An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare

Xuan Hung Le, Murad Khalid, and Ravi Sankar
University of South Florida, Tampa, FL 33620, USA
Email: xhle@usf.edu, mkhalid@mail.usf.edu, sankar@usf.edu

Sungyoung Lee
Kyung Hee University, Yongin-si, Gyeonggi-do, 449-701, Korea
Email: sylee@oslab.khu.ac.kr

Abstract— **Wireless sensor networks (WSNs) will play an active role in the 21th Century Healthcare IT to reduce the healthcare cost and improve the quality of care. The protection of data confidentiality and patient privacy are the most critical requirements for the ubiquitous use of WSNs in healthcare environments. This requires a secure and lightweight user authentication and access control. Symmetric key - based access control is not suitable for WSNs in healthcare due to dynamic network topology, mobility, and stringent resource constraints. In this paper, we propose a secure, lightweight public key - based security scheme, Mutual Authentication and Access Control based on Elliptic curve cryptography (MAACE). MAACE is a mutual authentication protocol where a healthcare professional can authenticate to an accessed node (a PDA or medical sensor) and vice versa. This is to ensure that medical data is not exposed to an unauthorized person. On the other hand, it ensures that medical data sent to healthcare professionals did not originate from a malicious node. MAACE is more scalable and requires less memory compared to symmetric key-based schemes. Furthermore, it is much more lightweight than other public key-based schemes. Security analysis and performance evaluation results are presented and compared to existing schemes to show advantages of the proposed scheme.[1]**

Index Terms—**elliptic curve cryptography, user authentication, access control, wireless sensor networks**

I. Introduction

Electronic patient records and wireless sensor networks for patient monitoring are at the current forefront of new technologies to improve the quality of healthcare, cost-efficiency, and health information delivery. While there are great benefits of technologies, associated data confidentiality and patient privacy need to be enhanced to make these technologies socially acceptable. The security requirements are very diverse as they are based on differing usage scenarios ranging from pre-hospital, in-hospital, ambulatory and home monitoring. It could be dangerous, or even fatal, if this medical monitoring data is corrupted. Thus, strict security mechanisms must always be in place to prevent malicious interactions with the healthcare systems. Such mechanisms should also be scalable since it is expected that thousands of WSNs will be deployed within the current decade.

Most of the research work has mainly focused on how to seamlessly collect and wirelessly transmit health data (e.g. vital signs) in the presence of extreme resource-limitations in terms of power, computation, and bandwidth [1]-[9]. Security is an important factor for WSN's success and acceptance in medical applications. One of the most critical security concerns is how to protect patients' privacy, which requires secure authentication and access control. User authentication is to allow legitimate healthcare professionals to access medical information while declining malicious persons or attackers. After authentication, access control has to restrict authenticated healthcare professionals to access only data that they have privilege for proper healthcare services. In healthcare environments, authentication and access control face a big challenge due to dynamic network topology, mobility of nodes, and resource constraints. Currently, many security mechanisms have been proposed for WSNs based on symmetric key cryptography (SKC) due to its extremely fast computation and energy efficiency for resource-constraint sensor platforms. However, SKC is not scalable, requires large memory for storing keys and a complicated key pre-distribution scheme, and difficult to maintain the key infrastructure when a new node is added. These barriers have impeded SKC being practically deployed in healthcare WSNs. Public key cryptography-based schemes are ideal to overcome these challenges due to their high scalability, low memory requirements, easy key-addition/revocation for a new node, and no requirement of complicated key pre-distribution [10]-[14]. However, it is computationally expensive to apply

Dr. Sungyoung Lee is the corresponding author.

doi:10.4304/jnw.6.3.355-364

public key cryptography to such resource-limited devices like sensors [15].

In this paper, we propose a new method, Mutual Authentication and Access Control based on Elliptic Curve Cryptography (MAACE). It uses public key approach, which is more scalable and requires less memory compared to symmetric key-based schemes. More importantly, it is more energy-efficient than existing public key-based approaches and practically feasible to implement it on sensor platforms. This paper is an extended version of our previous paper presented at ICUIMC-2010 [11] with detailed description and simulation results.

The remainder of the paper is organized as follows. We highlight open research challenges of WSNs in healthcare applications in Section II. Section III briefly reviews related work. Background of Elliptic Curve Cryptography, which forms the foundation for this proposed method, is described in Section IV. In Section V, we briefly describe our earlier work and its drawbacks. Then, the proposed security scheme is presented in Section VI. Section VII and Section VIII present the security analysis and performance evaluation of MAACE. Finally, Section IX concludes the paper and outlines investigation for future work.

II. Open Research Challenges

The introduction of WSNs into healthcare applications poses unique challenges in security and privacy implementation due to the following factors:

- **Resource constraints**: medical sensors are usually smaller than ordinal ones, and thus have more limited capacity in terms of power supply, memory, and computation. Security functions must be lightweight, yet secure enough to protect medical data.
- **Dynamic network topology**: The sensor network topology is constantly changing overtime. As the topology changes, re-establishing security parameters such as secret key must not generate too much overhead.
- **Mobility**: medical sensor and coordination nodes are mobile every time as patients are moving. Existing security schemes are not suitable because they depend on node relational information such as neighborhood, locations, etc. Established security materials (e.g. secret keys) may no longer work. When nodes change the location, all necessary cryptographic functions and keys must reside and be executable efficiently within the nodes. The security architecture also needs to be scalable to account for varying numbers of mobile nodes as well as for making best use of the scarce radio resources.

III. Related work

A number of security schemes have been proposed for WSNs [10]-[29] to solve the problem of how to pre-distribute pair-wise shared keys (symmetric keys) to a large number of nodes that are scattered over a large field. Most of them have not taken into account challenges in healthcare domain. For example, [16]-[18] are based on node deployment knowledge (i.e. node location information) to efficiently and securely pre-distribute key rings to a number of group. In healthcare environments, node locations are not fixed. Furthermore, node location retrieval and frequent location updates increase network overhead and energy consumption significantly. Several work introduced efficient approaches using symmetric key [12][13]. However, symmetric key based authentication requires complicated key pre-distribution scheme, large memory to store keys, and is difficult to deploy a new node.

Wang *et al*. [14] (HBQ scheme) applied public key cryptography based on ECC to solve the problem of symmetric key approaches in terms of scalability, key storage, and key pre-distribution. However, the performance evaluation in [14] has shown that HBQ is still burdensome for sensors leading to impracticability of implementation. Le *et al*. [10] (ENABLE scheme) has solved security limitations and performance issues in [14]. However, it relies on a trusted third-party (e.g. Key Distribution Scheme) to handle significant ECC operations. Always communicating with an on-line KDC introduces significant cost increase in healthcare. Furthermore, failure of KDC may lead to failure of the security function for the network.

