제27회 한국정보처리학회 춘계학술발표대회 논문집 제14권 제1호 (2007. 5)

An Efficient Public Key Based Security Architecture for Wireless Sensor Networks*

Md. Mokammel Haque, Al-Sakib Khan Pathan, and Choong Seon Hong
Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Yongin, Gyeonggi 449701, Korea
{malinhaque, spathan}@networking.khu.ac.kr and cshong@khu.ac.kr

ABSTRACT

In this paper, we propose a public key based security architecture for Wireless Sensor Networks (WSNs). The basic architecture comprises of two schemes; a key handshaking scheme based on simple linear operations for fast computation and an identity based cryptosystem which does not require any certificate authority. Our analysis shows that, the combined scheme ensures a good level of security and is very much suitable for the energy constrained trend of wireless sensor network.

1. INTRODUCTION

The major challenge of employing a public key security scheme directly in wireless sensor networks is the limited energy, computation and memory 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 [1], [2]. 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, we propose such an identity based scheme which is assisted by a bilateral key handshaking phase, on the way to implement a complete public key based security architecture for WSN. Our target is to get a good level of security with efficient use of the available resources of the sensors in the network.

The rest of the paper is organized as follows: Section 2 states the related works, Section 3 mentions the preliminaries, Section 4 contains the description of our proposed scheme, Section 5 presents the analysis and finally Section 6 concludes the paper with future research directions.

2. RELATED WORKS

In [1], the authors analyzed the energy efficiency of two prime PKC algorithms, RSA and ECC for low power WSNs. They also presented an abbreviated certificate based scheme which is actually a simplified version of SSL handshake. Jing et al. [2] proposed a fully certificate less scheme called C4W and made comparison with the scheme proposed in [1]. In [3], another certificate less identity based scheme is proposed but it is not efficient considering the energy usage and thus not feasible for WSN. None of these works provides an overall security architecture based on PKC that is suitable for sensor networks. Our work is novel in the sense that, we design a complete public key security architecture which consists of a key handshaking phase based on simple matrix operation and an encryption/decryption phase based on certificate less public key scheme.

3. PRELIMINARIES

3.1. Pseudoinverse Matrix

The pseudoinverse matrix or generalised inverse matrix [4], [5] has a very nice property that could be used for cryptographic operations. For a general matrix of dimension $m \times n$, there exists more than one pseudoinverse matrix. If X be a binary $m \times n$ matrix and Y be a binary $n \times m$ matrix, then Y is a pseudoinverse matrix of X only when, $\mathrm{YXY} = \mathrm{Y}$ and $\mathrm{XYX} = \mathrm{X}$. Accordingly X is also pseudoinverse matrix of Y.

3.2. Identity Based Cryptosystem

Identity based Cryptosystem was first propose by Shamir in [6]. 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 certficate given authority. So this scheme could be exploited for providing support for the ultra low power sensor networks.

4. OUR PROPOSED SCHEME

In this section, we propose our scheme with two phases; key handshaking phase between a sensor node and the base station, and the encryption/decryption phase.

4.1. Key Handshaking Phase

Let a node in the network is denoted as *A* and the base

* This paper was supported by ITRC and MIC

station is *B*. To get a shared key on demand, *A* and *B* perform the following operations:

1. Node *A* generates a matrix X of dimension $m \times n$ and its pseudoinverse matrix X′.
2. Keeping X and X′ secret, *A* sends X′X to *B*.
3. *B* generates another matrix Y of order $n \times k$ and its pseudoinverse matrix Y′ randomly.
4. Keeping Y and Y′ secret, *B* sends the matrices X′XY and X′XYY′ to *A*.
5. Upon receiving this, *A* calculates XX′XYY′= XYY′ and sends it to *B*.
6. Then both *A* and *B* are able to compute the common secret key XY from XX′XY=XY and XYY′Y=XY respectively.

Throughout the rest of the paper, we use the term $\mathrm{E_k}$ instead of the key XY, as it is used for data encryption.

