IEICE TRANS. INF. & SYST., VOL.E93–D, NO.3 MARCH 2010

PAPER Special Section on Trust, Security and Privacy for Pervasive Applications

Secure Message Distribution Scheme with Configurable Privacy in Heterogeneous Wireless Sensor Networks

YaHui LI[†a)], JianFeng MA[††], *Nonmembers*, *and* SangJae MOON[†††b)], *Member*

SUMMARY Security and privacy of wireless sensor networks are key research issues recently. Most existing researches regarding wireless sensor networks security consider homogenous sensor networks. To achieve better security and performance, we adopt a heterogeneous wireless sensor network (HWSN) model that consists of physically different types of sensor nodes. This paper presents a secure message distribution scheme with configurable privacy for HWSNs, which takes advantage of powerful high-end sensor nodes. The scheme establishes a message distribution topology in an efficient and secure manner. The sensor node only need generate one signature for all the messages for all the users, which can greatly save the communication and computation cost of the sensor node. On the other hand, the user can only know the messages that let him know based on a pre-set policy, which can meet the requirement of the privacy. We show that the scheme has small bandwidth requirements and it is resilient against the node compromise attack.

key words: *configurable privacy authenticated encryption, message distribution, wireless sensor networks*

1. Introduction

Wireless sensor networks (WSNs) have been studied extensively in the past decade because they provide one of the missing connections between the Internet and the physical world. There are many different applications for WSNs, the sensor nodes can be deployed in controlled environment such as factories, homes, or hospitals; they can also be deployed in uncontrolled environment such as disaster or hostile area, in particular battlefield, where monitoring is crucial [1], [2]. As the most common communication paradigm, the network users are expected to issue the queries to the network in order to obtain the information of their interest. There could be a large number of users in the WSNs, which might be either mobile or static; and the users may use their mobile clients to query or command the sensor nodes from anywhere in the WSN. Most existing studies assume that the sensor nodes are homogeneous with the same capabilities for each sensor node. In hierarchical WSNs, except the base stations (or cluster supervisors), the rest of the wireless sensor nodes are homogeneous with the same capabilities within each cluster. Recently, heterogeneous WSNs (HWSNs) are getting more and more attention. To provide secure communications for the WSNs, all the messages should be encrypted and authenticated. Consequently, it is important to design strong and efficient secure mechanisms for WSNs. Clearly, using a single shared key in the whole WSN is not a good idea because an adversary can easily obtain the key. Therefore, as a fundamental security service, pairwise key establishment shall be used, which can enable the sensor nodes to communicate securely with each other using cryptographic techniques.

At the time when SNEP [3] was proposed, sensor nodes were assumed to be extremely resource constrained, especially with respect to computation capability, bandwidth availability, and energy supply. Therefore, public key cryptography (PKC) was thought to be forbiddingly computationally expensive, although it could provide much simplified solutions with much stronger security strengths. However, recent studies [4], [5] showed that, contrary to widely held beliefs, PKC with software implementations only is very viable on sensor nodes. With the advance of fast growing technology, PKC is no longer impractical for WSNs [6], although still expensive for the current generation of sensor nodes. And its wide acceptance is expected in the near future.

Most exiting secure protocols regard broadcast or peer-to-peer mode of messages transmission in WSNs. To achieve the distribution of important messages from sensor nodes to different users in a secure mode, we need consider the limited channel among sensor nodes and privacy prevision among different users. So the message send by a sensor node should be adopted the authenticated encryption scheme and configurable secure policies, which can be verified by the user and keep the secret from others.

Contributions: In this paper, we will give a secure message distribution with configurable privacy (SMDCP) scheme based on the authenticated encryption scheme [7] for heterogeneous wireless sensor networks. Suppose that a sensor node wants to send different messages to different users, the sensor node also wants to encrypt a part of messages and sign on all messages. If he utilizes authenticated encryption scheme with every user, he has to generate a signature for every message to every user. In our scheme, the sensor node only needs to generate one signature that can be utilized to protect all of the messages. It can not only re-

Manuscript received July 2, 2009.
Manuscript revised October 7, 2009.

