A Group Key Management Scheme for WSN Based on Lagrange Interpolation Polynomial Characteristic

Xiaogang Wang[1,2*], Weiren Shi[2] and Dan Liu[1]
[1] Artificial Intelligence Key Laboratory of Sichuan Province, School of Automation & Information Engineering, Sichuan University of Science & Engineering, Sichuan 644000, China
[e-mail: wxg@suse.edu.cn; liudangbr@sina.com]
[2] College of Automation, Chongqing University, Chongqing 400044, China
[e-mail: wrs@cqu.edu.cn]
*Corresponding author: Xiaogang Wang

Received May 18, 2018; accepted February 9, 2019; published July 31, 2019

Abstract

According to the main group key management schemes logical key hierarchy (LKH), exclusion basis systems (EBS) and other group key schemes are limited in network structure, collusion attack, high energy consumption, and the single point of failure, this paper presents a group key management scheme for wireless sensor networks based on Lagrange interpolation polynomial characteristic (AGKMS). That Chinese remainder theorem is turned into a Lagrange interpolation polynomial based on the function property of Chinese remainder theorem firstly. And then the base station (BS) generates a Lagrange interpolation polynomial function f(x) and turns it to be a mix-function f(x)' based on the key information m(i) of node i. In the end, node i can obtain the group key K by receiving the message f(m(i))' from the cluster head node j. The analysis results of safety performance show that AGKMS has good network security, key independence, anti-capture, low storage cost, low computation cost, and good scalability.

Keywords: Wireless sensor networks, security, Chinese remainder theorem, Lagrange interpolation polynomial, group key management

This work is funded by the Nature Science Foundation of Sichuan University of Science &Engineering (No. 2017RCL12), the Foundation of Artificial Intelligence Key Laboratory of Sichuan Province (No.2017RZJ02), Sichuan Science and Technology Program(No.2018JY0197, 2016SZ0074), the Foundation of Sichuan Educational Committee of China (18ZA0357), the National Natural Science Foundation of China (No.61473050, 11705122).

http://doi.org/10.3837/tiis.2019.07.020 **ISSN : 1976-7277**

1. Introduction

Wireless sensor network (WSN) has become an active research branch in the field of internet of things (IoT) and has a very wide application prospect [1, 2]. Compared with the communication mode of point to point unicast in traditional internet network, the main communication mode of WSN is broadcasting or multicast [3,4], but the broadcast communication mode is more vulnerable to security threats because of the characteristic of the open channel mode which makes it vulnerable to be eavesdropped by malicious nodes [5-8]. Therefore, the multicast broadcast security schemes in traditional network can't be fully applied to WSN because of the reason that WSN is a resource constrained network limited in computing speed, power supply, communication ability and storage space [9-11].

Multicast technology can solve the problem that the primary node sends messages to multiple receiving nodes efficiently for reducing unnecessary repeated transmission, utilizing network bandwidth effectively, reducing server load and network congestion. So, WSN is the most suitable multicast technology for solving this problem based on the technical features of WSN.

For the network security problem that the multicast communications are accessed by unauthorized users associated with WSN broadcast features, which can be solved by making a message encryption that all group members share a group key to encrypt or decrypt the data packets [12-15]. While, the group keys must be updated to meet forward security and backward security when some node joins or leaves the group because of the dynamic WSN network structure [16,17].

The existing group key management schemes can be divided into 3 types: the centralized, the distributed and the clustered.

1. The centralized group key management scheme

The centralized key management scheme is the earliest form of group key management, in which there is a trusted third party referred to as the group controller GC (Group Controller) commonly or the key distribution center KDC (Key Distribution Center). GC is responsible for the key generation, distribution, update, revocation and identity authentication for all group members. The advantage of this class scheme is easy to control the group members based on the simple structure, while the disadvantage is that the whole system will be in a state of paralysis and easily become the performance bottleneck of the system because of the problem of single point failure. The most representative of this class scheme are the group key management protocol (GKMP) [18], the logic key hierarchy (LKH) [19] and the exclusion basis systems(EBS) [20].

In GKMP, all group members can communicate with GC, GC manages the group key and controls all group members' personal key, the member only saves the group key and his personal key. It's obviously, the scalability of GKMP is poor and inefficient when the members of the group change frequently. In addition, the computation cost and communication overhead of GKMP are linearly related to the group size.

In LKH, a trusted GC is used to manage the network keys by building a key tree. There are 3 types of nodes in the key tree: the root node, the intermediate node and the leaf node. The root node represents the only group key, the intermediate node represents the encryption key which is used to deliver the new key when the group membership changes, leaf node represents the group member which has all the keys from his leaf node to the root node. The

advantage of LKH is that it has good scalability with the increase of the group members, and the messages, computation, the number of keys stored in each member are all linearly related to the group size when updating the new key, and the number of keys stored in GC is linearly related to the group size too. In addition, it has the ability to support multiple members to drop out the network at the same time and prevent the withdrawn members getting the new group key. While the disadvantage of LKH is like GKMP that the whole system will be in a state of paralysis and easily become the performance bottleneck of the system because of the problem of single point failure.

In EBS, Eltoweissy proposed the concept of dynamic key management based on the clustered structure of sensor networks. Compared with static key management, the advantage of EBS is that it can delete all the keys owned by any node dynamically and efficiently and expel the nodes captured by the enemy to ensure the security performance of the network, storage space and energy efficiency. The drawback of EBS is the existence of collusion problem in which the enemy can obtain the nodes' keys by capturing nodes and affect the safety of the internet. In addition, when the captured nodes are within the radius of node communication, these captured nodes can make the collusion problem which can destroy the whole key system and made the network loses security.

2. The distributed group key management scheme [21-24]

There is no group controller (GC) in this class scheme , and in which the nodes are peer to peer and build the group key by negotiating together. The advantage of distributed scheme is that it avoids the problem of single point failure and has stronger fault-tolerant ability. The disadvantage is that it is not good for the control of the group, and the communication cost will increase linearly with the number of the group members. The most representative of this class scheme is CLIQUES [24], in which the key transmission delay is $O\left(N\right)$, the computation cost for group key updating is $O\left(N^2\right)$, and the communication cost for group key updating is $O\left(N^2\right)$, where the N is the size of group, so the CLIQUES scalability is poor.

3. The clustered group key management scheme [25-28]

The clustered group key management scheme combines the characteristics of the centralized and the distributed schemes. In this scheme, group members are divided into several subgroups and each sub group has one control node, in which there are two layers structure consisting of a management layer by the control nodes and a member layer by the member nodes. The management layer and the member layer can choose different key management schemes independently. The most representative of this class scheme is lolus[24], in which each member of the sub group shares a secret key and the control node will decrypt the new encrypted information and send the decrypted information to each group member by the shared key. Although lolus has good reliability and scalability, it needs the control nodes fully trusted.

In recent years, the problem of the group key management scheme has been widely studied, where the main objective of the study is to reduce the communication cost, the computing cost and the storage cost for the group key updating. In addition, the updating cost of the group key is one of the important criteria to evaluate a group key management scheme, so the group key management scheme should reduce the updating cost of as much as possible.

1. The computing cost

In general, the greater the encryption strength, the more secure the system is, and it is not easy to be cracked, but the cost is increased in the ratio of the computing cost. In addition, the amount of computation produced by different encryption methods is different in the process of computing the group key.

2. The storage cost

The group members and the group controllers generally have a certain amount of storage space to store some key information for assisting the generation and distribution of the group key. In general, the key information stored by the group controller is much larger than the group members for managing the whole group, so the storage cost of group members and group controllers should be reduced as much as possible when designing some new group key management schemes.

3. The communication cost

In the large-scale wireless multicast network, the group members will frequently join or leave because of the mobility of the members, which will cause the group key updating and make some more communication cost. Therefore, it is an important content for WSN research to find a secure and efficient group key management scheme.

