi-node authentication model of the RSA method to perform effective high-speed authentication of other nodes in the wireless sensor network. The simulation results show that compared with the current node authentication scheme, the authentication scheme can resist external attacks and camouflage attacks. Computational complexity was low, and the network communication node consumed low.

2. Multi-Node Random Joint Authentication Method

Before multi-node random joint authentication in wireless sensor networks, multi-node data security needs to be verified and analysed. The data security verification of multi-node joint authentication in wireless sensor networks generally includes the following three types: ensuring multi-node data confidentiality, multi-node data integrity, multi-node data authenticity and freshness.

(1) Multi-node data confidentiality: Multi-node data confidentiality is one of the most important security issues in multi-node joint authentication methods in wireless sensor networks. All sensitive messages about node authentication should be kept confidential during storage or transmission. Any unauthorized user cannot know the true verification of the message. In wireless sensor networks, multi-node data confidentiality mainly includes the following two points: ensuring that sensitive multi-node sensing information is leak-free and ensuring sensitive multi-node protocol information without leakage. The usual way to guarantee data confidentiality is to encrypt. Only authorized users have a decryption key. This is the key to ensuring the confidentiality of sensitive nodes.

(2) Multi-node data integrity: Based on the guarantee of multi-node data confidentiality described in (1) above, the attacker will not be able to obtain the true content of the message, but the verifier cannot guarantee that the message it receives is complete. Multi-node data integrity is an important means of ensuring data is correct. By providing data integrity authentication, it can ensure that the multi-node data does not change during the verification process, thereby effectively preventing the interception, tampering, etc. of the malicious intermediate node.

(3) Multi-node data authenticity: The data integrity authentication process described in (2) above ensures that the data is correct but does not verify the authenticity of the data. The recipient cannot know if the message is from a legitimate sender. Therefore, a multi-node random joint method in a wireless sensor network is required to authenticate a message to ensure that the message originates from a legitimate sender.

(4) Multi-node data freshness: In a wireless sensor network, an attacker can intercept a legitimate message and send it again after a period of time, causing a replay attack. Therefore, the recipient needs to verify the freshness of the message to ensure that the message is sent by the sender. The message can be freshly updated by adding a random number or a timestamp to the sent message.

The above series of security verifications for multi-node data is the basis of the multi-node random joint authentication method. After the security verification, the wireless sensor network is initialized, and the multi-node authentication model of the RSA method is used to effectively authenticate other nodes in the wireless sensor network, thereby providing a better update mechanism [6]. The specific process is as follows.

2.1. Structure

RSA is currently the most influential public key encryption algorithm. It is capable of resisting most of the password attacks known to date and has been recommended by ISO as the public key data encryption standard [7]. The RSA algorithm is based on a very simple number theory fact. It is very easy to multiply two large prime numbers, but it is extremely difficult to factorize the product. So, the product can be exposed as an encryption key [8], which is the secret of RSA two-factor authentication. In this paper, it is applied to multi-node random joint authentication of wireless sensor networks, which

requires a trusted entity TA. For the wireless sensor node, select a point in the elliptic curve as the identifier id, after processing by the mapping function φ, a multi-node public key $P_X = \varphi(id_x)$. TA generates a master key s and calculates the communication node private key $S_X = sP_X$. Before the communication node of the wireless sensor network deploys, the identity of the node id_x and the private key S_X of the communication node are loaded for the communication node. Except for TA, only communication node X knows S_X. The network function is loaded as $\left(q, E/F_q, G_1, G_2, E, Q, H_1, H_1, F, \varphi\right)$, where q represents a prime number, and E represents a curve of an ellipse on the finite field F_q. G_1, G_2 represent the F_q group and the multiplicative group. e represents the mapping of the elliptic curve. W indicates that the generator is selected on the G_1. H_1 and H_2 represent different hash functions. f represents a function of a symmetric cipher. φ denotes a mapping function. After the wireless sensor network is deployed, each communication node broadcasts the identity *id* within the neighbourhood. The neighbour node saves to the received *id* and sets the initial value of the node parameter.