[†]The author is with the School of Computer Science, Xidian University, Xi'an 710071, China.
[††]The author is with the Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an 710071, China.
[†††]The author is with the Mobile Network Security Technology Research Center Kyungpook National University Sankyuk-dong Buk-ku, Daegu 702–701, Korea.
a) E-mail: ml_0902@163.com
b) E-mail: sjmoon@ee.knu.ac.kr

DOI: 10.1587/transinf.E93.D.484

duce the computational burden of the sensor node, but also save the bandwidth of the channel from the sensor node. It is more appreciable for wireless sensor networks since the sensor node as sender is a power-restricted device and the channel from the sender is limited.

Organization of the paper: The remaining part of this paper is as follows: In Sect. 2, we introduce the cryptographic mechanisms that are to be used. Section 3 presents our system assumption, the adversary model, and security objectives. In Sect. 4, we introduce our scheme. Section 5 analyzes the security and efficiency of the proposed scheme, and we conclude our paper in Sect. 6.

2. Preliminary

2.1 Authenticated Encryption Scheme

Authenticated Encryption Scheme (AES) [7] is a term used to describe encryption systems which simultaneously protect confidentiality and authenticity (integrity) of communications. These goals have long been studied, but they have only recently enjoyed a high level of interest from cryptographers due to the complexity of implementing systems for privacy and authentication separately in a single application.

In addition to protecting message integrity and confidentiality, authenticated encryption can provide plaintext awareness and security against chosen ciphertext attack. In these attacks, an adversary attempts to gain an advantage against a cryptosystem (e.g., information about the secret decryption key) by submitting carefully chosen ciphertexts to some "decryption oracle" and analyzing the decrypted results. Authenticated encryption schemes can recognize improperly-constructed ciphertexts and refuse to decrypt them. This in turn prevents the attacker from requesting the decryption of any ciphertext unless he generated it correctly using the encryption algorithm, which would imply that he already knows the plaintext. Implemented correctly, this removes the usefulness of the decryption oracle, by preventing an attacker from gaining useful information that he does not already possess.

Many specialized authenticated encryption modes have been developed for use with symmetric block ciphers. However, authenticated encryption can be generically constructed by combining an encryption scheme and a Message Authentication Code (MAC), provided that the encryption scheme is semantically secure under chosen plaintext attack and the MAC function is unforgeable under chosen message attack.

Authenticated Encryption Scheme also can be constructed by combing signature and encryption which are the most important and widely used cryptographic tools. It was firstly presented in [8]. Improvements were then made in [9] and [10]. Most importantly, disputation arbitration is realized in [12]. However, the secret message must be released in the course of disputation arbitration in [11]. This problem was declared to be solved in [12]. Unfortunately, there exists a mathematical error in [12]. For more information about authenticated encryption scheme, please see the survey [7].

2.2 Identity-Based Cryptography

Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID.

As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt (or sign) messages without authorization. Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow. A number of variant systems have been proposed which remove the escrow including certificate-based encryption, secure key issuing cryptography and certificateless cryptography.

Let p, q be two large primes and E/Z_p indicate an elliptic curve $y^2 = x^3 + ax + b$ over $Z_p = \{i | 0 \le i \le p-1\}$. We denote by G_1 a q-order subgroup of the additive group of points on E/Z_p, and by G_2 a q-order subgroup of multiplicative group of the finite field $F^*_{p^2}$. The discrete logarithm Problem (DLP) is required to be hard both in G_1 and G_2. A pairing is a map $\hat{e} : G_1 \times G_1 \to G_2$ with the following properties:

(1) Bilinear: for all $P, Q \in G_1$ and all $c, d \in Z^*_q$, $\hat{e}(cP, dQ) = \hat{e}(cP, Q)^d = \hat{e}(P, dQ)^c = \hat{e}(P, Q)^{cd}$ etc.
(2) Non-degenerate: If P is a generator of G_1, then $\hat{e}(P, P)$ is a generator of G_2.
(3) Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G_1$.

Note that $\hat{e}$ is also symmetric, i.e., $\hat{e}(P, Q) = \hat{e}(Q, P)$ for all $P, Q \in G_1$, which follows immediately from the bilinearity of $\hat{e}$ and the fact that G_1 is a cyclic group. Modified Weil [18] and Tate [19] pairings are examples of such bilinear maps for which he Bilinear Diffie-Hellman Problem (BDHP) is believed to be hard. We refer to [13], [14] for a more comprehensive description of efficiency and security.