According to the schemes logical key hierarchy (LKH), exclusion basis systems (EBS) and other group key schemes are limited in the network structure, collusion attack, high energy consumption, and the single point failure, this paper presents a group key management scheme for wireless sensor networks based on Lagrange interpolation polynomial characteristic (AGKMS). It utilizes the special characteristic that Chinese remainder theorem can be expressed into the form of Lagrange polynomial interpolation to realize the generation of group key with no cluster nodes directly involved. Firstly, each cluster member (CM) generates key information $m(i)$ randomly and sends it to cluster head (CH) with the unique session key between cluster member and cluster head. Secondly, cluster head decrypts the key information $m(1), m(2), \ldots, m(n)$ and sends it to base station (BS) with the shared key between cluster head and base station. Thirdly, base station decrypts $m(1), m(2), \ldots, m(n)$ and generates a Lagrange interpolation polynomial function $f(x)$ and group key K_j, and then tends it to be a mix-function $f(x)' = f(x)K_j$ by $f(m(i)) = 1$ and sends it to cluster member by two encrypting. Lastly, cluster member obtains the group key K_j by receiving the message $f(m(i))' = K_j$ from the cluster head. The analysis results of safety performance show that AGKMS has good network security, key independence, anti-capture, low storage cost, low communication cost, low computation cost, and good scalability.

The paper is organized as follows. In Section 2, analyze the characteristics of Chinese remainder theorem, such as polynomial characteristic and Lagrange interpolation polynomial characteristic. In Section 3, discuss the specific steps of AGKMS and the method of group key update. In Section 4, analyze the security of AGKMS. In Section 5, make a simulation analysis to verify the effectiveness of AGKMS security features in cost. In Section 6, some summary and forecast are given.

2. Related Work

2.1 Chinese remainder theorem

Chinese remainder theorem sourced in ancient China, "Sun Tzu Suan Jing" [29], also known as "Sun Tzu theorem", for solving the congruence group. It is one of the important theorems in elementary number theory, and has important applications in the field of algebraic mathematics and computer security. The specific definition of the Chinese remainder theorem is as followed:

Definition 1: Set that $m_1, m_2, \ldots, m_r$ are positive integer and pairwise coprime, where $a_1, a_2, \ldots, a_r$ are integer, and the congruence equations are

$$\left\{\begin{array}{l} x \equiv a_1 (\bmod m_1) \\ x \equiv a_2 (\bmod m_2) \\ \ldots\ldots \\ x \equiv a_r (\bmod m_r) \end{array}\right\}, i = 1, 2, \ldots, r \tag{1}$$

There is a unique solution x for formula (1) $\bmod M$, where $M = m_1 m_2 \cdots m_r$, and

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \bmod M \tag{2}$$

Where $M_i = M / m_i$, $y_i = M_i^{-1} \bmod m_i$, $i = 1,2,\ldots,r$.

2.2 Polynomial characteristic of Chinese remainder theorem

Deduction 1: Set that $m_1(x), m_2(x), \ldots, m_r(x)$ are polynomial for x and pairwise coprime, where $r (r \geq 1)$ is the degree of $m_i(x)$, $i = 1,2,\ldots,r$, and $a_1(x), a_2(x), \ldots, a_r(x)$ are all polynomial for x, then there must be a polynomial $f(x)$

$$\left\{\begin{array}{l} f(x) \equiv a_1(x) (\bmod m_1(x)) \\ f(x) \equiv a_2(x) (\bmod m_2(x)) \\ \ldots\ldots \\ f(x) \equiv a_r(x) (\bmod m_r(x)) \end{array}\right\}, i = 1, 2, \ldots, r \tag{3}$$

And there is a unique solution $f(x)$ for formula (3) $\bmod M(x)$, where $M(x) = m_1(x) m_2(x) \ldots m_r(x)$. `

***Proof*:** Since $m_1(x)$ and $m_2(x)$ are relatively prime, using Euclidean algorithm find $p(x)$ and $q(x)$, and then

$$p(x) m_1(x) + q(x) m_2(x) = 1 \tag{4}$$

And multiplying by both sides with $a_1(x) - a_2(x)$ to formula (4), then

$$a_1(x) - a_2(x) = p(x)\left(a_1(x) - a_2(x)\right) m_1(x) + q(x)\left(a_1(x) - a_2(x)\right) m_2(x) \tag{5}$$

$$a_1(x) - p(x)\left(a_1(x) - a_2(x)\right) m_1(x) = a_2(x) + q(x)\left(a_1(x) - a_2(x)\right) m_2(x) \tag{6}$$

Set

$$f(x)=a_1(x)-p(x)\left(a_1(x)-a_2(x)\right)m_1(x)=a_2(x)+q(x)\left(a_1(x)-a_2(x)\right)m_2(x) \quad (7)$$

Then

$$\begin{cases} a_1(x)-f(x)=p(x)\left(a_1(x)-a_2(x)\right)m_1(x) \\ f(x)-a_2(x)=q(x)\left(a_1(x)-a_2(x)\right)m_2(x) \end{cases} \quad (8)$$

From formula (8) get

$$\begin{cases} m_1(x)\,|\left(a_1(x)-f(x)\right) \\ m_2(x)\,|\left(f(x)-a_2(x)\right) \end{cases} \quad (9)$$

Therefore

$$\begin{cases} f(x)\equiv a_1(x)\left(\bmod m_1(x)\right) \\ f(x)\equiv a_2(x)\left(\bmod m_2(x)\right) \end{cases} \quad (10)$$

Similarly, the same equation can be obtained in the rest of the formula (3).
Thus deduction 1 is proved.

2.3 Lagrange interpolation polynomial characteristic of Chinese remainder theorem

Definition 2: Because of the uniqueness of the n-th interpolation polynomial, define the corresponding n-th interpolation basis function $l_i(x)$ for each interpolation point x_i, where there are $n+1$ different interpolation points $x_i, i=0,1,2,...,n$.

Set that $x_0, x_1, ..., x_{i-1}, x_{i+1}, ..., x_n$ are the zero points of function $l_i(x)$, and it can be assumed that

$$l_i(x)=a_i(x-x_0)(x-x_1)...(x-x_{i-1})(x-x_{i+1})...(x-x_n) \quad (11)$$

If set $l_i(x)=1$, $x=x_i$, and

$$l_i(x_i)=a_i(x_i-x_0)(x_i-x_1)...(x_i-x_{i-1})(x_i-x_{i+1})...(x_i-x_n)=1 \quad (12)$$

And

$$a_i=\frac{1}{(x_i-x_0)(x_i-x_1)...(x_i-x_{i-1})(x_i-x_{i+1})...(x_i-x_n)} \quad (13)$$

Therefore

$$l_i(x)=\frac{(x-x_0)(x-x_1)...(x-x_{i-1})(x-x_{i+1})...(x-x_n)}{(x_i-x_0)(x_i-x_1)...(x_i-x_{i-1})(x_i-x_{i+1})...(x_i-x_n)} \quad (14)$$

And set

$$L_n(x)=\sum_{i=0}^{n} l_i(x)f(x_i) \quad (15)$$

It is shown in (15) that the degree of $L_n(x)$ is less than n, and $L_n(x_i)=f(x_i), i=0,1,2,...,n$. Therefore, $L_n(x)$ is the interpolation polynomial for $x_0, x_1, ..., x_n$ which known as Lagrange interpolation polynomial.

Deduction 2： Lagrange interpolation polynomial is a special form of Chinese remainder theorem.

