International Journal of Autonomous and Adaptive Communications Systems

ISSN online: 1754-8640 - ISSN print: 1754-8632
https://www.inderscience.com/ijaacs

Security key distribution method of wireless sensor network based on DV-hop algorithm

Gao Fei

DOI: 10.1504/IJAACS.2023.10039241

Article History:

Received:	29 April 2020
Accepted:	01 September 2020
Published online:	17 March 2023

Security key distribution method of wireless sensor network based on DV-hop algorithm

Gao Fei

Academic Affairs Office,
Nanyang Medical College,
Nanyang 473061, China
Email: gaofei@mls.sinanet.com

Abstract: In this paper, a wireless sensor network security key distribution method based on DV-Hop algorithm is proposed. The improved DV-Hop algorithm is used to locate the network security key distribution point, and the distributable point is separated according to the positioning result. According to the separation result, a key management tree is introduced to perform centralized classification management of allocable points, and the key management tree is used to complete the wireless sensor network device authentication, key distribution and update, and to realize the research of the wireless sensor network security key distribution method. Experimental results show that the method uses low energy for key establishment and update, the minimum update energy consumption is only 25 μJ, and it has strong anti-attack performance and high overall security.

Keywords: DV-hop; wireless sensor network; key management tree; key distribution; network security; simulation.

Reference to this paper should be made as follows: Fei, G. (2023) 'Security key distribution method of wireless sensor network based on DV-hop algorithm', *Int. J. Autonomous and Adaptive Communications Systems*, Vol. 16, No. 1, pp.66–83.

Biographical notes: Gao Fei graduated from School of Computer Science, Northwestern University of Technology in July 2006, Major in Computer Science and Technology. In July 2011, he graduated from the School of Software, Tongji University, major in Software Engineering. He is now working in the Academic Affairs Office of Nanyang Medical College. He is mainly engaged in the management of academic affairs in Colleges. At the same time, he was in charge of the teaching of computer science for the students.

1 Introduction

With the continuous progress of science and technology, the development and research of wireless sensor network has attracted extensive attention of people in various fields. It can be used in many fields, such as military, environment and security monitoring. In general, the network is composed of large-scale self-control nodes, each of which is powered by batteries. At the same time, digital signals and RF circuits are effectively integrated. Compared with the traditional wireless computer network, the characteristics

of the network are very significant (Cao et al., 2017a; Chun et al., 2017; Wang et al., 2016). Considering its limitations, the network research faces a series of problems such as key management and authentication. The security problem has always been the focus of public attention, especially in some important applications, security is very important and critical. To establish a secure and reliable wireless sensor network, it is necessary to have secure algorithms and protocols to realise network key control and information data encryption. The previous methods can not adapt to the sensor network very well. Because there is no authentication centre in the network centre, the communication point is in the peer-to-peer state, and the performance of calculation and storage is poor (Zhang et al., 2016a; Huang et al., 2018; Kiktenko et al., 2017). For this reason, the relevant researchers have carried out in-depth research on the security key distribution method of wireless sensor network, and achieved some research results, but there are still many problems in the existing research results.

In Sun et al. (2016), a secure key distribution method for wireless sensor networks based on quantum memory and entangled photon source is proposed, which applies EPS to quantum key distribution. The advantages and disadvantages of direct and indirect prediction quantum storage and EPS quantum storage are compared, and the correlation among key survival rate, safe transmission distance and quantum state holding time in independent quantum key management system of measurement equipment under quantum storage and EPS is analysed, so that the research on secure key distribution method of wireless sensor network is completed, but the distribution energy consumption of the method is higher. In reference (Ma et al., 2019), a secure key distribution method for wireless sensor networks based on the selection of basis vector is proposed. According to the random deviation parameter under the selection of basis vector, the quantitative description method of wavelength correlation of beam splitters is analysed. Through the entanglement purification security analysis method, the security of quantum key distribution is analysed, and the expression of security key distribution in the case of random deviation parameters is given, but the security of this method needs to be further improved. In Zheng and Huang (2016), a secure key distribution method for wireless sensor networks based on acoustooptic modulators is proposed. In the process of quantum communication using single spatial mode continuous variables, the polarisation state of light is generally used as the information carrier. This quantum key distribution method requires the polarisation controller to control the polarisation state of light, so as to select and code the local component and signal component. Based on the theory of polarised light matrix, the Stokes parameter formula of polarised light passing through the acoustooptic modulator is analysed. Through isotropic photoelasticity, the acoustooptic modulation system is constructed to complete BPSK coding and realise the distribution of security key in wireless sensor network. However, this method has the problem of low allocation accuracy, so it is difficult to ensure the communication security of wireless sensor network.

In order to solve the problem of high energy consumption and poor anti attack of the above-mentioned wireless sensor network security key distribution method, a DV-hop algorithm based security key distribution method is proposed to ensure the security of wireless sensor network information transmission.. Based on the location of key distribution point, the key distribution management is realised to further improve the security of network operation. The overall scheme of this method is as follows:

- In order to distinguish the assignable points of the security secret key in wireless sensor network accurately, the DV-hop algorithm is improved, and the improved DV-hop algorithm is used to locate the assignable points of the security secret key in wireless sensor network, and the assignable points are separated accurately, which lays the foundation for the subsequent realisation of the accurate distribution of the security secret key in wireless sensor network.
- According to the result of the separation of wireless sensor network security key distribution points, the key management tree is introduced to manage the key distribution points, and the key management tree is used to complete the authentication, key distribution and update of wireless sensor network equipment, so as to realise the research of wireless sensor network security key distribution method.
- Experimental verification. Taking the distribution energy consumption and anti attack performance as experimental indexes, the proposed method is compared with Sun et al. (2016), Ma et al. (2019) and Zheng and Huang (2016), and the experimental results are analysed.

According to the above scheme, the accurate distribution of wireless sensor network security key is realised, and the security of wireless sensor network communication is improved.