3. System Assumption

3.1 System Model

In this paper, we consider a very large and spatially-distributed heterogeneous WSN, consisting of a fixed sink and a large amount of sensor nodes. The sensor nodes are not necessarily homogenous in their functionalities and capabilities.

The WSN under consideration is aimed to offer information services to a large number of network users that access the fixed sink in the network. These WSN users may be mobile sinks, vehicles, and people with mobile clients and others. They are assumed to be more powerful than sensor nodes in terms of computation and communication abilities. For example, the network users could be a number of doctors, nurses, medical equipments (acting as actuators) and so on, in the case of CodeBlue [15], where the WSN is used for emergency medical response. These network users directly communicate with sink or the backend server and expect the replies that reflect the latest sensing results. However, they may be not allowed to know the information for the other users (For example, some information to the doctor may keep secret to nurses.) It is reasonable to assume that the sink is always trustworthy but the sensor nodes are subject to compromise. At the same time, the users of the WSN may be dynamically revoked due to either membership changing or compromise, and the revocation pattern is not restricted.

3.2 Adversary Model

We assume that the adversary's goal is to inject bogus messages into the network, deceive sensor nodes, and obtain the information of his interest.

Additionally, Deny of Service (DoS) attacks [16] such as bogus message flooding, aiming at exhausting constrained network resources, is another important focus of the paper. The adversary is assumed to be able to compromise both network users and sensor nodes. Hence he could exploit the compromised users/nodes for such attacks. More specifically, we consider the following types of attacks: 1) The adversary may use one or more compromised nodes to propagate bogus messages to the WSN by pretending that the messages are initiated by legitimate network users; 2) The adversary may reveal messages by the eavesdropping of the radio channel in the HWSN; 3) The adversary may impersonate a legal sensor to repudiate messages send by itself before; 4) The adversary may use one or more compromised users to obtain the privacy information of the other users. However, we do assume that adversary cannot compromise an unlimited number of sensor nodes. Neither can they break any cryptographic primitive on which we base our design. Otherwise, it is unlikely for any feasible security solution to be designed.

3.3 Security Objectives

Given the adversary model above, our security objective is straightforward. 1) The unforgeability of messages is needed so that illegal users will be excluded from injecting bogus messages; 2) The confidentiality of messages has to be implemented so that sensor nodes could preserve user data secret; 3) The non-repudiation of any message send by a sensor node should be able to be verified by every receiving user and the Trusted Third Part (TTP) [17]; 4) The privacy of one user data should be kept so that the other users cannot obtain them. In summary, all messages send to HWSNs should be authenticated and encrypted so that any bogus ones issued by the compromised sensor nodes can be efficiently and deterministically rejected/filtered.

4. The Proposed Scheme

There is an SDC (Secure Delivering Centre) in our scheme, which can be a trusty fixed sink node with high capability of computation, memory storage and energy. The sensor node uses SMDCP with SDC. Then, SDC decrypts the secret messages and verifies the signature. After this, based on a pre-set policy, SDC sends different messages to different users with all these messages the same signature. Especially, the users can only know that let him know. At the same time, every user can verify the signature. It is more appreciable if the sensor node has a restricted power or the channel CH is very limited and the network among the SDC and the users is an inner network, which is easy to build secure channels. Moreover, we assume that there are respective secure channels between the SDC and each user. It can be referred to Fig. 1.

4.1 Setup Process

In our scheme, the trust domain includes users, sensor nodes and SDC. SDC is the sink node for sensor nodes and is a trusted third party for users and nodes, which is the certificate authority organization for the temporary identities certificate issuance. Before sensor nodes and users run the protocol, a setup process of trust domain must be initialized as the following.

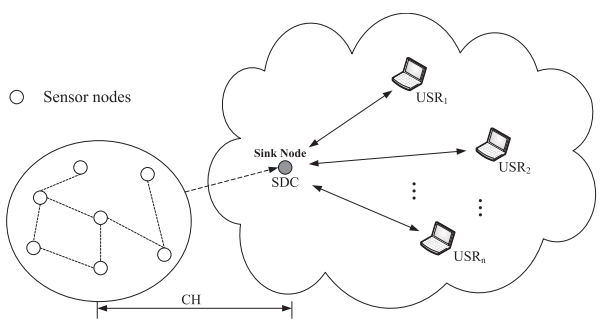

Fig. 1 SMDCP in HWSNs.