The use of e_i and $\left(d_i, n_i\right)$ indicates that the wireless sensor network generates private keys SK_i and PK_i. According to the characteristics of the RSA algorithm, $M = \left(M^e\right)^d \bmod n_i$, after m-node authentication, the encryption of the application node public key $\left(d_{new}, n_{new}\right)$ in d_{new} to K is expressed as:

$$K = \left(\left(\left(d_{new}{}^e \bmod n_1\right)^e \bmod n_2\right) L\right)^e \bmod n_m \tag{1}$$

In the last step of the node applying to join the wireless sensor network, the wireless sensor network will return the authentication result K in the Equation (1) to the requesting communication node through the route in the form of the list $\{ID_i\}$ (i = 1, 2, ⋯, m) of the authentication node for the communication node. Assume that the requested communication node $Node_{new}$ is recommended by m nodes, and $\left\{K, n_{new}, \left\{ID_1, ID_2, L, ID_m\right\} ID_{new}, S_{new}\right\}$ is used as the certificate of the node. Where K is the ciphertext after the part d_{new} of the node public key of the application is encrypted according to Formula (1). n_{new} denotes another part of the public key of the application communication node, and d_{new} constitutes the complete public key $\left(d_{new}, n_{new}\right)$ of the application node, ID_{new} is the identification of the application node in the wireless sensor network, and $\left\{ID_1, ID_2, \mathrm{L}, ID_m\right\}$ is a list of application node authentication qualifications. S_{new} indicates that the signature of the node after encrypting the private key $\left(e_{new}, n_{new}\right)$ to ID_{new} is expressed as:

$$S_{new} = (ID_{new})^e new \bmod n_{new} \tag{2}$$

After the node in the wireless sensor network receives the certificate, it searches for the storage qualification node $\left(ID_i, PK_i\right)$, and verifies the authenticity of the certificate according to Equation (3). Then, the node's certificate is valid if Equation (3) is true.

$$ID_{new} = S_{new}^{\left(K^{dm} \bmod e_m\right)^{d_{m-1} \bmod n_{m-1}}} \bmod n_{new} \tag{3}$$

In summary, the RSA-based multi-node authentication method is applied to multi-node random joint authentication in wireless sensor networks. The trusted entity 1 is required to process the mapping function 2 to obtain a multi-node public key and calculate the private key of the communication node. Before the communication node of the wireless sensor network is deployed, the communication node is identified, the communication node private key is set, and the network function is loaded into the wireless sensor network for deployment. Each communication node broadcasts the identifier 3 within the neighborhood and sets the initial value of the node parameter. The node applies to join the final link of entering the wireless sensor network, and the wireless sensor network passes the generated authentication result in Formula (1) through the list of the authentication node for authentication of the communication node and returns the route to the applied communication node. After the node in the wireless sensor network receives the certificate, it searches for the storage qualification node and determines whether the node certificate is valid according to Formula (3). If the judgment node certificate is valid, the multi-node random joint authentication method of the trusted node may be performed on this basis.

2.2. Multi-Node Random Joint Authentication Method based on Trusted Node

Regarding the multi-node random joint authentication method of trusted nodes, the reason for dividing time into time slices is to prevent selfish nodes from masquerading as normal nodes. Indirect trust is derived from the evaluation between nodes. The number of positive behaviours of nodes within a certain period of time recorded by the wireless sensor network node indicates the degree of frequent interaction between the nodes of the wireless sensor network at a certain moment. Enabling the communication node to obtain multiple praises can reduce the number of interactions of malicious communication nodes and obtain higher trust between multiple nodes [9]. Based on the credibility of the node recommendation, the accuracy of the information related to the recommended node is verified. According to the result of the interaction between the communication nodes, the wireless sensor network node is evaluated, and the behaviour of the communication node is expressed by the Beta distribution. On this basis, the time forgetting factor is introduced to adjust the impact on the reputation of the node, and the change of the Beta distribution parameter is obtained. The wireless sensor network is deployed according to changes in the distribution parameters. Analyse using existing geolocation-based authentication mechanisms. Introduce the concept of the area, divide the overall area of the wireless sensor network, and directly authenticate the adjacent nodes with the authentication key [10-11], so that it can operate with the wireless sensor network. The behaviour of the communication node and the reputation of the communication node change, and the communication node maintains the reputation at regular intervals. The wireless sensor network has an authentication key between multiple nodes for multi-node random joint authentication, which improves the security and authentication efficiency of the wireless sensor network. The specific process is as follows.