2 Security key distribution in wireless sensor networks

2.1 Key distribution point location based on DV-hop algorithm

DV-hop algorithm is a classical location algorithm without distance measurement. It is represented by the average distance and number of hops between unknown nodes and beacon nodes. The location information of unknown nodes is obtained by trilateral measurement. This algorithm has the advantages of simple calculation process and high accuracy of calculation results. In the process of using DV-hop algorithm to locate nodes in wireless sensor networks, there is no need for ranging algorithm. As long as based on network connectivity, unknown node coordinates can be estimated, which can effectively save the cost of hardware equipment, and the whole positioning process is simple and reliable (Li et al., 2016; Liang et al., 2016). In the actual positioning process, the optimal selection of anchor nodes and the average error of each hop distance will have a great impact on the positioning. Therefore, according to the random distribution network of nodes, considering the error factor of DV-hop algorithm in the process of trilateral positioning, in order to improve the positioning accuracy, the hop error correction is introduced into wireless sensor network node positioning.

(1) Node location discrimination

After comprehensive consideration, the following node location discrimination method is given to select anchor nodes that can be accurately located. The detailed process is as follows.

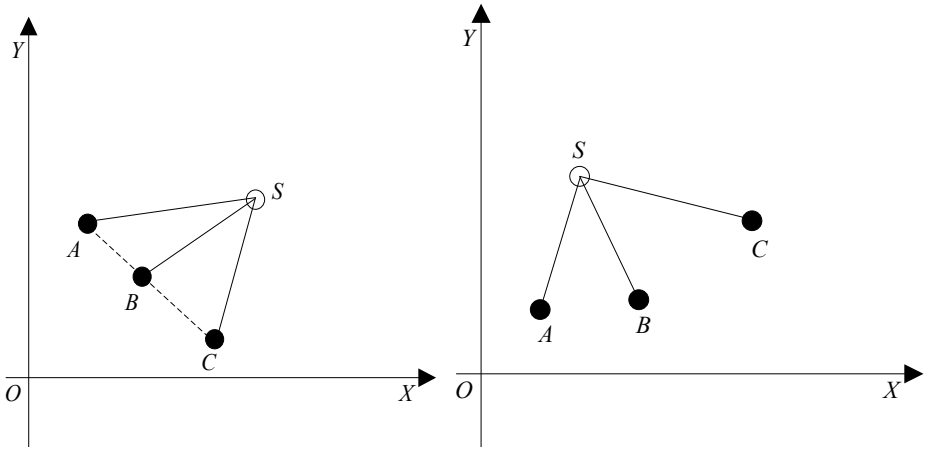
The three closest anchor nodes $A(x_A, y_A)$, $B(x_B, y_B)$, $C(x_C, y_C)$ are determined to the unknown node. In this process, A is closest to the unknown node, B is next, and C is last.

Whether *A*, *B* and *C* are collinear are judged, as shown in Figure 1. Assuming it is collinear, then *A* and *B* are kept, *C* is discarded, the anchor nodes closest to the unknown nodes are selected except *A*, *B* and *C*, and then the location discrimination operation is performed; assuming it is not collinear, then enter the next step.

Three anchor nodes are selected for unknown nodes to realise trilateral positioning, and the coordinates of unknown nodes are obtained.

Figure 2 is a judgement program of node location.

Figure 1 Judgement of node location: (a) collinear and (b) incoherent line



(2) Estimation of average jump distance under error correction

Supposing that i represents the known coordinates of the anchor nodes (x_i, y_i) in the wireless sensor network. If the anchor node i receives the location information from other nodes, the average calculation formula of i per hop distance is:

$$C_i = \frac{\sum_{i \neq j} \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}}{\sum_{i \neq j} h_{ij}} \tag{1}$$

Where, j represents the number of other anchor nodes in the data package i, and h_{ij} represents the number of hops between i and j.

Based on the solution of the distance between two anchor nodes, the actual distance d_{rij} between i and j can be obtained.

$$d_{rij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \tag{2}$$

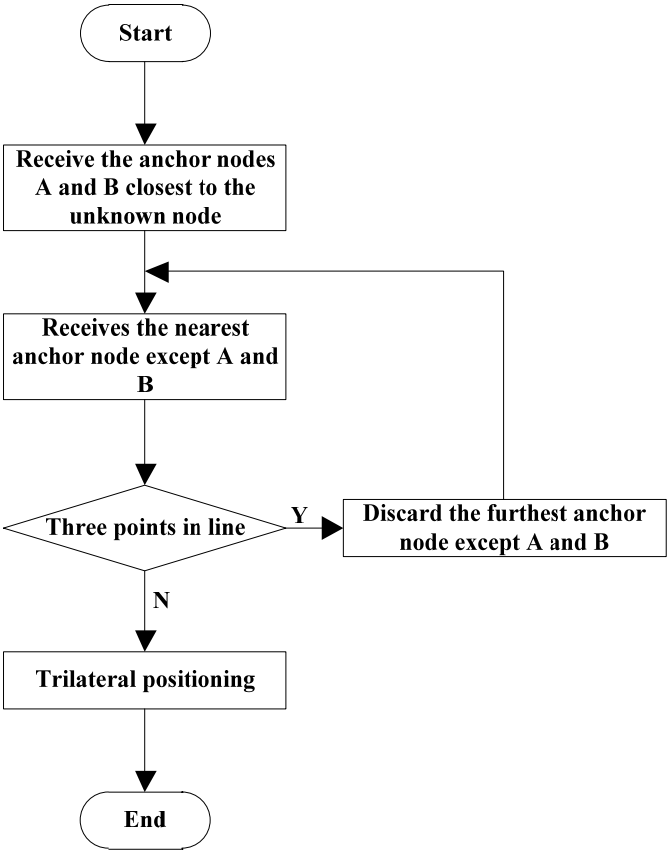
Then, the calculation formula of the measurement distance d_{eij} between i and j is:

$$d_{eij} = C_i \times h_{ij} \tag{3}$$

When there are M anchor nodes in the whole wireless sensor network, the calculation formula of the average error ε_i of i per hop distance is as follows:

$$\varepsilon_i = \frac{\sum_{i \neq j} \left| d_{rij} - d_{eij} \right| / h_{ij}}{M - 1} \tag{4}$$

