RESEARCH ARTICLE OPEN ACCESS

A Pre-shared Key Pool Scheme for Wireless Sensor Networks based on Time

Meixiu Zhou*, Hanying Chen **
*(Electronic EngineeringDepartment,Jinan University, Guangzhou,China)
** (Computing CenterDepartment, Jinan University, Guangzhou,China)

----------**********----------

Abstract:

In this paper, we describe the formatting guidelines for ACM SIG Proceedings. Based on the core issues of the wireless sensor network security model, this paper proposes a new design of pre-shared key pool, which is applied in the area-based key management scheme to ensure network security. This scheme designs a pre-allocated shared key pool architecture based time variables of one-way hash function, adds time parameters to key negotiation, node update, etc., updates the key through the time mechanism and detection mechanism, and effectively guarantees both forward and backward security of the node. For the problem that local nodes are easily captured, this paper designs a key update mechanism based on security events, namely a key pool update mechanism based on a one-way hash key chain. This new one is based on a one-way hash key chain. The key pool satisfies the security requirements for key generation and updating. After theoretical analysis and simulation, it is proved that node connectivity, node storage energy consumption, and anti-capture capability in the proposed improvement scheme are better than the original.

Keywords **—Shared key pool,Time based,Random predistribution,One-way hash function,Region grouping**

----------**********----------

I. INTRODUCTION

Wireless sensor networks are very different from traditional networks. It is a multi-hop self-organizing network. This determines that the security threats, security systems and security algorithms of wireless sensor networks are very different from traditional networks [1]. Therefore, it has very important significance for the further development of the sensor network to study wireless sensor network's own characteristics and its security requirements, and design an efficient key management program which can meet the actual application needs of the sensor network [2].In the traditional random key pre-distribution scheme, all nodes need to select their own pre-shared key from the key pool before deployment. As the deployment node runs out of battery or is removed from the queue of legitimate nodes, new nodes need to be added to join the network. The new node also selects the configuration key in the same key pool [3]. This configuration method brings the following new problems: First, when the captured node leaks its pre-allocated key, if these keys still exist in the key pool, it is possible to be chosen in the key groups by the new deployed node. Therefore, there is a possibility that the enemy may crack it. Secondly, if the leaked key still exists in the key pool where the new node select key, the adversary can use the leaked key to impersonate or falsify the new node and create a more serious

security attack[4]. In view of the above problems, this paper proposes a new pre-shared key pool design based on a one-way hash key chain, which is applied in the regional grouping key management scheme. This new key pool not only takes into account the security requirements of the key update, but also can effectively prevent the enemy from impersonating a new node and creating security attack during the establishment of communication keys between the old and new nodes.

II. IMPROVED REGIONAL GROUPING MODEL DESIGN

A. Regional Model Assumptions

Assume that the sensor nodes are spread through the aircraft in a target area of size X×Y. If a sowing deployment point is used as a central point for sowing, most sensor nodes distributefollowing a certain probability function in the area centered on the deployment point [5]. In order to simplify the practical problems, the schemes in most of the literature adopt methods of uniform deployment and two-dimensional Gaussian distribution.

(1) We use "G_{ij}"for the deployment area and "S_{Gij}"f or the regionarea.

The uniform probability model of nodes in G_{ij} is as follows:

$$f(x, y \mid k \in G_{ij}) = 1 / S_{Gij}$$

(2) The two-dimensional Gaussian distribution model of G_{ij} is as follows. The formula indicates that the location of the k-th sensor node around its deployment point obeys the Gaussian distribution, and the mean value is (X, Y), and the standard deviation is σ.

$$f(x, y \mid k \in G_{ij}) = 1/2\pi\sigma^2 \cdot e^{-[(x-X)^2+(y-Y)^2]/2\sigma^2}$$

When the nodes are evenly distributed, the distances between the adjacent deployment points and the spreading distances of the nodes are parameters that need to be carefully considered. When a two-dimensional Gaussian distribution is used to place a node, the distance between the distance d and the standard deviation "σ"of the model is a very important parameter[6]. In this schemewe use a two-dimensional Gaussian model.