***Proof*:** Based on deduction 1, set that $m_1(x), m_2(x), \ldots, m_n(x)$ are polynomial for x and pairwise coprime, where $a_1(x), a_2(x), \ldots, a_n(x)$ are all polynomial for x, then there must be a polynomial $f(x)$

$$\begin{cases} f(x) \equiv a_1(x) (\bmod m_1(x)) \\ f(x) \equiv a_2(x) (\bmod m_2(x)) \\ \cdots\cdots \\ f(x) \equiv a_n(x) (\bmod m_n(x)) \end{cases} \tag{16}$$

There is a unique solution for formula (16) When the degree of $f(x)$ is less than $M(x)$, where $M(x) = m_1(x) m_2(x) \ldots m_r(x)$.

Specially, when $m_i(x) = x - b_i \in Q[x]$ (or $R[x]$), $i = 1,2,\ldots,n$, $b_i (i = 1,2,\ldots,n)$ is constant and not equal each other, $m_i(x) (i = 1,2,\ldots,n)$ is polynomial and pairwise coprime, so we can get

$$m_i(x) \equiv m_i(b_i) (\bmod (x - b_i)) \tag{17}$$

And deduction 1 can be expressed into a polynomial $f(x)$

$$\begin{cases} f(x) \equiv a_1(x) (\bmod (x - b_1)) \\ f(x) \equiv a_2(x) (\bmod (x - b_2)) \\ \cdots\cdots \\ f(x) \equiv a_n(x) (\bmod (x - b_n)) \end{cases} \tag{18}$$

There is a unique solution for formula (18) when the degree of $f(x)$ is less than n, where $a_i(x)$ $(i = 1,2,\ldots,n)$ are random constant.

Because $f(x) \equiv a_i (\bmod (x - b_i))$ is equivalent to $f(b_i) \equiv a_i$ $(i = 1,2,\ldots,n)$, we can get from $f(b_i) \equiv a_i$ that there is a unique $f(x)$ which degree is less than n for each different b_i $(i = 1,2,\ldots,n)$. It is the existence and uniqueness of interpolation polynomial.

According to the proof of deduction 1, there is a polynomial $M_i(x)$ $(i = 1,2,\ldots,n)$, and

$$\begin{cases} M_i(x) \equiv 1 (\bmod (x - b_i)) \\ M_j(x) \equiv 0 (\bmod (x - b_j)) \end{cases}, i \neq j \tag{19}$$

And because $M_i(x) = \dfrac{(x - b_1) \cdots (x - b_{i-1})(x - b_{i+1}) \ldots (x - b_n)}{(b_i - b_1) \cdots (b_i - b_{i-1})(b_i - b_{i+1}) \ldots (b_i - b_n)}$ can meet up (19), there is a interpolation polynomial $f(x)$

$$f(x) = a_1 M_1(x) + a_2 M_2(x) + \cdots + a_n M_n(x) = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{(x - b_i)}{(b_j - b_i)} (i \neq j) \tag{20}$$

It's showed in (20) that $f(x)$ is a Lagrange interpolation polynomial. So Lagrange interpolation polynomial is a special form of Chinese remainder theorem.

3. AGKMS

3.1 Network model assumptions

Firstly, based on WSN broadcast communication, the group size is usually dynamically changing that can be varied from dozens to thousands or even tens of thousands. Secondly, the cluster members' computing ability is always a great difference in different network environment. Thirdly, the cluster members are dynamically changing that nodes joining or leaving are not regular. So, the larger the group size is, the more dynamic the members are. The above characteristics show the difference between group key management and unicast key management [30-32], where the multicast communication is carried out in a group, the cluster members are dynamic, and the group key can't be used in the whole process of group communication.

The key point of this paper is to discuss the Chinese remainder theorem how to generate the WSN group key with the special form of Lagrange interpolation polynomial. For ease of discussion, this paper is based on the following assumptions:

- Assume that the network is isomorphic and static, each group member has same configure in software and hardware, and will not move any more once they are deployed, where the network size is N , including 3 types of nodes: base station (BS), cluster head (CH), cluster members (CM), as shown in **Fig. 1**.
-

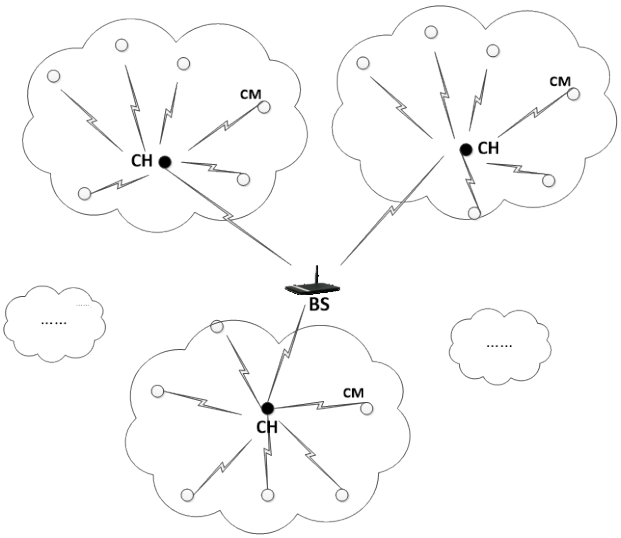

Fig. 1. The WSN framework

- Assume that base station (BS) is equipped with abundant software and hardware resources, it is responsible for storing the basic information of all the nodes in network and receiving the information from cluster head, it has the ability to detect compromised or captured nodes.
- Cluster member is responsible for collecting environmental data and sending the data to the cluster head. The ability to process data of cluster members is much low, which is limited by storage space, energy reserves, and communication distance.

The main symbols in the text are shown in **Table 1**:

Table 1. Explanation of the main symbols in AGKMS.

Symbol	Implication
BS / KDS	base station/ key distribution center
S_{ij}	node i of cluster j
CH_j	cluster head j
$h(x)$	$hash$ function
$m(i)$	key information of node i
ID_i	identity symbol of node i
$f(x)$	Lagrange interpolation polynomial function
$K_{a,b}$	key between node a and node b
$K_{CH_i,BS}$	key between cluster i and BS
K_{i,CH_j}	key between node i and head j
K_j	group key of cluster j

3.2 Establishing group key

Encrypting the broadcast message is one kind of methods to ensure secure broadcast, and the keys for encryption and decryption are only obtained by cluster members which can ensure the encrypted message only decrypted by cluster members. The key advantage of the multi-shared key to solve the security problem is to generate and distribute keys, and the generation and distribution must be exclusive, which means non-cluster members can't get the keys.

The specific step sfor establishing group key in AGKMS are as followed:

Step1. Initializing

- Assume that the network size is N and divided into m clusters, each node is assigned a random number ID_i that represents the unique identity of the node (such as cluster head and cluster members).
- Each cluster head is pre-distributed a session key $K_{CH_i,BS}$ shared with BS.
- The session keys between cluster members are generated by the pre-distributed quadratic $f_{\omega_i}(x_1, x_2, ..., x_n) = X^T AX$ [33].

Step2. Establishing group key

Assume that the group key of cluster j is K_j, where the cluster head is CH_j, the cluster size is n.

1. Sending key information

Firstly, each cluster member of cluster j generates their own key information $m(1), m(2), \ldots, m(n)$ randomly, where $m(i)$ is the key information of cluster member i.

Secondly, cluster member i encrypts the key information $E_{K_{i,CH_j}}(m(i))$ and sends it to cluster head CH_j, where K_{i,CH_j} is the session key between node i and cluster head CH_j. For K_{i,CH_j}, we refer to the definition of the session key in [33] by author Xiao-gang Wang which is used to generate a session key between neighbor nodes by pre-distributed quadratic. On the

one hand, the session key in [33] ensures the network connectivity and coverage rate which is 100%. On the other hand, each session key between neighbor nodes is absolute independent and secure, and it is hard to decrypt.

Thirdly, the cluster head CH_j decrypts the key information $m(1), m(2), \ldots, m(n)$ and sends $E_{K_{CH_j,BS}}\left(m(1), m(2), \ldots, m(n)\right)$ to base station.