1) Setup

(1) Select the bilinear pairing parameters $(q, G_1, G_2, \hat{e})$.
(2) Randomly select a generator of group $g \in G_1$.
(3) Select two cryptographic hash functions $H_1^{'} : \{0,1\}^* \rightarrow Z_q^*$, $H_2^{'} : \{0,1\}^* \rightarrow G_2$.
(4) Randomly select a $k \in Z_q^*$ as the private key for the trust domain, and calculate $X = g^k$.
(5) $((q, G_1, G_2, \hat{e}, H_1^{'}, H_2^{'}), X)$ are the public secure parameters of the trust domain.
(6) The n users $USR_1, USR_2, \ldots, USR_n$ have the secure channels with the SDC in the inner network.
(7) The sending messages are partitioned into a plaintext M_p and a secret part M_s with the length of l, where M_s is composed of the secrets $M_{s1}, M_{s2}, \ldots, M_{sn}$, where $M_{si}(1 \leq i \leq n)$ is the secret message for the ith user USR_i. (In order to detach M_s correctly, an end index may be padded to the end of every $M_{si}(1 \leq i \leq n)$.)
(8) The delivery policy of every user USR_i, which is a subset of $\{1, 2, \ldots, n\}$ denoted by $\Lambda_i = \{i_1, i_2, \ldots, i_t\}$. It means that the messages $\{M_{si_1}, M_{si_2}, \ldots, M_{si_t}\}$ are plain to him but the others are kept secret to him.
(9) General hash function H. The symbol $H_x(X)$ denotes an x bits derivation of X by H.
(10) Let notation $\|$ denote bit strings concatenation, let notation $\oplus$ denote XOR operation.

2) Identity certificate generation

The SDC generates the temporary identity certificate as the following steps.

(1) Selects a random number $R_i \in Z_q^*$ for the user U_i.
(2) Calculates the temporary public identity $UP_i = R_i H_1^{'}(U_i)$.
(3) Calculates the temporary private identity $US_i = g^{1/(kR_iH_1^{'}(U_i))}$.

3) Encryption and signature by users

(1) The user U_i randomly selects a number $r \in Z_q^*$.
(2) The user U_i calculates the encryption of the message $c = M_s \oplus H_l(US_i^r)$.
(3) The user U_i calculates the signature of the messages $w = H_2^{'}(H(Ms_1) \oplus \ldots \oplus H(Ms_n) \oplus X^r)$ and $s = w\hat{e}(US_i, X)^r$.

4) Decryption and verification by SDC

(1) SDC receives the message $m =< c, UP_i, X^r, s >$.
(2) SDC calculates $v = (X^r)^{1/k^2 UP_i} (= g^{r/kR_iH_1(U_i)} = US_i^r)$.
(3) SDC decrypts the message $M_s = c \oplus H_l(v)$.
(4) SDC calculates the signature as the following:

$$\begin{aligned} & s/\hat{e}\left(g^{1/k}, X^r\right)^{1/UP_i} \\ &= w\hat{e}\left(US_i, X\right)^r \Big/ \hat{e}\left(g^{1/k}, X^r\right)^{1/UP_i} \\ &= w\hat{e}\left(g^{1/kR_iH_1(U_i)}, g^k\right)^r \Big/ \hat{e}\left(g^{1/k}, g^{rk}\right)^{1/UP_i} \\ &= w\hat{e}\left(g, g\right)^{r/R_iH_1(U_i)} \Big/ \hat{e}\left(g, g\right)^{r/R_iH_1(U_i)} \\ &= w \end{aligned} \tag{1}$$

(5) SDC verifies the validity between w and $w^{'} = H_2^{'}(H(Ms_1) \oplus \ldots \oplus H(Ms_n) \oplus X^r)$.

