A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network

Sai Ji, Liping Huang and Jin Wang

Jiangsu Engineering Center of Network Monitoring and College of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China

Abstract

With the development of Wireless Sensor Network (WSN) technology, it has been adopted in a wide variety of applications such as the health care system and so on. Yet, there are still some problems need to be addressed, one of which is the security issue. A lot of schemes from different points of view were proposed to ensure the security in WSNs, however, most of them are proposed for static networks while it is less to consider the situation for the security of the dynamic topology update. Our paper is a novel key management scheme for the dynamic WSNs. The security authentication and random key distribution were initialized in the network deployment phase. During the network stable phase, in order to ensure the real-time update security for the network topology, our scheme proposed a dynamic updated key based on the AVL tree. Simulation result shows that this program can ensure the WSN's dynamic security as well as achieve the energy efficiency goal.

Keywords: *WSNs, Security authentication, Improvement of the leach algorithm, Dynamic network update, AVL tree*

1. Introduction

WSN is a wireless network which is constituted by a large number of randomly distributed sensor nodes through self-organization and multi-hop way. By means of these sensor nodes which have the capability of the perception, computing power, wireless communication, low-cost energy-efficient independent freedom organized, we can collaborate to perceive, collection, processing and transmission monitoring information in the network covering geographic areas and upload these to the users who needs the information. According with the network topology, it can be divided in two classes: the static WSN and the dynamic WSN.

Recent years, the dynamic WSN has been rapidly developed in many fields, for example, dynamic mobility applications [1]: (1) The transport sector, the wireless sensor nodes pre-arranged in the vehicle, can collect information such as traffic flow, vehicle status and so on, as well as transfer these information between vehicles; (2) Logistics services, sensor nodes can be used to detect specific equipment or track sold product usage information in the WSNs; (3) Living assistant, in the medical case, usually, wireless sensor nodes can be put into the patient's body for statistical monitoring of the patient's health status parameters which need to be concerned about, moreover, doctors also would have a better understanding and grasp the real-time status of the patient through an integrated health care system; (4) The wild environmental monitoring, through the dissemination of sensor nodes in some nature harsh environment, we can monitor the condition of animals and plants in real time which not only contributes to human understanding of nature, but also provides scientific clues to explore nature, and with these mobile nodes. Besides that we can also provide real-time monitoring data for the existing natural disaster warning system to improve forecast accuracy and reduce the risk of natural disaster; (5) In the military field, the sensor networks have many applications, especially in the enemy territory, wireless sensors can help us to understand the enemy information providing us a better grasp of the strategic plan.

However, because of the wireless sensor nodes are often placed in dangerous environment, coupled with their own characteristics, especially mobility, WSNs are more vulnerable to attack compared with the traditional network such as physical attack and so on. Therefore with the broaden application areas, WSN’s security become even more important. In order to enhance its security, many people proposed related authentication mechanisms and key management schemes, but these are usually for the fixed nodes. Solutions for the dynamic network efficient security options are less to be considered.

In this paper, a new key management scheme is proposed. Through security authentication and dynamic key update in the initialization phase as well as network running phase, we can ensure the safety of the dynamic WSN. At the same time, this paper used AVL tree to achieve the key dynamic real-time update, while took advantage of the improved cluster head election method to reduce the energy consumption of the network. The simulation results show that our scheme can ensure real-time network dynamic security in WSN, avoid conventional attacks such as replication attacks, and achieve the goal of energy efficiency.

The rest of the paper is organized as follows. Section 2 introduces the related work; Section 3 descries the proposed scheme, while simulation results with MATLAB R2008a are discussed in Section 4. Finally, Section 5 concludes the paper.

2. Related Work

With the development of science and technology, cryptography has also been considerable development both in theory and in practice. For different applications, there are many different cryptography systems, such as the symmetric cryptography, public key cryptography and so on. All of these algorithms have the strengths and weaknesses in different applications, but we have not found that a theory which would be able to meet all application requirements in the WSNs. Security aspects of applications usually need to have better consideration more than the traditional network security. For example, how to deal with the relationship between the safety factor and energy consumption coefficient of various algorithms, how to choose a compromise to meet the needs of existing applications, all of these should be taken into consideration.