Last, BS decrypts and get the key information $m(1), m(2), \ldots, m(n)$.

By now, transmitting the key information of cluster members to base station is completed.

2. Generating Lagrange interpolation polynomial function

Firstly, the base station generates a Lagrange interpolation polynomial function $f(x)$.

Set that $m_1(x), m_2(x), \ldots, m_n(x)$ are polynomial and pairwise coprime, where $a_1(x), a_2(x), \ldots, a_n(x)$ are polynomial for x, then there must be a polynomial $f(x)$ based on deduction 2.

In (20), $f(x) = a_1 M_1(x) + a_2 M_2(x) + \cdots + a_n M_n(x) = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{(x - b_i)}{(b_j - b_i)} (i \neq j)$, Where $M_i(x) = \frac{(x-b_1)\cdots(x-b_{i-1})(x-b_{i+1})\ldots(x-b_n)}{(b_i-b_1)\cdots(b_i-b_{i-1})(b_i-b_{i+1})\ldots(b_i-b_n)}$, $m_i(x) = x - b_i \in Q[x]$ (or $R[x]$), $i = 1,2,\ldots,n$, $b_i (i = 1,2,\ldots,n)$ is constant and not equal each other.

Secondly, regenerating $f(x)$ by $m(1), m(2), \ldots, m(n)$, set $b_i = m(i)$, and

$$f(x) = a_1 M_1'(x) + a_2 M_2'(x) + \cdots + a_n M_n'(x) = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{(x - m(i))}{(m(j) - m(i))}, (i \neq j) \tag{21}$$

Where $M_i'(x) = \frac{(x-m(1))\cdots(x-m(i-1))(x-m(i+1))\ldots(x-m(n))}{(m(i)-m(1))\cdots(m(i)-m(i-1))(m(i)-m(i+1))\ldots(m(i)-m(n))}$.

Thirdly, the base station generates a group key K_j randomly, and set

$$f(x)' = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{(x - m(i))}{(m(j) - m(i))} K_j, (i \neq j) \tag{22}$$

Last, encrypting $E_{K_{CH_j,BS}}\left(f(x)'\right)$ and sending it to CH_j.

3. Getting group key

Firstly, the cluster head CH_j decrypts $E_{K_{CH_j,BS}}\left(f(x)'\right)$.

Secondly, the cluster head CH_j encrypts $E_{K_{i,CH_j}}\left(f(x)'\right), i = 1,\ldots,n$ and sends it to each cluster member.

Thirdly, node i decrypts $E_{K_{i,CH_j}}\left(f(x)'\right)$ by K_{i,CH_j} and gets $f(x)'$.

Last, node i gets the group key K_j.

Because

$$\begin{cases} f(x)=a_1M_1'(x)+a_2M_2'(x)+\cdots+a_nM_n'(x)=\sum_{j=1}^{n}a_j\prod_{i=1}^{n}\frac{(x-m(i))}{(m(j)-m(i))},(i\neq j) \\ M_i'(x)=\frac{(x-m(1))\cdots(x-m(i-1))(x-m(i+1))\ldots(x-m(n))}{(m(i)-m(1))\cdots(m(i)-m(i-1))(m(i)-m(i+1))\ldots(m(i)-m(n))} \end{cases}$$

When $x=m(i)$, and

$$\begin{cases} M_i'(m(i))=1 \\ M_i'(m(j))=0, i\neq j \end{cases} \tag{23}$$

Therefore, $f(m(i))=a_i$

Similarly, $f(m(i))'=a_iK_j$

And if $a_i=1$, then $f(m(i))'=K_j$.

It shows that each cluster member can get group key by taking its own key information $m(i)$ into $f(x)'$.

By now, getting group key K_j is completed.

The group key generation process is shown in **Fig. 2**.

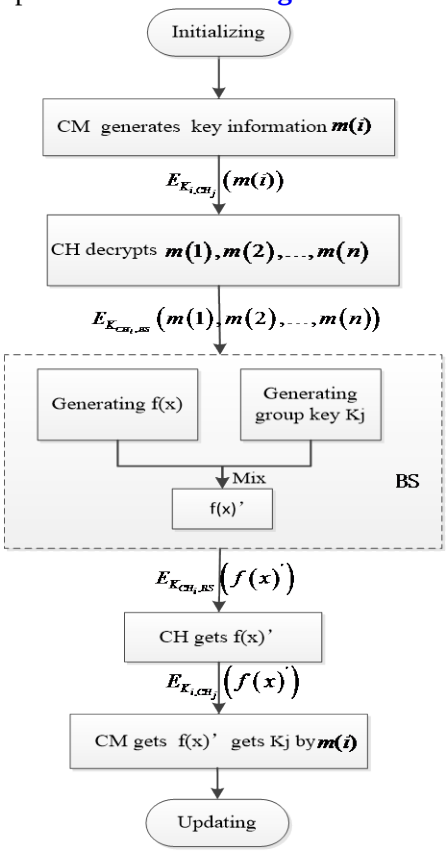

Fig. 2. The group key generation process in AGKMS

3.3 Group key update

1. Periodic group key update

In order to prevent the enemy from monitoring traffic and getting the entire network topology information when the nodes in the cluster run for a period of time, it is necessary to update the group key periodically.

On the one hand, the base station only need to regenerate a new Lagrange interpolation polynomial function $f(x)'$ which is generated by old $f(x)$ mixed with a new group key K_j, and sends it to the cluster members. The cluster members can get the new group key K_j by taking their own key information into $f(x)'$. This approach has a strong autonomy and can change group key K_j at any time without affecting the network.

On the other hand, the cluster members periodically change the key information and get the new group key K_j following as step 2 of section 3.2.

2. Adding new nodes

After the establishment of initial group key, if a new node wants to add in some cluster, the new node needs to submit an application through the cluster head to the base station first of all, and then the base station will judge whether is a good or malicious node. At last, the new node will be distributed some related key information after authenticated by the base station.

In AGKMS, the base station will notify the cluster head to update the group key if a new node wants to add in some cluster. For example, assume that node a wants to add in cluster j which has been authenticated by the base station, but it can't carry out multicast communication because of no group key. For establishing group key, node a needs to build session key K_{a,CH_j} with cluster head CH_j and send key information $m(a)$ encrypted by K_{a,CH_j} to CH_j. Then node a can get the new group key K_j following as step 2 of section 3.2.

In the whole process, the addition of new nodes does not affect the communication structure of the network, thus AGKMS has good scalability.

3. Removing the captured nodes

The sensor nodes need to consider the factors of manufacturing cost and deployment environment, and it's vulnerable to be captured without special physical protection. Once the nodes are captured, the enemy will get all the keys to decrypt information stored in the nodes in a limited time. Therefore, in order to ensure the authenticity, reliability and integrity of the monitoring nodes information, it is necessary to remove the captured nodes in time, and update and delete the captured keys dynamically.

In AGKMS, in order to ensure the removed nodes can't get the group key every time when the nodes are removed from clusters due to energy depletion or be captured by enemy, and we needs to follow as two steps.

Step1: If the removed nodes are the cluster members, it needs the base station deleting their key information and regenerate the new Lagrange interpolation polynomial function $f(x)'$ with the rest key information of good nodes. And the rest cluster members can get the new group key K_j from $f(x)'$ following as step 2 of section 3.2

Step2: If the removed nodes are cluster heads, it needs to regenerate the new cluster heads according to the routing protocol [34, 35], and the rest steps are same as section 3.1-3.2.

