International Journal of Autonomous and Adaptive Communications Systems

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

Dynamic key distribution method for wireless sensor networks based on exponential algorithm

Yun Zhao, Yong Xiao, Weibin Lin, Chao Cui, Di Xu

DOI: 10.1504/IJAACS.2023.10043736

Article History:

Received:	30 April 2020
Accepted:	01 September 2020
Published online:	17 March 2023

Dynamic key distribution method for wireless sensor networks based on exponential algorithm

Yun Zhao*, Yong Xiao, Weibin Lin, Chao Cui and Di Xu

Electric Power Research Institute of China Southern Power Grid,
Guangzhou, 510080, China
Email: yunzhao@mls.sinanet.com
Email: 710893476@qq.com
Email: 408222658@qq.com
Email: 743099892@qq.com
Email: 404484437@qq.com
*Corresponding author

Abstract: The purpose of this paper is to overcome the problems of high communication failure probability, high energy cost, low global connectivity and poor network robustness, a dynamic key distribution method based on exponential algorithm is proposed. In this method, the collusion characteristics of newly added nodes and revoked nodes in wireless sensor networks are used to establish a wireless sensor security model. The exponential algorithm is used to initialise, broadcast, self repair session key and mutual session key It can help repair, add nodes and cancel nodes to realise dynamic key distribution. The experimental results show that when the number of dynamic key nodes is 600, the probability of communication failure is 47%; when the number of hops is 10, the energy cost is only 1.64 mJ, and the network robustness is high. It reduces the pressure of wireless sensor network and plays a positive role in the root cause location of massive alarm information fault.

Keywords: exponential algorithm; wireless sensor; network; dynamic key; distribution; method.

Reference to this paper should be made as follows: Zhao, Y., Xiao, Y., Lin, W., Cui, C. and Xu, D. (2023) 'Dynamic key distribution method for wireless sensor networks based on exponential algorithm', *Int. J. Autonomous and Adaptive Communications Systems*, Vol. 16, No. 1, pp.97–111.

Biographical notes: Yun Zhao received his PhD in Electrical Engineering from Wuhan University, Wuhan, China, in 2013. He is currently a Senior Engineer in the Electric Power Research Institute of China Southern Power Grid. His research interests include big data application of electricity, cyber security defense of AMI.

Yong Xiao received his MS in Electronic Engineering from University of Electronic Science and Technology of China, Chengdu, China in 2005. He is currently the director of AMI Department in the Electric Power Research Institute of China Southern Power Grid. His research interests include big data application of electricity, cyber security defense of AMI.

Weibin Lin received his MS in Electrical Engineering from South China University of Technology, Guangzhou, China, in 2005. He is a Senior Engineer in the Electric Power Research Institute of China Southern Power Grid. His research interests include cyber security defense of AMI.

Chao Cui received his MS in Control Engineering from North China Electric Power University in 2016. He is an engineer in the Electric Power Research Institute of China Southern Power Grid. His research interests include cyber security defense of AMI.

Di Xu received her MS in Electrical Engineering from Xi'an Jiaotong University, Xi'an, China, in 2018. She is an Engineer in the Electric Power Research Institute of China Southern Power Grid. Her research interests include cyber security defense of AMI.

1 Introduction

Wireless sensor network can be applied to the environment where human beings cannot survive. Through the corresponding response of the nodes in the wireless sensor to the external environment, the sensor nodes are distributed in the task area. The sensor nodes collect various information data, and the nodes in the wireless sensor work are together to achieve the task (Cao and Xu, 2019; Liu et al., 2019). The wireless sensor is usually powered by battery, and the battery power determines the service life of the wireless sensor. The wireless sensor is usually arranged in the field and other harsh environment, so the battery power cannot be replenished in time to reduce the service life of the wireless sensor. Wireless sensor nodes are composed of sensing devices, which have poor data processing ability and radio communication ability. Wireless sensor networks are usually used in all kinds of information collection or military and other aviation fields. When wireless sensors are used in military and other fields, they are vulnerable to malicious attacks or monitoring (Li and Feng, 2018; Qiao, 2017). So the security problem is very important. In the military field, the wireless sensor is eavesdropped or damaged by the other party, which will cause a very serious impact. When wireless sensor is used in daily life, it is seriously damaged by hackers or lawbreakers. In order to ensure the security of wireless sensor communication, the key distribution problem in the process of communication content encryption is an urgent problem to be solved in wireless sensor network (Cao et al., 2019).

