TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 10, October 2014, pp. 7459 ~ 7462
DOI: 10.11591/telkomnika.v12i8.5579

On the Security of a Dynamic and Secure Key Management Model for Hierarchical Heterogeneous Sensor Networks

Pengshuai Qiao
North China University of Water Conservancy & Electric Power, Zhengzhou, China
email: pengshuaiqiao@163.com

Abstract

With the development of the wireless communication technology and the sensor technology, the wireless sensor network (WSN) has been used in many applications. However, WSNs suffer from some inherent weaknesses because of restricted communication and hardware capabilities. To achieve essentially secure communication in WSNs, a few of key management models have been proposed since it is the crucial important building block for all security goals in WSNs. Recently, Alagheband and Aref proposed a signcryption scheme and used it to construct a dynamic key management model for hierarchical heterogeneous sensor networks. They also proved that their signcryption scheme is provably secure if the elliptic curve discrete logarithm problem is infeasible. Unfortunately, by giving concrete attacks, we indicate that Alagheband and Aref's signcryption scheme is not secure in their secure model. The analysis also shows that their key management model is not secure. To solve those weaknesses, we also proposed an improved signcryption scheme.

Keywords: *key management, signcryption scheme, elliptic curve cryptography*

1. Introduction

With the rapid advancement the wireless technology and the sensor technology, the wireless sensor network (WSN) has been pervasively deployed in many applications. A wireless sensor network consists of many resource constrained sensor nodes which are capable of accomplishing various functions such as sensing, processing, transmitting and receiving to meet the application objectives. Generally speaking, sensors nodes are deployed in a hostile environment. Then they may be eavesdropped, captured and compromised by the adversary. Therefore, secure protocols are required to ensure confidentiality, integrity and availability of information transmitted in WSNs.

Among different secure protocols, the key management protocol is the first crucial function to get secure communication in WSNs since the both of the sensor nodes and the cluster leaders need valid common keys to use other secure protocols. Then a few of key management protocols for WSNs have been proposed to ensure secure communication in WSNs. According to they type of the encryption techniques, the key management protocols could be divided into three categories, i.e. symmetric key management protocol, asymmetric key management protocol and hybrid key management protocol [1]. In the first type of those protocols, some keys are pre-loaded in the sensors before the deployment phase. However, such protocols suffer from some problems such as probabilistic key distribution between the sensor nodes [2, 3], non-scalability after deployment [4-7], mounting weakness against node compromise, lack of mobility and a high-communication overhead [8]. In the second types of those protocols, public key cryptography, such as elliptical curve cryptography (ECC) [9] and identity-based cryptography (IBC) [10], is used to generate keys through on-line manner. Such protocols are more flexible but very heavyweight in sensor networks. The third type of protocols could inherent advantage of other two types of protocols. The it is very suitable hierarchical heterogeneous WSNs with different kinds of nodes.

Recently, Alagheband and Aref proposed [11] a signcryption scheme with forward security characteristic and used it to construct a hybrid key management infrastructure for hierarchical heterogeneous WSNs. They claimed that their scheme is provably secure if the

Received January 5, 2014; Revised July 17, 2014; Accepted August 10, 2014

elliptic curve discrete logarithm problem is infeasible. However, in this paper, by giving a concrete attack, we indicate that Alagheband and Aref's signcryption scheme is not secure in their secure model, i.e. an adversary could forge a legal ciphertext of any message. We also indicate that their scheme suffers from the private key compromised problem, i.e. the receiver could get the sender's private key from the ciphertext. The analysis also shows that their key management model is not secure.

The rest of this paper is organized as follows: Section 2 describes Alagheband and Aref's signcryption scheme. In Section 3, we give security analysis of their scheme. In Section, we propose a countermeasure to overcome weakness in their scheme. Finally, the conclusions are presented.

2. Review of Alagheband and Aref's scheme

In this section, we give the review of Alagheband and Aref's signcryption scheme using ECC. Some notations used in this paper are defined as follows.

a) q : a large strong prime number, where $q > 2^{160}$.

b) n : a large strong prime number, where $n > 2^{160}$.

c) a, b : two integer numbers which are smaller than q and satisfy $4a^3 + 27b^2 (\bmod q) \neq 0$.

d) E : elliptic curve defined by the equation $y^2 = x^3 + ax + b (\bmod q)$.

e) G : base point of the elliptic curve E with order q.

f) BS : base station.

g) p_{bs} : BS's private key.

h) U_{bs} : BS's public key, where $U_{bs} = p_{bs} \times G$.

i) CL_i : the i th cluster leader.

j) p_{cl_i} : CL_i's private key.

k) U_{cl_i} : CL_i's public key, where $U_{bs} = p_{bs} \times G$.

l) $E_k() / D_k()$: lightweight symmetric encryption/decryption algorithm with key k.

m) H : a lightweight and secure one-way hash function

Alagheband and Aref's signcryption scheme is the most important block of there key management framework. The detail of the *Signcryption* and *Unsigncryption* of the scheme is described as follows.