5) Verification by users

(1) The user U_j receives the message $m = (M_s, UP_i, X^r, s)$.
(2) The user U_j calculates the signature with his certificates $< UP_j, US_j >$ and the identity UP_i of the user U_i as the following:

$$\begin{aligned} & s/\hat{e}\left(US_j, (W)^{UP_j}\right)^{1/UP_i} \\ &= w\hat{e}\left(US_i, X\right)^r \Big/ \hat{e}\left(US_j, (X^r)^{UP_j}\right)^{1/UP_i} \\ &= w\hat{e}\left(g^{1/kR_iH_1(U_i)}, g^k\right)^r \Big/ \hat{e}\left(g^{1/(kR_jH_1(U_j))}, g^{rkR_jH_1(U_j)}\right)^{1/UP_i} \\ &= w\hat{e}(g,g)^{r/R_iH_1(U_i)} \Big/ \hat{e}\left(g^{1/(kR_jH_1(U_j))}, g^{rkR_jH_1(U_j)}\right)^{1/R_iH_1(U_i)} \\ &= w\hat{e}(g,g)^{r/R_iH_1(U_i)} \Big/ \hat{e}(g,g)^{r/R_iH_1(U_i)} \\ &= w \end{aligned} \tag{2}$$

(3) The user U_j calculates $w^{'}=H_2^{'}(H(Ms_1)\oplus\ldots\oplus H(Ms_n)\oplus X^r)$, and checks whether $w^{'} = w$ holds.

6) Update of parameters by SDC

(1) Randomly selects a number $t \in Z_q^*$.
(2) Calculates $X' = g^{kt}$.
(3) Sends $((q, G_1, G_2, \hat{e}, H_1), X', t)$ as the new secure parameters of the trust domain to users.

4.2 Protocol Description

When sensor nodes and users setup the secure scheme with configurable privacy, the message distribution can be executed as the following steps.

(1) The SDC periodically requests information from sensors for by the message (R, U_{SDC}), in which R is a random number selected by the SDC, and U_{SDC} is the identity of the SDC.
(2) When the sensor node receives the requesting message, he firstly randomly chooses an integer $r \in_R Z_q^*$, then computes $u = X^r$, $c = M_s \oplus H_l\left(US_i^r\right)$ and $w = H_2^{'}(H(M_{s1}) \oplus \ldots \oplus H(M_{sn}) \oplus X^r \oplus R)$, and $s = w\hat{e}(US_i, X)^r$. Finally the sensor node sends the message $\left(M_p \| c \| u \| s \| UP_t \| R\right)$ to the SDC.
(3) The SDC firstly verifies the freshness of R, then calculates $v = (X^r)^{1/k^2 UP_i} \left(= g^{r/kR_iH_1(U_i)} = US_i^r\right)$ and, decrypts c to $M_s^{'} = c \oplus H_l(v)$, where $M_s^{'}$ is detached into n blocks $M_{s1}^{'}, M_{s2}^{'}, \ldots, M_{sn}^{'}$. Then he continues to compute $w^{'} = H_2^{'}\left(H\left(M_{s1}^{'}\right) \oplus \ldots \oplus H\left(M_{sn}^{'}\right) \oplus X^r \oplus R\right)$. SDC can also calculate w from s, and checks whether $w^{'} = w$ holds. If yes, the signature is valid, then go to step 3). Otherwise, the SDC may discard the message and the protocol ends.
(4) Based on the pre-set delivery policy Λ_i, the SDC sends $\left(M_p \| M_{si_1}^{'} \| M_{si_2}^{'} \| \ldots \| M_{si_t}^{'} \| \left(H\left(M_{si_{t+1}}^{'}\right) \oplus \ldots \oplus H\left(M_{si_n}^{'}\right)\right) \| s \| UP_t\right)$ to every user USR_i.

(5) After receiving the message, every user USR_i verifies the signature s of the message $\left(M_p \| \left(H\left(M'_{s1}\right) \oplus H\left(M'_{s2}\right) \oplus \ldots \oplus H\left(M'_{sn}\right)\right)\right)$. If it is valid, he gets the right message from the right sensor node. Otherwise, he discards the message.

From the above descriptions, it can be easily seen that the user SDC can always decrypt the secret message and verify the signature of the sensor node correctly if the node is honesty. Moreover, the user USR_i can only know messages $\{M_{si_1} M_{si_2}, \ldots, M_{si_t}\}$ corresponding to the set Λ_i because he cannot retrieve M'_{si} from $H\left(M'_{si}\right)$ for the one-wayness of H. Of course, every user can verify the signature as s is a signature of all the messages to every user.

