SECURE AND EFFICIENT DATA TRANSMISSION IN WIRELESS MEDICAL SENSOR NETWORKS

#1M.Prasanth, #2 S.Madhavi

1B.Tech, Department of Computer Science and Engineering

2Assistant Professor, Department of Computer Science and Engineering

1,2 ManakulaVinayagar Institute of Technology

1vijiprasanth.prasanth2@gmail.com

2Madhavi11lakshmi @gmail.com

ABSTRACT

Wireless medical sensor networks (MSNs) have emerged as a promising technique which will revolutionize the way of seeking healthcare at home, hospital, or large medical facilities. E-healthcare collects patient's vital body parameters by wearable or implantable biosensors. However, designing a secure and efficient system for MSNs is a difficult task. In this paper, we propose a lightweight and secure system for MSNs. we have identified the security challenges facing an MSN for wireless health monitoring and then proposed a novel and lightweight system to achieve secure data transmission and access control for MSNs. The security analysis has demonstrated that our system can achieve the requirements of the protocol of this kind. Our system only requires symmetric-key encryption/decryption and hash operations and is thus suitable for low-power sensor nodes. To the best of our knowledge, this is the first secure data transmission and access control system for MSNs until now.

Index Terms: *MSNs, E-healthcare, symmetric-key encryption/decryption, hash operation.*

1. INTRODUCTION

An emerging application for wireless sensor networks involves their use in medical care. In a hospital or clinic, outfitting every patient with tiny, wearable wireless vital sign sensors would allow doctors, nurses and other caregivers to continuously monitor the status of their patients. In an emergency or disaster scenario, the same technology would enable medics to more effectively care for large numbers of casualties. First responders could receive immediate notifications on any changes in patient status, such as respiratory failure or cardiac arrest. Wireless sensors could augment or replace existing wired telemetry systems for many specific clinical applications, such as physical rehabilitation or long-term ambulatory monitoring.

We assume that the sensor network contains some sensor nodes that collect data from patients, one or more base stations to receive the data from the sensor nodes, and some relay nodes that deliver the data from the sensor nodes to the base stations. We classify potential security threats into two categories: outsider attacks and insider attacks. Outsider attacks are perpetrated by attackers who do not have control of a valid sensor node, base station, or any other nodes in the network. These attacks include, but are not limited to, the following: (1) eavesdropping on data; (2) spoofing of a base station to receive sensor data; (3) replay of previous queries to obtain sensor data; (4) modification or injection of data without the knowledge of the source or destination; (5) spoofing of a sensor to report forged data; and (6) replay of previous data. Among these attacks, (1)-(3) compromise the privacy of patient data, while (4)-(6) compromise the authenticity and integrity of patient data.

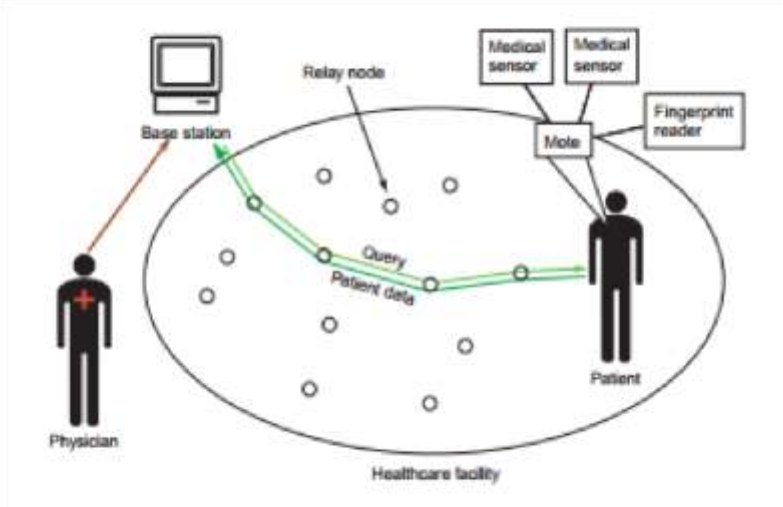

Figure 1 SNAP Architecture

Insider attacks are launched by attackers who have control of some nodes in the network. If the attacker controls a sensor node, s/he can easily forge data that appears to be from a legitimate patient. The attacker can also obtain any existing cached data in the node. If the attacker controls a base station, s/he can access the private data from the sensors. Insider attacks are much more difficult to handle, since other nodes cannot distinguish the attacker from a legitimate node by the use of shared secrets (by compromising a node, the attacker has access to these secrets).