4 Security Analysis

In WSN, the cluster members are dynamically changing, and the larger the group size is, the more dynamic the members are. This characteristic shows the difference between group key management and unicast key management. Unicast key management mainly includes two aspects: identity authentication and key distribution, and the secure communication channel between two neighbor nodes will be established after identity authentication and key agreement. The multicast communication is carried out in a group, the cluster members are dynamic, and the group key can't be used in the whole process of group communication. Therefore, the group key management is one of the most challenging problems to ensure the security applications of WSN broadcast communication.

AGKMS reflects its own security features which are much better than LKH and EBS in network security, key independence, anti-capture, low storage cost, low computation cost, and good scalability.

1. Key independence

It's showed in formula (20), the Lagrange interpolation polynomial function is $f(x)' = \sum_{j=1}^{n} a_j \prod_{i=1}^{n} \frac{(x - m(i))}{(m(j) - m(i))} K_j$, where $i \neq j$, K_j is the group key, and there are two factors affecting the group key K_j.

One is the base station, because K_j is randomly generated by the base station and has no relationship with cluster members, so it is impossible to capture the base station. It shows that the source of the group key is safe and indicates that the existing group key has no correlation with the abandoned group key.

The other one is the cluster members' key information $m(i)$. In section 3.2, we know that the cluster members get the group key K_j rely on $m(i)$, but $m(i)$ just is the key to get K_j and not the factor of generating K_j. It is indicated that the enemy can't find any rules from the old group keys to decrypt the existing or future group key though enemy can get all old used group keys. Similarly, even if the enemy can get the existing or future group key, but it is also impossible to get any key information from the group key.

Therefore, the group key K_j in AGKMS has good independence.

2. Anti-capture

Because of $E_{K_{i,CH_j}}(m(i))$ and $E_{K_{i,CH_j}}(f(x)')$, it would have to obtain the key K_{i,CH_j} if enemy wants to get the key information $m(i)$ and the group key K_j, where K_{i,CH_j} is the session key between node i and cluster head CH_j. For K_{i,CH_j}, this paper refers to the definition of the session key in [33] by author Xiao-gang Wang which is used to generate a session key between neighbor nodes by pre-distributed quadratic.

Define 3: assume that $f(x_1, x_2, ..., x_n)$ is a multiple asymmetric quadratic form polynomial in field P.

$$f(x_1,x_2,...,x_n)=a_{11}x_1^2+a_{12}x_1x_2+...+a_{1n}x_1x_n+a_{21}x_2x_1+a_{22}x_2^2+...+a_{2n}x_2x_n.....+a_{n1}x_nx_1+a_{n2}x_nx_2+...+a_{nn}x_n^2$$
$$=(x_1,x_2,...,x_n)\begin{bmatrix}a_{11} & a_{12} & ... & a_{1n}\\ a_{21} & a_{22} & ... & a_{2n}\\ & ..... & & \\ a_{n1} & a_{n2} & ... & a_{nn}\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ ...\\ x_n\end{bmatrix}=X^TAX \quad (24)$$

Where A is the quadratic matrix of $f(x_1,x_2,...,x_n)$, $a_{ij}=a_{ji}, i, j=1,...,n$, $A=A^T$.

For example, for building the session key between neighbor nodes a and m in [33], $f_{w_a}(x_1,x_2,...,x_n)$ is the quadratic polynomial of node a, $f_{w_m}(x_1,x_2,...,x_n)$ is the quadratic polynomial of node m, and their session key is $K_{am}=h(\boldsymbol{BF})=h(\boldsymbol{FB})=K_{ma}$, where B and F are the diagonal matrix of $f_{w_a}(x_1,x_2,...,x_n)$ and $f_{w_m}(x_1,x_2,...,x_n)$ respectively. So, the quadratic polynomial is key point to decrypt session key K_{i,CH_j} for the enemy.

Based on formula (24), it must decrypt A for decrypting $f(x_1,x_2,...,x_n)$, but there are $\frac{n(n+1)}{2}$ different elements in symmetric matrix A, and the difficulty of decrypting A will be multiplied when the matrix A dimension n is slightly changed (as shown in **Fig. 3**).

Assume that the size of cluster j is N_j, if $N_j<\frac{n(n+1)}{2}$, that enemy is unable to decrypt the matrix A, and also unable to decrypt $f(x_1,x_2,...,x_n)$.

Therefore, for small and middle size network, the session keys for neighbor nodes are absolutely safe as long as $N_j<\frac{n(n+1)}{2}$. And for large network, it also can guarantee the network security as long as distribute a reasonable network structure, such as increasing the number of clusters space, and limiting the number of cluster members. It is indicated that the session key in AGKMS built by quadratic polynomial has good anti-capture performance.

In addition, the quadratic polynomials $f_{\omega_i}(x_1,x_2,...,x_n)$ pre-distributed by the base station are independent and different between each other, and these keys only exist in a paired node which ensures that no same session key used in network. It's indicated that the nodes captured will not affect the other nodes.

Fig. 3 shows the illustration of the difficulty for decrypting matrix A when the dimension n of matrix A is slightly changed in AGKMS.

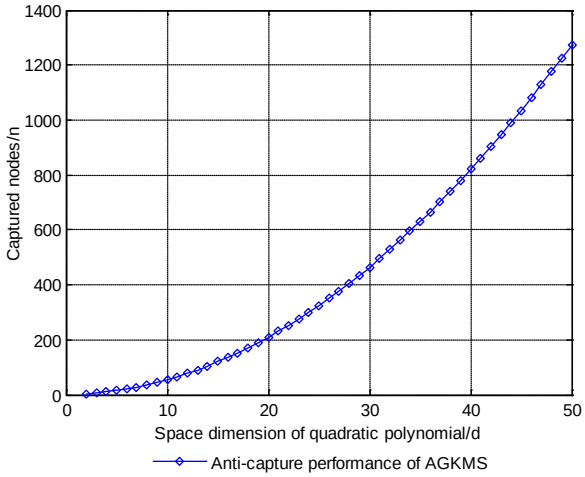

Fig. 3. The anti-capture performance of AGKMS

3. Scalability

The base station BS will notify the cluster header to update the group key when a new node joins the network. Assume that node a is the new node for joining the cluster j, and node a can't make broadcast communication because the group key is not assigned to node a. Firstly, node a needs to build the session key K_{a,CH_j} with the cluster header CH_j based on the quadratic form polynomial $f_{\omega_a}(x_1, x_2, ..., x_n)$ pre-distributed by BS. Secondly, node a sends the key information $m(a)$ encrypted by K_{a,CH_j} to CH_j. Then, CH_j will send $m(a)$ to BS with key $K_{CH_j,BS}$. Lastly, BS can get new the key information $m(1)\ldots m(a)\ldots m(n+1)$, and BS will generate a new group key $K_j^{'}$ by reference to AGKMS or **Fig. 2**.

Within the process, the new joining node a doesn't affect the steps of group key generation and else nodes of cluster j do not change their communication keys. So, the process of new node joining is safe and convenient.

5 Simulation Analysis

In order to verify the effectiveness of AGKMS security features in cost, the simulation is carried out on the MATLAB R2014a.

The main setting parameters of simulation process are shown in **Table 2**:

Table 2. The main parameters value of simulation in AGKMS

Parameters	Value
BS Number	1
Network Size	[100,200,300,400,500,600,700,800,900,1000]

Frequency	433MHZ
Area	1000m*1000m
Radius	500m
Modular	CC1110
Protocol	IEEE802.15.4
Rate	250kb/s
Power	27dBm

1. Storage cost

Assume that the storage cost is the number of keys stored by one node and the storage space occupied by one key is 1.

In LKH, the group controller (GC) is responsible for managing the keys of the network, and assume that the key tree in LKH is a binary tree (as shown in **Fig. 4**), the common nodes in group are the leaf nodes in the key tree which get all the keys on the path from their own leaf node to the root node. The number of keys stored in each leaf node is $\log_2{}^N+1$, where N is the network size.

In addition, all leaf nodes in LKH needs to save their own identity ID, computing parameter E, and public parameter P.