Figure 2 Judgement procedure of node location

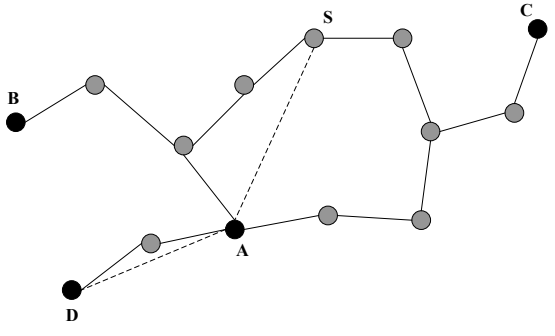


In the process of node location, the unknown node only receives the average per hop distance of the anchor node closest to its own distance, and takes it as the estimated value of its average per hop distance. Then the unknown node uses the estimated value of the number of hops and the average distance of each hop closest to its own distance to get the estimated distance between the unknown node and each anchor node. It can be seen from the analysis that the more the hops between the unknown node and the anchor node are, the greater the error value of the estimated distance is. Since the hop number information is a fixed value in the data package, it can take the average hop distance received by unknown nodes from anchor nodes as the entry point to achieve accurate positioning correction (Gao et al., 2016; Ding et al., 2016; Zhang et al., 2017). In Figure 3, the anchor node with the closest distance to the unknown node S is A, the number of hops between the two is 3, and the estimated value of the average hop distance of S is C_A, then the measured distance of S and A can be expressed as:

$$d_{eSA} = C_A \times h_{SA} \tag{5}$$

Because the measured distance between *S* and *A* is the skip distance between *S* and *A*, and the actual distance between *S* and *A* is the straight-line distance between two nodes, when the number of hops between two nodes is multi hop, that is, when it is greater than 2, the length of the straight-line distance is much smaller than the length of the skip distance. Therefore, the error of the average distance value per hop can be used to correct itself, so that the estimated value of the unknown node is closer to the actual value, and more accurate positioning results can be obtained.

Figure 3 Schematic diagram of skip between unknown node and anchor node *a*



When the number of hops between the unknown node and the anchor node is within two hops, the distance error between the nodes obtained according to the original average two hops distance is small, as shown in node *A* and *D* in Figure 3, so the comparison can reflect the actual situation of the network nodes. Considering that the estimated value C_i of the average distance per hop should be modified, the unknown node *S* and anchor node *j* are set, and the number of hops between *S* and *j* should be h_{Sj}, then the calculation formula of the estimated value *s – I* of the modified average *S* per hop distance is:

$$S_i = \begin{cases} C_i - e^{\varphi} \times \varepsilon_i & h_{Sj} > 2 \\ C_i & h_{Sj} \le 2 \end{cases} \tag{6}$$

Where, φ represents parameter variable, $\varphi < 0$. Therefore, the distance between the unknown node and the anchor node can be calculated more accurately. Then, the most suitable distance between the three anchor nodes and the unknown node obtained based on the above-mentioned node location judgement method is:

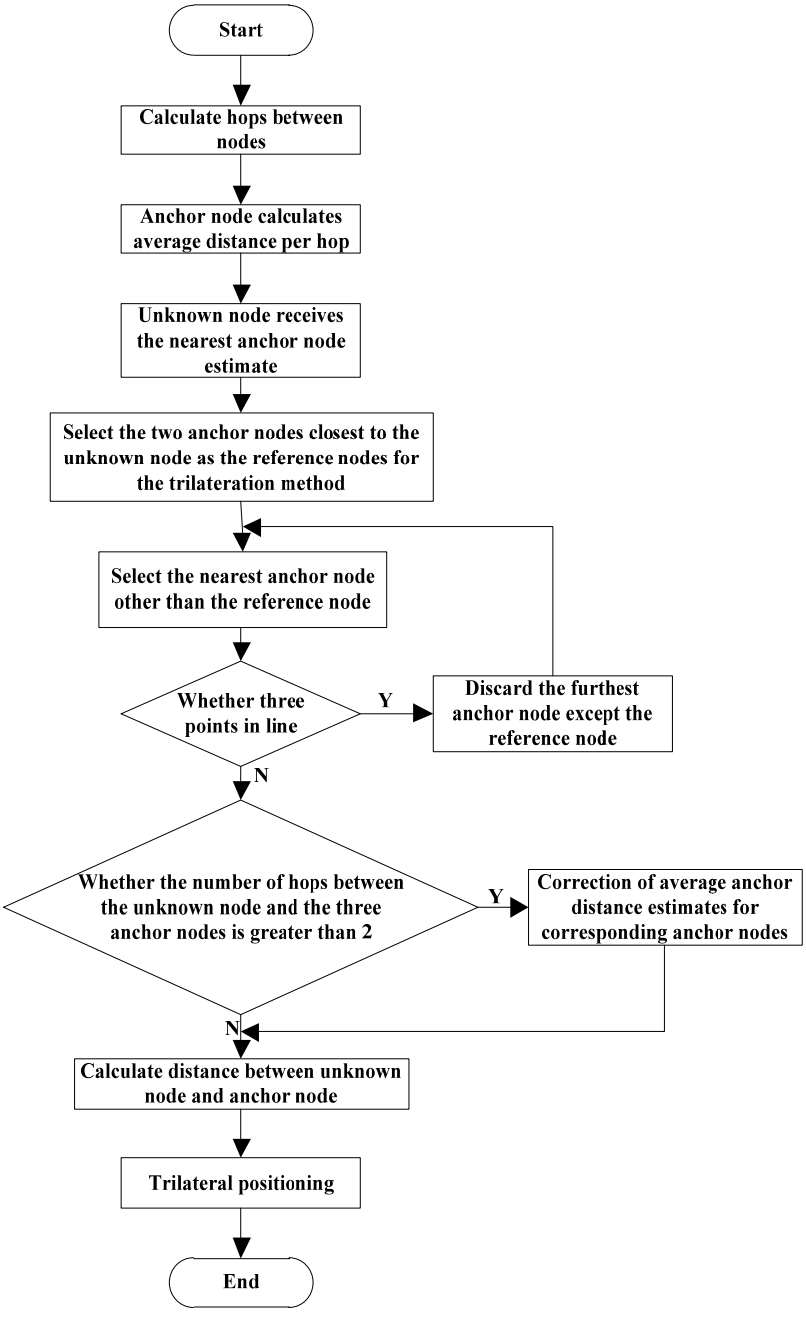
$$d_{Sj} = S_i \times h_{Sj} \tag{7}$$

After obtaining the distance between the unknown node and each anchor node by using the above calculation formula, the unknown node can be located based on the trilateral positioning method, thus effectively improving the accuracy of positioning information.

