http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (18): 4593-4596, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.4593.4596

Improvement of Key in ZigBee Wireless Network

[1]Wenjie Li, [1,2]Qianqian Cao and [2]Zhuzi Liu
[1]Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology,
[2]Key Laboratory of Computer Vision and System, Ministry of Education,
Tianjin University of Technology, China

Abstract: Zigbee provides a connection to a variety of wireless devices and solves the problem of the communicating between different protocols. ZigBee can provide wireless communication which is low rate, low complexity, short distance and low cost. Due to the existence of various attacks in the wireless transmission, security becomes a bottleneck for Zigbee applications. In the study, we designed the model based on dynamic key which is sent in Zigbee network and analyzed its performances.

Key words: ZigBee, wireless communication, dynamic key, network security

INTRODUCTION

ZigBee based on IEEE802.15.4 which defines physical layer and data link layer. ZigBee defines the standard of network layer and application layer. The protocol architecture is shown in Fig. 1. ZigBee is a low rate, low complexity, cost and short distance wireless communication technology. There are three standard ISM bands and 2.4 GHZ one is widely used in China. ZigBee protocol stack includes application layer, network layer and security service layer.

In the encryption process ZigBee uses three basic keys which are network key, linking key and master key. The master key is used to ensure long-term safe communication between two devices and can be used as a common link key to prevent eavesdropping. In the PAN link key is shared by two mutual communication equipment, it can be established in the manufacturing,

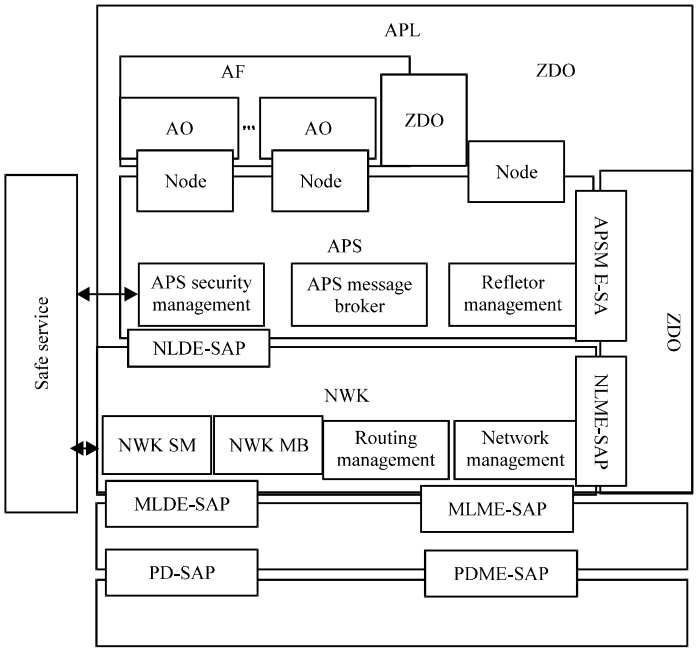

Fig. 1: ZigBee protocol framework

Corresponding Author: Wenjie Li, School of Computer and Communication Engineering, Tianjin University of Technology, Tianjin, 300384, China

installation or generated by the master key. Network key is applied to every layer above data link layer in ZigBee. Unlike the master key, network key and link key need updating periodically.

KEY MODEL

In ZigBee applications key management generally uses the mechanism of symmetric key management. Because it is easy to be implemented in a wireless surroundings which has features of low power consumption and low complexity but it can't guarantee the security of wireless communication. Now in the WSN there are two main key management technologies which are the asymmetric cryptography key management based on the station (Perrig *et al*., 2002; Anderson *et al*., 2004) and symmetric encryption one based on key pre-distribution (Eschenauer and Gligor, 2002; Chan *et al*., 2003). The front one increases the burden of communication and the last one can't effectively support to add and update new nodes. In the WSN nodes are generally used batteries so that the energy consumption must be taken into account. In the ZigBee WSN nodes normally make lower production process and low computing ability, memory and communication ability is limited, so the public key encryption and traditional asymmetric key technology don't apply.

In the study, we have considered the actual ability of network communication, memory and data processing and then proposed a dynamic session key management model based on sending information. We have analyzed the model from the security, performance and storage space. Theory of model and the network assumption are basic stone of our model.

