International Core Journal of Engineering Volume 6 Issue 7, 2020
ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

A Global Key Management Method for Hierarchical Wireless Sensor Networks

Xiaogang Wang[1,2,a,*], Huafeng Wu[1,b], Dan Liu[1,c], Dan Ye[1,d], Zhongfan Yang[1,e]

[1]School of Automation & Information Engineering, Sichuan University of Science & Engineering, Yibin 644000, China;

[2]Artificial Intelligence Key Laboratory of Sichuan Province Yibin 644000, China.

[a]wxg_zf@163.com, [b]974191367@qq.com, [c]1558045037@qq.com, [d]764685336@qq.com, [e]1344943768@qq.com

Abstract

In this paper, a global key management method for hierarchical wireless sensor networks is proposed. Firstly, a hierarchical network topology is established based on LEACH protocol. Secondly, the base station node receives the random key information from each cluster head node and builds a Lagrange interpolation polynomial function based on it, each cluster head can independently obtain the global key based on its own random key information and send it to its cluster members encrypted by a group key. Thirdly, the new random key information is generated periodically by each cluster head and handed to the base station to build a new Lagrange interpolation polynomial function to realize the periodic update of the global key. The establishment and update of global key peoposed in this paper do not need the direct participation of network nodes, which shows the good security, small calculation and time cost, and easy to obtain. In addition, it solves the problem of frequent encryption and decryption calculation and multi-level transmission in the whole network broadcast communication.

Keywords

Global; Key management; Wireless Sensor Network;LEACH.

1. Introduction

There are two kinds of wireless sensor network models: plane type and hierarchical type. The hierarchical type is usually used for the network with large scale and node density and it is also the main support network model for the research of various topics of wireless sensor network [1-2]. At present, the key management of hierarchical wireless sensor network mainly focuses on the research of session key and group key [3-7]. Without considering the efficiency of network management, these two keys can basically complete the security management of hierarchical network, but there are still some special cases to be considered, such as: the main communication mode of wireless sensor network is broadcast, if according to the current key management mode, the base station (BS) needs to send the information for broadcasting to the neighbor cluster head encrypted by the different private session key, and then these neighbor cluster heads decrypt the information and encrypt it again by another different private session key. Step by step, each cluster head transmits the broadcast information level by level until each cluster head gets the broadcast information. Finally, each cluster head broadcasts the initial broadcast information to its own cluster member with its own group key [8-10]. The disadvantage of this mode is that it requires multiple independent encryption and decryption calculations and multi-level transmission. If the network scale is large, there will be too many calculation cost and time cost.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

The global key is defined as the communication key shared by the base station and all network nodes, which is similar to the group key in understanding, as long as the whole hierarchical network is understood as a group. The global key distribution method is also clear, in which the global key is encrypted by BS and sent to each cluster head, and then it is encrypted by the cluster head with its own group key and broadcasted to each member. After that, each network member can obtain the global key.

The global key can be used for the information that all members need to know, such as the networking initializing command. Different from the method of building the group key, BS and all cluster heads are regarded as a group of nodes to build the global key, in which the whole network node is not required to participate. However, in order to prevent collusion attacks, it is suggested that the use of global key should be limited in the cluster heads, and group key should still be used between members in the cluster. In the broadcast stage, if the power of BS is large enough, all cluster heads will receive the broadcast information encrypted by the global key at one time, and then forward it to the group members at one time, which does not need frequent encryption and decryption calculation and multi-level transmission and greatly saves the calculation cost and time cost.

In this paper, the global key management method of hierarchical wireless sensor network includes the global key building method and the global key updating method.

2. Method of Global Key Building

As shown in Figure 1, this paper constructs a hierarchical network topology based on LEACH protocol [11], which includes BS, cluster heads and cluster members.

In LEACH, assume that each common sensor node generates a random number between 0 and 1, and it will be the cluster head if some random number is less than a certain threshold value $T(n)$.

$$T(n)=\begin{cases}1-p[r \bmod(\frac{1}{p})] & n \in G \\ 0 & else\end{cases} \quad (1)$$

Where, p is the percentage of desired cluster head nodes, r is the round, G is the common sensor nodes set in last $1/p$ round.