Similar threats exist in traditional ad hoc wireless networks and other types of sensor networks. However, addressing these threats in a medical sensor network poses several unique challenges. First, there is a stringent expectation for the system to ensure the privacy of medical data. Second, sensor nodes have much lower processor speed, memory, link bandwidth, and energy supply than mobile PCs or PDAs, so the security mechanisms must be resource-efficient. Third, due to their small size, the individual sensors can be easily stolen or simply lost. Patient mobility also makes it more likely for patients to lose sensors (most other sensor networks have stationary sensors). Furthermore, attackers can easily find their targets in local hospitals or healthcare facilities, as opposed to remote locations like forests or battlefields. Hence, physical compromise of sensor nodes is more likely in medical sensor networks than in other types of sensor networks. Fourth, there may be many users (physicians, nurses, patients) who are authorized to access the data, so a scalable solution to authenticate the users must be provided to ensure the privacy of the data.

2. RELATED WORK

Despite the need and importance, to the best of our knowledge, until now no secure and lightweight data transmission and access control platform for MSNs has been proposed. For example, the designers of CodeBlue [4] and MUSIC [5] point out the need for security in a medical environment, but their work do not focus on addressing security issues. Recently, an architecture called “SNAP” (Sensor Network for Assessment of Patients) [6] has been proposed to address the security challenges facing a sensor network for wireless health monitoring. However, we observe that SNAP does not deal with user authentication for medical data. Moreover, the collected data from a biosensor is transmitted to the controller in plaintext. Thus, an adversary can easily modify the medical data and/or inject polluted medical data into the network. Some researchers (e.g., [7], [8]) utilize physiological signals (e.g., heart rate interval, blood flow, and electrocardiography) obtained from the patient to enable biosensors to agree upon a symmetric (shared) cryptographic key in an authenticated manner. However, they demand that each biosensor can measure the same physiological parameter, this assumption is rather restrictive and makes this method not suitable for many MSN applications.

Based on public key cryptography, some novel protocols (e.g., [9]–[12]) have been proposed to ensure security of MSNs. The authors of [9] suggest to use elliptic-curve cryptography (ECC) algorithm to set up symmetric keys between sensor nodes and the base station. Also, a novel group key management and authentication mechanism is presented. However, they are computation-inefficient, cannot fulfill the stringent delay requirements in MSNs and are vulnerable to DoS attacks. For instance, as reported in [9], the ECC key agreement takes 7.198 s on a Tmote Sky mote, which features a 16-bit, 8 MHz MSP430 processor. Additionally, as described in [10], the elliptic curve Diffie-Hellman (ECDH) key generation used in sensorto-sensor authentication takes 5.97 s on a Tmote Sky mote. As common biosensor nodes have less computation power than Tmote Sky motes, public key cryptography is not favorable for biosensor nodes.

Also, a lightweight identity-based cryptography named IBE-Lite has been proposed [11]. It balances security and privacy with accessibility. However, we observe that there are security weaknesses and efficiency problems in IBE-Lite. Firstly, all medical data are encrypted by ECC, which is not efficient for MSNs. Secondly, their work does not consider sensor-to-sink (or user) data authentication. Thus, false medical data could be injected or treated as legitimate due to the lack of node authentication. Thirdly, IBELite cannot resist node replication attacks. That is, an adversary can insert additional hostile biosensors into the network. Fourthly, the master key of each PAN consists of n secret keys, which are picked by the patient. Each doctor uses the secret key from the certificate authority to decrypt the messages encrypted by a sensor node. Once a doctor sends n user queries to a target PAN, he/she is able to generate the master key of the PAN. Thus, to ensure the security of IBE-Lite, the number of use queries has to be limited. Le et al. [12] presented a mutual authentication and access control protocol, which is based on ECC. A recent study [13] has shown that the scheme is susceptible to information-leakage attacks.

Although there are a lot of works about generic WSNs and mobile ad hoc networks (MANETs) security (e.g., [14]–[16]), these mechanisms are not directly applicable in MSNs due to the unique and challenging operational and security requirements of MSNs. For instance, the authors of [14] introduce a novel approach to ensure distributed privacy-preserving access control, which is built on a ring signature technique. Also, in [15], a self-contained public key-management scheme has been proposed for wireless ad hoc networks, in which a small number of cryptographic keys are stored offline at individual nodes before deployment. Also, to avoid the weaknesses of a public key infrastructure, as a special form of public key cryptography, identity-based cryptography has been used in various areas of securing MANETs [16]. Unfortunately, as described before, solutions relying on public key cryptography are not directly applicable to MSNs.