At present, there are many key distribution methods used in wireless sensor networks. In Zhong and Lv (2019), a multi-space key distribution algorithm is proposed, which is mainly composed of key's pre distribution stage and key's negotiation stage. The specific implementation is to first construct ω key spaces based on single space key's pre distribution scheme, and then each sensor node carries key information from τ $(2 \leq \tau\ \omega)$ randomly selected key spaces, so as to calculate their paired keys from this information; when two nodes do not carry key information from public space, they can calculate their pairwise keys by receiving a broadcast message containing the node ID, the space index carried and the seeds carried and sharing the pairwise keys with other nodes; The simulation results show that the proposed algorithm not only has low communication overhead, but also is superior to some existing common pre distribution algorithms of key in terms of security and computational marketing. However, the communication failure probability of sensor nodes is high in this method. In He and Guo (2019), the measurement device of a real-time tracking compensation operation administration and maintenance (OAM) code independent quantum key distribution (OAM-MDI-QKD) scheme is proposed. In the scheme, wavefront compensation and phase conjugation are used to design an adaptive optical system with double compensation; the structure of single light source is used to solve the problem of wavelength pattern mismatch of double light sources; OAM is used to code to solve the problem of inaccurate measurement basis reference system of traditional MDI-QKD. The simulation results show that the loss tolerance of this scheme is higher when the channel loss is the same. However, the energy cost of nodes in this method is large. In Dai et al. (2019), a new key distribution scheme of mutual healing group (MGKD) is proposed. The MGKD scheme is based on exponential algorithm. It uses random numbers to hide the private keys of nodes, uses hash function to construct broadcast messages, and uses neighbour nodes to make up for the shortcomings of the scheme. Experiments show that the scheme is suitable for wireless sensor networks. However, the global connectivity of this method is low.

Based on the shortcomings of the above key distribution methods, the storage capacity of wireless sensor network is very limited in practical application, and the number of nodes in wireless sensor network is usually very large, so a dynamic key distribution method for wireless sensor network based on exponential algorithm is proposed. By building a wireless sensor model, considering all types of collusion attacks, the new key distribution method in wireless sensor network is proposed. The collusion characteristics of the added node and the revoked node are added to the wireless sensor's security model for processing. According to the principle of index algorithm, the dynamic key distribution of network is completed from the following aspects: initialisation, broadcast, self-repair of session key, mutual repair of session key, joining node and withdrawing node. This method does not need to set the pre distribution of key in wireless sensor networks, and increases the flexibility of dynamic key distribution in wireless sensor networks. When nodes are added or deleted in wireless sensor networks, the security of wireless sensor networks can still be guaranteed. The experimental results show that when the number of dynamic key nodes is 600, the probability of communication failure is 47%; when the number of hops is 10, the energy cost is only 1.64 mJ, and the network robustness is high.

2 Research on dynamic key distribution of wireless sensor networks

Based on the exponential algorithm, the cross-healing group key distribution scheme is designed by using the Lagrange interpolation method. On the basis of reducing the communication cost, it can ensure forward secrecy, backward secrecy and resist collusion attack.

2.1 Wireless sensor's security model

The communication group of wireless sensor network includes n group member nodes and a group key management center node (Yang et al., 2018). In wireless sensor networks, each group of member nodes has an independent ID number expressed by i, which meets the requirement of $i \in \{1,2,\ldots,n\}$. In wireless sensor network, the number of n group member nodes is represented by Q, which satisfies $Q = \{Q_1,\ldots,Q_n\}$, and Q_i is represented by n group member.

When the communication session is set to j, the legal communication group of wireless sensor network composed of group manager in wireless sensor network is $G_j \in Q$. When the wireless sensor network session is j, the private key of group member node Q_i is represented by $P_{i,j}$. When a group member node Q_i is added to the communication group G_j of the wireless sensor network, the private key obtained from the group manager of the wireless sensor network is represented by $P_{i,j}$. When the group manager of wireless sensor network sends the session key L_j to the group member node Q_i by using the broadcast message B_j during the session, L_j represents the group key when the session is j. When the session is j, the group key distribution message broadcast by the group manager of wireless sensor network is B_j. It can be seen that any group member node Q_i in wireless sensor network needs to meet $Q_i \in G_j$, and the session key L_j is obtained by B_j and $P_{i,j}$.

All the above operations need to be implemented in the finite field F_q and q is the prime number greater than n.

The enemy to obtain an unknown number of group member nodes in the wireless sensor network is set. When the group manager of the wireless sensor network finds that the enemy intrudes, the intruded node can be revoked (Gao, 2019). Nodes in wireless sensor networks are vulnerable to collusion attacks. When designing dynamic key distribution methods for wireless sensor networks, all types of collusion attacks need to be considered comprehensively. The invaded nodes can collude with other nodes (Banerjee and Sipra, 2017), and the newly added nodes can be used to obtain the non-infringing communication session key. In order to consider the collusion attack, the collusion characteristics of new and cancelled nodes are added to the wireless sensor security model.