B. Improved Double-Layer Regional Grouping Model

In order to improve the connectivity of the nodes and reduce the probability of key duplication, we divide the areas of the deployment area into double-layer area models, including the sub-regional and minimum-regional layers. The minimum-regionsis shown in Figure 1. Each hexagonal area acts as a minimum area. Each minimum-region corresponds to a minimum-key pool of the same size. All the minimum-regions are divided into two groups. The hexagonal group labeled CG is the core group, and the other hexagon group is the sensor group. The core area and the sensor group share the key in a certain proportion. Since the node can communicate with the nodes of the adjacent minimum-region as far as possible in the normal situation, this design enables the shared key between the minimum-key pools of the adjacent minimum - region to ensure the node connectivity rate.

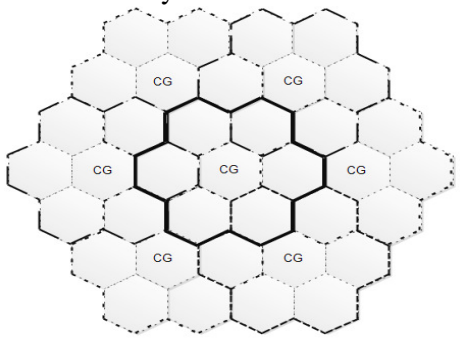

Fig.1Division of sub-regional layers and minimum-regional layers

Each sub-region includes a core group and its surrounding six sensor group, and each sub-region overlaps with its adjacent sub-region by one minimum-region. Each sub-region corresponds to a subkey pool, so we know that the adjacent subkey pool has shared keys. However, this scheme is designed that the non-adjacent subkey pool does not have shared keys. This ensures that each key exists in at most two adjacent sub-regions. If a node is captured, the cracked key can be quickly located and cleared, which reduces the affected range and ensures the security of other sub-regional nodes.

We use the one-way hash function (OWHF) as the basic design of the pre-shared key pool key. The hash function is a typical multi-to-one function. The input is variable-length data "X", and outputs a

string "h" of fixed length "n", which is called the hash value of the input "X" [7].

h = Hash (X) (the length of h is n).

III. AN ALLOCATION SCHEME BASED ON TIME PRE-ALLOCATION AND SHARED KEY POOL

A. Key Pool Generation

First, create a two-dimensional model for all regions. The horizontal direction is the X axis and the vertical direction is the Y axis. From the origin, the horizontal coordinates of the first row of minimum-regions are (1, j), where (j=1, 2) ,3.....), The minimum-region coordinates of the i-th row are (i,j).

We assign the pre-shared key pool as a subkey pool. Each sub-region corresponds to a core area in its center. We use the coordinates $MG_{i,j}$ of the core area to represent the sub-region . Assume that the size of the pre-shared key pool is $|S|$, the size of the subkey pool is $|S_M|$, and the overlap factor between adjacent subkey pools is t.

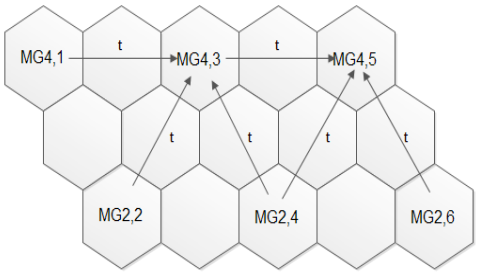

Fig. 2Key sharing relationship between adjacent sub-regions

Then we look at the generation method of the minimum-key pool in the sensorgroup. Each minimum-region selects the key from the shared key of the two adjacent subkey pools where it is located and the minimum-key pool of its corresponding sub- region. Assume that the size of the minimum-key pool is $|S_C|$, and the overlap factor is b. Figure 3 depicts the key sharing relationship between the sensor group and its corresponding sub-regions.

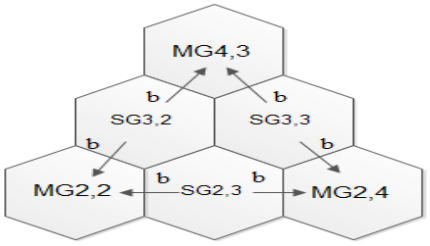

Fig. 3Key sharing between sensor groups and sub-regions

Finally, we look at the generation method of the minimum-key pool in the core area. Each core area selects the key from the minimum-key pools of its neighboring six sensorgroups and the subkey pool in which it is located. Assume that the overlapping factor of the core group and adjacent sensorgroupis a.

