A PKC-based security architecture for WSN

Jianbo Yao[1,*], and *Chaoqiong* Yang[2]

[1]School of Mathematics and Computer, Hezhou University, Hezhou Guangxi 542899, China
[2]Audit Division, Zunyi Normal College, Zunyi Guizhou 563006, China

Keywords: WSN, Security architecture, PKC, Identity based cryptosystem.

Abstract. It is an important challenge to find out suitable cryptography for WSN due to limitations of energy, computation capability and storage resources. Considering this sensor feature on limitations of resources, a security architecture based-on public key cryptography is proposed. The security architecture is based on identity based cryptosystem, but not requires key handshaking. The analysis shows that the security architecture ensures a good level of security and is very much suitable for the resources constrained trend of wireless sensor network.

1 Introduction

WSN are used in variety of applications for collecting information from monitored environments and objects, such as battlefield reconnaissance, environmental monitoring, and traffic monitoring.

A WSN is composing of a great lot sensors. Each sensor is usually limited power, computation, storage, sensing and communication capabilities.

The major challenge of employing a public key security scheme directly in WSN is the limited resources budgets of sensors participating in the network. Among several public key schemes, Elliptic Curve Cryptography (ECC) based algorithms have proven acceptable performance for low powered sensor nodes [7, 12]. Considering both the software and hardware configurations, elliptical curve based public key cryptography (PKC) has shown relatively better result on 8 bit mote platform. However, the use of certificates in such scheme consumes a huge amount of bandwidth and power. To gain better efficiency, identity based PKC could be used which does not use certificates.

In this paper, I propose a security architecture based-on public key cryptography. The scheme can ensure a good level of security and is very much suitable for the resources constrained trend of wireless sensor network, which is built on the basis of an identity based cryptosystem in the flat network topological structure of WSN.

The remainder of this paper is organized as follows: In Section Ⅱ, related work is presented. In Section Ⅲ, WSN model. In Section Ⅳ, describes our proposed scheme. In

* Corresponding author: 2055164364@qq.com

Section Ⅴ, analyzes our scheme. In Section Ⅵ, conclusions this paper with future research directions.

2 Related work

A wireless sensor network needs a secure infrastructure to protect itself from attacks. Eschenauer and Gligor proposed a random key pre-distribution scheme: before deployment, each sensor node receives a random subset of keys from a large key pool. To agree on a key for communication, two nodes find one common key within their subsets and use that key as their shared secret key [4]. The Eschenauer-Gligor scheme is further improved by Chan, Perrig, and Song [1], by Du, Deng, Han, and Varshney [2], and by Liu and Ning [9].

Recently a number of studies have been conducted to find out a practical way to use PKC in sensor networks [3,5,6,10].Their studies focus mostly on optimization of PKC. Though computing cost is still a crucial problem for PKC system; results in [6] indicate that ECC has some advantages in memory requirement and computing cost and that it is suitable for sensor networks.

In 1984, Shamir first proposed identity based cryptosystem [11]. Identity based cryptosystem is actually public key system which does not require the pair of keys (public-private). Instead of publishing any of these keys, user can provide any identification which is unique such as his name, phone number, street number etc. as public key. The system is free from managing any third party like a certificate given authority. So this scheme could be exploited for providing support for the ultra low power sensor networks.

Our work is inspired by [8]. A security architecture was proposed by Mo. kammel Haque, Al-Sakib Khan Pathan, Choong Seon Hong, Eui-Nam Huh, which has two schemes, one is a key handshaking scheme based on simple linear operations; the other is an identity based cryptosystem which does not require any certificate authority. This is different from our security architecture. In our scheme, there is not any key handshaking because there are some sensor nodes can not directly communicate with the based station.

3 WSN and threat models

In our security architecture, the flat network topological structure of WSN is used. The WSN consist of many sensor nodes and one base station. All sensor nodes have peer structure and totally same functions and properties. Each sensor node contains same function protocol, such as MAC, routing, management and security. The base station has adequacy energy and abundance resource. The base station is also absolutely security and trustful. the sensor node has minimum of energy and resource. The flat network topological structure of WSN is illustrated in Figure 1.

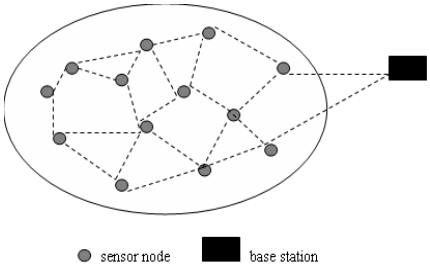

Fig. 1. Flat Network Topological Structure of WSN.

In the WSN model, a node can transmit information to base station by one hop or many hops.

4 Proposed scheme

This section describes the details of our proposed scheme.

Before deployment, base station assigns a unique identifier (ID) and corresponding key(K) to each node. The identifier (ID) is written in memory of node; the corresponding key(K) is written in memory of base station.

After deployment, the beacon message is sent through broadcast by the base station contains a level field. The base station sets the value of level to 0. When a node forwards a beacon message to neighbor nodes and lose any bigger beacon message from base station, it increases it by 1. So the value of level represents the number of hops that a node is from the base station along a particular path. A sensor node selects all neighbor nodes whose level value is 1 less than its level value as its parent nodes and more than its level value as its child nodes.

Each sensor node multicasts its unique identifier (ID) to all its child nodes and records all identifier (ID) from its parent nodes.