Model theory: The ideal model of exchanging key should use different keys in each communication and destroy it after using automatically, namely one-time key, destroy after use. The model is designed here which is based on matrix operation, the key K is an integer nHn matrix. The encryption operation can be described as making a choice in the m characters library to get n characters randomly to form a vector P, the process of encryption is that converting vector P into another vector C which formed by another n characters. Encryption rules can be expressed as $C = KHP \bmod_m$, the decryption is just the opposite.

In this example, 126 letters in the ACSII table, the hash codes are the values 0 to 125 integer. If n = 3:

$$k = \begin{pmatrix} 3 & 5 & 7 \\ 2 & 9 & 6 \\ 4 & 1 & 8 \end{pmatrix} \quad (1)$$

each value of k is generated by the random function. If the plaintext is "finish", before sending it must be grouped, it's divided into "fin", "ish" and is represented respectively for (5, 8, 13), (8, 18, 7) through using the vectors, then each is calculated as follows:

$$\left| \left| \left| 8 \right| \right| \right| \bmod 126 = \begin{pmatrix} 16 \\ 4 \\ 2 \end{pmatrix} \quad (2)$$

And:

$$\begin{vmatrix} 2 & 9 & 6 \\ 4 & 1 & 8 \end{vmatrix} \begin{pmatrix} 0 \\ 18 \\ 7 \end{pmatrix} \bmod 126 = \begin{pmatrix} 7 \\ 12 \\ 2 \end{pmatrix} \quad (3)$$

And the reverse operation gets the corresponding letter "qec", "mhc", so the ciphertext is "gecmhc".

Network hypothesis: Because existing sudden data in the ZigBee WSN, there are only some simple state information usually, data flow is very small. While unexpected events occur, the data transmitted in the network increases quickly, monitoring the burst data is very difficult. Assuming the malicious nodes don't exist before the ZigBee WSN is deployed. We are inspired by the model (Akyildiz *et al*., 2002) and put forward the hypothesis system model of network as follows:

- There is no attack existing in the network when sensor nodes are deployed and before the deployment is completed in a short time; after key exchanged, the network may have various types of attackers and attacks
- In the network type of communication can be divided into adjacent and not adjacent nodes, not adjacent ones which communicate with each other need intermediate nodes to transform

Basic model theory provides the theoretical support for the model; the network hypothesis is the condition of the model. The model is designed in the study based on both.

KEY MANAGEMENT MODEL

Figure 2 is the key process of the model, firstly monitoring nodes are deployed completely in the environment without loading any initial key or boarded key. The sender uses the initial key to encrypt plaintext key, then transforms it. The receiver uses the prior initial key consulted to decrypt the ciphertext. When they get the plaintext, they update their keys, respectively. In the

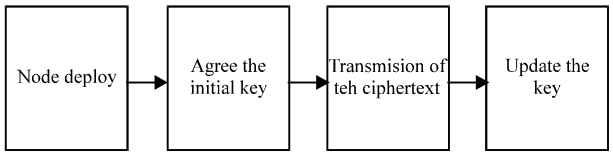

Fig. 2: Session key management

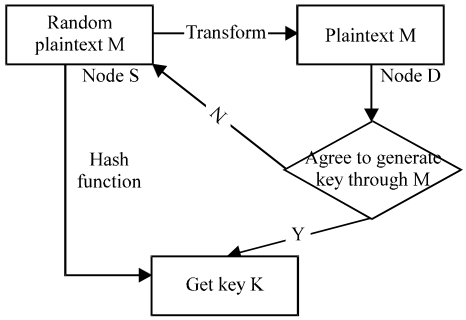

Fig. 3: Initial key generation

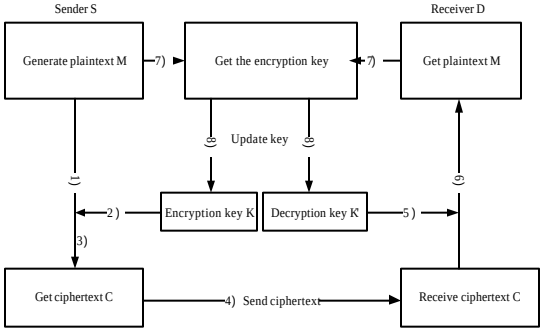

Fig.4: Session key update process

process not only the necessary information is transformed in one session but also updates the keys of the sender and receiver and the process does not add more sessions and extra communication cost (Li *et al*., 2013).

Initial key: The nodes deployed in the network must have completed the initial key agreement before communicating; the negotiation process is shown in Fig. 3.