In the process of calculating the node trust degree, in order to prevent the selfish node from masquerading as a normal node, the time is divided into N time slices, the size of the time slice is T_1, and the total time is $T = NT_1$. The direct trust of a node is expressed as Equation (4).

$$DT_{ij}(t)=\begin{cases}\dfrac{\sum P_{ij}(t)}{\sum P_{ij}(t)+a\times\sum N_{ij}(t)}F_{ij}(t)\end{cases} \tag{4}$$

In Equation (4), $DT_{ij}(t)$ represents the indirect trust degree obtained by the communication node i evaluating the node j at t, $P_{ij}(t)$ indicates the number of positive behaviors of node j within t hours recorded by the wireless sensor network node i, $N_{ij}(t)$ represents the number of negative behaviors of node j within t hours recorded by the wireless sensor network node i, a indicates the coefficient of node security action, $F_{ij}(t)$ indicates the degree to which the wireless sensor network node i interacts with the node j frequently at time *t*. The communication node obtains multiple praises to reduce the number of malicious communication node interactions and achieve higher trust.

Assume that $\{K_1, K_2, K, L, K_N\}$ is the neighbouring node of the communication node i, and is also the neighbouring node of the communication node j.

(1) At time t, the superimposed node i directly trusts the communication node k_x, which is defined as $DT(t)=\sum_{x=1}^{N} DT_{ik_x}(t)$.

(2) At t o'clock, the indirect trust of the wireless sensor network communication node i to the communication node j is expressed as

$$DT_{ij}(t)=\frac{\sum_{x=1}^{N} T_{ik_x}(t)\cdot w(k_x)}{DT}$$

Where the credibility recommended by node k_x is $w(k_x)$, which proves the accuracy of the information related to the recommended node.

(3) β_{DT} is the weight of direct trust, β_{IDT} is the weight of indirect trust, and the trust degree of wireless sensor network node j is expressed as $T_w(t) = \beta_{DT} \times DT(t) + \beta_{IDT} \times IDT_{ij}(t)$.

(4) Set the initial trust threshold of the wireless sensor network to 0.6. If the node's comprehensive trust is less than the value, the node is not trusted, and vice versa.

According to the result of the interaction between the communication nodes, the wireless sensor network node is evaluated, and the reputation of the communication node behaviour is represented by the Beta distribution. The Beta distribution has two parameters, which are expressed as $Beta(\alpha, \beta) = f(x|\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)}$. The expected value of the Beta distribution probability is expressed as Equation (5).

$$E(x) = \alpha/(\alpha+\beta) \tag{5}$$

Wireless sensor network node interaction events occur in two ways, success or failure. The number of successful communication events is represented by r pair, and s indicates the number of failed communication events. After $r+s$ events, the posterior distribution of the wireless sensor network obeys the Beta distribution, and the parameters in the function need to satisfy $\alpha = r+1,\ \beta = s+1;\ s \geq 0$.

It is assumed that the probability that the communication node A has a priori distribution with respect to the reputation of the communication node B at time t_1 is X, subject to the Beta distribution, which can be recorded as $X \sim Beta(\alpha+1, \beta+1)$ .After t_2 time, the communication node A and the communication node B perform $r+s$ events. The wireless sensor network reputation distribution obeys the Beta distribution and the new distribution X' satisfies Equation (6).

$$X' = Beta(\alpha+r+1, \beta+s+1) \tag{6}$$

In Equation (6), the communication node reputation problem is not considered, and the time forgetting factor is introduced to adjust the influence of the node reputation. The change of the Beta distribution parameter is expressed as Equation (7).

$$\begin{cases} \alpha' = \alpha\theta + r \\ \beta' = \beta\theta + s \end{cases} \tag{7}$$

After the wireless sensor network is deployed, the neighboring nodes use the authentication key for direct authentication. With the operation of the wireless sensor network, the behavior of the communication node changes, the reputation of the communication node also changes, and the communication node maintains the reputation every once in a while. The maintenance method (r, s) is that the communication node A interacts with the node B according to the historical reputation parameter of the storage node B. As time changes t_2, node reputation becomes historical reputation. At t_3 o'clock, the new node reputation needs to be calculated. The node reputation can be updated using Equation (8).