Ng *et al.* came up with security issues of wireless sensor networks in healthcare applications [19]. Authors discussed the unique challenges of security implementation in healthcare such as resource limitations of sensor nodes, uncontrollable environment, and dynamic network topology. In [9], the authors introduced a hierarchical network for in-home, in-hospital, nursing-house healthcare applications. The sensor network tier uses *BTnode* (Bluetooth-enable node) and relies on Bluetooth security. Since many current sensors are built on Zigbee standard (e.g. CodeBlue [1][2]), the proposed scheme lends itself to be impractical. Boukerche and Yonglin [20] proposed a secure mobile healthcare system using trust-based multicast system. The authors presented a secure multicast strategy that employs trust in order to evaluate the behavior of each node so that only trustworthy nodes are allowed to participate in communications, while the misbehavior of malicious nodes is effectively prevented. Chakravorty [21] introduced health-related service architecture (MobiCare) for mobile patient care. It satisfies the need of medical monitoring by deploying medical sensors to form a body sensor network, and provides the necessary protection to clinical services by applying secure and reliable dynamic software. The author further discussed issues with MobiCare, which include confidentiality, integrity, and privacy of patient's information. Many techniques were suggested, such as authentication, access control, encryption, and so on.

Kim *et al*. [22] discussed some potential threats for ubiquitous healthcare systems and described the security requirements for these u-healthcare systems. They proposed a systematic architecture in order to design a security policy for such healthcare systems and to allow a patient to control access to any sensing data recorded by a

personal healthcare device. Bao *et al.* [23] proposed an interesting scheme that solved the issue of entity authentication for BSN, in which the notion of biometrics is applied as an authentication approach that automatically verifies an individual's identity. In the established BSN, peer authentication can ensure secure connections between different entities. This method is however only designed for wearable biometric sensors. Jeong *et al*. [24] presented a mobile collaboration framework based on distributed systems. It supports the necessary security services by checking access rights for corresponding users. It then divides the collected data into secure and public data, and subsequently applies the access control technique to specify that each security object needs the corresponding access privilege.

Marti *et al*. [25] presented a specification of integrated network and security services for mobile e-health environments. It applies different security mechanisms to address threats such as eavesdropping or manipulating patient information, and thus guarantees the patient data confidentiality and integrity. Markovic *et al*. [26] considered the issues of mobile healthcare security and employ cryptographic techniques to address possible vulnerabilities. They made use of symmetrical cryptographic methods to protect data confidentiality, and asymmetrical cryptographic algorithms such as Public Key Infrastructure (PKI) and digital signature technique to achieve data integrity. PKI is the most preferable solution in healthcare, but their technique can be applied to powerful computing systems only.

In summary, none of the existing security schemes addressed the important challenges in healthcare WSNs. First, increased security vulnerability of medical sensors that are often deployed in unprotected environments. Second, the impracticality of SKC for WSN networks in healthcare since keys are usually pre-distributed according to node's static locations and/or network density, whereas in this application scenario the topology is dynamic (nodes are mobile and are free to join and leave the network at any time). Third, the impracticality of prior secure information exchange (e.g. secret keys) due to diversity of WSN security infrastructure. Fourth, the need for a lightweight security mechanism for pervasive access to WSN data from mobile devices (e.g. PDA) because both handhelds and sensor nodes have strict resource-constraints. Compared to SKC, Public Key Cryptography (PKC) (e.g. RSA scheme) is more scalable, requires less memory for storing keys, less communication overhead, and is easy-to-deploy. However, the computational cost is prohibitively high making conventional PKC impractical to implement on sensor platforms.

IV. BACKGROUND

A. Elliptic Curve Discret Logarithm Problem (ECDLP)

Elliptic Curve Cryptography (ECC) was suggested independently by Miller [32] and Koblitz [33] in 1985. Recently, ECC has attracted much attention as an efficient security solution for wireless networks due to the small key size and low computational overhead. It is an approach of public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Compared to conventional public key cryptography such as RSA, ECC achieves much better performance with the same security level. For example, ECC with 160-bit key length has equivalent security level to that of RSA with 1024-bit key length [31]. On the other hand, ECC multiplication operation has been shown to be feasible on a sensor mote that takes only 0.81 *second* on 8-bit CPU Atmel ATmegal128 MHz [15].

An elliptic curve consists of the points satisfying the equation:

$$y^2 = x^3 + ax + b,$$

where x, y, a and b are elements in $GF(q)$ (a *Galois Field* of order q, where q is a prime).

Each choice of (a, b) yields a different elliptic curve. For example, Figure 1 shows an elliptic curve of $y^2 = x^3 - 7x$.

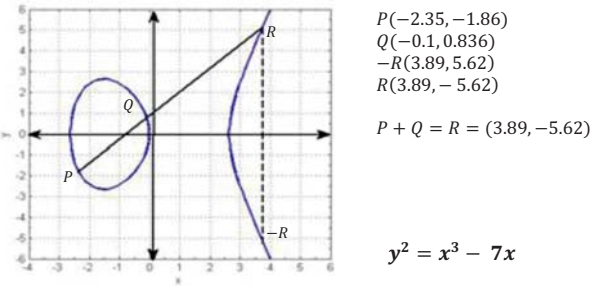

Figure 1 Elliptic curve and point addition

The elliptic curve group operation is closed under addition so that addition of any two points is also a point in the group. Given two points $P(x_1, y_1)$ and $Q(x_2, y_2)$, the addition results in a point $R(x_3, y_3)$ given by:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3).$$

such that

$$x_3 = \Psi^2 + \Psi + x_1 + x_2 + a$$

$$y_3 = \Psi(x_1 + x_3) + x_3 + y_1$$

where $\Psi = (y_1 + y_2)/(x_1 + x_2)$

An example of $P(-2.35, -1.86)$ and $Q(-0.1, 0.836)$ is illustrated in Figure 1.

If $P = Q$, then $R = P + P = 2 \times P$. Addition of multiple points P will give $R = k \times P$. ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), that is, given points P and Q of the group, it is practically infeasible to find a number k such as $Q = k \times P$.

B. Elliptic Curve Diffie-Hellman Protocol (ECDH)

Elliptic Curve Diffie-Hellman (ECDH) protocol is a secret key exchanging protocol to establish a secret key between two parties who have no prior knowledge about each other. Based on ECDLP, a typical ECDH is built as shown in Figure 2.