(3) Location algorithm

In the first two stages, the operation process of the DV-hop algorithm is the same as that of the DV-hop algorithm before the improvement, and the trilateral positioning process is improved, as shown in Figure 4.

Figure 4 Improved DV-hop algorithm program



After the initialisation of wireless sensor network, the number of hops between nodes is calculated, in which the anchor node calculates the average per hop distance, while the unknown node receives the closest estimate of the anchor node distance. The two anchor nodes closest to the unknown node are selected as the reference node of trilateral

positioning method, and the nearest anchor node except the reference node is selected to judge whether the three points are collinear or not. If they are collinear, the farthest anchor node except the reference node is discarded. If it is greater than 2, the average estimated distance per hop of the corresponding anchor node is modified, and if it is not greater than 2, the distance between the unknown node and the anchor node is calculated to realise the trilateral positioning.

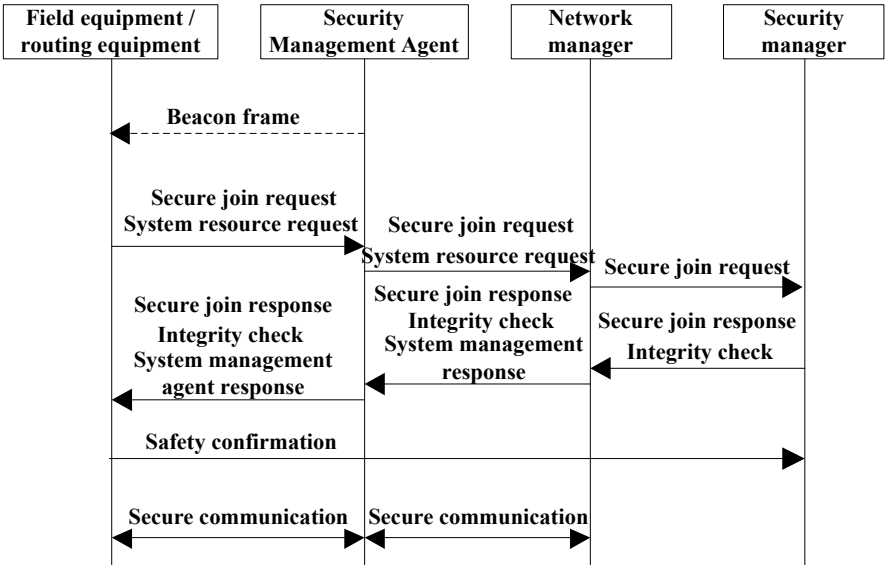
2.2 Key distribution management

By using the above-mentioned node location, the nodes that can perform key distribution and the nodes that cannot perform key distribution can be distinguished. On this basis, the TCC reactive power compensation device control strategy is introduced to realise the wireless sensor network security key distribution management.

(1) TCC strategy overview

The security manager, gateway, is responsible for the policy, which can complete the security policy distribution, key management and device authentication of the whole wireless sensor network. This strategy manages the key according to the combination of centralised and distributed mode, and uses centralised mode to manage the key in the MESH framework composed of routing devices, so as to ensure the key distribution and unified management between clusters. In the star framework constructed by field devices, the cluster head can independently control the members in the cluster and update the cluster key at the same time.

Figure 5 Device security access architecture



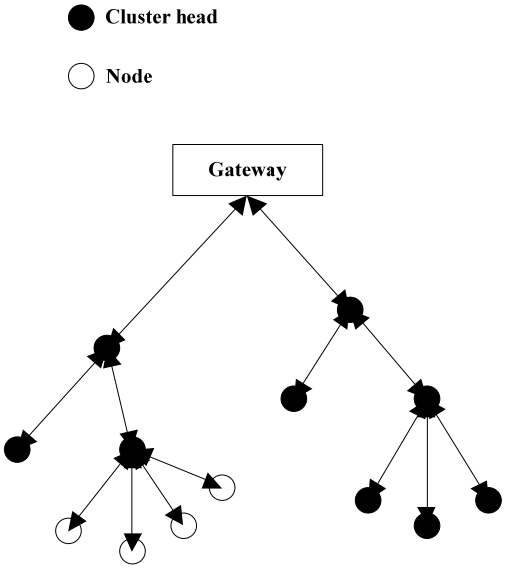
TCC strategy mainly uses the key management tree to manage the network key. The key types in the network can be divided into temporary shared key, personal key, pair key, cluster key, group key and communication key.

(2) TCC key management tree

In view of the topology of current wireless sensor network and centralised form of security management and control structure, in the initial stage of network operation, the key management tree is constructed to complete key security access, key management and broadcast authentication. Figure 5 shows the device security access architecture.

After the routing device and the field device enter the network safely, they can form a tree root with the gateway as the centre, and the security links between the routes constitute the backbone and branches of the key management tree, and the field device nodes constitute the leaves of the tree. Figure 6 shows the key management tree.

Figure 6 Key management tree



The key management tree is constructed as follows:

Gateway *GW* regularly transmits beacon frame Beacon encrypted by temporary key K_{init} based on relevant mechanism, which is applied in network device joining and time alignment. When the routing device listens to beacon, it sends the input network request to the gateway. *GW* uses and routes the personal key in the device to build secure communication as the first level of the network.

$$GW \to *: E\left(K_{\text{init}}, \text{Hello} \,||\, N_A\right) || \,\text{MAC}\left(K_{\text{init}}, E\left(K_{\text{init}}, \text{Hello} \,||\, N_A\right)\right) \tag{8}$$

$$CH_i \to GW: E\left(K_{CHi}, N_A \,||\, ID_{CHi}\right) || \,\text{MAC}\left(K_{CHi}, E\left(K_{CHi}, N_A \,||\, ID_{CHi}\right)\right) \tag{9}$$

$$GW \to CH_i: E\left(K_{CHi}, N_A \left\| K_G \right\| K_{CHi,CHj}\right) || \,\text{MAC}\left(K_{CHi}, E\left(K_{CHi}, N_A \left\| K_G \right\| K_{CHi,CHj}\right)\right) \tag{10}$$

Where, K_G represents the shared group key of the whole network, CH_i represents the *i*th cluster head, i.e., routing device, N_A represents the random value of fixed length, and MAC(·) represents message digest.