$$\begin{cases} \alpha = \alpha\theta + r \\ \beta = \beta\theta + s \end{cases} \tag{8}$$

Although the trust relationship between nodes in the wireless sensor network is changing, the node trust value is fixed for a period of time. Therefore, before the multi-node 1 and 2 authentications, it is necessary to verify the node trust degree according to the preservation new reputation using $T = E(Beta(\alpha+1, \beta+1))$. If the node trust is lower than the trust threshold, the node is considered to be untrustworthy. Otherwise, the node is considered to be trusted, thereby completing random joint authentication of multiple nodes in the wireless sensor network, improving wireless sensor network security and authentication efficiency. According to the obtained Beta distribution parameters, combined with the node trust degree, the existing geographic location information-based authentication mechanism is introduced for analysis, and the geographic

information of the node stored by its neighbour nodes can be authenticated [12-13]. Each node is equipped with a GPS device, and the base station assigns an ID number to each node. Array $T = E(Beta(\alpha+1, \beta+1))$ can be used to indicate the identity geographic information of the node i. By calculating the distance G_{ij} between the nodes i and j to determine whether the node is the captured node, considering the difference in the accuracy of the device, the likelihood index L_{ij} is introduced by Equation (9), where ε is the largest measurement error, and R is the communication diameter of the node to be measured. The exact position of the node can be determined by $M_{ij} = \left(id - x_j, x_i\right) L_{ij}$. This information is sent to the neighbour nodes, which are the verifiers of node i, and the corresponding geographic coordinates are calculated using the one-way hash function H in Equation (10).

$$L_{ij} = \begin{bmatrix} 1 & G_{ij} \le R - 3\varepsilon \\ 0 & G_{ij} \ge R - 3\varepsilon \\ \dfrac{1}{2} + \dfrac{R - G_{ij}}{5\varepsilon} & \end{bmatrix} + T \tag{9}$$

$$\begin{cases} \left\langle x_{ij}, 1, y_{ij}, 1 \right\rangle = H_i\left(id_j, x_i, y_j\right) \\ \left\langle x_{ij}, 2, y_{ij}, 2 \right\rangle = H_2\left(id_j, x_i, y_j\right) \\ \cdots \\ \left\langle x_{ij}, m, y_{ij}, m \right\rangle = H_m\left(id_j, x_i, y_j\right) \end{cases} \tag{10}$$

After collecting all the information of node i, each certifier node combines all the authentication information, and the merging possibility index is calculated as $L_j = \sum_{i=q}^{n} L_{ij} \left| n \right.$. When the number of certifiers' response information exceeds the set threshold, it indicates that node 1 is successfully authenticated. The network overhead model adopted by this authentication method is defined as $m = \dfrac{\pi R^2 N}{G} \times O\sqrt{N}$, where m indicates the authentication report sent to the verification node, N indicates the number of nodes, G indicates the deployment area. $O\sqrt{N}$ indicates the communication load caused by the mechanism.

A large number of sensor nodes are deployed in the random joint authentication area, and the ID information of each node i is initialized. the node i sends its own geographical location information and password to all trusted nodes in the communication range of the node and obtains the following information. M_i is the last message sent to the trusted node, and pwd_i represents the password unique to the node itself. The password is known only to itself and its trusted node, which is obtained by the hash value product of the location information generated by the node itself in Equation (11).

$$\begin{bmatrix} M_i = \left(ID_i, location, i, pwd_i\right) \\ M_i = send, M_i \left| H(M_i, M_j) \right. \end{bmatrix} \tag{11}$$

Equation (12) indicates that the node password is unique, mainly because the generation of the password is based on the security mechanism. In order to ensure the security of the location information, the password will be updated as needed to ensure the security of the node information. The period of the password update mechanism is set according to the size of the node deployed by the wireless sensor network and the security requirements of the network. Generally, when the network size is large, and the security requirement is high, the update cycle interval is set to be short. When node i in the network needs to authenticate to node O, it only needs to verify its trusted node. This is still based on the security authentication idea of the trusted node.

$$pwd_i = H\left(T \left| location \times i \right.\right) \tag{12}$$

3. Experimental Results and Analysis

The multi-node random unite authentication method is tested in the simulation environment of Matlab. The experimental area is 1500×1500m. 200 nodes are randomly set in the area; there may be *k* illegal communication nodes. The experimental parameters are shown in Table 1.