Definition 1 (Undo function)**:** Set $i \in \{1,2,\ldots,n\}$, and use D to represent the dynamic key distribution method for wireless sensor network with revocation function. D must meet the following conditions:

1 The group session key of random node $Q_i \in G_j$ can be determined by B_j and P_i;

2 The session key L_j cannot be determined by the node private key P_i and the broadcast message B_j.

3 The dynamic key distribution method D of wireless sensor network has the revocation characteristic. $R \subseteq Q$ is used to represent the set of revocation nodes in random session j, $|R| \leq t$. The group manager of wireless sensor network can make all $Q_i \in R$ by setting up broadcast message B_j, and Q_i can effectively recover session key L_j.

4 When the wireless sensor network has self-healing characteristics, the following conditions are met: for random j, it needs to meet $1 < j_1 < j < j_2$; when the session is j, the members of the random legal group in node Q_i recover the session key L_j in the broadcast message B_{j_1} and B_{j_2}.

Definition 2 (forward confidentiality**):** The dynamic key distribution method in wireless sensor networks needs to ensure forward secrecy (Johann et al., 2017), and the group member node set is set as $B \subseteq Q$ that exists in session *j* and before session *j* to meet $|B| \leq t$. The members in node set B still conspire to obtain session key L_j when they have all group session keys before session *j* and *j*.

Definition 3 (backward confidentiality**):** The dynamic key distribution method in wireless sensor networks needs to guarantee backward secrecy. It is assumed that there is a group member node set $J \subseteq Q$ added to session *j* randomly, which satisfies $|J| \leq t$. The members in node set J still conspire to obtain session key L_j when they have all group session keys after session.

Definition 4 (anti-collusion attack feature**):** The dynamic key distribution method of wireless sensor network needs to have the characteristics of anti-collusion attack (Mekikis et al., 2018), and it is assumed that there are random disjoint sets *B* and *C*, and $|B \cup C| \leq t$. All nodes in set B are revoked before session j_1 and j_1, and all nodes in set C join session j_2. At this time, the nodes in $B \cup C$ cannot recover session key L_j.

2.2 *Dynamic key distribution method based on exponential algorithm*

2.2.1 *Workflow*

The structure of dynamic key distribution method based on exponential algorithm obtained by using wireless sensor security model is shown in Figure 1.

In wireless sensor network, multiple sessions are used to represent the lifetime of group communication. The lifetime of wireless communication network ensures communication security by updating session key (Parisa and Abbas, 2017). Each session of wireless sensor network has a unique group key. The group manager of wireless sensor network uses the update broadcast key L_j to send the updated session key to each node of wireless sensor network.

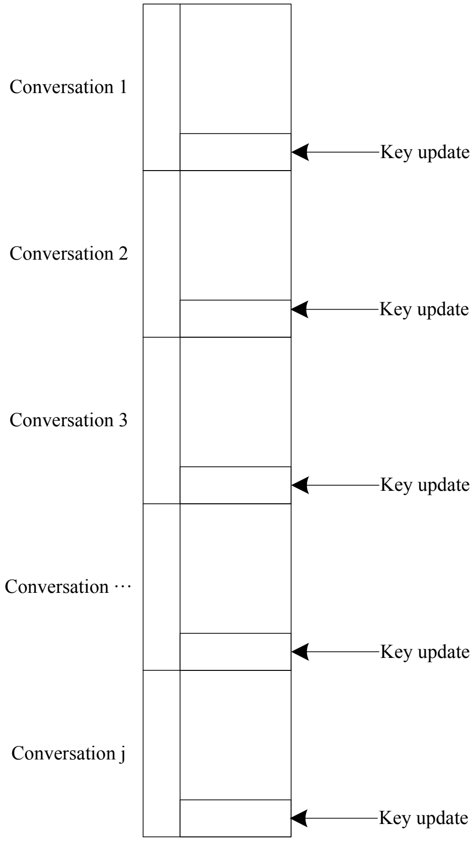
2.2.2 *Method description*

The dynamic key distribution method based on exponential algorithm includes five steps: initialisation, broadcast, self-healing of session key, mutual repairing of session key, joining node and withdrawing node.

1 *Initialisation*

The group manager of wireless sensor network selects the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_t x^t$ and ε_j in the finite field, where $j \in [1, m]$. Using $\varepsilon_j \cdot f(s_i)$ to hide the private key of the node in WSN can improve the security of WSN (Gong et al., 2019), establish the private key of the node in Q_i represented by $P_i = \{p_i, \varepsilon_j \cdot f(p_i)\}$, and the group manager uses the secure channel of WSN to allocate and send the private key of the node to the node Q_i joined by session *j*.