2.1 The Main Key Managements in WSNs

Usually, WSN’s key management schemes can be divided into three classes: a trusted server-based, self-protected, as well as the key randomly pre-distributed type [2]. Firstly, the trusted server-based programs mainly depend on a credible server provided the key management between nodes, but few of them was a permanent and credible framework in WSN, therefore this kind of schemes doesn’t be applied to large-scale WSNs. Secondly, the key management scheme based on self-protected, generally it adopts the asymmetric key encryption algorithms, such as RSA algorithm, which is a serious burden for the energy-limited sensor nodes, so it is rarely used in the actual operation. The third scenario is the random key pre-distribution scheme. The key generation method is pre-distributed to all the nodes in respect to the first two methods. Simultaneously, it was said that the safety factor of the third scheme was higher than the first two methods, however, a downside of this solution is that it is generally only applicable to static networks and difficult to apply in dynamic networks.

The representative scheme of trusted server-based solutions is SPINS [3] proposed by Perrig, *et al.*, which contains SNEP (Secure Network Encryption Protocol) and TESLA (micro Timed Efficient Streaming Loss-tolerant Authentication Protocol). SNEP is used to achieve communication confidentiality, integrity, freshness and point-to-point certification, on the other hand, TESLA is for the point-to-multipoint radio certification. In SPINS, each node will have a key, and the corresponding key is stored in the base station, while a one-way hash function is used during the time of broadcast in the authentication to create a release delay mechanism. However, a disadvantage of the protocol is that to establish a direct connection communication key between two nodes is undesirable.

The basic random key pre-distribution model proposed by Eschenauer and Gligor [4], is designed to under the premise of guarantee nodes to establish a secure channel minimize the model requirement for node resources. Before the network deployment, according to this program [4], each node will be assigned to a certain size keys randomly selected from a pre-generated keys pond as its key chain. Just to ensure that there is at least a sharing key between two nodes, they can establish direct communication key. Compared to the trusted server-based model, the model [4] does not need the base station as a communication bridge between any two nodes to establish communication key. Thereafter, on the basis of this model [4] Chan-Perrig-Song proposed improvement by introducing the concept of the "q-composite" [5], in this scheme, two nodes need to share at least q keys to establish a direct communication key. This not only can ensure network security but also enhance the network connectivity, and theoretically to improve the value of q, we can enhance the system's resistance. But there is a downside that each node needs to store a large number of keys, which requires a large memory overhead, thus to find the size of key pool for the model is a center applied practice. Liu [6] proposed the key management mechanism using node pre-deployment priority conditions to establish, coupled with Rabin's scheme [7] to reduce memory consumption which has a high degree of node connectivity and the strong restoring force of the network. Zhang [8] presented the NPKPS (a novel pair-wise key pre-distribution scheme) program, that is a pair-wise key pre-distribution scheme, compared to the literature [9] it is able to achieve better security, connectivity, efficiency and lower memory consumption. [10] and [11] proposed an effective authentication scheme, introducing the concept of security certification security key to the key management, which not only enhancing the security of the original program WSN, at the same time, reducing the certification load on the node and memory load requirements.

In order to find a scheme to support node mobility as well as reduce energy consumption, Kim proposed layer-based multiplex communication key management scheme in the literature [12], the program has reasonable routing load and lower mobile administrative overhead. A two-layer dynamic key management based on clustering supporting node mobility scheme is proposed by Chuang in wireless sensor networks [13]. Besides of that, a scheme proposed in the literature [14] supports node mobility based on polynomial key pre-distribution. The literature [15] proposed a method for authentication and key establishment real-time key generation scheme to reduce memory consumption and enhance the network fault tolerance. Camtepe and Yener proposed the combination design which is a key pre-distribution method [16]. Sanchez and Baldus improved the program [16], referred as the program [17] which can establish direct pair-wise key for a large number of physical connectivity independent sensor nodes in WSN. In order to reduce the memory load while supporting different network nodes mobility, Maerien [18] proposed a key management protocol in mobile wireless sensor network which is assigned to each node a symmetric key, and the key is just shared with its network back-end server, but the program needs to have a relationship of mutual trust between that nodes entered the network with its original network.

Literature [19] proposed a mobile heterogeneous aware network key management scheme with high energy and memory utilization, reducing energy consumption and memory load during the network initialization phase, introducing a new common certification, ensuring network security and network connectivity as well as anti-aggressive, but sometimes the updates of keys do not in real-time.

On the other hand, with WSN rapidly development in different applications, all the key management schemes need to be further improved in order to achieve the memory utilization optimization as well as the entire network resist attack (such as intrusion tolerance) enhancements during operations. Our paper is not only taking the advantage with these schemes but also improving the security for the dynamic network while in the meantime reducing memory consumption.