So, the storage cost of each leaf node is $l_1 = c_1 + \log_2{}^N + 1$, where c_1 is a constant and c_1 can be set to 3 in here (assume that the parameter ID, E, P all occupy the same storage space which can be set to 1), so $l_1 = 4 + \log_2{}^N$.

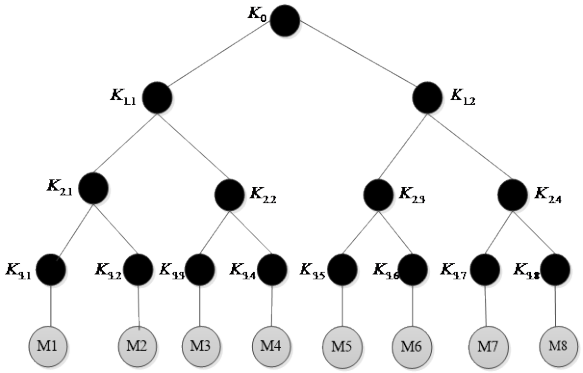

Fig. 4. 8 members LKH tree

In EBS, the EBS system is a triple system which is represented as $EBS(N,k,m)$ and defined as a set of user subsets. In which, each subset corresponds to a key, and each element in some subset all share this key. In addition to this, each element in one subset can be included in else k-1 subsets at the same time, which indicates that each node can store k keys at most, where N is the size of network, $k+m$ is the total number of keys. For instance, the key

distribution scheme of $EBS(8,3,2)$ is shown in **Table 3**, where M is the matrix, $M(i, j)=1$ indicates that the key K_i is assigned to the node S_j.

In addition, each node also needs to save its own identity ID and the group key S.

So, the storage cost of each node is $l_2 \le c_2 + k$, where c_2 is a constant and c_2 can be set to 2 in here (assume that the parameter ID and S occupy the same storage space which can be set to 1). However, the existence of subset Γ is the key problem for building $EBS(N,k,m)$, if Γ does not exist that $EBS(N,k,m)$ will not be established which indicates that k in (N,k,m) is not fixed.

Table 3. Matrix of EBS(8,3,2)

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
K_1	0	0	0	0	1	1	1	1
K_2	0	1	1	1	0	0	0	1
K_3	1	0	1	1	0	1	1	0
K_4	1	1	0	1	1	0	1	0
K_5	1	1	1	0	1	1	0	1

In AGKMS of this paper, each cluster common node needs to store group key K_j, session key $E_{K_{i,CH_j}}$, key information $m(i)$, identity ID. The cluster head CH_j needs to store N_j session keys between all common nodes of cluster j, a session key $K_{CH_j,BS}$, and N_j cluster members' identity ID.

So, the storage cost of each common node is $l_3 = c_3$, where c_3 is a constant and c_3 can be set to 4 in here (assume that the parameter ID and $m(i)$ occupy the same storage space which can be set to 1). And the average storage cost of each cluster head is $l_4 = \frac{2N}{M}$, where M is the number of cluster heads and take 2% of the network size.

The storage cost of these 3 schemes for common sensor nodes (LKH, EBS, AGKMS) are shown in **Fig. 5**, and it's indicated that AGKMS is much better than LKH and EBS in storage cost.

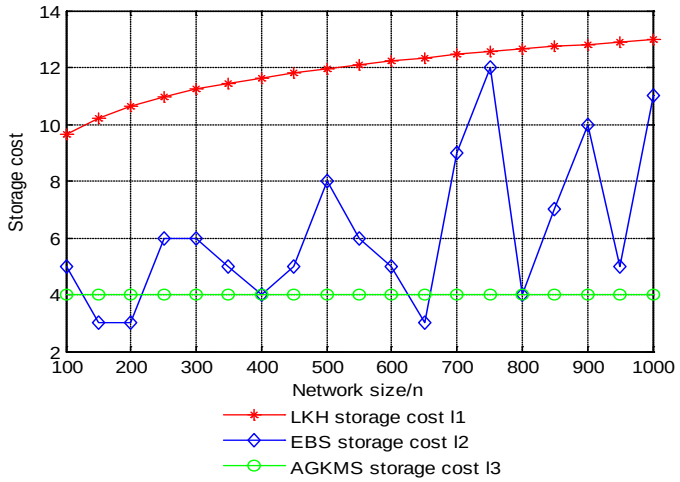

Fig. 5. Compare for storage cost

2. Communication cost

Assume that the communication cost is the number of communication for establishing group key.

In LKH and EBS, the group key is pre-distributed for each common node by the group controller (GC) when network initialization. It's indicated that communication cost is 0 in LKH and EBS, but the real cost is the sacrifice of network security which is analyzed in section 4.

In AGKMS, the group key K_j of cluster j can be obtained by 2 times communication shown in **Fig. 2**, one is sending key information $m(i)$, and the other one is receiving encrypted information $E_{K_{i,CH_j}}\left(f(x)'\right)$.

So, the AGKMS has a good communication cost in the condition of network security.

3. Computation cost

Assume that the computation cost is the amount of computation for building a group key or updating a group key.

In LKH, assume that the key tree is a binary tree (as shown in **Fig. 4**), the common nodes in group are the leaf nodes in the key tree which get all the keys on the path from their own leaf node to the root node. The number of keys stored in each leaf node is $\log_2{}^N+1$, where N is the network size.

Assume that some leaf node M_i is left or captured, and all left leaf nodes need to update the keys shared with M_i, where $\mathrm{N}/2$ nodes in the other side of binary tree need to update one key K (the group key), $\mathrm{N}/4$ nodes need to update two keys shared with M_i, and the neighbor node of M_i needs to update $\log_2{}^N$ keys shared with M_i step by step .

So, the updating computation cost of LKH for some leaf node M_i left or captured is $l_5 = \log_2{}^N + \left(\log_2{}^N \text{-1}\right)\cdot 2 + \ldots + \left(\log_2{}^N \text{-i}\right)\cdot 2^i \ldots + N/2$. It's indicated that the deeper the binary tree degree ($\log_2{}^N$) is, the more computation cost (l_5) is.

In EBS, assume that S_i is a node of some subset in $EBS(N,k,m)$ system. If S_i is left or removed, GC needs to broadcast m messages to update keys, and the left nodes need to make k times decryption operation to get the new keys.

Such as $EBS(8,3,2)$ shown in **Table 3**, each node needs to make 3 times decryption operation to get the new keys. Assume that node S_1 is removed, the left nodes (S_2~S_8) need to update keys K_3, K_4, K_5 belonged to S_1, and GC need to broadcast 2 messages:

(a) $E_{K_1}\left(K^{'}, E_{K_3}\left(K_3^{'}\right), E_{K_4}\left(K_4^{'}\right), E_{K_5}\left(K_5^{'}\right)\right)$,

(b) $E_{K_2}\left(K^{'}, E_{K_3}\left(K_3^{'}\right), E_{K_4}\left(K_4^{'}\right), E_{K_5}\left(K_5^{'}\right)\right)$.

Where $K_i^{'}$ is the new key for replacing K_i, $K^{'}$ is the new group key.

So, the updating computation cost of EBS for some node S_i left or captured is $l_6 = \left(\text{N-1}\right)\text{k}$, where k is an unfixed constant . It's indicated that l_6 is a fluctuating variable in some way, but the computation cost is basically proportional to the network size N .