3. OUR CONTRIBUTION

In this paper makes three main contributions:

(1) We show the security weaknesses and efficiency problems of the existing security systems in MSNs. Then we identify the characteristics of an MSN and present the requirements of a secure and lightweight system of MSNs. Considering the special features of an MSN, a powerful mobile adversary is introduced into MSNs.

(2) We propose a secure and lightweight system for MSNs, which not only enables lightweight key management but also provides fine-grained access control in MSNs. In addition, our theoretical analysis demonstrates that the proposed system can meet the requirements.

(3) We also implement the proposed system in a network of resource-limited sensor nodes and laptop PCs. Evaluation results show the efficiency of the system in practice. Accordingly, some suggestions on how to set the parameters of the proposed protocols are provided.

3.1 NETWORK MODEL, A DIVERSARY MODEL AND UNIQUE FEATURES OF MSNS

A. Unique Features of MSNs

MSNs are different from MANETs and WSNs in the following aspects [2].

(1) Data Rate: Events monitored by MANETs and WSNs usually occur at irregular intervals. On the contrary, MSNs are employed to monitor humans' physiological activities, which more or less may occur periodically. As a result, data streams of applications exhibits relatively stable rates. All nodes are assumed to have loosely synchronized clocks with the help of some existing secure time synchronization scheme. (2) Mobility: Relatively, there is no movement between sensors as they are all in the same patient. Movement between controllers and sensors is due to mobility of patients, which is very low. (3) Efficiency: The sensed signals can be efficiently processed by biosensors to obtain estimates of physiological information. Also, the power consumption on biosensors is low and thus batteries can last longer.

B. Network Model

All biosensor nodes in an MSN have limited power sup-ply, storage space and computational capability. Due to the constrained resources, computationally expensive and energy-intensive operations such as public key cryptography are not favorable for such nodes. We assume that the network server is secure. That is, the network server is equipped with a tamper-resistant component for storing the keying materials. According to the data rate feature of an MSN described in Section III.A, we assume that time is divided into equal and fixed collection rounds and each biosensor collects a single data item per round. The sensor nodes may be placed in, on or around the patient's body. Although there is no consensus on the communication technologies in PANs, the communication ranges of off-the-shelf technologies (e.g., Zigbee) are larger than 3 m. Thus, according to the mobility feature of an MSN described in Section III.A, we assume that all sensor nodes in a PAN can directly communicate with the controller, thus a star topology is assumed.

C. Adversary Model

We assume that an adversary can behave as both outside and inside attackers. Outside attackers can drop messages by jamming the communication channel, eavesdrop messages, modify messages, inject forged messages or replay old messages. Insider attackers can compromise a number of biosensor nodes, controllers and network users to obtain their data and keying materials. Considering the special features of an MSN, a powerful mobile adversary [17] is introduced into MSNs. One important feature that separates it from other adversary models is its mobility. More specifically, the adversary can compromise different subsets of biosensors in different time intervals.

The subset of compromised nodes might not be clustered or contiguous, that is, concurrently compromised nodes can be spread over the entire MSN. While in control of a biosensor node, the adversary acquires keying materials and status, reads all storage/memory, and can eavesdrop on all incoming and outgoing communications of the compromised node. There are two reasons to consider such a mobile adversary model. Firstly, since the biosensors are in, on or around the body of the patient, the compromised biosensors are easily detected by the patient or the health staff. Thus, the adversary roams around the MSN gradually to avoid being detected. Secondly, it is extremely difficult for the adversary to predict a patient's movement and follow him/her everywhere. As a result, the adversary may inevitably lose control of the already compromised biosensor nodes.

4. THE REQUIREMENTS OF A SECURE SYSTEM

In this section, we present several criteria that represent desirable characteristics in a secure and lightweight system for MSNs.

(1) Lightweight: Every PAN often consists of low-end sensor nodes, which rely on battery energy [1]. Furthermore, emergency situations in an MSN require the capability for fast medical reaction without disabling security functions. For example, secure PAN setup in emergency situations must be carried out in less than one second and the maximum allowable latency for electrocardiogram transmission is 250 ms [18]. To match the low-capabilities of the sensor nodes, it is important to minimize computation, communication and storage over-head on the sensors. Hence, cryptographic algorithms must be as fast as possible in order to satisfy these requirements and be invulnerable to DoS attacks.