Initially, Alice and Bob agree on system based point P and generate their own key-pair (Q_A, k_A) and (Q_B, k_B). To share a secret, Alice and Bob exchange their public keys,

and then use their own private key, k_A and k_B respectively, to multiply the other's public key, i.e.

Alice computes: $R_A = k_A \times Q_B$,

Bob computes: $R_B = k_B \times Q_A$.

Since $k_A \times Q_B = k_A \times (k_B \times P) = k_B \times (k_A \times P) = k_B \times Q_A$, thus $R_A = R_B = R(x_R, y_R)$.

The value x_R will be the secret key of Alice and Bob.

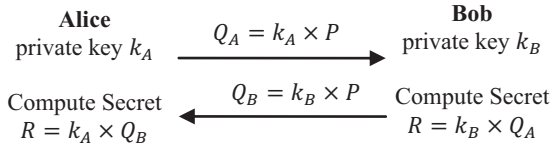

Figure 2 ECDH key exchange protocol

The protocol is secure because nothing is disclosed (except for the public keys and the based point P, which are not secret), and no party can derive the private key of the other unless it can solve the *Elliptic Curve Discrete Logarithm Problem*.

V. Brief Review of ENABLE Scheme

A. Protocol Description

In our earlier work, ENABLE scheme [10], we have applied ECC to eliminate the issues of symmetric key approaches in terms of scalability, key storage, and key pre-distribution. More importantly, ENABLE schemes achieved better performance compared with existing public key-based schemes such as HBQ scheme [14].

The network model of ENABLE scheme is shown in Figure 3. Whenever a user wants to access data on a particular node or a group of nodes, first he/she must sends a request to that node or the representative node of the group. Then the node will talk to the trusted third party (such as a Key Distribution Center (KDC) in our scenario). Upon receiving the decision from the KDC, the node can accept or reject the user's request.

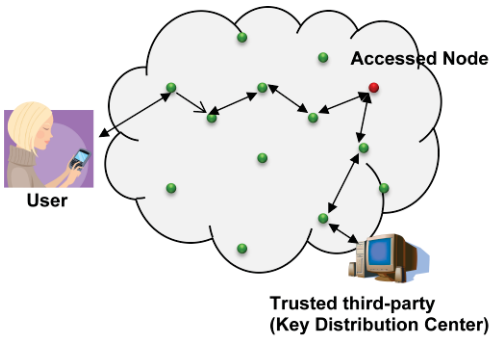

Figure 3 The network model of ENABLE scheme

Prior to accessing the network, the user, say Alice (A) comes generates her public key (Q_A), private key (k_A) using the same ECC parameters with KDC. KDC generates a certificate of the user's access list and public key by signing with its private key ($cert_A$ = {ac_A, Q_A, $sign_{KDC}(ac_A \,||\, Q_A)$. The certificate is then sent to the user. The structure of access control list is similar to that of HBQ scheme [8]. It is composed of user identification (*uid*), group identification (*gid*), and *user access privileges mask*. *user access privilege mask* is a set of binary bits. Each bit represents a specific information or service (see the example in Figure 4). The user A and sensor S compute a secret key (x_A) using ECDH key exchange protocol. The sensor S and KDC also compute a shared secret key (x_S) in the same way. Notations are explained in TABLE I.

TABLE I NOTATION

Symbol	Description
ID_A	Identifier of entity A
x_{AB}	Shared secret key between A and B
ac_A	Access control list issued to entity A
$sign_A(m)$	Message m is signed by entity A
$A \rightarrow B: m$	Entity A sends entity B a message m
$(m)K$	Symmetric encryption of message m with key K
$MAC(K, m)$	A message authentication code of message m with key K
$h(m)$	Hashing value of message m
$\|\|$	Concatenation

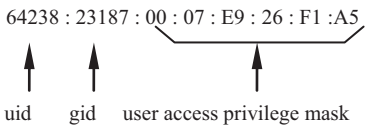

Figure 4 An example of user access list

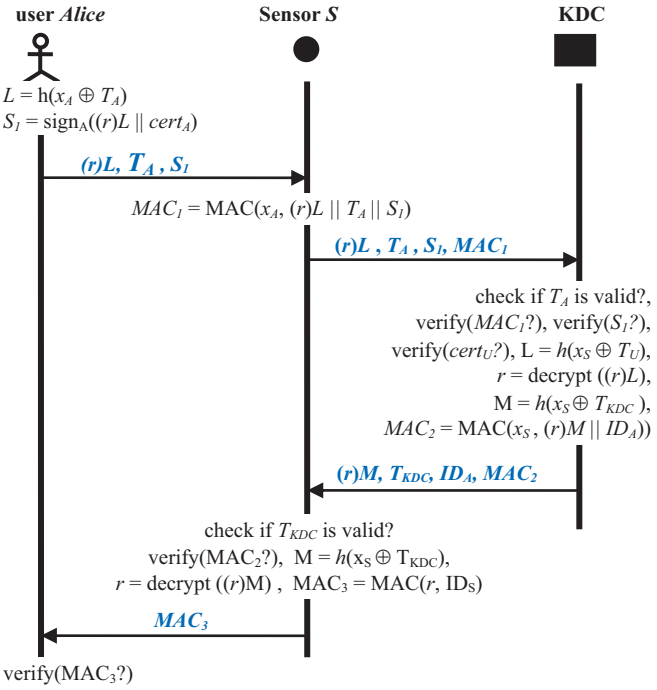

Figure 5 ENABLE protocol

The authentication and access control protocol is described in Figure 5. The protocol includes four steps. First, user A selects a random number $r \in GF(p)$ which will be used as a session key with S, creates a secret key $L = h(x_A \oplus T_A)$ (where T_A is the current timestamp generated by A), and encrypts r with key L ($(r)L$). A then signs this encrypted value along with its certificate ($S_1 = sign_A((r)L \,||\, cert_A)$) and sends to the sensor S. In second

step, upon receiving the message from A, S first checks if the time T_A is valid. If yes, then it builds a MAC by the shared secret key x_S (MAC_1 = MAC(x_S, $(r)L \parallel T_A \parallel S_1$)). The sensor then forwards the message along with MAC_1 value to KDC. In third step, KDC verifies MAC_1 value. If the verification is successful, then S is authentic to KDC. KDC then verifies S_1, which was signed by A. If the signature is valid, then A is also authentic. The $cert_A$ is also verified to check the validity of the access list ac_A. KDC now constructs a secret key L = $h(x_A \oplus T_A)$, and decrypts $(r)L$ to get r. It then generates a secret key M = $h(x_S \oplus T_{KDC})$ (where T_{KDC} is the timestamp created by KDC), encrypts r, and builds a MAC (MAC_2 = MAC(x_S, $(r)M \parallel ID_A$)). Afterward, KDC sends them to S. In the last step, when S receives the message, it verifies MAC_2 value. A successful verification indicates that the user is authentic to S. After that, S constructs the secret key M = $h(x_S \oplus T_{KDC})$ and decrypts (r)M to get r. Using this secret key, S builds a MAC (MAC_3 = MAC(r, ID_S)) and sends to the user. Upon receiving the MAC value from S, user A verifies it by the same key r. If the verification is successful, then S is authentic to the user.