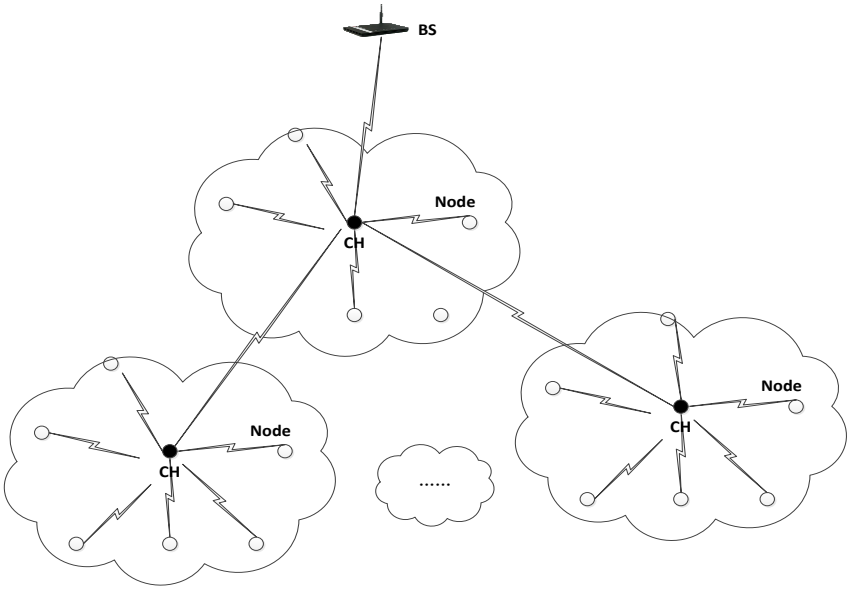

Figure 1. Hierarchical network topology

As shown in Figure 2, the global key management method of the hierarchical wireless sensor network is described and the specific steps of the global key building method are as follows:

ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

Step 1: initializing and presetting keys. Assume that the communication session key of neighbor nodes a and b in any network is $K_{a,b}$ and the encryption group key of broadcast communication in any cluster j is K_{CH_j}.

Step 2: sending key information. Assume that there are r cluster heads in the network, each cluster head randomly generates a key information $m(i)$ and the key information of these r cluster heads is recorded as $m(1), m(2), \ldots, m(r)$. Each key information is encrypted by the session key between adjacent cluster heads and sent to BS step by step. The process is as follows: some cluster head j sends its key information $m(j)$ and identity address ID_{CH_j}, sending the encrypted information $E_{K_{CH_j,CH_k}}\left(m(j)\|\mathrm{ID}_{CH_j}\right)$ to the upper cluster head k firstly, and then the cluster head k decrypts the information with the session key K_{CH_j,CH_k} and continues to encrypt the uploaded information in the same way until BS receives the information. If the cluster head j is adjacent to the BS, it can be directly transmitted to the BS by the key $K_{CH_j,BS}$ encryption;

Step 3: BS decrypts the key information $m(1), m(2), \ldots, m(r)$ and the identity information $ID_{CH_1}, ID_{CH_2}, ..., ID_{CH_r}$ corresponding to each cluster head, and then using $m(1), m(2), \ldots, m(r)$ as the interpolation nodes to generate Lagrange interpolation polynomial:

$$L(x) = a_1 M_1(x) + a_2 M_2(x) + \cdots + a_n M_r(x) = \sum_{j=1}^{r} a_j \prod_{i=1}^{r} \frac{(x - m(i))}{(m(j) - m(i))}, (i \neq j) \tag{2}$$

Where $M_i(x) = \frac{(x-m(1))\cdots(x-m(i-1))(x-m(i+1))\ldots(x-m(r))}{(m(i)-m(1))\cdots(m(i)-m(i-1))(m(i)-m(i+1))\ldots(m(i)-m(r))}$ and $a(1), a(2), \ldots, a(r)$ are polynomial functions or real constants that are not zero.