From the above rules to complete the key distribution of other core group key pools, we can obtain the following properties: Each core group and its neighboring sensorgroup at least share $a|S_C|$common keys.

After the deployment of sensor nodes in each area is completed, the nodes negotiate information with each other to establish a secure communication key pair, and subsequent node updates, node joins, and node deletions.

B. Time-based Pre-shared Key Pool Design

This section proposes a new pre-shared key pool design. This new key pool based on one-way hash key chain can well meet the security requirements of key generation and update, and it can also effectively prevent intruders from making security attacks.The steps for designing a one-way hash keychain key pool based on time variables are as follows:

(1) The base station server randomly generates $|S_C|$ different fixed-length random data X_i, and selects the appropriate hash function, such as MAC or SHA.

(2) Generate a hash list. Recursive hash function operation:

$Hash^n(X_i) = Hash(Hash^{n-1}(X_i))$ （i=1，2，3…k）

Hash (X) is a one-way hash function. X_i is a fixed-length data, L is the total number of keys in

the shared key pool, and n is the power of hash recursion.

Then put the random number into the formula, you can get the hash value of the sequence, that is, multiple one-way hash chains. For example, sequence $Hash(X_i)$ - $Hash^2(X_i)$ ..... $Hash^{n-1}(X_i)$ - $Hash^n(X_i)$. And its reverse order is $Hash^n(X_i)$ - $Hash^{n-1}(X_i)$ ... ... $Hash^2(X_i)$ - $Hash(X_i)$, This constitutes a reverse hash chain. We set the time axis in the reverse hash chain sequence to obtain the key pre-allocation hash list [9].

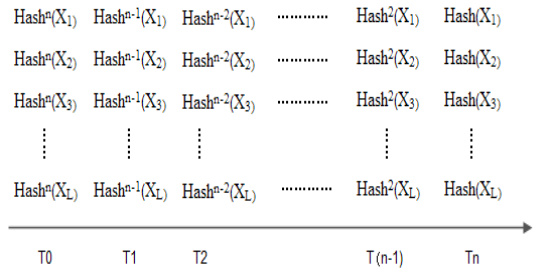

Fig. 4Time-based key pre-allocation hash table

(3) Time-based key pre-distribution mode: different time points correspond to different hash function recursive operation power number sets, that is, the vertical sequence in the table. For example, when each node is deployed for the first time, the time period for selecting the key is the time period T0. At this time, the corresponding key pool is the set{ $Hash^n(X_1)$, $Hash^n(X_2)$ ... ... $Hash^n(X_m)$ }. In the time period after the first deployment, when a new node is deployed in the network, or if the key is leaked and the key pool needs to be updated, the current key set of the shared key pool will also change according to the time period. For example, at the time point T_k, the key pool is updated as a set { $Hash^{n-k}(X_1)$, $Hash^{n-k}(X_2)$ ..... $Hash^{n-k}(X_m)$ }.

The key pool design of the time-based one-way hash key chain proposed in this paper ensures the security of the pre-shared key in the shared key pool in the latest time period. On the one hand, if a node is captured, this design can reduce the impact of key leakage and diffusion time. The node obtains a key from a different key pool at different times. The secure link that the node network has implemented will not affected by the leaked key. On the other hand, due to the one-way nature of the one-way hash function, even if the enemy masters the leaked key on the hash chain of a certain period of time, the subsequent key of the key chain cannot be calculated and the intruder cannot impersonate the new one. Leaked key will become invalid when the key chain is updated at the next time.

As described in the previous section, after the shared key pool key chain table is generated, each region of the sensor network generates its corresponding minimum-key pool. Then each node determines its own region group according to the deployment information, and randomly selects m one-way hash key chains from its corresponding minimum-key pool, and selects the key elements on the key chain with time period T0as the node's key ring. Before node deployment, the content to be pre-stored in the memory of each node includes node identifiers, randomly selected m different key elements, and key identifiers corresponding to each key element.

C. Key Negotiation Process

1) Creating Direct Keys

After the sensor nodes in each region are deployed, the nodes establish a secure communication key pair by negotiating information with each other. Here we introduce a time variable in the process of the direct key creationto solve the problem of pre-shared key leakage.