4.3 Typical Medical Application Scenario

With the development of wireless sensor network, applying wireless sensors toward health care monitoring allows for new ways to provide quality health care to patients. A diverse array of specialized sensors can be deployed to monitor, for instance, at-risk patients with history of heart attacks, or senior citizens living independently at home. These sensors provide continuous, long term monitoring in an unobtrusive manner, allowing doctors to diagnose problems more effectively.

From the scenario presented in Fig. 2, we provide the following security and privacy protections for the typical medical application scenario.

(1) Protect patient privacy from eavesdropping by the malicious adversary in the wireless network. Since the data are transmitted by wireless networks, a patient's data need encrypted by sensors with his identity certificate and only the SDC can decrypt the patient's data.
(2) Tolerate compromised sensors. The sensors may be misplaced or stolen, so we should periodically update the public parameters of the trust domain by the SDC to prevent a compromised sensor node from forging the patient's data.
(3) Prevent unauthorized access to information. This includes a doctor with permissions to access some data and not others. We assume that a doctor may attempt to obtain additional data about a patient beyond what was authorized. Since the SDC sends the data with the pre-set policy, a doctor cannot receive other's data, and access control can only be performed by the SDC.
(4) Flexibility in granting permissions. The patient may decide to allow different doctors and nurses to access his data, and the SDC can configure the policy to allow some doctors and nurses obtain their concerned data but others. For example, a sensor node sends a message, which includes the patient's information of body temperature and heart, the nurse only need to obtain the information of body temperature, and the doctor need know all information of the patient. So the SDC need to configure the policy to protect the patient privacy.

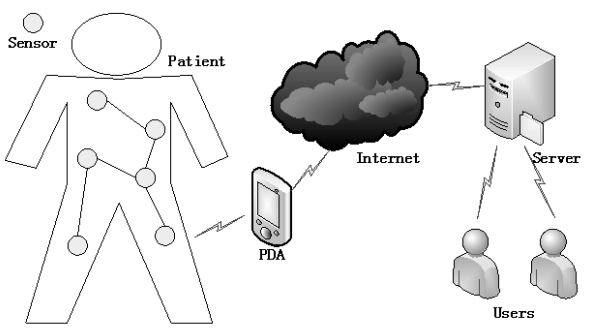

Fig. 2 Typical medical application scenario.

5. SMDCP Analysis

In this section, we present the security and performance analysis of SMDCP scheme. Our main concern is the several secure characters and the advantages of the flexible topology of SMDCP scheme.

5.1 Security Analysis

Our scheme can be analyzed to meet the security characters of unforgeability, confidentiality, non-repudiation and privacy as following.

Unforgeability From the logistic structure of our scheme, it is evident that the pair s is a signature of the message $\left(M_p \| H(M_{s1}) \oplus H(M_{s2}) \oplus \ldots \oplus H(M_{sn})\right)$ by the sensor node. As the hard problem [18] of BDHP of the signature, no adaptive attacker [19] can forge a valid message $\left(M_p, c, s\right)$ that can be correctly decrypted and verified by SDC for any message $m = M_p \| M_s$.

Confidentiality If any an attacker except SDC wants to decrypt c to $M_{s1} \| M_{s2} \| \ldots \| M_{sn}$, he has to know k due to the one-wayness and collision resistance of the ideal hash function H. However, as he can't know k and r assuring by the security of signature, obtaining k and r from X^r is a CDH problem which is computational unfeasible.

Non-repudiation Firstly, any user USR_i can release his receiving the message $\left(M_p \| M'_{si_1} \| M'_{si_2} \| \ldots \| M'_{si_t} \| \left(H\left(M'_{si_{t+1}}\right) \oplus \ldots \oplus H\left(M'_{si_n}\right)\right) \| UP_t \| s\right)$, in which s is a signature on the message $\left(M_p \| \left(H\left(M'_{s1}\right) \oplus H\left(M'_{s2}\right) \oplus \ldots \oplus H\left(M'_{sn}\right)\right)\right)$ by the sensor node and can be publicly verified with the node's public identity. Furthermore, SDC can public $\left(M_p \| M_s \| UP_t \| s\right)$ that can also be verified.

Privacy Any user USR_i can only know the secret message M_{sj} where j belongs to Λ_i but for others because of the one-wayness of the ideal hash function H. That is to say, the privacy of the user USR_j with j exclusive of Λ_i is kept to the user USR_i.