2.2 The Self-balancing Binary Search Tree—the AVL Tree

Nowadays, in the network system design, we often need to find relevant information in large amounts of data, such as determining whether an element is presented in the data set; accessing to the specified value lower bound and so on. Different search ways have various performances. Self-balancing binary search tree is a better relative performance search way. It has effectively insert operation tree appropriate treatment in order to control the height of the tree. The most common self-balancing binary search tree is the AVL tree and red-black tree. Red-black tree is more complex than the AVL tree. Our scheme learned from the concept of AVL tree. The maximum difference height of any two different nodes in the two AVL subtrees is 1, so it is also called a high degree balanced tree. The average time for search, insert, and delete operations and the time of the worst case of the tree are O (log n). When execute the insert or delete operation, it may be necessary to re-adjust the angle of one or more subtrees. The balance factor of a node is the difference between the height of the right subtree and the left subtree. When a node of the balance factor of 1, 0 or -1, it is considered that the node is balanced, of course the node for other values is imbalanced which need to re-adjust the angle. Generally speaking, the balance factor can be directly stored in each node, or may be stored in the nodes in the sub-tree height calculated [20]. As the AVL tree node position can be adjusted dynamically, this feature can be applied to support dynamic data management mechanism. In the program, during the network stable operation, the key real-time update takes the advantage of this concept, letting each cluster into a virtual self-balancing binary search tree, and then get the node’s corresponding key in the tree, ensuring key real-time updates while reducing the energy consumption of the respective nodes.

3. The Proposed Scheme

3.1 The Network Model of this WSN

The network model of this proposed scheme is mainly consisted with three type nodes which randomly distributed in the network. They are BS node (Basic Station node), CS node (Center Sensor node), and the ordinary MS node (Mobile Sensor node).The most stable energy is given to BS, and CS has a relatively high energy. In addition to the BS node, all other nodes are moving 360 degrees. These three kinds of nodes constitute a 100m * 100m WSN through a random distribution, in which BS node is just only one, CS nodes up to 10, and the other are MS nodes. The total number of the nodes is 100, specifically illustrated in Figure 1.

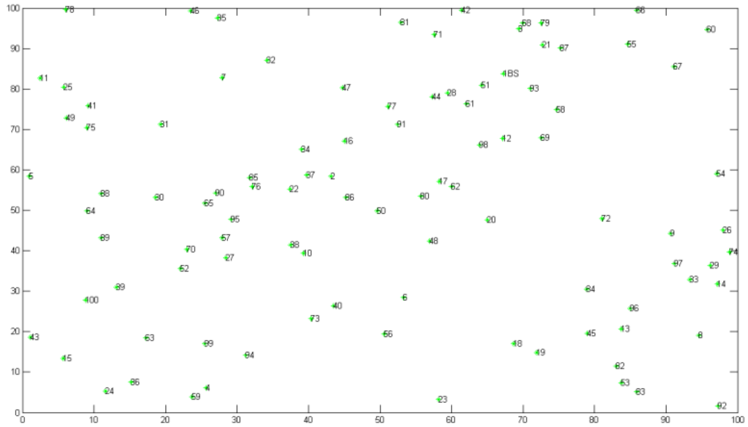


Figure 1. The Network Model

3.2 Initialization Phase

Assuming that all nodes which joined in the network are safety. Each node have their own identity that is the master number, the figures displayed in Figure 1. All these information will be transferred to the BS in the initial time, and then BS will take a record of these information to form a list. In the stable operation stage, if a new node wants to join the network, the first thing is to determine whether its master number is the same with the original format which is called a certification. Specific initialization operations are as follows:

(1) The energy level of all nodes as energy state is divided into five levels, referred to the strongest, stronger, strong, usually, weak states. Because BS node energy is generally unrestricted, so it is set to 5 (the strongest state showing in the Table 1); the energy of other nodes uses the formula (1) to determine the state:

$$E(n) = \frac{l(n)}{a(n)} \qquad n \in N \tag{1}$$

Where *E(n)* represents the percentage of the residual energy of the n node, *l(n)* is the remaining energy, and *a(n)* is the total energy of the node. In this scenario, the total energy initialized as 1, and then the residual energy value and state obtained from the node energy shown in Table 1.

Table 1. The Corresponding Relationship between the *E(n)* Intervals and State

E(n) intervals	State
80%~100%	5
60%~80%	4
40%~60%	3
20%~40%	2
5%~20%	1
0%~5%	0

Notice: An especial state is set when the node N's *E(n)* interval is 0% ~ 5%, at this moment, the node needs to broadcast energy emergency message. The disposal of such nodes is to be exited the network or got into hibernation waiting for energy supply.