Figure 1 Structure of a dynamic key distribution method based on an exponential algorithm



2 *Broadcasting*

The nodes added in session j_1 and the nodes still included in session j are represented by G_{j_1}; the set of undo nodes in session j and the node whose identity ID number is s_i are represented by R_j and R_i^j respectively. The group manager randomly selects the seed P_1^{FB} in the finite field F_q, and uses Haas function $H(\bullet)$ to establish Haas chain with length m as follows:

$$\begin{cases} P_1^{FB} = H\left(P_1^{FB}\right) \\ P_2^{FB} = H^2\left(P_1^{FB}\right) \\ P_3^{FB} = H^3\left(P_1^{FB}\right) \\ \quad \cdots \\ P_m^{FB} = H^m\left(P_1^{FB}\right) \end{cases} \tag{1}$$

In order to hide the group session key (Chun et al., 2017) of wireless sensor networks, $l_1(0 < j \leq m)$ selected randomly from the finite domain F_q is calculated as follows:

$$\begin{cases} l_2 = l_1 \cdot H\left(P_1^{FB}\right) \\ l_3 = l_2 \cdot P_2^{FB} = l_2 \cdot H^2\left(P_1^{FB}\right) \\ \cdots \\ l_j = l_{j-1} \cdot P_{j-1}^{FB} = l_{j-1} \cdot H^{j-1}\left(P_1^{FB}\right) \end{cases} \tag{2}$$

The group manager of wireless sensor network randomly selects ∂_i and θ_{j_1} in the limited domain, and the selected ones cannot be used as the identity of nodes. The polynomials of using node identity are as follows:

$$\begin{cases} A_{j_1}(x) = \left(x - \theta_{j_1}\right) \prod_{i=1}^{\left|G_{j_1}\right|} (P_i) \prod_{i=1}^{t-1-\left|G_{j_1}\right|} (\partial_i) \quad \left(\left|G_{j_1}\right| \leq t-1\right) \\ A_{j_1}(x) = \left(x - \theta_{j_1}\right) \prod_{i=1}^{\left|G_{j_1}\right|} (P_i) \quad \left(\left|G_{j_1}\right| > t-1\right) \end{cases} \tag{3}$$

The group manager of wireless sensor network is calculated as follows:

$$P_{j_1}(x) = \left(1 + A_{j_1}(x)\right) \cdot l_{j-1} \cdot H^{j-1}\left(P_1^{FB}\right) + \varepsilon_{j_1} \cdot f(x) \tag{4}$$

$$g^{P_{j_1}(x)} = g^{\left(1 + A_{j_1}(x)\right) \bullet l_{j-1} \bullet H^{j-1}\left(P_1^{FB}\right) + \varepsilon_{j_1} \bullet f(x)} \tag{5}$$

Using group manager of wireless sensor network to build broadcast message B_j, the process is as follows:

$$\begin{cases} g^{P_{j_1}(x)} = g^{\left(1 + A_{j_1}(x)\right) \bullet l_{j-1} \bullet H^{j-1}\left(P_1^{FB}\right) + \varepsilon_{j_1} \bullet f(x)} \qquad j_1 = [1, j] \in Z^+ \\ \left\{E_{k1}(K_1), E_{l_1 \bullet H\left(P_1^{FB}\right)}(K_2) \cdots, E_{l_{j-1} \bullet H^{j-1}\left(P_1^{FB}\right)}\left(E_{l_j}\right)\right\} \end{cases} \tag{6}$$

3 *Self-repair of session key*

The formula obtained by formula (4) is as follows:

$$g^{l_{j_1}} = g^{l_{j-1} \bullet H^{j-1}\left(P_1^{FB}\right)} = g^{\frac{P_{j_1}(p_i) - \varepsilon_{j_1} \bullet f(P_i)}{1 + A_{j_1}(P_i)}} \tag{7}$$

When Q_i is the legal node in G_{j_1}, $A_{j_1}(p_i) = 0$ can be obtained, otherwise $A_{j_1}(p_i)$ is a random value, and $L_{j_1} \neq l_{j-1} \cdot H^{j-1}\left(P_1^{FB}\right)$ can be obtained.

When there is session j_2 in wireless sensor network, formulas (1) and (2) are used to obtain the wireless sensor node Q_i, and l_{j_2} is obtained through the encryption function $E_k(\cdot)$ of formula (6).