B. Major Drawback

Although ENABLE scheme has solved the main issues of symmetric key cryptography by significantly improving performance, it possesses a major disadvantage. As shown in Figure 3, the sensor S must communicate with the KDC to authenticate the user and verify the access request. First, this requires an on-line KDC all the time. Any failure or security breach of the KDC will lead to serious problem to the network. Second, communicating with the KDC requires a significant extra overhead to the network. This extended version will eliminate the drawback.

VI. The Proposed Scheme: MAACE

A. Network Model

A typical health information network is shown in Figure 6. Wearable biosensors and embedded sensors are deployed in hospital wards to continually monitor patient's physiological signal and health related information. Due to the short communication range, these sensors transmit data to a coordination point (e.g. a handheld device). The coordination point aggregate sensor data and transmit it to physicians or to the hospital information server for further fusion and accessing. Local hospital practitioners can access to health information either at the centralized/distributed information servers, or at wards provided by wireless biosensors and coordination nodes. Besides, remote practitioners from other healthcare providers also can access to the hospital information server via Internet with a limited permissions.

We define this network as a hierarchical (layered) network consisting of three layers as shown in Figure 7: *Sensor Network* (SN) layer, *Coordination Network* (CN) layer, and *Data Access* (DA) layer.

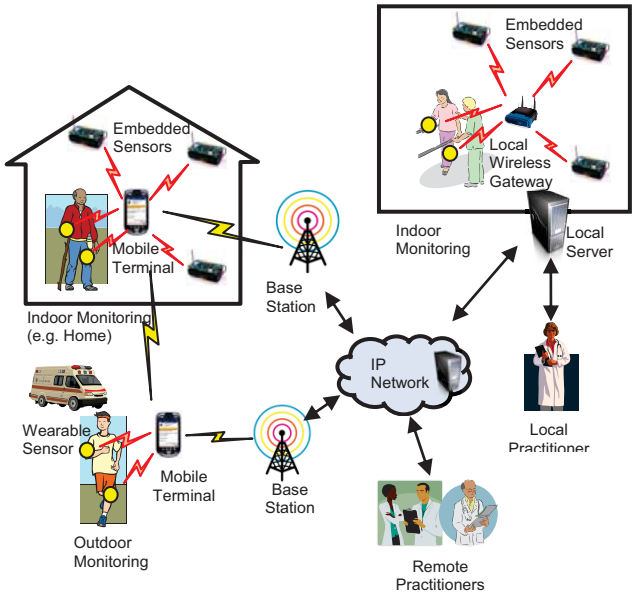

Figure 6 Typical wireless sensor network in healthcare

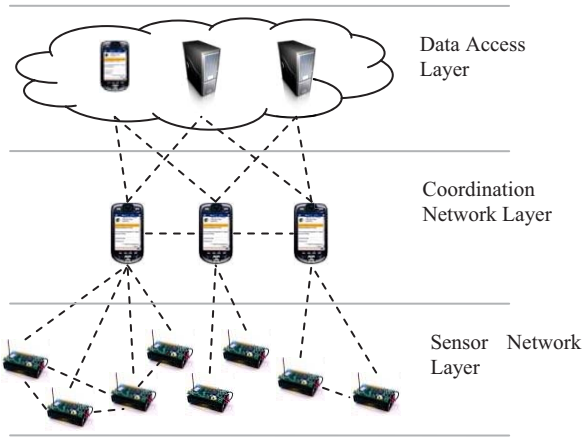

Figure 7 Hierarchical structure of a WSN in Healthcare

- **Sensor Network (SN) Layer**: In SN layer, different types of medical sensors are wearable on the human body to monitor vital signs such as blood pressure, electrocardiogram (EKG), heart rate, blood oxygen saturation (SpO_2). Furthermore, embedded sensors are also deployed in indoor areas (e.g. patient's home, hospital ward) to monitor context conditions (e.g. human activity, temperature) which is necessary for healthcare services. These sensors use either ZigBee (IEEE 802.15.4) or Bluetooth (IEEE 802.15.1) wireless technology. Since these sensors have a short communication range (10 - 100 *m*), they must be connected to more powerful devices in CN layer to deliver sensed data to healthcare professionals.
- **Coordination Network (CN) Layer**: In CN layer, a number of computing devices such as *PDA*, laptop, cell phone, are organized regionally using an ad hoc network or an infrastructure-based network to connect to a fixed remote or local station. CN nodes collect and analyze data from SN layer because SN node does not have mass data storage capability over a long

period (such as a few months or years). Further, CN nodes are tamper-resistant.

- **Data Access (DA) Layer**: The DA layer includes a number of database servers and accessing points that physicians can use to access sensory data. The database servers store patient medical records for long-term periods from the monitored individuals along with their residence environmental data. The accessing points provide an interface to physicians to access sensory data from their computers or handheld devices (e.g. PDAs, tablet PCs). A third-party, e.g. a *Key Distribution Center* (KDC), set up on the Internet can be trusted to open access areas such as hospitals or nursing homes supporting the proposed healthcare monitoring service. The third-party issues effective certificates and keys to valid SN and CN nodes.

B. *Mutual Authentication and Access Control based on ECC (MAACE)*

The first step is to establish key between nodes. To meet scalability requirements for a large number of sensor nodes, we propose a public key management scheme based on Elliptic Curve Cryptography (ECC). Compared to symmetric key cryptography, ECC is more scalable, requires lesser memory for storing keys, introduces low communication overhead, and is easy to deploy [10].

1) *Key Establishment*

There is one or more trusted third-parties on the network called *Key Distribution Center* (KDC) to generate all security materials (e.g. keys, certifiates), issue and revoke users's access privileges. Note that this KDC is not required to be online all the time like in ENABLE scheme [10]. Initially, KDC selects a particular elliptic curve over a finite field $GF(p)$ (where p is a prime) and publishes a base point P with a large order q (where q is also a prime). It picks a random number $x \in GF(p)$ as a private key, and publishes its corresponding public key $Q = x \times P$. It also generates a random number $x_i \in GF(p)$ as a private key for a sensor s_i and generates a corresponding public key $Q_i = x \times P$. The key-pair $\{x_i, Q_i\}$ is then loaded to s_i. For each node in CN and DA layers, it generates this key-pair based on the base P by itself since it is more powerful than a sensor node. After this step, every node in the network has an ECC key-pair which will be used to establish secret (symmetric) key for secure communication. The proposed scheme is based on Elliptic Curve Diffie-Hellman (ECDH) [34] to establish a shared secret key between two nodes.