Table 1. Experimental parameters

Parameter	Value
Packet length/Byte	4200
Network running time/s	120
Node communication radius/m	12
Memory size/GB	4
Shared key package size/bit	210
Sub-key package size/bit	20
PC frequency/GHz	2.54
Number of sub-shares	60

Figure 1 shows the relative transmission rate between the proposed method and the method proposed in [14] and [15]. In Figure 1, during the operation of the wireless sensor network for 100s, the rate of random transmission of multiple nodes during the operation of the entire wireless sensor network is recorded. In Figure 1, compared with the methods proposed in [14] and [15], the probability of illegal nodes being selected is gradually reduced as the transmission time of communication data increases. The wireless sensor network is guaranteed to be secure and suitable for multi-node authentication, and the rate of transmission between multiple nodes is reduced. Thereby, the congestion of the wireless sensor network is reduced, the wireless sensor network has better communication efficiency, and the energy consumed by the network node is minimized.

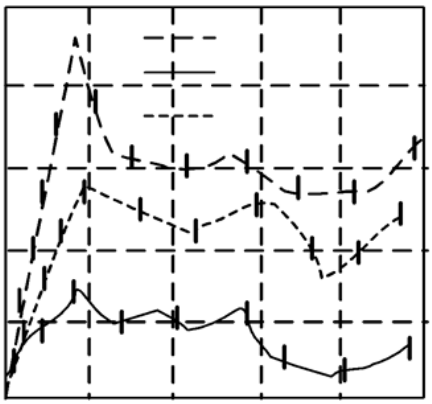

Figure 1. Comparison of node transmission rates for different methods

Table 2 shows the comparison of statistical results between the proposed method and the methods proposed in [14] and [15] in wireless sensor network communication. Table 2 compares the node authentication method proposed in ref. [14] and ref. [15]. The proposed multi-node random unite authentication method reduces the number of data packets generated by the communication node. Nodes can send up to 305 sending packets. Node forwarding packets can be reduced by 29,818. Node receiving packets can be reduced by up to 1860. The method proposed in this paper mainly reduces the network communication to alleviate network congestion based on the wireless sensor network security certification.

Table 2. Comparison of processing packets of communication nodes

Method	Ref. [14]	Ref. [15]	Proposed
Sending package/piece	1150	1042	845
Receiving package/piece	5061	3203	3201
Send and receive rate/%	4.3615	4.109	3.7589
Forwarding package/a	70375	65745	40557

The proposed method is compared with the methods in ref. [14] and ref. [15] for the maximum occupancy and percentage of the wireless sensor network operating memory. Table 3 shows that when the wireless sensor network is running, the network memory usage of the proposed method is reduced by 2 times compared with the method proposed in ref. [14]. Compared with the method proposed in ref. [15], the network memory usage is reduced by 1.7 times. The percentage of memory usage by the method proposed in this paper is 1.8 times smaller than that proposed in ref. [14].

Compared with the method proposed in ref. [15], the percentage of memory usage is reduced by 1.6 times. The main reason is that the proposed method uses a combination of symmetric cipher and information authentication code to achieve multi-node authentication.

Table 3. Comparison of memory usage of different methods

Method	Percentage/%	Memory usage/kB
Ref. [14]	2.81	57583
Ref. [15]	2.55	50426
Proposed	1.52	28690

Table 4 shows the timeliness comparison between the proposed method and the methods proposed in ref. [14] and ref. [15] in the wireless sensor network. The node authentication time and the key establishment time are compared. the method proposed in this paper is significantly faster in time than other methods, as seen in Table 4. The multi-node random authentication time is 2.5 times faster than the method proposed in ref. [14] and relatively 2.6 times faster than the method proposed in ref. [15]. The key establishment time is 2.1 times faster than the method proposed in ref. [14] and relatively 2.2 times faster than the method proposed in ref. [15]. Because the method proposed in this paper can effectively jointly authenticate multiple nodes in the wireless sensor network, fast node authentication time can effectively reduce the consumption of communication nodes.