Signcryption: BS could generate a ciphertext through the following steps.

1) BS generates a random number r_i and computes $R = r_i \times G = (r_1, r_2)$ and $K = r_i \times U_{cl_i} = (k, l)$.

2) BS computes $C = E_k(m)$, $h = H(C \| r_1)$, $E = H(h \| r_1) \times G$, $s' = p_{bs} - H(h \| r_1) (\bmod q)$ and $s = s' + h$.

3) BS outputs $\sigma = (C, R, s, E)$ as the ciphertext of the message m.

Unsigncryption: CL_i runs the algorithm to decrypt the ciphertext.

1) CL_i computes $K = p_{cl_i} \times R = (k, l)$, $m = D_k(C)$, $h = H(C \| r_1)$, and $s' = s - h$.

2) CL_i checks whether $s' \times G + E$ and U_{bs} are equal. If they are not equal, CL_i rejects the ciphertext; otherwise, CL_i accepts the ciphertext and outputs the message m.

3. Analysis of Alagheband and Aref's Scheme

3.1. Attack Against Existential Unforgeability

As a signcryption scheme, Alagheband and Aref's scheme should provide the confidentiality and the unforgeability. Confidentiality means that any adversary without the private key of the receiver (CL_i) cannot decrypt of the message m. Unforgeability means that any adversary without the private key of the sender (BS) cannot generate a legal ciphertext.

Alagheband and Aref claimed that their scheme is secure if the elliptic curve discrete logarithm problem is infeasible. In this section, we will show an adversary without BS's private key could forge a legal ciphertext $\sigma=(C,R,s,E)$, i.e. σ could pass CL_i's verification. The attack is described as follows.

1) The adversary generates a random number r_i and computes $R=r_i\times G=(r_1,r_2)$ and $K=r_i\times U_{cl_i}=(k,l)$.

2) The adversary generates a random number s', computes $C=E_k(m)$, $h=H(C\,||\,r_1)$, $s=s'+h$ and $E=U_{bs}-(s'-h)\times G$.

3) The adversary outputs $\sigma=(C,R,s,E)$ as the ciphertext of the message m.

Since $R=r_i\times G=(r_1,r_2)$, $K=r_i\times U_{cl_i}=(k,l)$, $C=E_k(m)$, $h=H(C\,||\,r_1)$, $s=s'+h$ and $E=U_{bs}-(s'-h)\times G$, then we have $s'=s-h$ and:

$$\begin{aligned}&s'\times G+E\\&=(s-h)\times G+(U_{bs}-(s'-h)\times G)\\&=U_{bs}\end{aligned}\qquad(1)$$

From the above description, we know that the adversary could forge a legal ciphertext without BS's private key p_{BS}. Therefore, Alagheband and Aref's scheme cannot provide unforgeability.

3.2. Attack Against the Sender's Private Key

In this subsection, we will indicate that Alagheband and Aref's scheme suffers from the private key compromised problem, i.e. the receiver (CL_i) could get the private key of the sender (BS) from a ciphertext. This is a very dangerous vulnerability since a receiver could impersonate the sender to other receivers once he gets the private key. Suppose CL_i is a malicious cluster leader and receives a ciphertext $\sigma=(C,R,s,E)$ from BS, where $R=r_i\times G=(r_1,r_2)$ and $K=r_i\times U_{cl_i}=(k,l)$, $C=E_k(m)$, $h=H(C\,||\,r_1)$, $E=H(h\,||\,r_1)\times G$, $s'=p_{bs}-H(h\,||\,r_1)(\bmod q)$ and $s=s'+h$. He could get BS's private key through the following steps.

1) CL_i computes $K=p_{cl_i}\times R=(k,l)$, $m=D_k(C)$, $h=H(C\,||\,r_1)$, and $s'=s-h$.

2) CL_i computes $p_{bs}=s'+H(h\,||\,r_1)(\bmod q)$.