4 *Mutual repair of session key*

When the key update package of the final session *m* in wireless sensor network is lost by node Q_i, the session key can be repaired by using the legitimate neighbour node $Q_{i'}$ of node . The repair process is as follows:

(1) *Message sending request*

When the time is t_i, node Q_i sends the request information to node $Q_{i'}$ to obtain the final key update package.

(2) *Message reply*

When the time is t_i, node $Q_{i'}$ needs to determine whether $|t_{i'} - t_i| \leq \Delta t$ is true after obtaining the request message. When $|t_{i'} - t_i| \leq \Delta t$ is not established, it means that the transmission time is too long (Kiktenko et al., 2017; Li et al., 2018; Zou et al., 2019; Hossain et al., 2019), and there is no need to reply to the request information of Q_i; when $|t_{i'} - t_i| \leq \Delta t$ is established, node $Q_{i'}$ needs to send node ID number i' and broadcast message to node Q_i.

(3) *Key recovery*

After the node $Q_{i'}$ sends the reply message to the node Q_i, the final session key is obtained by formulas (6) and (7).

(4) *Joining node and withdrawing node*

When the session is set to $j-1$, the node Q_i of the wireless sensor network joins the communication group, and the group manager of the wireless sensor network transmits the node key $P_i = \{p_i, \varepsilon_j \cdot f(p_i)\}$ and identity ID number p_i of the newly joined node by using the secure channel encryption.

If there is a node joining and withdrawing in session j_1 and session j respectively, then the group manager of WSN will delete $(x - p_i)$ from $A_{j_1}(x)$.

When a node is added or removed from the wireless sensor network, the group manager of the wireless sensor network will restart a new session and update the broadcast message. To sum up, dynamic key distribution can be completed.

3 Experimental conclusion

3.1 Experimental scheme

In order to verify the dynamic key distribution of wireless sensor network, in the computer with Intel G5400 8-generation Pentium Dual Core CPU and 8GB memory, MATLAB software is used to simulate the wireless sensor network topology. The number of sensor nodes in the wireless sensor network is 600, and the number of key pools and sub key pools are 10 and 50, respectively. The multi-space key distribution algorithm, the independent quantum key distribution method and the mutual healing group key distribution method are selected as the comparison methods to show the dynamic key distribution of the proposed method.

3.2 Performance index research

(1) *Communication failure probability of sensor nodes*

$$p(\xi = q) = \binom{n}{q} \times \left(\frac{1}{r}\right) \times \left(1 - \frac{1}{r}\right)^{n-q} \tag{8}$$

In the above formula, q represents the probability of the same configuration of the massive big data, ξ represents the probability of reducing the storage space of the massive big data, n represents the attribute of the massive big data, and r represents the configurable value of the attribute of the massive big data.

(2) *Energy cost of node*

$$E_{sensor} = P_s t_s + P_{ts} t_{ts} \tag{9}$$

In the above formula, P_s and P_{ts} are node sensing power and node transmission data power respectively, t_s and t_{ts} are data sensing time and data transmission time respectively.

(3) *Global connectivity*

$$P = 1 - \frac{C_{|S|-m}^{m}}{C_{|S|}^{m}} \tag{10}$$

In the above formula, *m* means to increase the key ring size, and $|s|$ means to decrease the key pool size.

(4) *Robustness of the network*

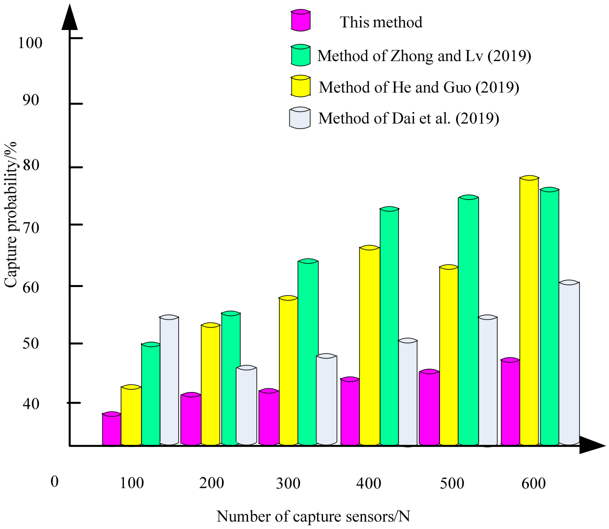
Robustness refers to the processing ability of software for input conditions beyond the specification requirements. The so-called robust system refers to the input beyond the specification requirements can determine that the input does not meet the specification requirements, and can have a reasonable way of processing.

3.3 Analysis of experimental results

1 When the number of capture sensor nodes is different, the communication failure probability of sensor nodes in wireless sensor network is calculated, and the method in this paper is compared with multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method. The comparison results are shown in Figure 2.