2) *Authentication and Access Control Protocol*

MAACE is enhanced from our previous work (ENABLE [10]) to meet security requirements in healthcare environment. We consider a situation that a medical practitioner or a healthcare server (generally called *Alice*, or *A*) wants to access data from a particular sensor, a group of sensors, or data on the coordination node. Similar to ENABLE scheme, *Alice* obtains the base P from a KDC and generates her private key (k_A) and public key $Q_A = k_A \times P$. KDC issues a proper access control list ac_A via a certificate $cert_A$. The ac_A list has similar structure as ENABLE scheme [10] (see Figure 4). We use the same notations as presented in TABLE I.

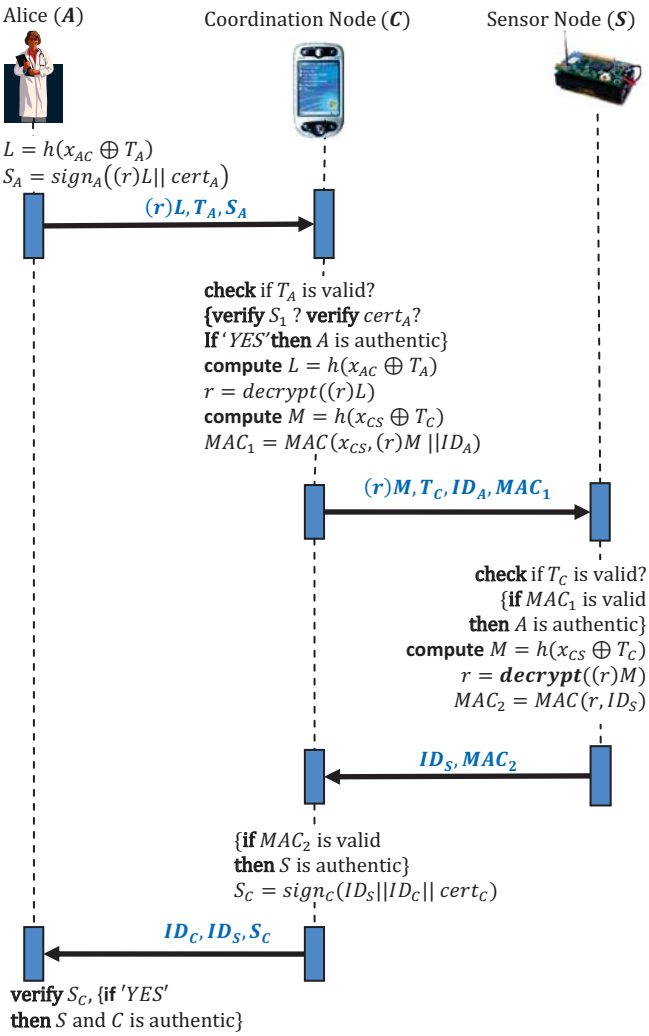

Figure 8 MAACE protocol

MAACE protocol is described in Figure 8, which includes the following steps.

- **Step 1.** $Alice \rightarrow C: (r)L, T_A, S_A$

Alice selects a random number $r \in GF(p)$ which will be used as a session key with C and S, creates a secret key $L = h(x_{AC} \oplus T_A)$ (where T_A is the current timestamp generated by *Alice*), and encrypts r with the key L (i.e. $(r)L$). *Alice* then signs this encrypted value along with its certificate (i.e. $S_A = sign_A((r)L \,||\, cert_A)$) and sends a combination $(r)L, T_A, S_A$ to the sensor *S*.

- **Step 2.** $C \rightarrow S: (r)M, T_C, ID_A, MAC_1$

Upon receiving the message from *Alice*, node C first checks if the timestamp T_A is valid (i.e. by verifying if $T_A < T_{now}$, where T_{now} is current timestamp). Then it

verifies *Alice'* signature S_A. If valid, then *Alice* is authentic to C. *Alice's* certificate $cert_A$ is also verified to check the validity of the access list ac_A which was assigned to her. *Alice* is authorized if $cert_A$ is valid. Node C now constructs a secret key $L = h(x_{AC} \oplus T_A)$, and decrypts $(r)L$ to get r. It then generates a secret key $M = h(x_{CS} \oplus T_C)$ (where T_C is the timestamp created by C), encrypts r, and builds a MAC value (i.e. $MAC_1 = MAC(x_{CS}, (r)M \,||\, ID_A)$). Finally, the coordination node C sends $(r)M, T_C, ID_A, MAC_1$ to S.

- **Step 3.** $S \rightarrow C: ID_S, MAC_2$

When S receives the message, it checks if $T_C > T_{now}$. Then, it verifies MAC_1 value. If valid, it indicates that *Alice* is authentic to S. After that, S constructs the secret key $M = h(x_{CS} \oplus T_C)$ and decrypts $(r)M$ to get r. Using this secret key, S builds a *MAC* ($MAC_2 = MAC(r, ID_S)$ and sends to *Alice*. Node S sends ID_S, MAC_2 to node C.

- **Step 4.** $C \rightarrow A: ID_C, ID_S, S_C$

Node C verifies MAC_2. If valid, it generates a signature $S_C = sign_C(ID_S||ID_C)$ and sends ID_C, ID_S, S_C to Alice.

Upon receiving the ID_C, ID_S, S_C from C, *Alice* verifies C's signature S_C. If valid, then S and C is authentic to *Alice*.

VII. Security Analysis

Note that security level of the proposed protocol depends on the security level of ECC signature, message authentication code (CBC-MAC), and encryption algorithm (RC5). Those have been proven secure in literature. So in the scope of this paper, we focus on possible vulnerabilities to the proposed protocol.

A. It provides mutual authentication

In *step 2* of the protocol, node C verifies the signature S_A. If S_A is valid, then the user is authentic to C because only *Alice* can generate the signature S_A by his private key. Consequently, the user is also authentic to sensor S because S trusts C (*step 3*). On the other hand, only S shares the secret key x_{CS} with C. It means that only S can decrypt (r)M (where $M = h(x_{CS} \oplus T_C)$). So if S can achieve r from $(r)M$ to build $MAC_2 = MAC(r, ID_S)$), then S is authentic to the user. The mutual authentication is provided through trust relations between $Alice - C$, and $S - C$.