(1) At the time point T_{i0}, the sensor node i broadcasts the identifier IDs and the time points T_{i0} of all the keys in its own key ring to surrounding neighbor nodes,in order to find all the neighbor nodes that have their own common key.

(2) At the time point T_{j0}, the sensor node j broadcasts the identifier ID and the time point T_{j0} of all the keys in its own key ring to surrounding neighbor nodes including the node i. After receiving the broadcast of node i, node j establish its own neighbor node pre-allocation key table [10].

Assuming that the same pre-shared key K_{X1} , K_{X2} …… K_{Xk} is found.Then we can calculate the same pre-allocated key and time parameters $|T_{j0}|$ using the selected one-way hash function, that iscalculate $Hash(T_{j0} \| K_{X1} \| K_{X2} \| \ldots\ldots K_{Xk})$ 。

(3) If node i receives the broadcast of node j, it finds that node j has the same key“K_{X1} 、 K_{X2} …… K_{Xk} ”as itself. Then the sensing node i uses the selected one-way hash function to encrypt the same pre-allocated key and time parameter $|T_{j0}|$ and sends it to node j at the time T_{i1} .

$$K'_{ij} = Hash(T_{j0} \| K_{X1} \| K_{X2} \| \ldots\ldots K_{Xk})$$

(4) Node j receives the message of node i and compares it with its own calculation result. If the result is the same, a secure link can be established. Continue to perform the hash operation on parameters $|T_{i1} - T_{j0}|$ and K_{ij} :

$$K_{ij} = Hash((T_{i1} - T_{j0}) \| K'_{ij})$$

The hash calculation result obtained by the above equation is used as a direct communication link key between nodes. The basic communication interaction process is shown in Figure 5.

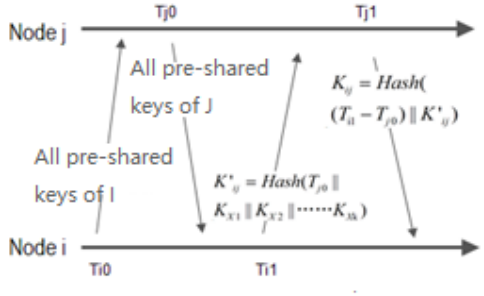

Fig. 5Direct Communication Key Generation Process.

This paper proposes a direct key creation mechanism that introduces time variables, so that the link key between two nodes does not directly adopt the same pre-distribution key received by broadcasting, but introduces a new time variableassociated with the moment when the node broadcasts the information. This mechanism can effectively guarantee the uniqueness of communication keys between nodes. Even if a node is captured during the deployment phase, the intruder breaks the pre-configured key, but the intruder cannot calculate the real communication key based on this.

2) Creating Direct Keys

According to the topology structure of the network, somesensor nodes and theirneighborsensor nodes maynot have shared keys, and the direct key cannot be established by using the broadcast key identifier. In this case, the node must first determine the security path to reach the neighbor node, and then negotiate the communication key with the node through the security path.

(l) The sensor node i belongs to a certain sub-region. According to the topological structure, the sensor node j can be found along the horizontal direction, oblique 60 degrees and 120 degrees of the sub-region. Because two adjacent sub-regions have a certain shared key, theoretically, a secure path can be established through the layer hierarchy.

(2) According to the above method, the sensor node i finds the path ($i \to v_1 \to v_2 \to \ldots\ldots \to j$) to the sensor node j, where there is a public key between any two consecutive sensor nodes. Assume that there are k such paths and they do not intersect.

(3) Taking one of the paths ($i \to v_1 \to v_2 \to \ldots\ldots \to j$) as an example, assume that the direct communication key between the node i and v_1 is K_{iv1} , thedirect communication key between the node v_1 and v_2 is K_{v1v2} , and the direct communication key between the node v_n and j is K_{vnj} . Then the path key for this path is $K_{ij1} = K_{iv1} \oplus K_{v1v2} \oplus \cdots\cdots \oplus K_{vnj}$.

(4) There are K paths for nodes i to j, so that the final communication key of the sensor nodes i to j is $K_{ij} = K_{ij1} \oplus K_{ij2} \oplus \cdots\cdots \oplus K_{ijk}$, and then divide K_{ij} into k packets K_{ij1} 、 K_{ij2} …… K_{ijk} , through which the datais sent to the sensor node j.