From the experimental results in Figure 2, it can be seen that three methods are used to distribute the dynamic key of wireless sensor network, and the probability of communication failure between points increases with the increase of the number of acquisition sensor nodes. When the number of capture sensor nodes is 600, the probability of communication failure between nodes using the proposed method is 47%, while the probability of communication failure among nodes using multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method is 74%, 76% and 58%, respectively. The communication failure probability of dynamic key nodes in wireless sensor networks distributed by the proposed method is significantly lower than that of multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method. It shows that the network security of dynamic key distribution in wireless sensor networks distributed by the proposed method is significantly higher than that of multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method.

Figure 2 Node destruction rate when capturing the number of sensor nodes (see online version for colours)



2 Three methods are used to allocate the dynamic key of WSN in different hops. The comparison results are shown in Table 1.

Table 1 Energy cost of three methods at different hop counts

Hop count	*This method/mJ*	*Multi-space key distribution algorithm/mJ*	*Independent quantum key distribution method/mJ*	*Mutual healing group key distribution method/mJ*
1	0.05	0.12	0.16	0.15
2	0.23	0.45	0.53	0.52
3	0.34	0.74	0.94	0.98
4	0.52	0.89	1.35	1.25
5	0.73	0.92	1.54	1.56
6	0.95	1.32	1.85	1.88
7	1.26	1.75	2.23	2.25
8	1.54	1.95	2.64	2.69
9	1.85	2.45	2.85	2.86
10	1.64	2.85	3.05	3.06

According to the experimental results in Table 1, we can see that the energy cost of key distribution between source sensor node and destination sensor node by using the proposed method is far less than that of multi space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method. Using the proposed method to distribute dynamic key hops in wireless sensor network, when the number of dynamic key hops is 10, the energy cost is only 1.64 mJ; while that of the multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method are 2.85 mJ, 3.05 mJ and 3.06 mJ, respectively, when the number of dynamic key hops is 10. The main reason is that multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method need to send a random number of keys to all sensor nodes in the process of dynamic key distribution, and the paths of sensor nodes that are not related to communication also need to be sent, which increases a lot of energy overhead. It is verified that the proposed method used to distribute dynamic key devices in wireless sensor networks has high allocation performance.

The probability of key sharing of random sensor nodes in wireless sensor network is set to 0.4, and the energy cost of sensor nodes are calculated when using three methods to distribute dynamic key of wireless sensor network with different number of sub key pools. The comparison results are shown in Table 2.

Table 2 Energy cost of the three methods with different numbers of subkey pools

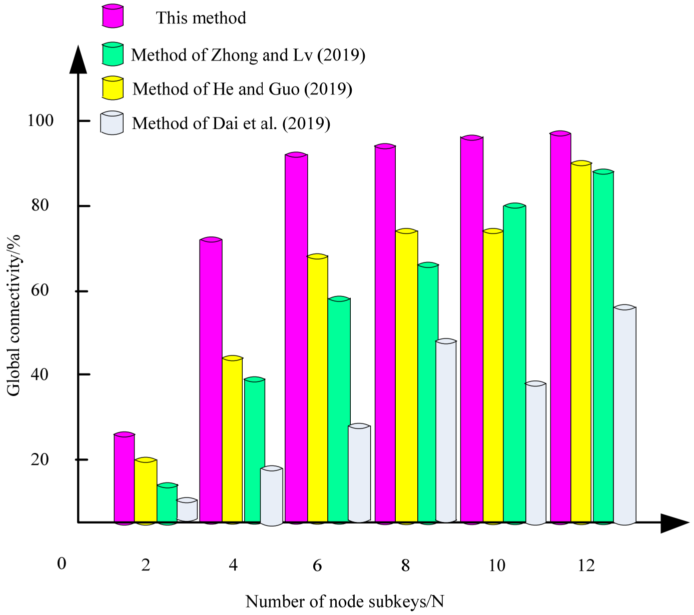
Number of child key pools	*This method/mJ*	*Multi-space key distribution algorithm/mJ*	*Independent quantum key distribution method/mJ*	*Mutual healing group key distribution method/mJ*
5	0.52	0.85	0.75	0.82
10	0.67	1.12	1.26	1.14
15	0.75	1.52	1.85	1.56
20	0.82	1.84	2.34	2.25
25	0.94	2.23	2.75	2.86
30	1.03	2.56	2.95	2.65
35	1.46	2.84	3.32	3.21
40	1.76	3.26	3.52	3.41
45	2.23	3.54	3.75	3.25
50	2.45	3.85	4.05	4.06

It can be seen from the experimental results in Table 2 that the energy consumption of key distribution between the source sensor node and the destination sensor node is far less than that of multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method when the dynamic key pools of wireless sensor network are distributed by the method in this paper. When the number of dynamic key sub key pools is 50, the energy cost is only 2.45 mJ, while that of the multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method are 3.85 mJ, 4.05 mJ and 4.06 mJ, respectively, when the number of dynamic key sub key pools is 50. Using this method to distribute the dynamic key of wireless sensor network has low energy cost, which verifies the performance of this method again.