Step 4: BS randomly generates a global key K_G and generates a another Lagrange interpolation polynomial function $L_1(x)$ in combination with $L(x)$.

$$L_1(x) = \sum_{j=1}^{r} a_j \prod_{i=1}^{r} \frac{(x - m(i))}{(m(j) - m(i))} K_G, (i \neq j) \tag{3}$$

Step 5: BS will send $L_1(x)$ to each cluster head through session key encryption step by step, the process is as follows: assume cluster head i is adjacent to BS, then BS encrypts and sends information $E_{K_{CH_i,BS}}\left(L_1(x)\|\left\{\mathrm{ID}_{CH_1}\|a_1\|\mathrm{ID}_{CH_2}\|a_2\|...\|\mathrm{ID}_{CH_r}\|a_r\right\}\right)$ by using the session key $K_{CH_i,BS}$. Cluster head i decrypts the information $L_1(x)$ and obtains the coefficient a_i after its own identity address, where $\left\{ID_{CH_i}\|a_i\right\}$ will be deleted from the next level of transmission information. and then sends the information to the next cluster heads in the same encryption way. Similarly, each cluster head will decrypt the information $L_1(x)$ and obtain the coefficient after its own identity address which also will be deleted from the next level of transmission information. In order to obtain the global key K_G, each cluster head will bring its own key information $m(i)$ into $L_1(x)$, and

$$\begin{cases} M_i(m(i)) = 1 \\ M_j(m(i)) = 0, i \neq j \end{cases} \tag{4}$$

Therefore, $L_1(m(i)) = a_i K_G$, and the cluster head gets the global key $K_G = L_1(m(i)) \Big/ a_i$ by a_i.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

Step 6: the cluster head group key encrypts the global key and broadcasts it, such as cluster j encrypts K_G based on the group key K_{CH_j}, recorded as $E_{K_{CH_j}}(K_G)$ broadcasted to all cluster members, so that all network nodes obtain the new global key K_G.

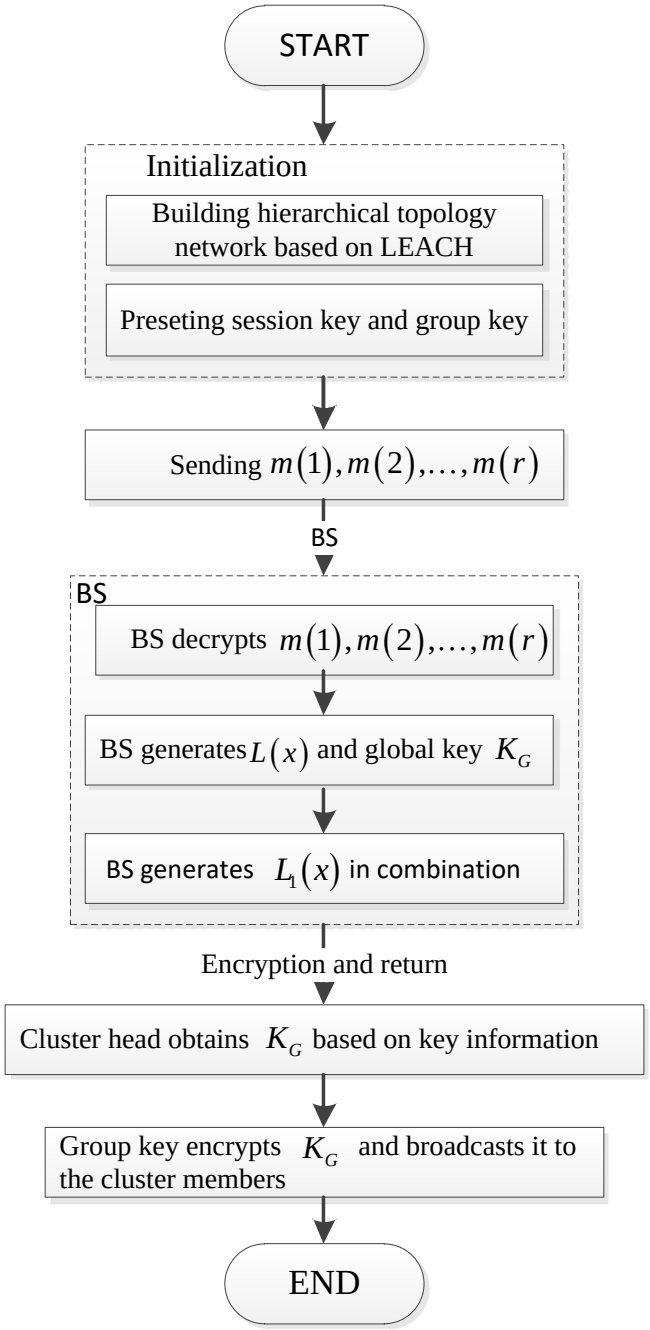

Figure 2. Flow chart of global key generation

3. Method of Global Key Updating

As shown in Figure 3, the global key management method of the hierarchical wireless sensor network is similar to the key establishment method, and the specific steps are as follows:

Step 1: the r cluster heads in the network re-generate the new key information of two mutual prime $m(1)_{new}, m(2)_{new}, \ldots, m(r)_{new}$ randomly and encrypt their own key information and identity address $\left(m(i)_{new} \| \mathrm{ID}_{CH_i}\right)$ by using the session key between adjacent cluster heads, and then send them to BS step by step.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

Step 2: BS decrypts the step 1 information and obtains $m(1)_{new}, m(2)_{new}, \ldots, m(r)_{new}$ and uses these new key information as the interpolation nodes to generate a new Lagrange interpolation polynomials $L(x)_{new}$ and $L_1(x)_{new}$, where

$$L_1(x)_{new} = \sum_{j=1}^{r} a_{jnew} \prod_{i=1}^{r} \frac{\left(x - m(i)_{new}\right)}{\left(m(j)_{new} - m(i)_{new}\right)} K_{Gnew}, (i \neq j) \tag{5}$$

Step 3: different from the global key building method, BS encrypts $L_1(x)_{new}$ with the old global key K_G and broadcasts it to the neighbor cluster heads, which is recorded as $E_{K_G}\left(L_1(x)_{new} \| \left\{ \mathrm{ID}_{CH_1} \| a_{1new} \| \mathrm{ID}_{CH_2} \| a_{2new} \| \ldots \| \mathrm{ID}_{CH_r} \| a_{rnew} \right\}\right)$. All the neighbor cluster heads of BS decrypt the information $L_1(x)_{new}$ and obtain the coefficients after their own identity addresses which will be deleted from the next level of transmission information. And using the same encryption broadcast method to send the information to the next level of cluster heads until all cluster heads obtain $L_1(x)_{new}$ and their own coefficients. Each cluster head can bring its new key information into $L_1(x)_{new}$ to obtain the global key $K_{Gnew} = L_1\left(m(i)_{new}\right) \Big/ a_{inew}$.

Step 4: the cluster head group key encrypts the global key and broadcasts it, such as cluster j encrypts K_{Gnew} based on the group key K_{CH_j}, recorded as $E_{K_{CH_j}}(K_{Gnew})$ broadcasted to all cluster members, so that all network nodes obtain the new global key K_{Gnew} and delete the old K_G after the global key update.

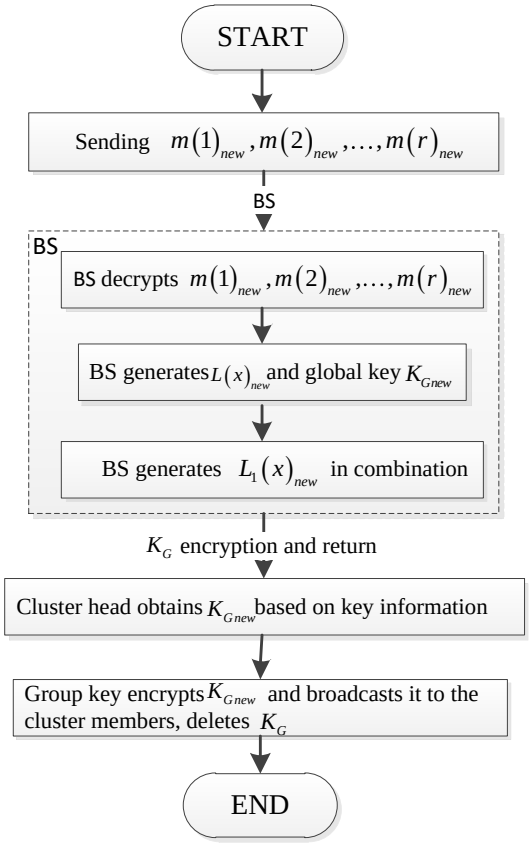

Figure 3. Global key update flowchart

4. Security

There are two factors that affect the security of the global key.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

One is BS, because the global key is generated randomly by the base station and has no relationship with the nodes in the cluster. It is completely impossible to capture BS so that the key source is absolutely safe.