The *i*-level routing device CH_i transmits Beacon at a fixed cycle time to wait the joined routing device CH_j monitors and hears Beacon. The gateway personal key K_{CHj} is used to encrypt the information related to the access request and transmit it to CH_i.

$$CH_i \to *: E\left(K_{\text{init}}, \text{Hello} \,||\, N_A\right) || \,\text{MAC}\left(K_{\text{init}}, E\left(K_{\text{init}}, \text{Hello} \,||\, N_A\right)\right) \tag{11}$$

$$CH_j \to CH_i : E\left(K_{CHj}, N_A \,||\, ID_{CHj}\right) || \,\text{MAC}\left(K_{CHj}, E\left(K_{CHj}, N_A \,||\, ID_{CHj}\right)\right) \tag{12}$$

After receiving the information, the routing CH_i detects the network access information of the request and forwards it to the gateway.

$$CH_j \to \cdots \to GW : E\left(K_{CHj}, N_A \,||\, ID_{CHj}\right) || \,\text{MAC}\left(K_{CHj}, E\left(K_{CHj}, N_A \,||\, ID_{CHj}\right)\right) \tag{13}$$

When the gateway receives the request, it firstly calculates the MAC value to verify the authenticity of the device. After verification, the resource and the neighbouring node pair key are configured based on its joining information.

$$GW \to \cdots \to CH_j : E\begin{pmatrix} K_{CHj}, N_A \left\| K_G \right\| K_{CHi,CHj} \left\| \cdots \right\| K_{CHi,CHm} \,|| \\ \text{MAC}\left(K_{CHj}, N_A \left\| K_G \right\| K_{CHi,CHj} \left\| \cdots \right\| K_{CHi,CHm} \,||\right) \end{pmatrix} \tag{14}$$

Iterating the above steps can realise the secure joining and key distribution of routing devices in the whole wireless sensor network.

The on-site device S_j monitors and hears the Beacon of CH_k, encrypts the information related to the access request through the personal key K_{Sj} applied to the gateway, and transmits it to CH_k.

$$S_j \to CH_k : E\left(K_{Sj}, N_A \,||\, ID_{Sj}\right) || \,\text{MAC}\left(K_{Sj}, E\left(K_{Sj}, N_A \,||\, ID_{Sj}\right)\right) \tag{15}$$

CH_k collects the field device requests in the cluster, and forwards the collection results to the gateway for authentication within its own communication time slot.

$$\begin{aligned} CH_k = GW : E\left(K_{Sj}, N_A \,||\, ID_{Sj}\right) || \,\text{MAC}\left(K_{Sj}, E\left(K_{Sj}, N_A \,||\, ID_{Sj}\right)\right) \left\| \cdots \right\| \\ E\left(K_{Sn}, N_A \,||\, ID_{Sn}\right) || \,\text{MAC}\left(K_{Sn}, E\left(K_{Sn}, N_A \,||\, ID_{Sn}\right)\right) \end{aligned} \tag{16}$$

After receiving the information, the gateway authenticates all devices and assigns random number N_A and cluster member number Num to each cluster.

$$GW \to CH_k : E\begin{pmatrix} K_{CHk}, N_A \left\| \text{Num} \right\| E\left(K_{Sj}, N_A \,|\, \left\| \text{Num} \right\| K_G\right) \right\| \cdots \left\| E\left(K_{Sn}, N_A \left\| \text{Num} \right\| K_G\right)\right. \\ \text{MAC}\left(K_{Sj}, E\left(K_{Sj}, N_A \left\| \text{Num} \right\| K_G\right)\right) || \cdots \\ \left\| E\left(K_{Sn}, N_A \left\| \text{Num} \right\| K_G\right)\right\| \text{MAC}\left(K_{CHi}, N_A\right) \end{pmatrix} \tag{17}$$

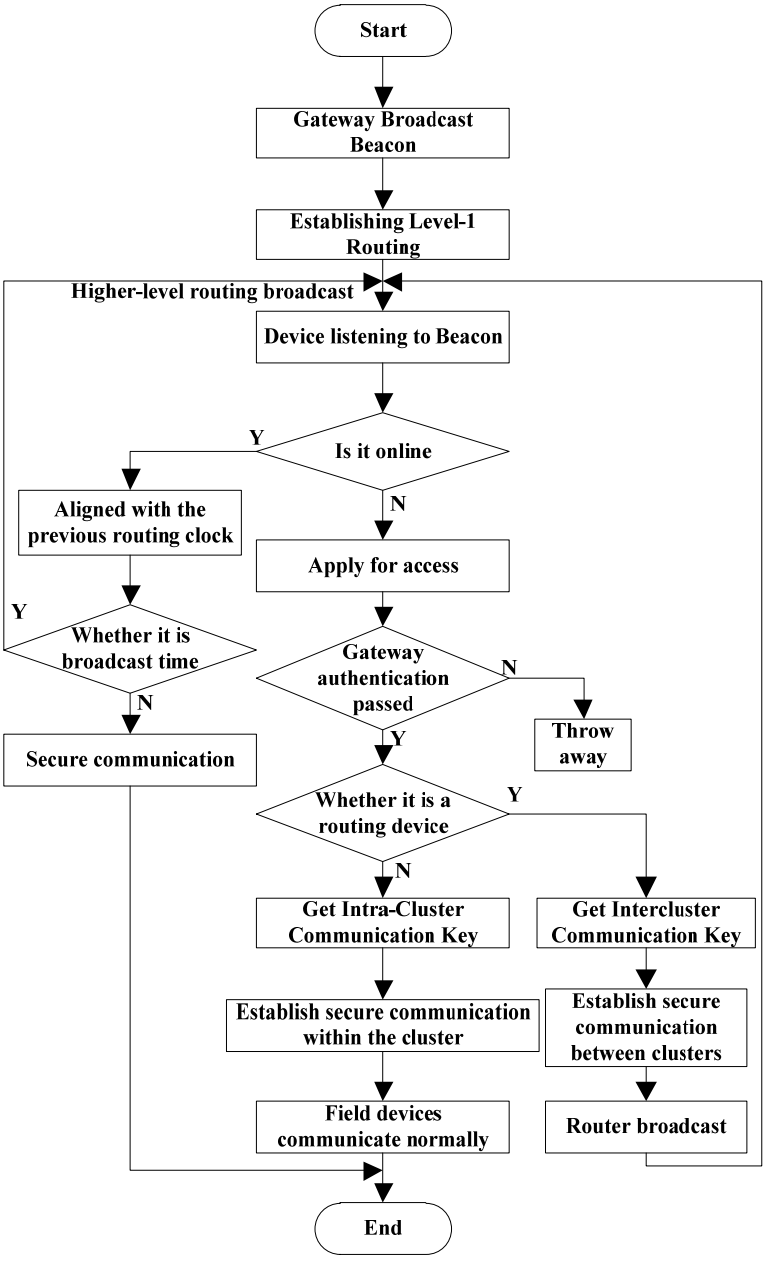
After receiving the returned cluster information, the routing K_{CHk} extracts the random number and the number of cluster members, calculates the cluster key K_{Ck}, encrypts the broadcast message according to K_{Ck}, updates the cluster key, and transmits the random number and the number of cluster members to the newly added device S_j.