3 According to the statistics, three methods are used to distribute the dynamic key of wireless sensor network. When the number of sub key pools is different, the probability that two random wireless sensor nodes establish a secure key channel is the global connectivity. The comparison results are shown in Figure 3.

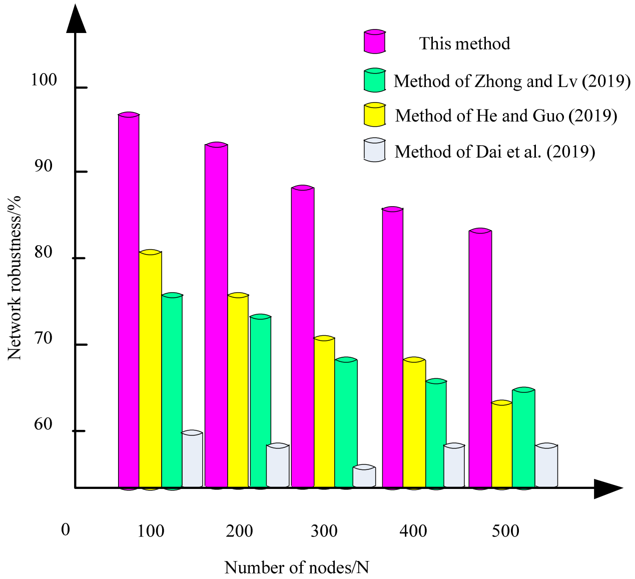
From the experimental results in Figure 3, we can see that the global connectivity of the proposed method is significantly higher than that of multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method when the number of sub key pools is different. When the number of nodes and hops increases, the probability of establishing a secure key channel increases. When the number of sub key pools is 6, the probability of establishing a secure key channel for two random wireless sensor nodes using the proposed method is close to 1, and the global connectivity of the other two methods is significantly lower than that of the proposed method, so that the validity of dynamic key distribution in wireless sensor networks is verified.

Figure 3 Global connectivity rates of different dynamic key distribution methods (see online version for colours)



4 The network robustness of dynamic key distribution of wireless sensor network by three methods is statistically analysed, and the comparison results are shown in Figure 4.

Figure 4 Comparison of network robustness of different methods (see online version for colours)



From the experimental results in Figure 4, it can be seen that the network robustness of dynamic key distribution method in this paper is significantly higher than that of multi-space key distribution algorithm, independent quantum key distribution method and mutual healing group key distribution method. When the dynamic key distribution method in this paper is used to distribute the dynamic key of wireless sensor network, when the exchange public parameters are stolen, the thief still cannot obtain the key, and the reason is that the key of each node is not the same, stealing the key of each node has no effect on other nodes, so as to improve the robustness of wireless sensor network.

In order to further verify the security performance of the method in this paper for dynamic key distribution in wireless sensor networks, the method in this paper is compared with different key distribution methods, and the security performance of the method in this paper is compared through three aspects: forward security, backward security and anti-collusion attack. The comparison results are shown in Table 3.

Table 3 Comparison of confidentiality of different methods

Method name	*Forward secrecy*	*Backward secrecy*	*Anti-collusion attack*
This method	Yes	Yes	Yes
Multi-space key distribution algorithm	Yes	Yes	No
Multi-space key distribution algorithm	Yes	No	Yes
Multi-space key distribution algorithm	Yes	Yes	No

From the statistical results in Table 3, it can be seen that the forward secrecy, backward secrecy and anti-collusion attack of dynamic key distribution in wireless sensor network by the method in this paper are all optimal. It is verified again that the distribution of dynamic key in wireless sensor network by the method in this paper plays an important role in improving the security performance of wireless sensor network.

4 Conclusions

This paper studies the dynamic key distribution method of wireless sensor networks based on the exponential algorithm. The exponential algorithm is applied to the dynamic key distribution of wireless sensor networks, and the collusion characteristics of new and cancelled nodes in wireless sensor networks are added to the wireless sensor security model for processing. According to the principle of exponential algorithm, the dynamic key distribution method includes initialisation, broadcast, self-repair of session key, mutual repair of session key, joining node and withdrawing node index, which can effectively improve the security performance of wireless sensor network. A large number of simulation results verify the effectiveness of this method, and can effectively improve the network robustness. It can solve the problem that wireless sensor is eavesdropped or damaged by the other party in the military field. When wireless sensor is applied in daily life, it can avoid being damaged by hackers or lawbreakers. However, there is still a problem of uneven distribution for large-scale data, so the next research direction is to predict the number of keys, and predict the number of keys in the future. When the prediction value is exceeded, the alarm key information is combined and displayed by the method of this paper.