(2) BS node generates a pair of keys using the RSA encryption algorithm that is PK (Public Key) and SK (Secret Key) and broadcast PK.

(3) In addition to the BS node, other nodes should send a hello message encrypted by the PK (This contains the node's unique master number, which is pre-set in each node) to the BS node.

(4) BS forms a list of all nodes' information throughout the network initialization. While the BS designs a counter, according to the time stamp which is obtained by responding the time of other nodes' hello message.

(5) Based on a first-come, first-served rule, an ID number will be assigned to each node, as the initial value of this node to generate a variety of keys. And the ID number is not repeated, so that we can achieve the goal of the safe transfer.

3.3 Cluster Head Election Phase

However, after the network initialization, it does not really form a network that can effectively run, in fact, it also needs to go through the cluster head election and cluster formation stage. Whether a node is elected as CH node (Cluster Head), is initialized with the energy level and a random algorithm in the initialization stage.

(1) The node's energy level update: usually, the higher the energy of the node is, the greater chance of the node to elect as CH node has. That is we should preselected CHs based on the node status.

(2) At the same time, the backup CHs entering a preselected spare should be take the random algorithm as follows:

$$T(n) = \begin{cases} \dfrac{p}{\{1-p[r \bmod (1/p)]\}\times[(i\times p)(1-E(n))]} & n\in G \\ 0, \quad otherwise & \end{cases} \qquad (2)$$

Where p is the proportion of all CH nodes in the network node, and is generally set to 5%, r represented by the number of the current round of elections, $E(n)$ is the percentage of the remaining energy level, i is the total number of the idle rounds by the node, when the node elected as the cluster head node, the value of i must be cleared. G is a set that nodes not be elected as CHs in the current $1/p$ round. So, after this round of screening, there will be many nodes to be excluded.

(3) Finally, a node is elected as a CH node, must pass the authentication with its direct connect neighbors by a pair-wise key. That is to establish the pair-wise key between two nodes adjacent. Generation of pair-wise key is generated by a one-way hash function [21].

```
Algorithm 1 A pair-wise Key Establishment
Input: Node N’s ID and master number, Node M’s ID
Output:  the pair-wise key
Initialize: Node M and N are the direct connect neighbors
Repeat executing Step 1 to Step 5 until all neighbors have been called.
Step 1 ：Node N uses its ID and a one-way hash function $F(\quad)$ to generate a master key: $K(n) = F(ID(n))$
Step 2: Node N broadcasts the message and then waits for an answer message from the neighbor node M, the broadcast message is :
        $message(ID(n), \quad master \quad number(n))$
Step 3: At this time, the adjacent node M generates its own master key which is a similar process in accordance with Step 1, that is $K(m) = F(ID(m))$;
Step 4: For the neighbor node N’s broadcast message, the response message is given by node M:
    $\mathrm{message}(ID(m), MACK(m))$ , $MACK(m) = F(ID(m)| \quad master \quad number(n))$
Step 5:Output the pair-wise key, the formula is: $K(mn) = FK(m)(ID(n))$
```

In this way, each node can calculate the directly adjacent node key value based on its ID. This means that each node can be authenticated directly connected nodes. After state value preselecting and random algorithms filter out, candidate CH nodes will become true CH nodes only that directly connected nodes of the pair-wise key authentication is correct.

3.4 Cluster Formation Stage

(1) CH broadcasts a hello message containing CH’s master number encrypted with a symmetric key. Note that the symmetric key is generated by the DES algorithm code stored in each node.

(2) Non-cluster head nodes form a neighboring CH information list by receiving the message continually from CHs, and automatically recorded the corresponding CHs as backup CHs. If the non-cluster head node does not get a list of neighboring CH information, it will broadcast a hello message (contains its master number encrypted with its symmetric key) and wait for the response of other nodes as well as filter out the list of neighboring CH information from them.

(3) Non-cluster head node joins a cluster：When the non-cluster head node decides to join a cluster, the node needs to send a "join request" message to the CH. The message includes the CH master number recorded as CHMN, the non-cluster head node master number encrypted with its symmetric key referred as NCHMN and authentication key K_{auth}, the authentication key generated by the function $f()$, denoted by $K_{auth} = f(CHMN, NCHMN)$. After receiving the message, firstly, CH will decrypt the message using the authentication key $\mathrm{K}_{\mathrm{auth}}$ to get NCHMN, and match the result with the NCHMN decrypted using the DES decryption algorithm. If the match is successful, the node is legitimate, that is, the node certification success. Then CH node will sends the "joining conformation" message to the node preventing a replay attack and replication attack.