Table 4. Comparison of execution time of node authentication

Method	Execution time		Total time comparison/%
	Authentication time/ns	Key time/ns	
Ref. [14]	175470	77869	59.0
Ref. [15]	178150	79479	59.6
Proposed	68150	35620	-

In addition to the fast authentication time of nodes, the multi-node random unite authentication method in wireless sensor networks also has certain stability in node authentication results. The stability of the node authentication results of the ref. [14] and [15] method is simulated. The experimental results are shown in Figure 2. Under the same experimental time environment, the node authentication scheme of wireless sensor network proposed in [15] has a large fluctuation of the node authentication result curve, and no fluctuation law can be found. The highest stability rate is 45%, while the lowest point is 31%. Observing the trend of the curve in the experimental diagram, the multi-node authentication protocol for information network protocol logic security proposed by the ref. [14] has a steady upward trend. The stability rate of node authentication result of the multi-node authentication protocol for information network protocol logical security is too low, indicating that the node authentication result has low credibility.

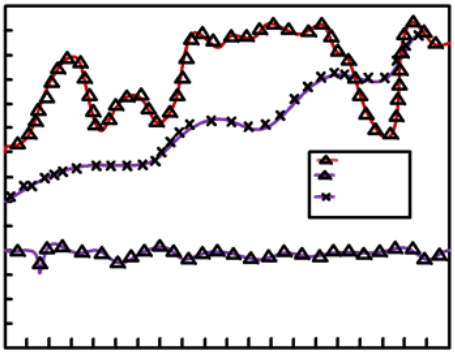

Figure 2. Comparison of node authentication stability

However, the curve of the stability rate of the node authentication result of the multi-node random unite authentication method in the wireless sensor network proposed in this paper is gentle. There are certain rules for fluctuations. The highest point of stability rate fluctuations is 21% and the lowest point is 18%. The comparison results under the same experimental environment show that the node authentication result of this method is more accurate, the change range is small, and the result is highly reliable.

The following is a comparison of the fault tolerance (refers to the ability of software to detect errors in software or hardware running on an application and recover from errors) of the multi-node random unite authentication method for wireless sensor networks with the ref. [14] and ref. [15] methods. The comparison results are shown in Figure 3. Fault

tolerance refers to the probability of reducing some fault factors or choosing to have an unstable effect on a system in a system. The higher the fault tolerance rate, the smaller the impact of the failure factor on the verification effect. The lower the fault tolerance rate, the greater the impact of the fault factor on the verification effect. Figure 3 shows the results of comparing the fault-tolerant rates of the nodes proposed in the ref. [14] and ref. [15] with the proposed authentication method in the same experimental environment.

Experiments show that the trend of the ref. [14] is getting lower and lower, indicating that the fault tolerance of the method to the system fault point is also decreasing. The multi-node authentication protocol method for information network protocol logical security is low in fault tolerance, and the fault point has a great influence on the node authentication result. The node authentication scheme of wireless sensor network proposed in ref. [15] is slower than the ref. [14], but it still shows a downward trend. The fault point in this method has a great influence on the node authentication result. The fault-tolerant rate curve of the multi-node random unite authentication method in wireless sensor networks proposed in this paper shows a continuous upward trend, which proves that the method has high fault tolerance. In summary, the method node authentication result is stable, the result data is accurate, the change range is small, the credibility is high, the fault tolerance rate is high, and the fault point has little influence on the node authentication result.