References

Banerjee, R. and Sipra, D.B. (2017) 'An energy efficient image compression scheme for wireless multimedia sensor network using curve fitting technique', *Wireless Networks*, Vol. 25, No. 3, pp.1–17.

Cao, J., Su, J.X. and Zhao, Y.Z. (2019) 'Nondeterministic public key cryptography and its implementation', *Journal of Jilin University (Science Edition)*, Vol. 57, No. 4, pp.860–868.

Cao, T.R. and Xu, X.Y. (2019) 'Design of collision adaptive protocol for smart home based on wireless ad hoc networks', *Journal of China Academy of Electronics and Information Technology*, Vol. 14, No. 5, pp.492–496+501.

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

Dai, M.Z., Wang, F.W. and Wang, C.G. (2019) 'Mutual healing group key distribution scheme based on exponential algorithm in WSN', *Computer and Digital Engineering*, Vol. 47, No. 1, pp.180–185.

Gao, J. (2019) 'Simulation of dynamic user network connection anti-interference and security authentication method', *Computer Simulation*, Vol. 36, No. 5, pp.230–233+254.

Gong, S.Q., Ma, S.D. and Xing, C.W. (2019) 'Optimal beamforming and time allocation for partially wireless powered sensor networks with downlink SWIPT', *IEEE Transactions on Signal Processing*, Vol. 51, No. 99, pp.1–1.

He, Y.L. and Guo, B.H. (2019) 'The real-time tracking and compensation OAM measurement equipment is independent of the quantum key distribution', *Optical Communication Technology*, Vol. 35, No. 8, pp.42–46.

Hossain, J., Fida, H. and Graham, T. (2018) 'A multifunctional three-phase four-leg PV-SVSI with dynamic capacity distribution method', *IEEE Transactions on Industrial Informatics*, Vol. 39, No. 99, pp.1–1.

Johann, A.B., Hoang, D.T. and Trung, Q.D. (2017) 'Joint sensor and relay power control in tracking Gaussian mixture targets by wireless sensor networks', *IEEE Transactions on Signal Processing*, Vol. 41, No. 99, pp.1–1.

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

Li, X.Y. and Feng, L. (2018) 'Design and application of automatic welding system for space solar cells components', *Chinese Journal of Power Sources*, Vol. 42, No. 4, pp.527–528.

Li, Y., Zhu, L.H. and Zhu, J.G. (2018) 'Core loss calculation based on finite-element method with Jiles–Atherton dynamic hysteresis model', *IEEE Transactions on Magnetics*, Vol. 54, No. 3, pp.1–5.

Liu, Z.G., Zhang, X.F. and Ma, L. (2019) 'Principle and accuracy analysis for inductive wireless power transfer based on ultrasonic positioning', *Journal of Power Supply*, Vol. 17, No. 4, pp.87–93.

Mekikis, P.V., Kartsakli, E. and Antonopoulos, A. (2018) 'Connectivity analysis in clustered wireless sensor networks powered by solar energy', *IEEE Transactions on Wireless Communications*, Vol. 43, No. 99, pp.1–1.

Parisa, R. and Abbas, J. (2017) 'Toward the evolution of wireless powered communication networks for the future internet of things', *IEEE Network*, Vol. 53, No. 99, pp.12–19.

Qiao, Y.C. (2017) 'Design of surface pressure test system of missile based on single chip microcomputer and miniature pressure sensor', *Automation and Instrumentation*, Vol. 47, No. 7, pp.104–105.

Yang, X., Chen, P.P. and Gao, S.W. (2018) 'CSI-based low-duty-cycle wireless multimedia sensor network for security monitoring', *Electronics Letters*, Vol. 54, No. 5, pp.323–324.

Zhong, J.L. and Lv, L.P. (2019) 'Multi-space key distribution algorithm for sensor network security', *Journal of Electronic Measurement and Instruments*, Vol. 37, No. 4, pp.125–132.

Zou, G.P., Wei, X.C. and Yang, S.Y. (2019) 'An integral equation hybrid method for the impedance calculation of the grid power distribution network with an arbitrary shape', *IEEE Transactions on Magnetics*, Vol. 29, No. 99, pp.1–4.