(5) After sensor node j receives the k slices, it synthesizes K_{ij1} 、 K_{ij2} … … K_{ijk} to the communication key K_{ij} .

D. Key Updates

There are two conditions that trigger the update of the key: captured node update or time-based update are detected. If the intrusion detection system of the wireless sensor network detects the captured node, all pre-stored shared keys of the captured node are already unreliable. The key of the node needs to be cleared in time, and other nodes having the same key are notified to clear it accordingly. Then the key update operation is triggered to update the shared key pool, the shared key, and the security node list in real time. This scheme uses a one-way hash function key pool design based on time period, when the next time point, the key update mechanism is automatically started, and each key in the node is replaced with the next key of its reverse hash functionchain. In this way, even if the attacker masters the leaked key and hash function on the hash chain of a certain period of time, it cannot derive the subsequent key. When the key is updated, the intruder cannot impersonate the attacked node. The key becomes invalid.

E. Joining New Nodes

The addition of new nodes also applies a time-based key update mechanism. According to the previous section, the key pool removes the leaked pre-shared key chains in time according to the real-time security detection, so thatall the keys in the key pool are secure key chains. And when the new node joins the key, it get the key ringfrom the key chain that has never been leaked.

In addition, according to the pre-allocation key hash chain described in section 3.3, we set the time axis for the working state of the wireless sensor network. As new nodes are added to the sensor network at different time intervals, the deployment nodes in different time periods will correspond to different sets of key pool, thus ensuring the security and reliability of newly added node keys.

Since the newly added node has already determined its deployment group, it selects a certain number of pre-assigned keys randomly from the corresponding minimum-key pool. After the new node is deployed, the configured pre-assigned key ring and the old node's key ring are verified through the broadcast of the key identifier and hash function calculation, and the communication key is established according to the key negotiation method described in section III. It not only ensures the identity security of the new node, but also completes the security upgrade of the shared key.

IV. KEY MANAGEMENT SCHEME PERFORMANCE ANALYSIS

We analyze the performance of this schemefrom four aspects: anti-capturing capability, storage consumption, communication consumption, and scalability.

A. Analysis of Anti-capture Capability

The probability of node's anti-capture is measured by the probability of leaking communication links in the sensor network caused by t nodes being captured. The key in the pre-shared key pool is generated by a one-way hash function. After the key negotiation, it has the capability of interval update, so the node's anti-capturing capability is divided into two situations. One is that the node is captured during the initial deployment period. The other is that the node is captured after completing the key negotiation.

(1) If the sensor node is captured during the initialization, the calculation process is similar to that of the classical regular hexagonal region. Assume that the size of the minimum-key pool is $|S_C|$, the size of the key ring is m, and a common communication key between two sensor nodes is K. Let the probability of cracking the captured node's key is P_{key}. Then the probability that the key K will not be cracked is $(1-\frac{m}{|S_C|}P_{key})^n$ when n nodes are captured. According to this scheme, when there are k shared keys of neighboring nodes, these k keys are hashed as a communication key. The probability that the communication key is cracked is $(1-(1-\frac{m}{|S_C|}P_{key})^n)^k$.

For the same region, the probability that two nodes have k common keys is:

$$P_k = \frac{C_{|S_C|}^{k} C_{|S_C|}^{m-k} C_{|S_C|}^{m-k}}{(C_{|S_C|}^{m})^2}$$

From the above formula, the probability that the n nodes are captured and the other nodes in the same group are captured is:

$$P = \sum_{k=1}^{m} (1 - (1 - \frac{m}{|S_C|} P_{key})^n)^k \times P_k$$

The base station key pool size is 70000, and the region is 20×21. Assume that when the node is captured, the probability P_{key} of cracking the node's key is 1, the value of P can be calculated as the key rings is m, and the relationship between the number of trapped nodes and the node's anti-capturing capability is shown in Figure6.