$$CH_k \to *: E\left(K_{Ck}, N_A \,||\, \text{Num}\right) || \,\text{MAC}\left(K_{Ck}, E\left(K_{Ck}, N_A \,||\, \text{Num}\right)\right) \tag{18}$$

Iterative above process can achieve the whole field device security join and key distribution of wireless sensor network.

To sum up, the key tree is constructed. The detailed process is shown in Figure 7.

Figure 7 Builder of key management tree



When the cluster head and the devices in the cluster receive the number of cluster members sent by the manager, based on the number of cluster members and the random number, the key K_{Ci} of the cluster is generated through the pre distribution single item hash function.

$$K_{Ci} = H\left(\text{Num} \,||\, N_A\right) \tag{19}$$

Therefore, all nodes in the cluster and the cluster head will obtain a shared cluster key.

The key and cluster key are distributed by hop-by-hop, and the group key is included in the returned information when the device is confirmed to join.

The communication key is composed of the temporary initial key and the end of the one-way key chain.

$$K_{\text{Com}} = H\left(K_{\text{init}} \,||\, X_n\right) \tag{20}$$

(3) Network security communication

After the initialisation of system operation and the realisation of routing and field equipment entering the network, it starts to work stably. At this time, the member nodes transmit the data to the cluster head within their own time slot range, implement the data processing in the cluster head, and then transmit it to the gateway (Cao et al., 2017b; Kang et al., 2017).

In the same cluster, each member node and its own time slot can only transmit data to the cluster head in its own time slot. The rest of the time is in a dormant state. After the time slot comes, the collected data is encrypted with K_{Ci}, and the additional MAC value is transmitted to the cluster head.

$$S_j \rightarrow CH_i : E\left(K_{Ci}, \text{data}\right) \,||\, \text{MAC}\left(K_{Ci}, E\left(K_{Ci}, \text{data}\right)\right) \tag{21}$$

The messages transmitted by all member nodes are decrypted by the cluster key, and the data authentication is realised at the same time. If the authentication is passed, the data will be fused, and the useless and redundant data will be removed, so as to reduce the traffic (Zhang et al., 2016b; Wang et al., 2017; Liang et al., 2016).

After the cluster head realises data fusion, it is encrypted according to the communication key and transmitted to the gateway.

$$CH_i \rightarrow GW : E\left(K_{\text{Com}}, \text{data}\right) \,||\, \text{MAC}\left(K_{\text{Com}}, E\left(K_{\text{Com}}, \text{data}\right)\right) \tag{22}$$

At this time, the gateway can judge whether the member node is legal or not based on MAC. If it is illegal, then the node is excluded.

For mobile device's key update, after the device enters a certain cluster, it receives the update instruction transmitted from the cluster head key, extracts the data in the instruction content, and obtains the cluster new key through calculation.

(4) Authentication broadcast and key update

Wireless sensor network needs to implement point-to-multipoint broadcast authentication, which is the key component of the network to complete the command given by the gateway, and can avoid false instructions. Here, we introduce the μTESLA protocol to realise broadcast authentication. In the process, a data packet that has been

proved by K_{mac} is firstly broadcasted, and then K_{mac} is published. Furthermore, it can prevent the forgery of broadcast data before the release of K_{mac}.

The update of the key is divided into the following parts:

Key update: If no routing device has been captured or deleted, the new key will be encrypted by the original key after the key expires, and updated according to the way of gateway distribution. On the contrary, it needs to implement key request through backup route, and uses backup route and personal key in gateway preset to achieve device authentication, so as to obtain the key.

Cluster key update: In general, the cluster key will be updated after a period of time. Since the number of cluster members does not change, the route assigns a new random number N_A^* to the cluster based on the encryption of cluster key. When the cluster members receive it, they decrypt it through the old cluster key to get the new cluster key:

$$K_{Ci}^* = H\left(\text{Num} \,||\, N_A^*\right) \tag{23}$$

If the routing device recognises that a field device has been captured, or a new field device has been added, the routing device will assign a new device number Num^* and N_A^* to the whole cluster. After receiving the new cluster key, the new cluster key is calculated:

$$K_{Ci}^* = H\left(\text{Num}^* \,||\, N_A^*\right) \tag{24}$$

Personal key update: If the device is captured, the device is installed and the network is removed, so the key does not need to be updated.

Communication key update: The main part of the key generation is temporary initial key and key chain. Since the initial key will be removed after the device enters the network safely, the communication key update can only be realised by key chain. In this paper, the communication key is updated at the end of the key chain during each broadcast.

$$K_{\text{Com}} = H\left(K_{\text{init}} \,||\, X_i\right) \tag{25}$$

Group key update: In general, this key encrypts the new group key according to the original group key to implement the whole network broadcast. If the device is captured, the group key is updated by updating the key and the cluster key.

3 Experimental verification

In order to verify the performance of the DV-hop based secure key distribution method in wireless sensor networks, an experiment is carried out. During the experiment, the experimental platform is built on eclipse, the program is written by java language, and the data analysis is realised by MATLAB. The experimental data is selected from the key data of wireless sensor network in MySQL database. The data size is 5GB, and the number of sensor network nodes is 600.