5.2 Performance Analysis

We study these energy consumptions as the function of the

HWSN size W, future compare the performance of SMDCP scheme with the directly Schnorr [20] signature by sensor nodes.

As reported in [4], a Chipcon CC1000 radio used in Crossbow MICA2DOT motes consumes 28.6 and 59.2 μJ to receive and transmit one byte, respectively, at an effective data rate of 12.4 kb/s. Furthermore, we assume a packet size of 41 bytes, 32 for the payload and nine bytes for the header. The header, following an 8-byte preamble, consists of source, destination, length, packet ID, CRC, and a control byte. We assume that the number of users is n in HWSNs, and the total message size in Schnorr signature scheme is 71 bytes, which includes $|Mp||Ms| = 2$ bytes, $|c| = 20$ bytes, $|r| = 20$ bytes and $|s| = 20$ bytes, and that in SMDCP scheme is 103 bytes, which includes $|M_p||M_s| = 2$ bytes, $|c| = 20$ bytes, $|u| = 16$ bytes, $|s| = 20$ bytes, $|UP| = 16$ bytes and $|R| = 16$ bytes, when a typical ECC group is used. So we can compare the energy consumption on message sending of SMDCP scheme and Schnorr signature scheme by a sensor node in HWSNs.

Figures 3 and 4 illustrate these energy consumptions as a function of network size W. Clearly, we see that the SMDCP scheme offers the much lower energy consumption as compared to that of directly Schnorr signature when the number of users is 2 and 5 in HWSNs. The user number does not change the size of $Mp||Ms$, but results in the fragment number of Ms. Figures 3 and 4 show that the energy consumption of SMDCP scheme is unchangeable with the number of users, because the sender only need send one signed message to all receiving users. However, the energy consumption of directly Schnorr signature is linear change with the user number in HWSNs, because the sender needs to send a signed message to each receiving user.

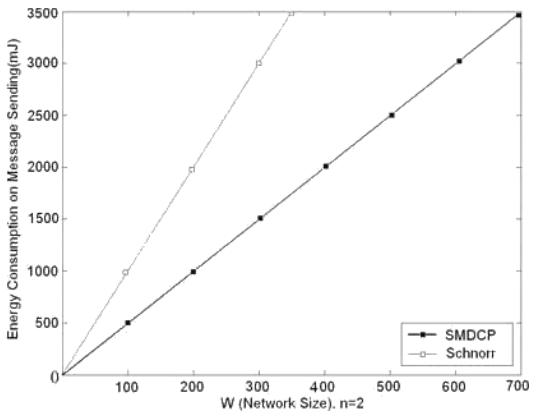

Fig. 3 Energy consumption on message sending with two users in HWSNs.

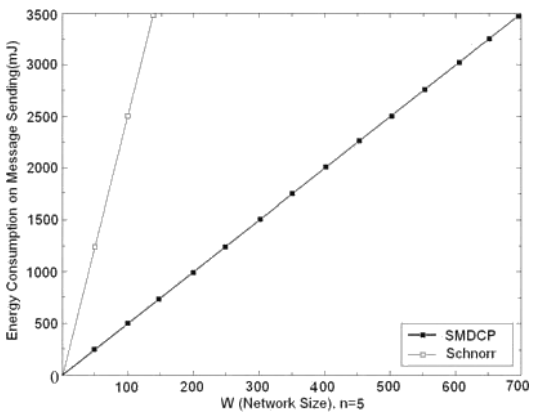

Fig. 4 Energy consumption on message sending with five users in HWSNs.

6. Conclusion

In this paper, we studied the secure scheme for the message distribution in wireless sensor network. Based on authenticated encryption scheme which is an efficient integration of signature and encryption, we present our SMDCP scheme for heterogeneous wireless sensor networks. It can be configured to release or keep the secret during disputation arbitration in which an SDC is required. The sensor node need generate only one signature of the messages for all the users, which can greatly save the communication and computation cost of the sensor node. On the other hand, the user can only know the messages that let him know based on a pre-set policy, which can meet the requirement of the privacy. As a result, it can be suitably applied in heterogeneous wireless sensor networks.

Acknowledgments

This paper was supported in part by the Major Program of National Natural Science Foundation of China (60633020), the National Natural Science Foundation of China (60573036, 60702059, 60503012), the National High Technology Research and Development Program of China (2007AA01Z429), and the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-521-D00449).