B. It can defend against replay attacks

There are two possible ways for an adversary to launch replay attacks as follows:

- The adversary can intercept the message sent out from *Alice* (in *step 1*) or from the sensor S (*step 3*). However, both cases are not possible in MAACE because C can easily detect by verifying timestamp T_A (*step 3*). If T_A is older than a predefined threshold, it is invalid because it has been used for previous authentication. If T_A was changed, then S_A ($S_A = sign_A((r)L \,||\, cert_A)$, where $L = h(x_A \oplus T_A)$) is not valid.
- The adversary can intercept the message sent out from C (*step 2*). Node S can detect by checking timestamp T_C. If T_C is older than the predefined threshold, it is not valid. If T_C has been changed to T_C^*, then the MAC_1^* value ($MAC_1^* = MAC(x_{CS}, (r)M \,||ID_A)$, where $M = h(x_{CS} \oplus T_C^*)$ is not consistent to MAC_1.

C. It can mitigate DoS attack

Upon receiving the message from C (*step 2*), sensor node S first checks the validity of timestamp T_C. If it is not valid, then S discards the message. Otherwise, it computes a MAC value to compare with MAC_1 received. A message authentication code (MAC) generation, e.g. CBC-MAC algorithm, is very fast [28]. A CBC-MAC operation on Mica2 mote takes 3.12 ms [28], which is very fast compared to ECC point multiplications used by HBQ (which in total takes 3.5 s, about 1121 times longer). Therefore, the proposed scheme significantly reduces *DoS* compared to HBQ.

VIII. Performance Evaluation

A. Analysis-based Performance Evaluation

This section presents performance analysis of the proposed scheme and compares with ENABLE [10] and HBQ [14]. Since *Alice* and coordination node C are powerful devices, the computational overhead is trivial compared to that of the sensors. Therefore, we only consider computational overhead for sensors. We use the computational overhead (the computation time required by sensors, denoted by *T*) to analyze the performance. According to practical implementations on Mica2 motes [21][28][15], the computational time of each security primitives is listed in TABLE II.

TABLE II Execution Times On Mica2

Notation	Description	Time (ms)
T_H	Time to perform one-way hash function (e.g. SHA-1)	3.636
T_{MAC}	Time to generate MAC value (e.g. CBC-MAC)	3.12
T_{RC5}	Time to encrypt/decrypt by RC5	0.26
T_{MUL}	Time to perform ECC point multiplication	810

The total computational time of the proposed scheme, ENABLE, and HBQ are shown in TABLE III. In MAACE, both user authentication and node authentication take $2T_{MAC}+T_H+T_{RC5}$. For user authentication, ENABLE requires $1T_{MAC}$ (approximately 3.12 ms), while HBQ scheme requires $2T_H$, $2T_{MAC}$, $2T_{RC5}$, and $3T_{MUL}$ (total cost is approximately 2,451.04 ms). For node authentication, ENABLE requires $2T_{MAC}+1T_{RC5}+1T_H$, while HBQ scheme does not support it. Based on TABLE II, MAACE takes only 10.136 ms, which is less than ENABLE (13.256 ms) and HBQ

(2,451.04 ms). We used the formula $E = U*I*t$ to estimate the energy consumption of security computations [27][28]. For Mica2 mote, when processor is in active mode, $I = 8$ *mA*. Typically, $U = 3.0$ *V* if two new AA batteries are used [28]. Total energy consumption is shown in Figure 9. Our approach consumes 0.24 *mJ*, which is more efficient than ENABLE (0.381 *mJ*) and HBQ (58.82 *mJ*).

TABLE III COMPARISON OF COMPUTATIONAL TIME

	MAACE	ENABLE	HBQ
User Authentication	$2T_{MAC}+T_H+T_{RC5}$	T_{MAC}	$2_{TH}+2T_{MAC}+T_{RC5}+3T_{MUL}$
Node Authentication		$2T_{MAC}+1T_{RC5}+1T_H$	None
Total	$2T_{MAC}+T_H+T_{RC5}$	$2T_{MAC}+1T_{RC5}+1T_H$	$2T_H+2T_{MAC}+2T_{RC5}+3T_{MUL}$
Total Time	10.136 *ms*	13.256 *ms*	2,415.04 *ms*

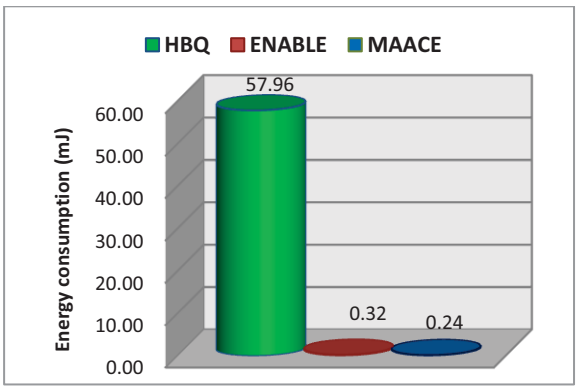

Figure 9 Comparison of energy consumption

B. Simulation-based Performance Evaluation

We customized SENSE simulator (*Sensor Network Simulator and Emulator*) [36] to simulate and evaluate performance of MAACE in terms of energy consumption and delay. Since SENSE only provides energy consumption and delay for communication, we have modified it to compute security computational cost. Our simulation results included not only security computational cost, but also communicational cost to transmit security messages. Since the coordination nodes are much more powerful than sensors, we only considered energy consumption of the sensor nodes.

For the simulation, 400 sensors and 20 CHs were randomly distributed in a 2000 m × 2000 m area. The transmission range of sensor *S* and coordination node *C* is 60 m and 150 m, respectively. For communication, we used the same energy model used in *ns-2.1b8a* [37] that requires 0.66 W, 0.359 W, and 0.035 W for transmitting, receiving, and idling, respectively. We set the power consumption rate according to [28] for SHA-1 and CBC-MAC calculation 0.48 W. As analyzed in [28][38], we set the time consumption for computing a CBC-MAC and SHA-1 is 7.1 ms and 3.5 ms, respectively. At the link layer, the simulation used Medium Access Control (MAC) 802.11 Distributed Coordination Function (DCF). Two-ray ground was used as the radio propagation model. At the network layer, *Ad hoc On-Demand Distance Vector* (AODV) was used for routing protocol. User ID length is 8 bytes, SHA-1 value is 20 bytes. As discussed in [28], the choice of 4-bytes MAC is not security detrimental in the context of sensor networks. Therefore, we applied 4-byte CBC-MAC for every message. We repeated a hundreds scenarios, in which location of user and the sensor node *S* was randomly selected. The results were then averaged for all scenarios.