At this point, the entire network is formed. The next step is the safe operation in the stable phase. Of course, to note that during the formative stage of cluster heads, between any clusters heads will be the mutual authentication.

3.5 Communication Key Establishment and Management Stage

To establish communication key: the formation of communication key includes between MSs as well as MS and CH. Notice that the information exchanges between CH and BS mainly using RSA's PK and SK which has higher security relative to the first two keys, so it needn't to update in real time, instead, using the method of regularly updated.

The former two communication key's formula is:

$$CK = \quad g(ID1, ID2) \tag{3}$$

Algorithm 2 AVL tree algorithm

```
Input: the list of the cluster nodes' IDs ;
Output: the corresponding key with the node;
Initialize: the CH node is the root of the AVL tree recorded as 0;
Step 1：Using the obtained list to form a virtual AVL tree[21] in the CH end;
Step 2: If the node is the left child of a parent node, we record it as 0,on the contrary, the right is 1;
Step 3: Output the list of the corresponding keys in the virtual tree
```

The communication key generation is dynamic, in the formative stages of the cluster, cluster head will record the node ID which was entered the cluster, then the CH node will form a cluster ID list, and we use the AVL tree(Algorithm 2) self-balancing these IDs (mainly node insert operation) to form a balanced binary search tree. In this tree, each node will have a fake id, and the fake id will be sent to the node encrypted with CH node's own symmetric key. This makes the g ( ) function of two ID1, ID2 parameters dynamically updated so that the communication key is carried out dynamically updated once the cluster structure changes. After that, each node's key associated with the balance of the tree, this is the dynamic key update. Dynamic key profile contributes to the protection of the entire network in the stable operating phase of the security.

The communication between a cluster: if the nodes in a cluster want to communicate with each other, both of them should get the dynamic ids of them from the CH, and establish their own communicate key for security communication.

The communication between different clusters: if two nodes in the different clusters should be found a session, firstly, one of them must send a hello message to the other one. For example, the node A would send the hello message to the node B, at this point, the CH node of the node A will perceive the message and try to communicate with the CH node with the node B. If the communication is successful, then the A's CH will response node A with the B's virtual id, that is node A has got node B's id, so it can establish the communicate key, on the contrary, the node B will have the node A's id and using equation (3) can be generated the communication key CK_{AB} and thus between the two can communicate securely.

3.6 Network Topology Dynamic Update in Real Time

The new nodes joining the network:

(1) First, the BS test and verify the new node's master number, this master number must has the same format with the original format in the BS. If not, then the node is not allowed to enter. After the success of the format matching, the BS will provide its ID number for the node to avoid Sybil attack.

(2) New MN broadcast the hello message to get the information about the list of its entire neighboring CHs.

(3) The neighboring CHs will verify its authentication message with the BS, if the match is successful, the cluster head will give a reply message, and the mobile node will select a CH based on the signal strength of the CH to join the cluster. Then the CH test the balance, if unbalanced, it will be self-balanced, then the node can be obtained the corresponding key, enter into the communication key establishment and update stages.

Node moving between clusters: Because the energy of each node is constantly consumed in the operation, as CH node, its energy should be better than the MS node energy. Therefore, this program set threshold value of the CH node's energy state to 2.

(1) When the MS nodes found the energy state of the current CH has dropped the threshold, the node will send a hello message to find a new cluster head and update its current owned adjacent cluster head list.

(2) Once a new CH responded, the node will have a sort based on its energy state and distance, then select the maximum coefficient CH as the next CH, while the MS node sends a leaving message to current CH node (This message contains a new CH's master number to the original CH was mutual authentication, so we can reduce the repeated operation of the certification [19]).

(3) At the same time, it will also sends "join request message" to the new CH node.

(4) The new CH node tries to obtain the MS node ID from the original CH node.

(5) The original CH received leaving message would confirm the MS node has been moved to the new CH, and then sent the MS's ID to the new CH (where the communication key between the two CHs is given by BS node) while notify the BS to update its own list avoiding node replication attacks.

4. Simulation Results

In order to simulate the security design scheme, we use the MATLABR2008a software. During the network deployment, we randomly deployed 100 wireless sensor nodes, one of which is the highest energy level of a BS node, then 10 CS nodes of a relatively high energy level node, and the remaining MS nodes. 100 nodes form the size of the network coverage of 100m * 100m. In addition to BS nodes, all other nodes are 360 degrees move, but its movement speed is a constant, and here is set to 1m / s, the moving direction is updated once every 0.1s.