4.2. Encryption/Decryption Phase

This phase is adopted from the identity based public key encryption technique. Identity based encryption does not require generating certificates from certificate authority. The main component of this phase is a central key generator (CKG) located at the base station which generates private key for nodes and a master secret key which could be used to transmit the private keys to the nodes. Now, if a node *A* wants to send a message to another node *A*′, *A* encrypts the message with $\mathrm{E_k}$. Receiving the encrypted message, *A*′ places its identity to the CKG. In turn, CKG generates the private key on demand and transmits it to *A*′ encrypting it with the master key. Now, *A*′ can decrypt the message from node *A*. The network address of the sensor node can be chosen as the ID, which is both unique and public.

5. ANALYSIS OF OUR SCHEME

The advantage of our PK security architecture is two folds. It depends on the superiority of the two basic schemes stated earlier. We have used an identity based cryptosystem which is certificateless in nature. Our identity based encryption has several benefits. As we calculate keys instead of generating those randomly, no pre-assigning of nodes is required. No need for keeping a look up table in the base station. Again, this scheme gives us a key recovery capability as we can recalculate any key at later times. The calculation of public key is extremely beneficial for communications with unknown parties in the network (for example, a node in a different group in the network or a node that joined the network newly). As soon as the unknown party is authenticated by the CKG and gets the message containing the private key provided by CKG, a secure channel is established and it could participate in the secure communications within the network.

In the key handshaking phase, we have used linear matrix operations, more specifically matrix multiplication. The complexity of matrix multiplication is very low, and hence it can be performed very quickly. In our scheme, X sends Y an $n \times n$ matrix of n^2 bits. In turn, Y sends X an $n \times k$ matrix and an $n \times n$ matrix which requires $n(n+k)$ bits. Again X sends Y an $m \times n$ matrix in next step. So total transmitted data for this handshaking process is,

$$n^2 + n(n+k) + nm$$
$$= n(m+k+2n) \text{ bits}$$

All the calculations are linear and can be performed very easily.

For wireless sensor networks, it is very advantageous as it requires low computational cost and memory usage. Again, the identity based scheme does not require maintaining and managing a central certificate authority; hence, there is no additional data transmission required for this purpose. It reduces the extra communication overhead in WSN.

The most prominent feature of our public key architecture is the use of a shared key as the encryption key. Shared secret key could be used for security enhancement and at the same time could be used to communicate with the CKG privately. Besides these, this combined architecture can be used on demand basis to provide greater adaptability to the various sensor network contexts. That means, if too much packet transmission is a problem for key handshaking scheme from power aware point of view, then only the second phase could be used in the architecture as this scheme itself is a complete identity based public key cryptosystem. So, our scheme could be well-suited for low power wireless sensor networks.

6. CONCLUSIONS AND FUTURE WORKS

In this paper, we have proposed an efficient resource-aware public key based security architecture for wireless sensor networks. Our combined scheme shows good level of security and requires less resource for implementation. As our future works, we would like to perform a detailed analysis of the efficiency of our proposed architecture for wireless sensor networks.

REFERENCES

[1] Wander, A.S., Gura, N., Eberle, H., Gupta, V., and Shantz, S.C., “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, In proceedings of PerCom 2005, pp. 324-328.

[2] Jing, Q., Hu, J., and Chen, Z., “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.

[3] Libert, B. and Quisquater, J.-J., “On Constructing Certificateless Cryptosystems from Identity based Encryption”, PKC 2006, LNCS 3958, International Association for Cryptologic Research, 2006, pp. 474-490.

[4] Israel, Greville, “Generalized inverses: theory and applications”, John Willey & Sons, New York, 1974

[5] Boullion, Odell, “Generalized inverse matrices”, Wiley-Interscience, New York, 1971.

[6] Shamir. A., “Identity-Based Cryptosystems and Signature Schemes”, CRYPTO 1984, LNCS 196, Springer-Verlag, 1985, pp. 47-53.