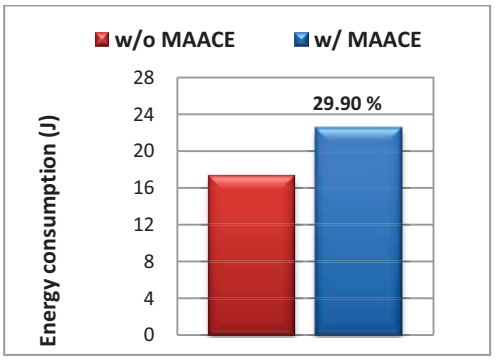

Figure 10 Energy consumption

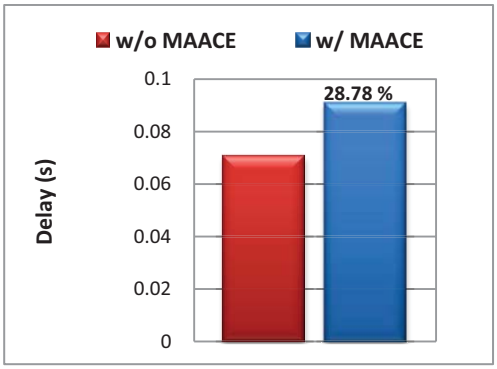

Figure 11 Delay performance

The results are shown in Figures 10 and 11, which compare energy consumption and delay of cases without (w/o) and with (w/) MAACE. For the former case, there were only plain messages transferred between the user and accessed node. In the latter case, all MAACE security computations and communications were taken into account. As shown in Figure 10, w/ MAACE computation and communication cost is 22.48 J, while w/o MAACE is 17.31 J. That means MAACE only increases only by 29.9 % energy consumption. In Figure 11, w/ MAACE delay is 90.74 ms, which is longer 28.78 % compared with the case of w/o MAACE (70.5 ms).

In summary, the simulation results have shown a small increment of MAACE cost compared with a normal communication. Besides, it is important to note that MAACE is only performed once for a number of data communications. Therefore, such energy consumption and delay are insignificant for the network.

IX. Conclusion And Future Work

One of the most critical security concerns before deploying a WSN in healthcare applications is patient privacy because their vital signs and activities are monitored all the time. To achieve this, authentication and access control must be enforced to ensure that only authenticated healthcare professionals can access, and further can access data that they have privilege for their healthcare services. This paper introduces a public key cryptography called Mutual Authentication and Access Control based on Elliptic Curve Cryptography (MAACE). MAACE provides mutual authentication (a healthcare professional can authenticate to an accessed node (a PDA or medical sensor) and vice versa) and ensures a healthcare professional can only access data that he/she has privilege. By applying elliptic curve cryptography, MAACE provides a public key approach, which is more scalable and requires lesser memory compared to symmetric key-based schemes. Its performance makes it practically feasible to be implemented on sensor platforms. Security analysis and performance evaluation results have shown that MAACE is 238 times and 1.3 times faster than HBQ and ENABLE, respectively. In addition, MAACE consumes 0.41 % and 75 % energy compared to HBQ and ENABLE, respectively. The simulation results have shown that MAACE only increases energy consumption and delay about 30 % compared to a normal communication. However, since MAACE is only performed once for a number of data communications, such energy consumption and delay are insignificant for the network.

One of the main issues in ECC is that Point Multiplication operation takes significant time (810 ms) (and consequently, increases energy consumption) compared with Point Adding. Reducing the ECC's Point Multiplication operation cost will be our next goal to provide a more secure and energy-efficient scheme for WSNs. Another future work is to implement MAACE on Crossbow Mica2 motes [39] in order to observe its real performance.

Acknowledgment

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency)" (NIPA-2009-(C1090-0902-0002)).

References

[1] K. Lorincz, D. Malan, T. F. Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, S. Moulton, M. Welsh, *Sensor Networks for Emergency Response: Challenges and Opportunities*, , IEEE Pervasive Computing, Oct/Dec, 2004, pp. 16-23.

[2] http://fiji.eecs.harvard.edu/CodeBlue

[3] R. Jafari, R.Bajcsy, S. Glaser, B. Gnade, M. Sgroi, S. Sastry. *Platform Design for Health-care Monitoring Applications*, Joint Workshop on High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and-Play (MD PnP) Interoperability, June 2007, Boston, MA.

[4] http://bsn.citris.berkeley.edu/home/

[5] http://web.mit.edu/wockets/

[6] http://smart.csail.mit.edu/

[7] http://www.mobihealth.org/

[8] http://www.doc.ic.ac.uk/vip/ubimon/home/index.html

[9] Trossen, D.; Pavel, D.; *Sensor Networks, Wearable Computing, and Healthcare Applications*. IEEE Pervasive Computing. Vol. 6(2), April-June 2007, pp. 58 – 61.

[10] X. H. Le, S. Lee, I. Butun, M. Khalid, R. Sankar, M. Kim, M-H. Han, Y-K. Lee, H. Lee. *An Energy-Efficient Access Control Scheme for Wireless Sensor Networks based on Elliptic Curve Cryptography*. Journal of Communications and Networks, Special Issues on Secure Wireless Networking, December 2009 (in press).

[11] X. H. Le, R. Sankar, M. Khalid, and S. Lee, Public Key Cryptography - based Security Scheme for Wireless Sensor Networks in Healthcare, *4th International Conference on Ubiquitous Information Management and Communication* (ICUIMC), Suwon, Korea, January 2010 (in press).

[12] M. Das, Two-Factor User Authentication in Wireless Sensor Networks, IEEE Transactions on Wireless Communications, Vol. 8(3), March 2009, pp. 1086-1090.

[13] B. Vaidya, M. Chen, J.J.P.C. Rodrigues, Improved Robust User Authentication Scheme for Wireless Sensor Networks, Fifth IEEE Conference on Wireless Communication and Sensor Networks (WCSN), Allahabad, India, 2009, pp. 1-6.

[14] H. Wang, B. Sheng, Q. Li, *Elliptic curve cryptography-based access control in sensor networks*, Int. J. Security and Networks, Vol. 1, Nos. 3/4, pp.127–137 (2006).

[15] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-it CPUs. In CHES 2004, Vol. 3156, LNCS , pp.119-132.

[16] W. Du, J. Deng, Y. Han, P. Varshney, *Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge*. IEEE Trans. Depend. Secure 2006, 3, 62–77.

[17] X. H. Le, S. Lee, Y-K. Lee, H. Lee. A Secure Coordination - based Data Dissemination for Mobile sinks in Sensor Networks. IEICE Transaction on Communication, 2009, Vol E92-B(01).