3.1 Experimental indexes

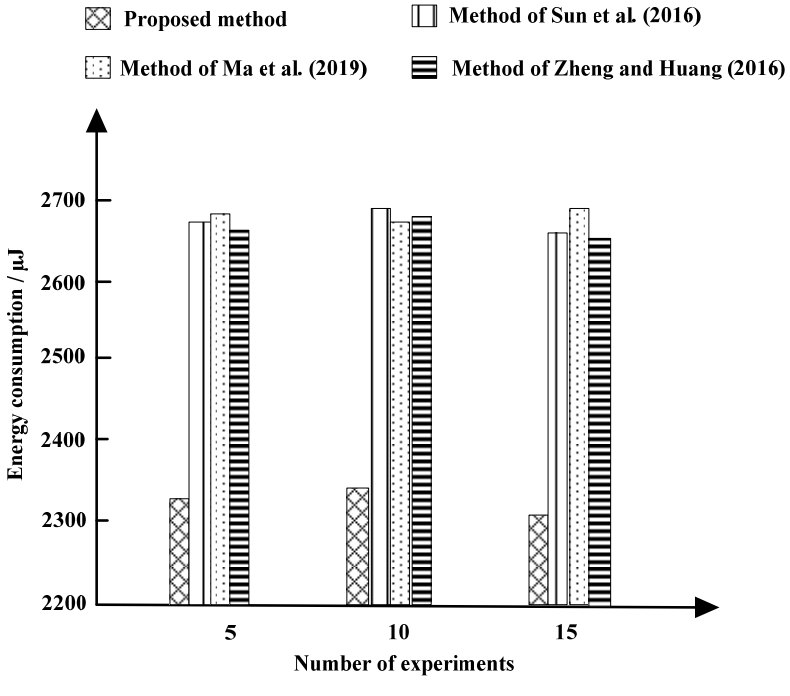
In order to improve the accuracy of the experimental results, the proposed method is compared with the methods in Sun et al. (2016), Ma et al. (2019) and Zheng and Huang (2016) by taking the distribution energy consumption (building energy consumption, distribution energy consumption) and anti-aggression as the experimental comparison indexes.

- *Energy consumption distribution*: The energy consumption of sensor network security key distribution is divided into security key establishment energy consumption and security key allocation energy consumption. The lower the establishment energy consumption and the distribution energy consumption, the lower the energy saving effect of the security key distribution method.
- *Anti-attack*: Anti-attack can directly reflect the performance of security key distribution. The higher the success rate of wireless sensor networks in resisting attacks, the higher the rationality of security key distribution.

3.2 Comparison of distribution energy consumption

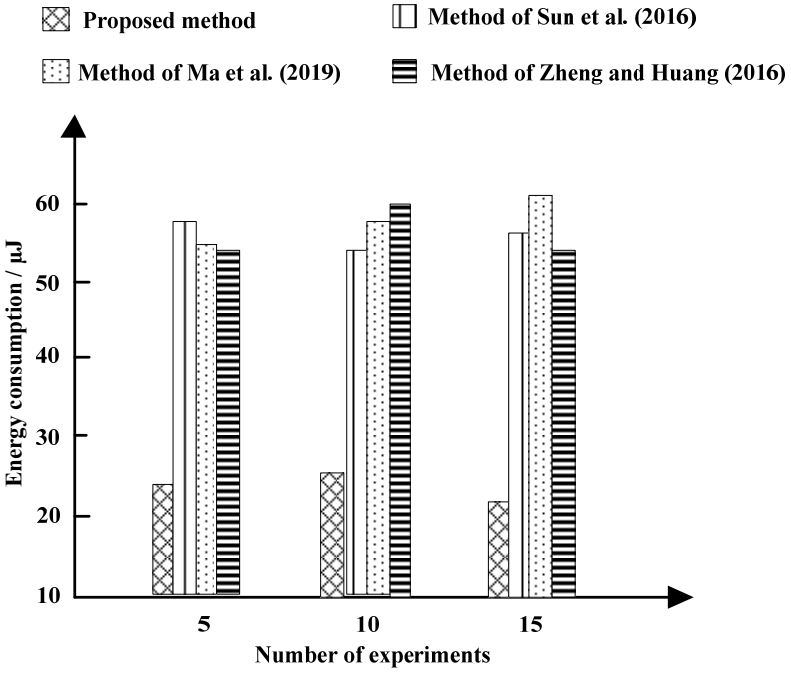
The key distribution is simulated for 15 times to obtain the simulated values of the file data. The experimental indexes are to establish energy consumption/μJ, distribution energy consumption/μJ, and the energy consumption results are shown in Figure 8.

Figure 8 Comparison of key distribution energy consumption of four methods: (a) establishing energy consumption and (b) allocating energy consumption



(a)

Figure 8 Comparison of key distribution energy consumption of four methods: (a) establishing energy consumption and (b) allocating energy consumption (continued)



(b)

Analysis of the experimental results in Figure 8 shows that the distribution energy consumption of the proposed method in 15 simulation experiments is lower than that of the three literature comparison methods. In the comparison of communication energy consumption, the energy consumption of the proposed method is reduced by up to 400 μJ. In the calculation of energy consumption comparison, the maximum energy consumption of the proposed method does not exceed 30 μJ, which fully proves that the proposed method can effectively reduce the allocated energy consumption. Because the proposed method can transmit the requests within the same superframe to the gateway in a combined manner, which effectively reduces the number of requests sent, which is very beneficial to the reduction of computing and communication energy consumption.

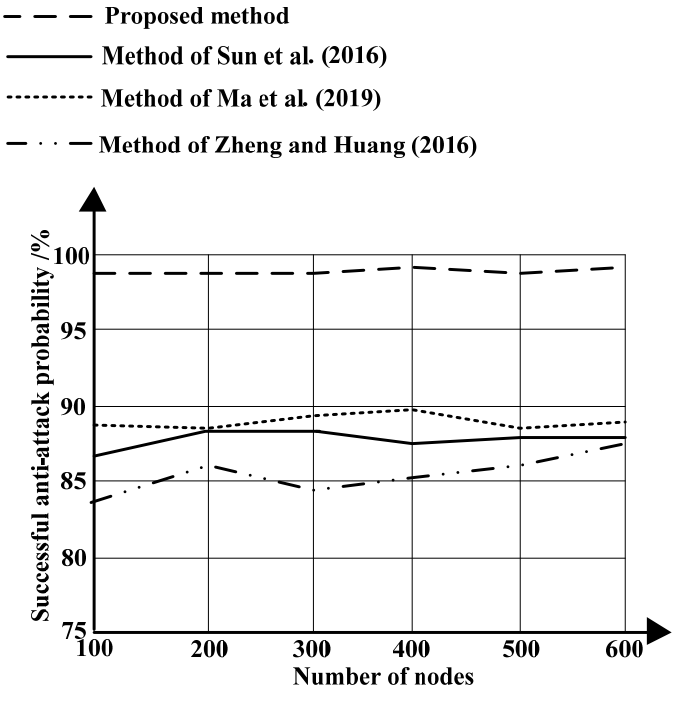
3.3 Comparison of anti-attack performance

Figure 9 shows the experimental results of four allocation methods.