In AGKMS, as shown in **Fig. 2**, the computation cost for establishing a group key K_j of cluster j is as follows: according to the steps of AGKMS, each cluster common node needs to encrypt its own key information $E_{K_{i,CH_j}}\left(m(i)\right)$ first of all, and the cluster head needs to get $m(1), m(2), \ldots, m(n)$ by n times decryption and make one encryption $E_{K_{CH_j,BS}}\left(m(1), m(2), \ldots, m(n)\right)$, then the base station BS needs to get $m(1), m(2), \ldots, m(n)$ by one decryption and generate a Lagrange interpolation polynomial function $f(x)^{'}$ and make one encryption $E_{K_{CH_j,BS}}\left(f(x)^{'}\right)$, the cluster head needs to get $f(x)^{'}$ by one decryption $E_{K_{CH_j,BS}}\left(f(x)^{'}\right)$ and make n times encryption $E_{K_{i,CH_j}}\left(f(x)^{'}\right)$ sent to cluster common nodes, and each cluster common node needs to get $f(x)^{'}$ by one decryption and get the group key K_j by taking $m(i)$ into $f(x)^{'}$ at last.

It's indicated that each cluster common node needs to make 3 times computation to get the group key K_j and the main computation cost are concentrated in the cluster heads. So the whole computation cost is very small based on the cluster head accounted for less than 2% of network size. In addition, it can balance the network load by replacing the cluster heads periodically.

According to the above analysis, assume that BS has the ability to detect the occurrence of node captured or energy exhaustion for ensuring that the captured node can't obtain the group key K_j , and the following steps are required: assume that the captured node S_i is a common

node of cluster j, BS only needs to delete the key information $m(i)$ of S_i and generates a new Lagrange interpolation polynomial function $f(x)'_{\text{new}}$ by the key information of the remaining common nodes, where $f(x)'_{\text{new}}$ contains the new group key $K_{j\text{new}}$, and remaining common nodes will get the new group key $K_{j\text{new}}$ by getting $f(x)'_{\text{new}}$ following the steps of AGKMS.

For computing the computation cost of AGKMS in the situation of existing one captured node, assume that the size of cluster j is N, BS needs to make a routine computation for generating the new Lagrange interpolation polynomial function $f(x)'_{\text{new}}$, and each node of the remaining $N-2$ common nodes (removing the cluster head CH_{j} and the captured node S_i) has 2 computation cost (getting $f(x)'_{\text{new}}$ by one decryption and getting $K_{j\text{new}}$ by taking $m(i)$ into $f(x)'$), and the cluster head CH_{j} has $N-1$ computation cost (getting $f(x)'_{\text{new}}$ by one decryption $E_{K_{CH_j,BS}}\left(f(x)'_{\text{new}}\right)$ and making $N-2$ times encryption $E_{K_{i,CH_j}}\left(f(x)'\right)$ sent to the remaining common nodes).

Assume that one computation cost is 1, so the computation cost of AGKMS in the situation of existing one captured node is $l_7=3N-4$.

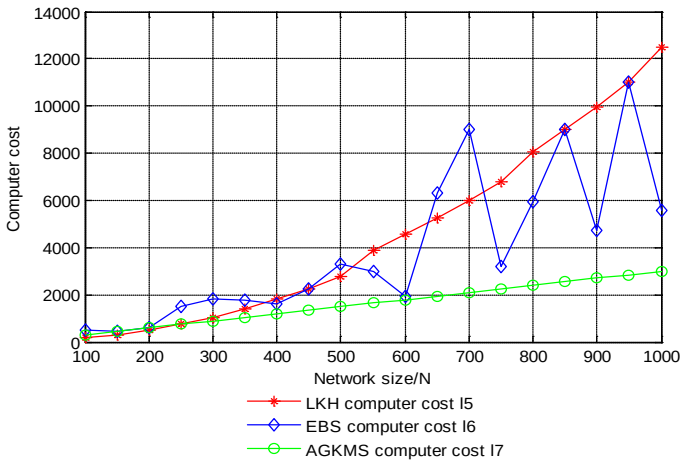

Fig. 6. Compare for computer cost

The computation cost of the 3 schemes (LKH, EBS, AGKMS) is shown in **Fig. 6**, and it's indicated that the computation cost of AGKMS in the situation of existing one captured node is much better than LKH and EBS.

In addition, if a new node S_{new} want to join cluster j in AGKMS, the following steps are required: S_{new} needs to submit a joining application to BS firstly, BS will judge whether S_{new} is a malicious node secondly, and then BS will allow the new node S_{new} to join

cluster j after the judgment and set a key information $m(\text{new})$ and quadratic form $f_{\omega_{S_{new}}}(x_1, x_2, ..., x_n)$ for S_{new}.

Since the new node S_{new} is added to cluster j, BS will notify the cluster head CH_{j} to update the group key, the following steps are required: S_{new} needs to build a session key K_{S_{new},CH_j} between CH_{j} based on the pre-distributed quadratic form $f_{\omega_{S_{new}}}(x_1, x_2, ..., x_n)$ by BS firstly, S_{new} will send the encryption information $E_{K_{S_{new},CH_j}}\left(m(new)\right)$ to CH_{j}, and then all cluster common nodes will get the new group key $K_{j_{\text{new}}}$ following the steps of AGKMS.

Compared with LKH and EBS, the computation cost for new node joining in LKH and EBS is very small because of the management by GC. Though the computation cost for new node joining in AGKMS a little larger than LKH and EBS, AGKMS scheme does not affect the structure of the network for new nodes and has a good scalability, and AGKMS can avoid the collusion problem and keep more security.

So, the AGKMS in this paper has a good computation cost.

6 Conclusions

This paper presents a group key management scheme for wireless sensor networks based on Lagrange interpolation polynomial characteristic, it utilizes the characteristic that Chinese remainder theorem can be expressed into the form of Lagrange polynomial interpolation to realize the generation of group key with no cluster nodes directly involved. The analysis results of safety performance show that AGKMS has good network security, key independence, anti-capture, low storage cost, low computation cost, and good scalability.

Building group key management of wireless sensor networks is a hot research topic, many scholars have carried out the research, but no scheme can meet all the security requirements. At present, there are still many problems that need to be further solved by building some wireless sensor networks group key management protocols:

1. Performance of group key management scheme

In the existing schemes, there is no scheme which can meet all the security performance and have low cost in all aspects at the same time. Most schemes could reduce one kind of cost, but will increase the cost of other aspects. So, there is no group key management scheme that is applicable to all types of groups.

2. Application of group key management scheme

How to use the existing network security technologies to realize the group key management scheme, how to combine group key management schemes and group communication application system to achieve secure group communication, how to deal with the practical application of secure channels and the trusted third party in some group key management schemes, they are all important problems which should be considered to make group key management schemes from theory to reality.

References

[1] M. M. Ge, J. B. Hong, W. Guttman and D. S. Kim, "A framework for automating security analysis of the internet of things," *Journal of Network and Computer Applications*, vol. 83, pp. 12-27, April, 2017. Article (CrossRef Link) .

[2] S. Y. Cheng, Z. P. Cai and J. Z. Li, "Approximate sensory data collection: a survey," *Sensors (14248220)*, vol. 17, no. 3, pp. 564, March, 2017. Article (CrossRef Link).

[3] I. Jang, D. Pyeon, H. Yoon and D. Kim, "Channel-quality-aware multihop broadcast for asynchronous multi-channel wirelesssensor networks," *Wireless Networks (10220038)*, vol. 22, no. 7, pp. 2143-2158, October, 2016. Article (CrossRef Link).

[4] V. V. Phan and O. Hoon, "RSBP: A reliable slotted broadcast protocol in wireless sensor networks," *Sensors (14248220)*, vol. 12, no, 11, pp. 14630-14646, November, 2012. Article (CrossRef Link).

[5] Z. B. Wang, J. H. Hu, R. Z. Lv, J. Wei, Q. Wang, D. J. Yang and H. R. Qi, "Personalized Privacy-preserving Task Allocation for Mobile Crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 18, no. 6, pp. 1330-1341, July, 2018. Article (CrossRef Link).