Through the simulation, we select the following parameters of the program to compare with existing programs.

(1) The security of the dynamic network

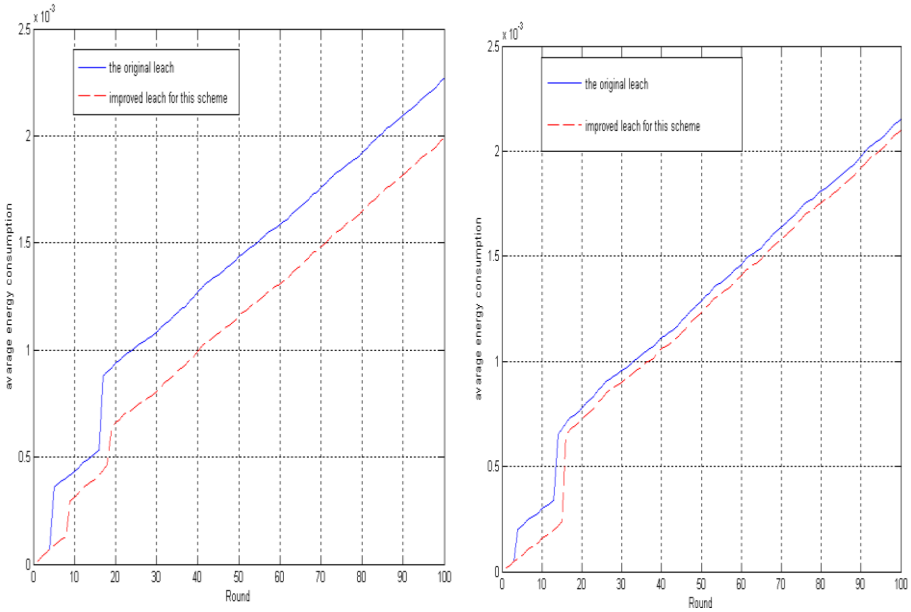
In the network initialization phase, this scheme does not abandon the RSA algorithm which usually is not adapted to the WSN. Instead it is applied to the communication between CH and BS which could be ensured the high security between the two levels.

At the same time, compared to the program [21], our program improved the leach algorithm and learned from the philosophy of the AVL tree which is applied to the key dynamic update, reducing the computing load while guarantee the node mobile security. Besides, the program can guarantee the conventional attack immunity (Table 2) when node moves as well as improve the update rate of the key which help the adjustment of the dynamic security of the network.

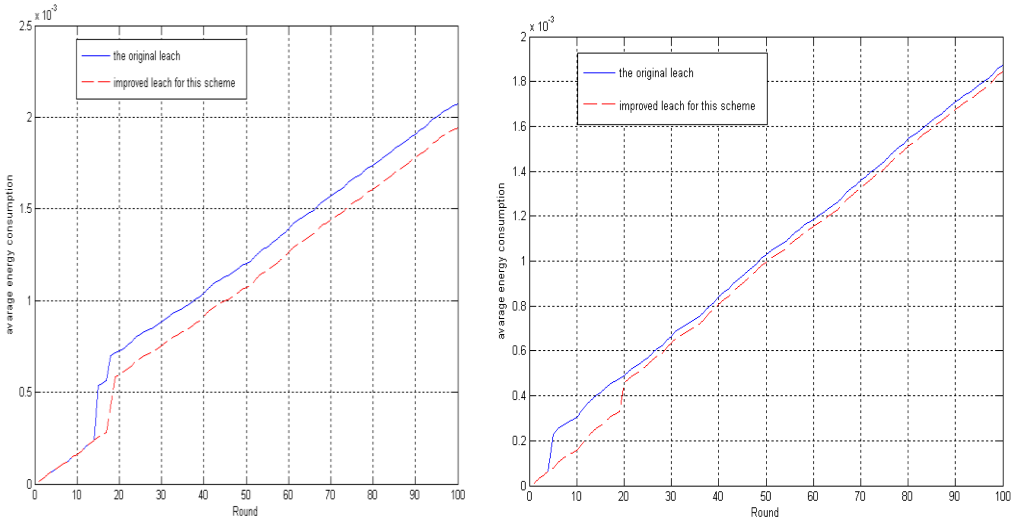
Table 2. Immunity to the Common Attacks

Attack type	AVL tree[21]	Our scheme
Selective-Forwarding	Y	Y
Sink-Hole attack	Y	Y
replay attack	N	Y
replication attack	N	Y
Sybil attack	Y	Y