It can be seen from Figure 9 that compared with the three traditional methods, the proposed method has stronger anti-attack performance, and the probability of successful anti-attack of the proposed method can reach up to 98%, while the successful anti-attack probability of the three traditional methods does not exceed 90%. This method is based on the positioning result of the DV-hop algorithm. In the face of an attack, the Beacon information is encrypted with a temporary initial key, which can verify the legitimacy of the information. Assuming that it is false information, the request will be rejected. At the same time report to the gateway, so this method can effectively prevent network attacks.

Because the proposed method authenticates the routing device through the gateway and uses the gateway to specify routing information based on various routing states, a black hole cannot be formed. The data transmission of the device is implemented based on random numbers, which can guarantee the novelty of the data. During the process of replaying the data, the illegal node cannot obtain the random number, so the data cannot be modified, and the replay attack can be effectively avoided.

Figure 9 Comparison results of anti-attack



4 Conclusions

To solve the security problem of wireless sensor network, a DV-hop algorithm based security key distribution method is proposed. The following conclusions are proved in theory and experiment. This method has low energy consumption and high anti attack performance when it is used in wireless sensor network security key distribution. Specifically, compared with the allocation method based on vector selection, the allocation energy consumption is significantly reduced, up to 400 μJ; compared with the allocation method based on acoustooptic modulator, the anti attack performance is greatly improved, and the probability of successful anti attack is up to 98%. Therefore, the proposed method based on DV-hop algorithm can better meet the requirements of wireless sensor network security key distribution. In the future research, we should further improve the anti attack performance of wireless sensor network.

References

Cao, M., Yu, B.J., Liu, X.T. and Chai, W.G. (2017a) 'Simulation of secure storage of high density information for network data transmission', *Computer Simulation*, Vol. 34, No. 12, pp.153–156.

Cao, Y., Zhao, Y., Meixner, C.C. and Yu, X.S. (2017b) 'Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)', *Optics Express*, Vol. 25, No. 22, pp.26453–26467.

Chun, H., Choi, I., Faulkner, G. and Clarke, K. (2017) 'Handheld free space quantum key distribution with dynamic motion compensation', *Optics Express*, Vol. 25, No. 6, pp.6784–6795.

Ding, Y.Y., Chen, W., Chen, H. and Wang, C. (2016) 'Polarization basis tracking scheme for quantum key distribution with revealed sifted key bits', *Optics Letters*, Vol. 42, No. 6, pp.1023–1026.

Gao, F., Ma, H.Q. and Jiao, R.Z. (2016) 'The optimization of measurement device independent quantum key distribution', *Modern Physics Letters B*, Vol. 30, No. 11, pp.090501–1132.

Huang, M., Yu, B. and Li, S. (2018) 'PUF-assisted group key distribution scheme for software-defined wireless sensor networks', *IEEE Communications Letters*, Vol. 22, No. 2, pp.404–407.

Kang, G.D., Zhou, Q.P. and Fang, M.F. (2017) 'Side channel passive quantum key distribution with one uninformative state', *International Journal of Theoretical Physics*, Vol. 56, No. 3, pp.833–840.

Kiktenko, E.O., Pozhar, N.O., Duplinskiy, A.V. and Kanapin, A.A. (2017) 'Demonstration of a quantum key distribution network in urban fibre-optic communication lines', *Quantum Electronics*, Vol. 47, No. 9, pp.798–802.

Li, H., Wang, C., Huang, P. and Huang, D. (2016) 'Practical continuous-variable quantum key distribution without finite sampling bandwidth effects', *Optics Express*, Vol. 24, No. 18, pp.20481–20493.

Liang, J.Q., Jin, X.J., Tong, W.M. and Li, Z.W. (2016) 'Key management scheme for wireless sensor networks in advanced metering infrastructure', *Automation of Electric Power Systems*, Vol. 40, No. 19, pp.119–126.

Ma, Y.Y., Jia, G.T., Liu, Y. and Huang, X.L. (2019) 'Security of quantum key distribution with wavelength attack', *Chinese Journal of Quantum Electronics*, Vol. 36, No. 3, pp.342–347.

Sun, Y., Zhao, S.H. and Dong, C. (2016) 'Measurement device independent quantum key distribution network based on quantum memory and entangled photon sources', *Acta Optica Sinica*, Vol. 36, No. 3, pp.238–244.

Wang, L., Wang, H., Khan, M.K. and He, D.B. (2016) 'Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography', *IET Communications*, Vol. 10, No. 14, pp.1795–1802.

Wang, Y.H., Ling, Y.H., Liao, L.Q., Sun, K.H. and Liu, W.H. (2017) 'Novel chaotic block encryption scheme for WSN based on dynamic sub key', *Journal on Communications*, Vol. 38, No. 12, pp.144–152.

Zhang, J., Zhu, J.H., Jiang, Z.P. and Yan, X.X. (2016b) 'Energy-saving and privacy-preserving range query in wireless sensor networks', *Application Research of Computers*, Vol. 33, No. 4, pp.1199–1202+1206.

Zhang, M.H., Li, H.F., Peng, J.Y. and Feng, X.Y. (2017) 'Fault-tolerant semiquantum key distribution over a collective-dephasing noise channel', *International Journal of Theoretical Physics*, Vol. 56, No. 25, pp.2659–2670.

Zhang, Y.Y., Bao, W.S., Zhou, C. and Li, H.W. (2016) 'Practical round-robin differential phase-shift quantum key distribution', *Optics Express*, Vol. 24, No. 18, pp.20763–20773.

Zheng, Y.F. and Huang, C.H. (2016) 'Application of acousto-optic modulator in BPSK quantum key distribution', *Optical Communication Technology*, Vol. 40, No. 8, pp.27–29.