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol.40, no.8, pp.102–116, 2002.
[2] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks: Research challenges," Ad Hoc Networks, vol.2, no.4, pp.351–367, 2004.
[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security protocols for sensor networks," Proc. MobiCom'01, 2001.
[4] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, "Energy analysis of public-key cryptography on small wireless devices," IEEE PerCom, March 2005.
[5] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," Proc. MobiHoc, pp.58–67, 2005.
[6] C.C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: An entity-based cryptography approach (short paper)," ACM WiSec, 2008.
[7] M.-S. Hwang and C.-Y. Liu. "Authenticated encryption schemes:

Current status and key issues," International Journal of Network Security, vol.1, no.2, pp.61–73, Sept. 2005.
[8] K. Nyberg and R.A. Rueppel, "A new signature scheme based on the DSA giving message recovery," ACM Computer & Communications Security, vol.1, pp.58–61, 1993.
[9] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," IEEE Electron. Lett., vol.30, no.15, pp.1212–1213, 1994.
[10] W.B. Lee and C.C. Chang, "Authenticated encryption scheme without using a one way function," IEEE Electron. Lett., vol.31, no.19, pp.1656–1657, 1995.
[11] T.S. Wu and C.L. Hsu, "Convertible authenticated encryption scheme," J. Syst. Softw., vol.39, no.3, pp.281–282, 2002.
[12] G. Wang, F. Bao, C. Ma, and K. Chen, "Efficient authenticated encryption schemes with public verifiability," IEEE Vehicular Technology Conference (VTC 2004) - Wireless Technologies for Global Security, IEEE Computer Society, 2004.
[13] D. Boneh and M. Franklin, "Identify-based encryption from the weil pairing," Proc. CRYPTO'01, ser. LNCS, vol.2139, pp.213–229, Springer-Verlag, 2001.
[14] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," Proc. CRYPTO'02, ser. LNCS, vol.2442, pp.354–368, Springer-Verlag, 2002.
[15] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervasive Computing, Special Issue on Pervasive Computing for First Response, 2004.
[16] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," Proc. INFOCOM, 2003.
[17] N. Jefferies, C. Mitchell, and M .Walker, "A proposed architecture for trusted third party services," Proc. Cryptography: Policy and Algorithms, Brisbane, Australia, July, LNCS, 1029, pp.98–104, Springer, Berlin, 1995.
[18] J. Zhou and K. Lam, "Undeniable billing in mobile communication," in: ACM MobiCom'98, Dallas, TX, Oct. 1998.
[19] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," J. Cryptol., vol.13, no.3, pp.361–369, 2000.
[20] C.-P. Schnorr, "Efficient signature generation by smart cards," J. Cryptol., vol.4, no.3, pp.161–174, 1991.

YaHui Li received his B.S. degree in Computer Science from Air force Engineering University, China in 1998, and obtained his M.E. and Ph.D. degrees in computer architecture and communications engineering from Xidian University, China in 2004 and 2009, respectively. Now he is a lecture in the School of Computer Science at Xidian University, Xi'an, China. His current research interests include wireless and mobile computing systems, computer networks, and information and network security. He has published over 10 refereed articles in these areas.

JianFeng Ma received his B.S. degree in mathematics from Shaanxi Normal University, China in 1985, and obtained his M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University, China in 1988 and 1995, respectively. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. He is an IEEE member and a senior member of Chinese Institute of Electronics (CIE). Now he is a Professor and Ph.D. supervisor in the School of Computer Science at Xidian University, Xi'an, China, and the director of the Key Laboratory of Computer Networks and Information Security of Ministry of Education (China). His current research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security. He has published over 150 refereed articles in these areas and coauthored ten books.

SangJae Moon is a Professor in the School of Electrical Engineering and Computer Science, Kyungpook National University, Korea. Professor Moon received his B.S. and M.S. degrees from Seoul National University in 1972 and 1974, respectively, all in Electronic Engineering, and Ph.D. degree from UCLA (USA). He is now the President of Korea Institute of Information Security & Cryptology. His research areas are wireless networks, network security, and mobile computing. He has published more than 200 papers in major journals, referred conference proceedings, book chapters related to these research areas.