(2) The entire network communication load of the cluster head election stage



(a) Change from the fifth round (b) Change from the third round



(c) Change from the fifteenth round (d) Change from the fourth round

Figure 2. The Original Leach and Our Leach Consumption

From the Figure 2, we can see that usually the average energy consumption is in $[2.0\times10^{-3},2.5\times10^{-3}]$ for the 100 rounds to elect the CHs. Compared with the original leach [22] this improved leach can reduce the energy in the CHs formation stage. Moreover, as we see on the picture Figure 2, generally, the strongest difference between the two leach occurred in the first 20 screening, sometimes they have the same energy consumption(c) at the first rounds. However, the tendency for such big change is not always maintained, instead, both programs' average energy consumption will get into a parallel graph accompanied by the increase in the screening rounds. In short, the improved leach algorithm has a significant improvement in the energy consumption aspect compared with the original one [22].

(3) The energy consumption load of each node

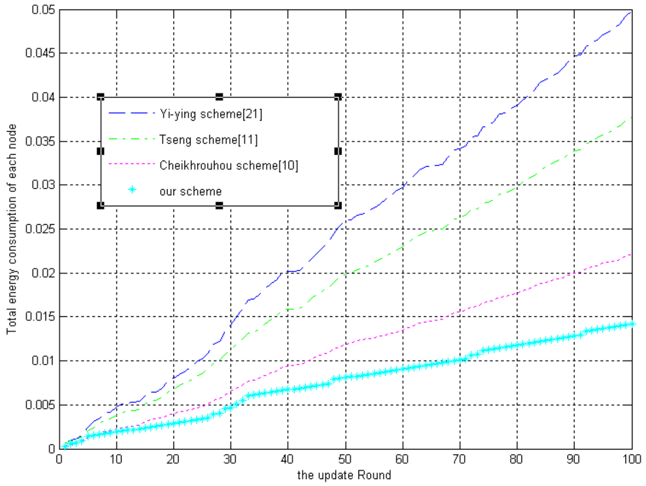


Figure 3. The Energy Consumption Load of Each Node

Figure 3 shows the different energy consumptions of our scheme compared with scheme [10, 11, 21]. From this picture, on the whole, our scheme has the minimal energy consumption of all the schemes showed on the figure. In the first thirty update rounds, their difference is not great, however, after then, the difference become greater and greater. At this point, our scheme will have a great potential to adapt to the large-scale dynamic WSNs. Meanwhile, this scheme needs store less keys compared with the existing programs such as [19], so different from the others, the memory overhead is very small. In addition, through the main two authentications, we can ensure the security of the network at the same time to achieve the goal of energy saving, because its certification consumption is very small.

5. Conclusions and the Future Work

In this paper, we proposed a novel key management scheme for dynamic WSNs security. Through the certification realization as well as the dynamic key update, we can ensure the dynamic security of the entire network. Simultaneously, during the node dynamic update stage, we add the idea of the self-balanced binary search tree to ensure the dynamic security of the network while reduce the entire cluster node energy consumption. In the view of the memory load, each node in this program just needs to save some code which generates random number, so compared to the storage of a large number of key chains [4, 5], our scheme has a smaller memory. However, we have only take the dynamic WSNs in the consideration. With the development of science and technology, there have been a lot of cross application between different networks and how to ensure the security in mobile communications between different networks is the future studied work.

Acknowledgments

This work was a project supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 11KJB520011) and a Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions. It was also supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Knowledge Economy (MKE) Korea, and by the Natural Science Foundation of Jiangsu Province (No. BK2012461).

References

[1] N. Sultana, K. -m. Choi and E. -n. Huh, “Mobility Support Secure Coverage Protocol for Monitoring Applications using Wireless Sensor Network”, International conference on Computational Sciences and its Applications ICCSA, **(2008)**.

[2] W. Du, J. Deng, Y. S. Han, S. Chen and Pr. K. Varshney, “A Key Management Scheme for Wireless Sensor Network Using Deployment Knowledge”, IEEE INFOCOM, **(2004)**.

[3] A. Perrig, R. Szewczyk, J. Tygar, Victorwen and D. E. Culler, “Spins: Security Protocols for Sensor Networks”, ACM Wireless Networking, **(2002)** September.

[4] L. Eschenauer and V. D. Gligor, “A key management scheme for distributed sensor networks”, Proc. of the 9th ACM Conference on Computer and Communication Security, **(2002)** November, pp. 41-47.