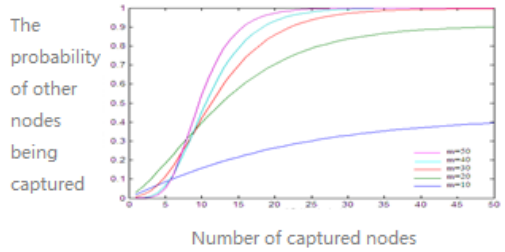

Fig. 6Node anti-capturing capability with different key ring sizes

As can be seen from the figure, with the increase of the key ring, the overall anti-capability of the node is weaker. However, the connectivity of this solution is quite good, the node does not need to store many keys under the condition of good connectivity. Therefore, the key ring does not need to be too large. And because the common key of this scheme only exists in two adjacent sub-regions, even if a node is captured, the impact has been reduced to two sub- regions, and the key can be quickly located and removed.

(2) If the sensor node is trapped after completing the communication key negotiation, as the node storage the key already calculated by the hash function. Because of the character of one-way hash function, even if the sensor node is captured, the attacker cannot break out any original key. And because the scheme introduces a time variable determined between the two nodes in the direct key establishment phase, the established direct key is not the original hash key. Therefore, even if an attacker obtains the key of the captured node, it will not bring security risks to other communication links created using the same key.

At the same time, the time-based pre-shared key pool management method can dynamically manage key information, and ensure the security of the network when individual nodes are damaged. Therefore, the keys of the captured nodes can be promptly removed from the network. When the key is updated, the current key of the captured node has been replaced, the leaked key becomes invalid, and the entire network is still secure.

Therefore, if the sensing node is trapped after completing the communication key negotiation, it will not affect any other sensor nodes, and the probability of trapping of other security nodes is always zero.

B. Storage Consumption Analysis

In order to analyze the storage space, we only need to compare the values of m in the node key ring under the condition of the same connectivity probability [11]. Given a base station key pool size of 70,000 and a group of 20×21. According to the minimum-key pool allocation algorithm and the analysis in section 4.1 and section 4.2, the required m of key ring size at the same connectivity rate can be calculated. As shown in the table below.

TABLE I
NODE CONNECTIVITY RATE IN THE COMMUNICATION AREA

	Node connectivity			
Communication radius and regionradius	**0.3**	**0.5**	**0.7**	**0.9**
r=0.5D	9	13	17	22
r=D	12	16	21	29
r=2D	21	30	40	54

From the results in the table, we can see that the sensor node only needs to store fewer keys and can obtain the same connectivity as the original solution in this scheme. Therefore, under the same connection rate, this scheme can greatly save storage space.

C.Communication Consumption Analysis

In terms of communication consumption, during the key negotiation process, a single node A only needs to send the key identifiers set and node identifiers of node key rings. After receiving the data packet, the neighbor node compares the key identifiers set in the data packet with its own key identifiers set. If there is the same key identifier, the

source node's key identifiers set and the neighbor node identifiers are sent back [12]. In this process, the key does not need to be calculated. Neighboring node keys require only a few packets to be transmitted between neighboring nodes from negotiation to establishment.

However, in the process of negotiation, if there is a key located on the same key chain, the hash key H(x) is used to obtain the key, and the average number of required hash times is L/2. In this scheme, the node key ring m is the same as the basic random key pre-allocation scheme, but a single node needs L/2 hash calculations on average. When the key negotiation is completed, the A node needs to change the original key stored in the key ring, and each key K calculates H(K) through a hash function. At this point, the computational complexity is m. Therefore, the total number of calculations required for the entire scheme is (m+L/2), and the computational complexity is a linearly increasing o(n), which is not required in the original scheme.

Since this scheme also adds time variables, it also adds a communication process and a hash function calculation process for adding a time variable. The node's energy costs have increased. However, in this scheme, nodes only need to store a small number of key rings to ensure connectivity. The computational complexity is also linearly related to the number of key rings. The fewer number of key rings in this scheme also reduces the computational complexity to some extent. Since the communication consumption of the nodes is mainly concentrated on the data transmission after the network initialization, the initialization overhead in this scheme can be not considered when compared with the data communication consumption.

D.Extensibility Analysis

Extensibility refers to the ability of key management schemes to adapt to different scales of wireless sensor networks. The node communication of this scheme runs in a distributed manner. It does not need to rely on the central base station after the initialization, and can adapt to wireless sensor networks of different scales. Even if the network size increases, the storage and communication overhead of each node will not change.