[18] X. H. Le, N. Canh, S. Lee, Y-K. Lee, H. Lee. An Energy-Efficient Secure Routing and Key Management Scheme for Mobile Sinks in Wireless Sensor Networks using Deploying Knowledge. Journal of Sensor, Special Issue "Wireless Sensor Technologies and Applications", 2008, Vol.8(12) pp. 7753-7782.

[19] H. S. Ng, M. L. Sim, C. M. Tan. Security issues of wireless sensor networks in healthcare applications. BT Tech. Journal, Vol. 24 No 2, 2006, pp. 138 – 144.

[20] A. Boukerche and R. Yonglin, *A secure mobile healthcare system using trust-based multicast scheme*. IEEE J. Selected Areas Comm., vol 27(4), 2009 pp:387 – 399.

[21] R. Chakravorty, *A Programmable Service Architecture for Mobile Medical Care*. 4th IEEE International Conference on Pervasive Computing and Communications, 2006.

[22] J. Kim, A. R. Beresford, and F. Stajano, *Towards a Security Policy for Ubiquitous Healthcare Systems*, Proc. 1st International Conference on Ubiquitous Convergence Technology, pp. 263–272, 2006.

[23] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, *Physiological Signal Based Entity Authentication for Body Area Sensor Networks and Mobile Healthcare Systems*, Proc. 27th Annual International Conference of Engineering in Medicine and Biology Society, pp. 2455–2458, 2005.

[24] C.-W. Jeong, D.-H. Kim, and S.-C. Joo. *Mobile Collaboration Framework for u-Healthcare Agent Services and Its Application Using PDAs*, Proc. 1st KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, pp. 747–756.

[25] M. Markovic, Z. Savic, and B. Kovacevic, Secure mobile health systems: principles and solutions, M-Health: Emerging Mobile Health Systems, Kluwer Academic Publishers, pp. 81–106, 2007.

[26] R. Marti, J. Delgado, and X. Perramon, Network and Application Security in Mobile e-Health Applications, Proc. International Conference on Networking Technologies for Broadband and Mobile Networks, pp.995–1004, 2004

[27] Y. M. Huang, M. Y. Hsieh, H.C. Chao, S. H. Hung, J. H. Park, *Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks*. IEEE Journal on Selected Areas in Communications, Vol. 27, No 4, May 2009.

[28] C. Karlof, N. Sastry, D. Dagner, *TinySec: A Link Layer Security Architecture for Wireless Sensor Networks*. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys04), Baltimore, Maryland, November 2004; pp. 162-175.

[29] S. Zhu, S. Setia, S. Jajodia, LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. ACM Trans. Sens. Netw. 2006, 2, 500–528.

[30] A. Biryukov, C. Cannière, G. Dellkrantz, Cryptanalysis of SAFER++. CRYPTO 2003: 195-211.

[31] W. Joppe, M. Kaihara, T. Kleinjung, A. K. Lenstra, and P. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography Cryptology, Report on Cryptology ePrint Archive, Vol. 389, 2009.

[32] V. Miller, Use of elliptic curves in cryptography, CRYPTO 85, 1985.

[33] N. Koblitz, Elliptic curve cryptosystems, in Mathematics of Computation 48, 1987, pp. 203–209.

[34] ANSI X9.63, Elliptic Curve Key Agreement and Key Transport Protocols, American Bankers Association, 1999.

[35] R. Rivest, The RC5 Encryption Algorithm. Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994e. pp. 86–96.

[36] G. Chen, J. Branch, M. J. Pflug, L. Zhu, B. Szymanski, SENSE: A Sensor Network Simulator, Advances in Pervasive Computing and Networking; Springer, NY, 2004; pp. 249-269.

[37] NS-2, http://www.isi.edu/nsnam/ns

[38] H. Lee, Y. Choi, H. Kim, Implementation of TinyHash based on Hash Algorithm for Sensor Network. Proceedings of World Academy of Science, Engineering and Technology vol.10 December 2005.

[39] Wireless Measurement System, MICA2", Crossbow Technology, Inc.41 Daggett Dr. San Jose, CA 95134

Xuan Hung Le received BS degree in Computer Science from Hanoi University, Vietnam, in 2003, M.S, Ph.D degree in Computer Engineering from Kyung Hee University, Korea, in 2005 and 2008, respectively. From 2002 to 2003, he served as a software engineer at FPT Software Corporation, Vietnam. From Dec 2008 to Aug 2009, he was a research professor at Dept. of Computer Engineering, Kyung Hee University, Korea. Since Sept 2009, he has been a Postdoctoral Research Associate at Dept. of Electrical Engineering, University of South Florida, USA. His research interests are wireless sensor networks, cryptography and information security.

Murad Khalid received B.S. and M.S. degrees in Electrical Engineering from the City College of the City University of New York, USA, in 1993 and 1995, respectively. He is currently a research assistant working towards a Ph.D. degree in Wireless Communication and Networking area in the Department of Electrical Engineering at the University of South Florida. His research interests include mobile wireless communications and networks, with emphasis on cross-layer design, resource allocation and performance optimization of wireless Ad hoc networks. He was with Bahria University as the Asst. Professor in Computer Engineering Department. Before that, he served as senior systems engineer for Motorola, Bosch Telecom, and Ericsson Radio Systems.

Ravi Sankar received the B. E. (Honors) degree in Electronics and Communication Engineering from the University of Madras, India, in 1978, the M. Eng. degree in Electrical Engineering from Concordia University, in 1980, and the Ph.D. degree in Electrical Engineering from the Pennsylvania State University, in 1985. Since then, he has been with the Department of Electrical Engineering at the University of South Florida, Tampa. He is currently a USF Theodore and Venette Askounes-Ashford Distinguished Scholar Award winning Professor of Electrical Engineering, and Director of the Interdisciplinary Communications, Networking and Signal Processing (iCONS) Research group (http://icons.eng.usf.edu) and Interdisciplinary Center of Excellence in Telemedicine (ICE-T). His main research interests are in the areas of wireless communications, networking, signal processing and its applications. For further details see http://www.eng.usf.edu/~sankar/bio.html.

Sungyoung Lee received his BS in Material Science from Korea University in 1978, MS, PhD. in Computer Science from Illinois Institute of Technology, USA in 1987, and 1991, respectively. Since 1993, he has been a professor at the Dept. of Computer Engineering, College of Electronics and Information, Kyung Hee University, Korea. From 1992 to 1993, he was a assistant professor at the Dept. of Computer Science, Governors State University, University Park, USA. His research interest includes Ubiquitous Computing Middleware, Java Virtual Machine, Real-Time System, and Embedded.