[5] H. Chan, A. Perrig and D. Song, “Random key pre-distribution schemes for sensor networks”, Proc. IEEE Symp on Research security privacy, **(2003)** May 11-14, pp. 197- 213.

[6] F. Liu, M. J. Rivera and X. Cheng, “Location-Aware Key Management in wireless sensor networks”, IWCMC’06, **(2006)**.

[7] M. O. Rabin, “Digitalized signatures and public-key functions as intractable as factorization”, Technical Report MIT/LCS/TR-212, Laboratory for Computer Science, MIT, **(1979)**.

[8] J. Zhang, Y. Sun and L. Liu, “NPKPS: A novel pairwise key pre-distribution scheme for wireless sensor networks”, IET Conference on Wireless, Mobile and Sensor Networks 2007, (CCWMSN07), **(2007)** December 12-14, pp. 446-449.

[9] L. Girod, T. Stathopoulos, N. Ramanathan, *et al.*, “A System for Simulation, Emulation, and Deployment of Heterogeneous Sensor Networks”, Proc. of ACM SenSys, **(2004)**.

[10] O. Cheikhrouhou, A. Koubaa, M. Boujelben and M. Abid, "A lightweight user authentication scheme for Wireless Sensor Networks", 2010 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), **(2010)** May 16-19, pp. 1-7.

[11] H. -R. Tseng, R. -H. Jan and W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks", Global Telecommunications Conference 2007, GLOBECOM '07. IEEE, **(2007)** November 26-30, pp. 986-990.

[12] K. T. Kim, R. S. Ramakrishna, "A Level-based Key Management for both In-Network Processing and Mobility in WSNs", IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, MASS 2007, **(2007)** October 8-11, pp. 1-8**.**

[13] I. -H. Chuang, W. -T. Su, C. -Y. Wu, J. -P. Hsu and Y. -H. Kuo, "Two-Layered Dynamic Key Management in Mobile and Long-Lived Cluster-Based Wireless Sensor Networks", Wireless Communications and Networking Conference, WCNC 2007, IEEE, **(2007)** March 11-15, pp. 4145-4150.

[14] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences", **(1992)** pp. 471–486.

[15] S. U. Khan, L. Lavagno, C. Pastrone and M. Spirito, "An effective key management scheme for mobile heterogeneous sensor networks", 2011 International Conference on Information Society (i-Society), **(2011)** June 27-29, pp. 98-103.

[16] S. A. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", Networking, IEEE/ACM Trans. on, vol. 15, no. 2, **(2007)** April, pp. 346-358.

[17] D. S. Sanchez and H. Baldus, "A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks", SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, **(2005)** September 5-9, pp. 277- 288.

[18] J. Maerien, S. Michiels, C. Huygens and W. Joosen, "MASY: MAnagement of Secret keYs for federated mobile wireless sensor networks", Wireless and Mobile Computing, Networking and Communications (WiMob), **(2010)** October 11-13, pp. 121-128.

[19] S. U. Khan, C. Pastrone, L. Lavagno and M. A. Spirito, "An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks", 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS), **(2011).**

[20] D. E. Knuth, "Sorting and Searching", vol. 3 of The Art of Computer Programming, section 6.2.2, Reading, Massachusetts: Addison-Wesley, second ed., **(1997)**, pp. 430–31.

[21] Y. -Y. Zhang, W. -C. Yang, K. -B. Kim and M. -S. Park, "An AVL Tree-Based Dynamic Key Management in Hierarchical Wireless Sensor Network", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, **(2008)**.

[22] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", IEEE Transactions on Wireless Communications, vol. 1, no. 4, **(2002)**, pp. 660-670.

Authors

Dr. Sai Ji is an associate professor in Computer Sciences at Nanjing University of Information Science & Technology, China. He received his Bachelor (NUIST, China, 1999), Master (NUAA, China, 2006). His research interests are in the areas of Data Mining, Computer Measurement and Control and Wireless sensor networks. He has published more than 20 journal/conference papers. He is principle investigator of three NSF projects.

Liping Huang is currently a student of graduate school in Nanjing University of Information Science & Technology. She received her bachelor's degree in Network Engineering from Nanjing University of Information Science & Technology in 2007. Her research interest includes network security, mobile computing, machine learning and WSN.

Dr. Jin Wang received the B.S. and M.S. degree in the Electronical Engineering from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received his Ph.D. degree from the Ubiquitous Computing laboratory in the Computer Engineering Department of Kyung Hee University Korea in 2010. Now, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and technology. His research interests mainly include routing protocol and algorithm design, performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.