[6] L. G. Liu, L. Chen and H. L. Jia, "Social milieu oriented routing: a new dimension to enhance network security in WSNs," *Sensors (14248220)*, vol. 16, no. 2, pp. 247, February, 2016. Article (CrossRef Link).

[7] Diaz Alvaro and Sanchez Pablo, "Simulation of attacks for security in wireless sensor network," *Sensors (14248220)*, vol. 16, no. 11, pp. 1932, November, 2016. Article (CrossRef Link).

[8] M. Jef, M. Sam, H. Danny, H. Christophe and J. Wouter, "SecLooCI: A comprehensive security middleware architecture for shared wireless sensor networks," *Ad Hoc Networks*, vol. 25, no. PA, pp. 141-169, February, 2015. Article (CrossRef Link).

[9] Fayed N S, Daydamoni E M, Atwan A, "Efficient combined security system for wireless sensor network," *Egyptian Informatics Journal*, vol. 13, no. 3, pp. 185-190, November, 2012. Article (CrossRef Link).

[10] Davut Incebacak, Kemal Bicakci and Bulent Tavli, "Evaluating energy cost of route diversity for security in wireless sensor networks," *Computer Standards & Interfaces*, vol. 39, no. 3, pp. 44-57, March , 2015. Article (CrossRef Link).

[11] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors (14248220)*, vol. 12, no1, pp. 55-91, December, 2012. Article (CrossRef Link).

[12] M. L. Messai and H. Seba, "A survey of key management schemes in multi-phase wireless sensor networks," *Computer Networks*, vol. 105, pp. 60-74, August, 2016. Article (CrossRef Link).

[13] M. Damiano and M. Massimo, "A semantic analysis of key management protocols for wireless sensor networks," *Science of Computer Programming*, vol. 81, pp. 53-78, February, 2014. Article (CrossRef Link).

[14] X. B. He, N. Michael and M. Hermann, "Dynamic key management in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 611-622, February, 2013. Article (CrossRef Link).

[15] A. S. J. Marcos, S. L. M. B Paulo, B. M. Cintia and C. M. B. C. Tereza, "A survey on key management mechanisms for distributed Wireless Sensor Networks," *Computer Networks*, vol. 54, no. 15, pp. 2591-2612, October, 2010. Article (CrossRef Link).

[16] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Transaction on Software Engineering*, vol. 29, no. 5, pp. 444-458, May, 2003. Article (CrossRef Link).

[17] Cheikhrouhou Omar, "Secure group communication in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 115-132, February, 2016. Article (CrossRef Link).

[18] L. Veltri, S. Cirani, S. Busanelli and G. Ferrari, "A novel batch-based group key management protocol applied to the Internet of Things," *Ad Hoc Networks*, vol, 11, no. 8, pp. 2724-2737, November, 2013. Article (CrossRef Link).
[19] D. Tsitsipis, A. Tzes and S. Koubias, "TALK: Topology aware LKH key management," *International Journal of Distributed Sensor Networks*, vol, 10, no. 11, November, 2014. Article (CrossRef Link).
[20] M. Eltoweissy, M. H. Heydari, L. Morales and I. H. Sudborough, "Combinatorial optimization of group key management," *Journal of Network and System Management*, vol. 12, no. 1, pp. 33-50, March, 2004. Article (CrossRef Link).
[21] S. Sharma and C. R. Krishna, "An efficient distributed group key management using hierarchical approach with elliptic curve cryptography," in *Proc. of IEEE International Conf. on Computational Intelligence and Communication Technology, CICT 2015*, pp. 687-693, April 1, 2015. Article (CrossRef Link).
[22] Q. N. Niu, "ECDH-based scalable distributed key management scheme for secure group communication," *Journal of Computers*, vol. 9, no. 1, pp. 153-160, January, 2014. Article (CrossRef Link).
[23] C. Guo and C. C. Chang, "An Authenticated group key distributed protocol based on the generalized Chinese remainder theorem," *International Journal of Communication Systems*, vol. 27, no. 1, pp. 126-134, January, 2014. Article (CrossRef Link).
[24] X. X. Lv, H. Li and B. C. Wang, "Group key agreement for secure group communication in dynamic peer systems," *Transactions on Parallel and Distributed System*, vol. 72, no. 10, pp. 1195-1200, October, 2012. Article (CrossRef Link).
[25] M. Abbas, H. Fazirulhisyam and O. Mohamed, "Lighted weighted decentralized multicast-unicast method in wireless IPv6 networks," *Journal of Network and Computer Application*, vol. 42, pp. 59-69, June, 2014. Article (CrossRef Link).
[26] Y. Zhang, J. X. Liang, B. X. Zheng and W. Chen, "A hybrid key management scheme for WSNs based on PPBR and a tree-based path key establishment method," *Sensors*, vol. 16, no. 4, pp. 509-526, April, 2016. Article (CrossRef Link).
[27] H. S. Juan, V. D. C. Juan, P. Josep and G. Carlos, "Low-cost group rekeying for unattended wireless sensor networks," *Wireless Networks*, vol. 19, no. 1, pp. 47-67, January, 2013. Article (CrossRef Link).
[28] M. Suvo, "Iolus: a framework for scalable secure multicasting," in *Proc. of the 1997 ACM SIGCOMM Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp. 277-288, September 14-18, 1997. Article (CrossRef Link).
[29] D. Y. Pei, X. Xu and J. W. Dong, "Information Security Based on Basic Mathematics," *2nd Edition, People's Posts and Telecommunications Press, Beijing*, 2007. Article (CrossRef Link).
[30] A. Datta, A. Derek, J. C. Mitchell and D. Pavlovic, "A Derivation System and Compositional Logic for Security Protocols," *Journal of Computer Security*, vol. 13, no. 3, pp. 423-482, May, 2005. Article (CrossRef Link).
[31] C. K. Wong, M. G. Gouda and S. S. Lam, "Secure Group Communications Using Key Graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp. 16-30, February, 2000. Article (CrossRef Link).
[32] N. P. Alireza, K. Kazuya, K. Toshihiko and I. Shuichi, "A hierarchical group key management scheme for secure multicast increasing efficiency of key distribution in leave operation," *Computer Networks*, vol. 51, no. 17, pp. 4727-4743, December, 2007. Article (CrossRef Link).
[33] X. G. Wang, W. R. Shi, W. Zhou, P. Gao and Y. S. Jiang, "A Key Management Scheme Based on Quadratic Form for Wireless Sensor Network," *Chinese Journal of Electronics*, vol. 41, no. 2, pp. 214-2192, February, 2013. Article (CrossRef Link).
[34] W. B. Heinzelman, A. P. Chandrakasan, H. Balkarishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660-670, October, 2002. Article (CrossRef Link).

[35] P. Ji, C. D. Wu, Y. Z. Zhang and Z. X. Jia, "DAST: A QoS-aware routing protocol for wireless sensor networks," in *Proc. of 2008 International Conf. on Embedded Software and Systems Symposia, ICESS2008*, pp. 259-264, July 29-31, 2008. Article (CrossRef Link).

Xiaogang Wang received his Ph. D degree from the Chongqing University, Chongqing, China. He is currently a lecturer, with Artificial Intelligence Key Laboratory of Sichuan Province, School of Automation and Information Engineering, Sichuan University of Science and Engineering. His current interests are in the area of wireless sensor network and security, IoT, artificial intelligence.

Weiren Shi received his Master's degree from the Chongqing University, Chongqing, China. He is currently a full professor, with College of Automation, Chongqing University. His current interests are in the area of wireless sensor network and applications, information control and intelligent systems, embedded systems, pervasive computing, etc.

Dan Liu received her bachelor degree from the Sichuan University of Science and Engineering, Sichuan, China. She is currently a Master student, with School of Automation and Information Engineering, Sichuan University of Science and Engineering. Her current interests are in the area of intelligent control and system optimization，information security.