From the description, we know that the malicious cluster leader CL_i could get BS's private key when he gets a ciphertext. From then on, he could impersonate BS to other cluster leader. Therefore, Alagheband and Aref's scheme suffers from the private key compromised problem.

4. Countermeasure

To withstand the above weaknesses, we propose an improved scheme based on Alagheband and Aref's scheme with lightweight modification.

$Signcryption$: BS could generate a ciphertext through the following steps.

1) BS generates a random number r_i and computes $R=r_i\times G=(r_1,r_2)$ and $K=r_i\times U_{cl_i}=(k,l)$.

2) BS computes $C=E_k(m)$, $h=H(C\,||\,r_1)$, and $s=p_{bs}-H(h\,||\,r_1)r_i(\bmod q)$.

3) BS outputs $\sigma=(C,R,s)$ as the ciphertext of the message m.

$Unsigncryption$: CL_i runs the algorithm to decrypt the ciphertext.

1) CL_i computes $K=p_{cl_i}\times R=(k,l)$, $m=D_k(C)$ and $h=H(C\,||\,r_1)$.

2) CL_i checks whether $s \times G + H(h \| r_1)R$ and U_{bs} are equal. If they are not equal, CL_i rejects the ciphertext; otherwise, CL_i accepts the ciphertext and outputs the message m.

In the improved scheme, Schnorr's signature scheme [12] is used to generate the signature of the message C. Schnorr has demonstrated that his scheme is provably in the random oracle. Therefore, the proposed scheme could provide unforgeability.

In order to get BS's private key from the ciphertext $\sigma = (C, R, s)$, CL_i has to compute r_i from $R = r_i \times G$, where $R = r_i \times G = (r_1, r_2)$, $K = r_i \times U_{cl_i} = (k, l)$, $C = E_k(m)$, $h = H(C \| r_1)$ and $s = p_{bs} - H(h \| r_1) r_i (\bmod q)$. Then he will face the elliptic curve discrete logarithm problem. Therefore, the proposed scheme could solve the private key compromised problem in Alagheband and Aref's scheme.

5. Conclusion

In this paper, we indicated that Alagheband and Aref's signcryption scheme [11] is not secure against the existential unforgeability. We also indicate that their scheme suffers from the key compromised problem. The signcryption scheme is the most important block of their dynamic key management model for hierarchical heterogeneous sensor networks. Therefore, their key management model is also not secure for practical applications.

References

[1] Zhang J, Varadharajan V. Wireless sensor network key management survey and taxonomy. *J. Netw. Comput. Appl*., 2010; 33: 63–75.

[2] Eschenauer L, Gligor VD. *A key management scheme for distributed sensor networks.* Ninth ACM Conf. on Computer and Communication Security. 2002: 41–47.

[3] Chan H, Perrig, A. *Random key predistribution schemes for sensor networks*. IEEE Symp. Security and Privacy, 2003; 197–213.

[4] Liu D, Ning P. *Establishing pairwise keys in distributed sensor networks*. 10th ACM Conf. on Computer and Communications Security (CCS03), ACM Press, Washington, DC, 2003; 41–7.

[5] Blundo C, Santix, AD, Herzberg A, Kutten S, VaccaroU, Yung M. *Perfectly secure key distribution for dynamic conferences*. 12th Annual Int. Cryptology Conf. on Advances in Cryptology, Springer. 1992; 471–486.

[6] Camtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. J. *ACM/IEEE Trans. Netw., Springer.* 2007; 15(2): 346–358.

[7] Yu Z, Guan Y. *A robust group-based key management scheme for wireless sensor networks*. IEEE Wireless Communications and Networking Conf. (WCNC), New Orleans, LA, USA, 2005; 137.

[8] Perrig A, Szewczyk R, Wen V, Cullar D, Tygar JD. *SPINS: Security protocols for sensor networks.* Seventh Annual ACM/IEEE Int. Conf. Mobile Computing and Networking. 2001; 189–99.

[9] Koblitz N. Elliptic curve cryptosystems. *Math. Comput.,* 1987; 48: 203–209.

[10] Boneh D, Franklin, M. *Identity-based encryption from the Weil pairing, advances in cryptology-CRYPTO.* Lect. Notes Comput. Sci., 2001; 2139: 213–229.

[11] Alagheband MR, Aref MR. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. *Information Security, IET,* 2012; 6(4): 271-280.

[12] Schnorr CP. Efficient identification and signatures for smart cards, in G. Brassard, ed. Advances in Cryptology-Crypto '89, *Springer-Verlag*. Lecture Notes in Computer Science, nr 435. 1990; 239-252.