In addition, from the analysis of the new node's join algorithm in this scheme, we can see that, although the new node needs to increase the computational overhead through the key update mechanism, the pre-shared key pool design based on one-way hash key chain ensures the reliability of the pre-distribution key for the new node. If a node has been captured, and it has not been detected in time.The key update mechanism introduced with the time variable can also ensure that the newly-joined node obtains from the pre-shared key pool corresponding to the new time period. The key will not be configured to the leaked pre-distribution key. It can be seen that the nodes can easily and safely join the network at any time. This solution fully supports the scalability of the network.

V. CONCLUSIONS

This paper studies the key issues in key management in wireless sensor networks, and implements a time-based pre-distribution shared key pool design scheme.

Weanalyze the practicality, security, scalability, communication storage energy consumption and other related performances of the scheme, and conducts experimental demonstration. This scheme proposes the design of a pre-shared key pool using a one-way hash function key chain. Based on the unidirectionality of the hash function, even if an enemy masters a certain node's leak key for a certain period of time, it cannot be derived the updated new key.It prevents the attacker from impersonating a new deployment node. The features of the one-way hash function ensure the security of the key in the latest time period, and ensure the forward security of the pre-shared key of the wireless sensor network. In addition, the scheme proposes a key chain design based on the time variable, which is applied in the process of key pool generation, key negotiation, key update, and new node addition. It can not only prevent the attacker from disguising the node when the node establishes the communication key, but also can eliminate the leaked unreliable key in time and prevent the attacker from posing as the old node.Thereby, it ensures the backward security of the wireless sensor network key. Analysis of experimental results confirms that this design of key chain increases the

computation and communication consumption a little, but greatly enhances the link security and scalability.

REFERENCES

[1] N Liu.2011. Key Management Scheme for Wireless Sensor Network.Computer Knowledge & Technology.

[2] Harsh KupwadePatil, Thomas M. Chen. 2017. Wireless Sensor Network Security: The Internet of Things. Computer and Information Security Handbook (Third Edition). Pages 317-337

[3] Khan Imran, BelqasmiFatna; GlithoRoch. 2016. Wireless Sensor Network Virtualization: A Survey. IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. Volume 18, Pages 553-576

[4] Choi, Kae Won; Ginting, Lorenz; Rosyady, PhiscaAditya. 2017. Wireless-Powered Sensor Networks: How to Realize. IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. Volume 16,JAN Pages 221-234

[5] PriyankaAhlawat, Mayank Dave. 2018. An attack model based highly secure key management scheme for wireless sensor networks. Procedia Computer Science. Volume 125, Pages 201-207

[6] Mohamed-LamineMessai, Hamida Seba.2016. A survey of key management schemes in multi-phase wireless sensor networks. Computer Networks. Volume 105, 4 August 2016, Pages 60-74.

[7] Yantao Li, Di Xiao, Shaojiang Deng. 2012. Keyed hash function based on a dynamic lookup table of functions.Information Sciences. Volume 214, 10 December 2012, Pages 56-75

[8] Basar, Mehmet Sinan.Summarizing data for secure transaction: A hash algorithm.AFRICAN JOURNAL OF BUSINESS MANAGEMENT. DEC 28 2011, Volume 5, Pages 13211-13216.

[9] Jianmin Zhang, Hua Li, Jian Li. 2018. Key establishment scheme for wireless sensor networks based on polynomial and random key predistribution scheme. Ad Hoc Networks. Volume 71, 15 March 2018, Pages 68-77

[10] SaritaAgrawal, Manik Lal Das. 2017. Mutual healing enabled group-key distribution protocol in Wireless Sensor Networks. Computer Communications. Volume 112, 1 November 2017, Pages 131-140

[11] C Wu, S Li , Y Zhang. 2013. Key Management Scheme Based on Secret Sharing for Wireless Sensor Network. International Conference on Emerging Intelligent Data & Web Technologies. 2013 , 7 (2/3) :574-578

[12] Marcos A. Simplício, Paulo S.L.M. Barreto, Cintia B. Margi, Tereza C.M.B. Carvalho. 2010. A survey on key management mechanisms for distributed Wireless Sensor Networks. Computer Networks. Volume 54, Issue 15, 28 October 2010, Pages 2591-2612

[13] Yanan Wang, Yongjin Liu, Huishang Jin. 2012. The Study on Key Pre-distribution Methods for Wireless Sensor Networks. Physics Procedia. Volume 25, 2012, Pages 560-567