If node S and node D are the adjacent nodes, S negotiates for the initialization key as a sponsor, D is the consultative recipient and the process is as follows:

- M which the system randomly generated message will be sent to D by S, in the process M doesn't get any treatment
- D get M from S, if D agrees to use M as the key generation element of their communication, then uses Hash function to deal with M and gets a reversible integer n×n matrix K, K is their initial key, at the same time sends the agreement to S as the feedback
- S receives the agreement, similarly uses the same hash function to get the initial key K. If node S obtained the message whose meaning is sending a new string again, then redo (1) Until two sides establish the initial key

Session key update: From the front we have gotten the initial key through consultation, here we put our attention on the updating dynamic key. In each session keys are not same, they will be destroyed on the end of every session, the sender and receiver will get a new session key after the session finished. Updating key is shown in Figure 4.

In Figure 4 when the process updating key happens between connected multiple sessions which have the same content, there are possibility to be attacked by analysis of frequency. In order to prevent that we have improved the model, adding the pre-treated, shows Fig. 5.

Figure 5 before sending the plaintext we use transform function T to express M and it was transformed as M (= T^t (-1) (M, T) together.

PERFORMANCE ANALYSIS

We mainly analyze the performances of the model in security, cost and so on and then we have proved the model to meet the performance requirements of ZigBee wireless network:

- **Security:** In the model each key can be obtained by the Hash function with unidirectional characteristics, from them people can't get plaintext and encrypted matrix from the key. The key will be updated in each session, even though there are wireless wiretapping in the network, it can ensure the security of network
- **Cost:** Generally in WSN transmitting energy consumption is far greater than the computation. In our model updating and transforming concurrence comparing to the other key updating mechanism, energy consumption of our model decreased significantly

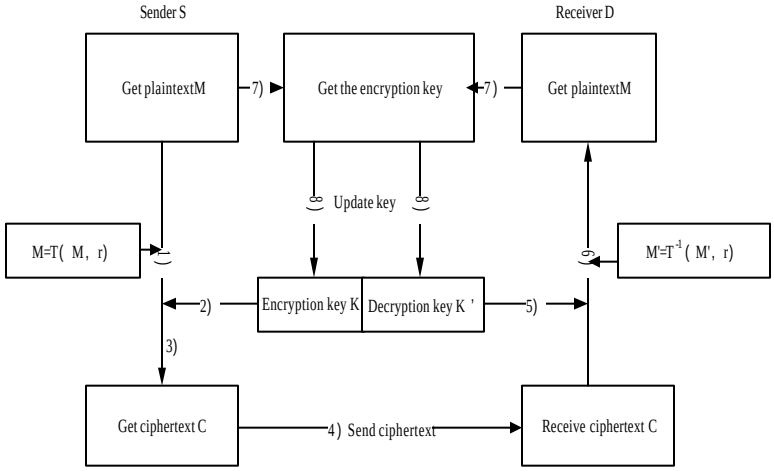

Fig. 5: Improved key management process

- **Store key:** Compared with the other two key distribution mechanism, nodes in our model can communicate directly. In addition to good connectivity, each node just stores the key which is only adjacent to them

CONCLUSION

With the development of wireless network application, ZigBee has its own advantages in wireless network, so its applications continue widely. But the security problem restricts the wider application of ZigBee. Based on the above we proposed an improvement model of managing key in the ZigBee WSN and turned out that it has some advantages compared to the others.

ACKNOWLEDGMENTS

The research was sponsored by the National Natural Science Foundation of China (Grant No. 61202169 and No. 61170173), Tianjin Natural Science Foundation (Grant No. 10JCYBJC00500), Key Project of Ministry of Education of China (Grant No. 208010) and Program for New Century Excellent Talents in University of China (Grant No. NCET-09-0895).

REFERENCES

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Anderson, R., H.W. Chan and A. Perrig, 2004. Key infection: Smart trust for smart dust. Proceedings of the 12th IEEE International Conference Network Protocols, October 5-8, 2004, Berlin, Germany, pp: 206-215.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 11-14, 2003, Berkeley, CA., pp: 197-213.

Eschenauer, L. and V. D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, November 18-22, 2002, Washington, DC, USA, pp: 41-47.

Li, W.J., S. Liu and Y. Hu, 2013. Research on XML-based exchanging system between databases. Adv. Mater. Res., 651: 789-794.

Perrig A., R. Szewczyk, J.D. Tygar, V. Wen and D.E. Culler, 2002. SPINS: Security protocols for sensor networks. Wireless Networks, 8: 521-534.