The other is the key information $m(i)$, all cluster heads obtain the global key through $m(i)$. From the building process of the global key, it is known that $m(i)$ is the key to obtain the key, but it has nothing to do with the key itself. Meanwhile, the transmission of $m(i)$ is completed by the session key, so it needs to resolve the session key in order to obtain the key information. This equivalent security relationship is that the security of key information $m(i)$ is equivalent to the security of the global key, while the security of $m(i)$ is equivalent to the security of the session key, which means that the security of global key is equivalent to the security of the session key, so the security of the global key can be guaranteed as long as the pre-set session key is strong enough to resist capture.

5. Conclusion

In this paper, aiming at the problem of frequent encryption and decryption calculation and multi-level transmission in traditional key management method of hierarchical wireless sensor network, and a large amount of calculation and time cost in large-scale network, a key management method of hierarchical wireless sensor network is proposed, which is based on random key information to build Lagrange interpolation polynomial function. Each cluster head obtains the global key independently based on its own random key information and broadcasts it to the cluster members through a group key encryption. The network cluster head periodically generates a new key information randomly to update the global key. This method has the advantages of small computation cost, convenient acquisition and fast and secure broadcast communication in the whole network.

Acknowledgments

This work was jointly supported by National Natural Science Foundation of China (grant no. 61902268), Sichuan Science and Technology Program of China (grant no. 2018JY0197, 20ZDYF0919), Open Foundation of Artificial Intelligence Key Laboratory of Sichuan Province (grant no. 2017RZJ02), Research Foundation of Department of Education of Sichuan Province (grant no. 18ZA0357), Foundation of Deyang Open School-City Cooperative Technology Research and Development (Grant No. 2018CKJSD017), Nature Science Foundation of Sichuan University of Science & Engineering (grant no. 2017RCL12).

References

[1] R. Chaudhary, G. S. Aujla, N. Kumar and S. Zeadally: Lattice-based public key cryptosystem for internet of things environment: challenges and solutions, IEEE Internet of Things Journal, vol. 6(2019)No. 3, p. 4897-4909.

[2] X. G. Wang, W. R. Shi: Secure time synchronization protocol for wireless sensor network based on μTESLA protocol, International Journal of Network Security, vol. 20(2018)No. 3, p.536-546.

[3] L. Eschenauer, V. D. Gligor: A key management scheme for distributed sensor networks, Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington. DC, United States, (2002), p.41-47.

[4] D. G. Liu, P. Ning, R. F. Li: Establishing pairwise keys in distributed sensor networks, ACM Transactions on Information and System Security., vol. 8(2005)No.1, p.41-77.

[5] Y. H. Liu, Y. M. Wu: A key pre-distribution scheme based on sub-regions for multi-hop wireless sensor networks, Wireless personal communications., vol. 109(2019)No. 2, p.1161-1180.

[6] Y. C. Zhou, T. Wang, Y. F. Wang: A novel WSN key pre-distribution scheme based on group-deployment, International Journal of Sensor Newtworks,. vol. 15(2014)No. 3, p. 143-148.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202007_6(7).0046

[7] X. G. Wang, W. R. Shi and D. Liu: A group key management scheme for WSN based on Lagrange interpolation polynomial characteristic, KSII Transactions on Internet and Information Systems., vol. 13(2019)No. 7, p. 3690-3713.

[8] J. H. Son, J. S. Lee, S. W. Seo: Topological key hierarchy for energy-efficient group key management in wireless sensor networks, Wireless Personal Communication., vol. 52(2010)No. 2, p. 359-382.

[9] A, Albakri, L. Harn, S. Song: Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN), Security and Communication Network,(2019), doi: 10.1155/ 2019/ 3950129.

[10] B. W. Sun, Q. Li, B. Tian: Local dynamic key management scheme based on layer-cluster topology in WSN, Wireless Personal Communication., vol. 103(2018)No. 1, p.699-714.

[11] A. Salim, W. Osamy, M. A. Khedr: IBLEACH: intra-balanced LEACH protocol for wireless sensor networks, WIRELESS NETWORKS, vol. 20(2014)No. 6, p. 1515-1525.