Once a sensor node i, which is i hops apart from base station, collects required data, the sensor node will add its identifier (ID_i) on the data, then use a parent node identifier (ID_{i-1}) to encrypt (ID_i, Data), that is$E_{ID_{i-1}}(ID_i, Data)$, then unicate this encrypted message to the sensor node with identifier (ID_{i-1}). After the sensor node with identifier (ID_{i-1}) receives the message $E_{ID_{i-1}}(ID_i, Data)$, it also use a parent node identifier (ID_{i-1}) to encrypt the message, that is $E_{ID_{i-1}}(ID_i, Data)$, then unicate this encrypted message to the sensor node with identifier (ID_{i-3}). Repeating in this way, until encrypted message reaches the base station.

After the base station receives encrypted message $E_{ID_0}(\cdots(E_{ID_{i-2}}(E_{ID_{i-1}}(ID_i, Data)))\cdots)$, it will use key K_0, key K_0 corresponding with identifierID_0, to decrypt the encrypted message, this is

$$D_{K_0}(E_{ID_0}(\cdots(E_{ID_{i-2}}(E_{ID_{i-1}}(ID_i, Data)))\cdots)) = E_{ID_1}(\cdots(E_{ID_{i-2}}(E_{ID_{i-1}}(ID_i, Data)))\cdots)$$

where after, the base station use keyK_1 corresponding with identifierID_1 to decrypt

$$E_{ID_1}(\cdots(E_{ID_{i-2}}(E_{ID_{i-1}}(ID_i, Data)))\cdots), \textit{ that is}$$
$$D_{K_1}(E_{ID_1}(\cdots(E_{ID_{i-2}}(E_{ID_{i-1}}(ID_i, Data)))\cdots)) = E_{ID_2}(\cdots(E_{ID_{i-2}}(E_{ID_{i-1}}(ID_i, Data)))\cdots)$$

Repeating in this way, until the base station get $(ID_i, Data)$. Finally, the base station not only receive $Data$, but also know the $Data$ from sensor node with identifierID_i.

5 Performance analysis

5.1 Security analysis

Our proposed the security architecture, which is based on an identity based cryptosystem, is essentially a PKC based security architecture. For security intensity about PKC being higher than about private key cryptosystem, our scheme has more security intensity than pairwise keys scheme.

Compared to the security architecture of Md. Mokammel Haque.et.al, our scheme has more security intensity than their scheme, for our security architecture not transmitting private key and all private key are written in memory of base station.

5.2 Energy analysis

For the base station being not limited on energy, computational and memory storage capacity and decryption being only executed in base station, the energy consumption of sensor nodes is only considered. Numerous energy of sensor node will be consumed on radio transmitting.

Our proposed the security architecture has not key agreement phase. For getting public key, each node only transmits its unique identifier (ID) to its child node, our scheme has lower energy consumption than pairwise keys scheme except pre-distribution global key scheme.

Compared to the security architecture of Md. Mokammel Haque.et.al, our scheme has lower energy consumption than their scheme, for our security architecture not having the key handshaking phase.

5.3 Computational overhead analysis

For pre-distribution key scheme having key agreement phase except pre-distribution global key scheme, but not having in our scheme, our scheme has lower computational overhead than pre-distribution key scheme except pre-distribution global key scheme.

Compared to the security architecture of Md. Mokammel Haque.et.al, our scheme has lower computational overhead than their scheme, for our security architecture not having the key handshaking phase.

5.4 Key storage overhead

For pre-distribution key scheme, each node must storing its a unique identifier (ID) and corresponding key(K), but only storing a unique identifier (ID) in our scheme, our scheme has less key storage overhead than pre-distribution key scheme.

Compared to the security architecture of Md. Mokammel Haque.et.al, our scheme has the same key storage overhead as of their scheme.

6 Conclusions and future work

In this paper, to the flat network topological structure of WSN I have proposed a PKC based security architecture which is based on an identity based cryptosystem. The analysis shows that the security architecture ensures a good level of security and is very much suitable for the resources constrained trend of wireless sensor network.

As future work, we will use PKC to the hierarchical network topological structure and the mixed network topological structure of WSN.

This research was supported by the Doctor Fund project of Hezhou University under grant HZUBS201809.

References

1. H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.
2. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pairwise key predistribution scheme for wireless sensor networks,” in Proceedings of the 10th ACM Conference on Computer

and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42–51

3. W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," MobiHoc'05, May 25–27, 58-67, UrbanaChampaign, Illinois, USA, 2005.
4. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, November 18-22 2002, pp. 41–47
5. G. Gaubatz, J. Kaps, and B. Sunar, "Public keys cryptography in sensor networks – revisited," in The Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS), 2004
6. N. Gura, A. Patel, A. Wander, H. Eberle, and S. C Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," in Proceedings of the Workshop on Cryptography Hardware and Embedded Systems (CHES 2004), Boston, August 11-13 2004.
7. Q. Jing., J. Hu and Z. Chen. "C4W: An Energy Efficient Public Key Cryptosystem for Large-Scale Wireless Sensor Networks", In IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Oct. 2006, pp. 827-832.
8. Mo. kammel Haque, Al-Sakib Khan Pathan, Choong Seon Hong, Eui-Nam Huh. "An asymmetric key-based security architecture for wireless sensor networks", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 2, NO. 5, OCTOBER 2008,pp. 265-279.
9. D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 52–61
10. D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, pp. 71-79, October 2004.
11. A. Shamir. "Identity-Based Cryptosystems and Signature Schemes", CRYPTO 1984, LNCS 196, Springer-Verlag, 1985, pp. 47-53.
12. A. S. Wander , N. Gura, H. Eberle, V. Gupta and S. C. Shantz. "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", In proceedings of PerCom 2005, pp. 324-328.