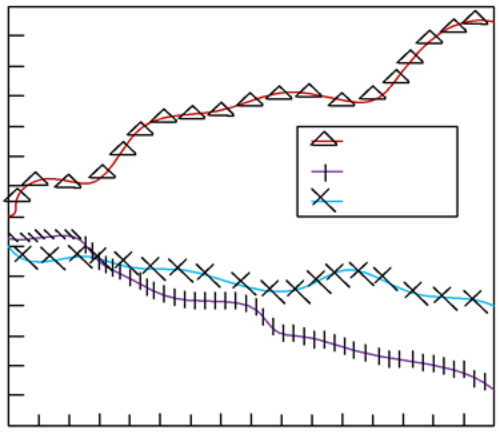

Figure 3. Comparison of fault tolerance rates of node authentication process

4. Conclusions

The existing multi-node authentication method in wireless sensor networks had the problems of high network energy consumption and high communication overhead of wireless sensor networks. Multi-node random unite authentication method based on RSA and trusted nodes was proposed. Network key negotiation was performed using wireless sensor network node identity and relativity. Node trust was introduced. The node trust degree was calculated by using the behavioural reputation management based on the Beta distribution node. This method reduced the amount of node calculations in this process. The authentication mechanism of the node authentication geographical location information required by the method in this paper was analysed to introduce the concept of the region. The overall area of the wireless sensor network was segmented. The communication node was authenticated according to the authentication process of the trusted node. It effectively improved the effectiveness of multi-node random unite authentication and reduced the consumption of network communication nodes. Experimental results showed that the proposed method can effectively reduce the complexity of the network authentication process and the space cost of the algorithm, reduce the network communication consumption, and improve the security of the wireless sensor network.

References

1. T. Shang, G. Du, and J. -W. Liu, "Opportunistic Quantum Network Coding based on Quantum Teleportation," *Quantum Information Processing*, Vol. 15, pp. 1743-1763, 2016
2. D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-based Conditional Privacy-Preserving Authentication Scheme for Vehicular ad hoc Networks," *IEEE Transactions on Information Forensics and Security*, Vol. 10, pp. 2681-2691, 2015
3. S. Liu, W. Fu, W. Zhao, J. Zhou, and Q. Li, "A Novel Fusion Method by Static and Moving Facial Capture," *Mathematical Problems in Engineering*, Vol. 2013, pp. 503924, 2013
4. G. Yang and S. Liu, "Distributed Cooperative Algorithm for k-M Set with Negative Integer k by Fractal Symmetrical Property," *International Journal of Distributed Sensor Networks*, Vol. 10, pp. 398583, 2014
5. G. Huang, T. Liu, and Y. Guan, "Secure Authentication Scheme of WSN based on Tri-element Node Evaluation," *Computer*

Engineering, Vol. 41, pp. 115-119, 2015
6. M. Liu, S. Liu, W. Fu, and J. Zhou, "Distributional Escape Time Algorithm based on Generalized Fractal Sets in Cloud Environment," *Chinese Journal of Electronics*, Vol. 24, pp. 124-127, 2015
7. H. Liu, R. Yin, B. Liu, and Y. Li, "A Scale-Free Topology Model with Fault-Tolerance and Intrusion-Tolerance in Wireless Sensor Networks," *Computers & Electrical Engineering*, Vol. 56, pp. 533-543, 2016
8. K. -A. Shim, "BASIS: A Practical Multi-User Broadcast Authentication Scheme in Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, Vol. 12, pp. 1545-1554, 2017
9. S. Amri, F. Khelifi, A. Bradai, A. Rachedi, M. L. Kaddachi, and M. Atri, "A New Fuzzy Logic based Node Localization Mechanism for Wireless Sensor Networks," *Future Generation Computer Systems*, 2017
10. I. Strumberger, M. Beko, M. Tuba, M. Minovic, and N. Bacanin, "Elephant Herding Optimization Algorithm for Wireless Sensor Network Localization Problem," in *Proceedings of the 9th IFIP WG 5.5/SOCOLNET Advanced Doctoral Conference on Computing, Electrical and Industrial Systems*, pp. 175-184, Costa de Caparica, Portugal, May 2-4, 2018
11. J. -B. Li and B. -C. Mu, "Moving Node Localization Algorithm based on Cooperated Prediction for Wireless Sensor Networks," *Computer Application Research*, Vol. 34, pp. 186-187, 2017
12. S. Guo, J. Li, and S. Gao, "Design and Realization of Multi-Node Software Trigger Bootloader," *Modern Electronics Technique*, Vol. 18, pp. 011, 2017
13. Z. Wan, N. Xiong, and L. T. Yang, "Cross-Layer Video Transmission over IEEE 802.11 E Multihop Networks," *Multimedia Tools and Applications*, Vol. 74, pp. 5-23, 2015
14. Y. Bai, X. Shao, W. Yang, W. Wang, P. Feng, S. Liu, et al., "Nodes Contact Probability Estimation Approach based on Bayesian Network for DTN," in *Proceedings of NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1-4, 2018
15. C. -C. Chang and H. -D. Le, "A Provably Secure, Efficient, and Flexible Authentication Scheme for ad hoc Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, Vol. 15, pp. 357-366, 2016