(2) Fine-grained data access control: Access control needs to be enforced for patient-related data in the whole MSN so that private information will not be obtained by unauthorized users. More importantly, a secure system should provide different privileges for different network users.

(3) Scalability: The system should be efficient even in a large scale MSN with many users and many PANs [1].

(4) Flexibility: The access policy should be adapted dynamically to contexts, such as time, location, or certain events related to patients. Note that in MSNs, the access policy should be defined by both patients and healthcare units. For example, on-demand authorization to read a patient's PHI can be given temporarily to an available doctor who is not on the access list when a medical emergency happens. Obviously, inability or irresponsiveness in adapting the access rules may threaten a patient's life [1].

(5) Confidentiality: In order to prevent patient-related data from leaking, the data needs to always be kept confidential at a node or local server (i.e., the network server). Data con-fidentiality should be resistant to device compromise attacks (e.g., node compromised and controller compromised attacks). That is, compromising one node helps the adversary to gain nothing or little from the data stored at that node.

(6) Data integrity assurance: In MSNs the patient-related data is vital, and modified data would lead to disastrous consequences. Therefore, data integrity shall be protected all the time.

(7) Forward secrecy: It means that even if an adversary obtains the current secrets of a node, it cannot decrypt (or forge authentication tags for) those data collected and encrypted (or authenticated) before compromise.

(8) Backward secrecy: It means that even an adversary has compromised (and then released) a node, it cannot decrypt (or forge authentication tags for) those data collected and encrypted (or authenticated) by the node after releasing.

(9) Strong contextual privacy preservation: We divide privacy issues in MSNs into content oriented privacy and contextual privacy. Here we just focus on contextual privacy, since the content oriented privacy has been considered in Requirements (5), (7) and (8). Contextual privacy means an adversary has the ability to link the source and the destination of a message. In an MSN, if an adversary can link the patient with a specific physician, then the patient's privacy will be lost. Thus, it is very important to protect contextual privacy, which includes sensor identity privacy and PAN identity privacy of every collected data, and each user's privilege content privacy in addition to the privacy of every user command content.

For example, if an adversary searches the whole MSN for a specific parameter, protecting the privacy of sensor identity of every collected data is desirable. Similarly, if an adversary searches the whole MSN for a specific patient, protecting the privacy of PAN identity of every collected data is desirable. In addition, we illustrate the importance of user privilege content privacy by considering the following two scenarios. One is that often each user's privilege content indicates the user identity information and the relation between the user and some patients (i.e., the owner of some PAN), thus exposing the patients' privacy. The other is that with the knowledge of some user privileges, an adversary can seek the important users and then launch attacks on the MSNs.

4.1 THE BASIC IDEA OF OUR SYSTEM

The basic idea of the proposed system is given as follows. After a user registers to the network server, he/she is allowed to issue commands to access the collected PHI or control the biosensors according to his/her privilege. To achieve this goal, proxy-protected signature by warrant (PSW) [19] is introduced into our system. This technique is a special digital signature. There are two kinds of participants, i.e., an original signer and proxy signers. The original signer gives the proxy signer a warrant, which specifies the identity of the proxy signer, the identity of the original signer, the expiration time of the delegation of signing power, etc. The proxy signer generates proxy signatures only with the proxy signature key given by the original signer. Verifiers validate proxy signatures only with the public key of the original signer and pay attention to the legality of the warrant.

The detailed information about applying the PSW technique into the proposed system is given as follows. The network server of an MSN plays the role of original signer while the users of the MSN play the role of proxy signers. Through registration, the users obtain one or more proxy signature keys from the network server before they enter to an MSN. The key can subsequently be used to make signature on a command. Thus, authorized users generate valid commands only with the proxy signature keys given by the network server. The validity of each command can be verified by the controller of any PAN or the network server with the public key. Through this way, the network server can prevent unauthorized commands on the MSN. Additionally, our proposed system only requires lightweight cryptographic operations (i.e., symmetric-key encryption/decryption and hash function operation) and do not need verification tables to be stored on a biosensor. Hence the computational and storage requirement on a biosensor is low.

Quite a number of of PSW schemes have been proposed in the literature. However, some of them suffer from some security weaknesses, and most of them are not efficient enough for biosensors. After a thorough evaluation, we have found that Shao's PSW scheme [20] is most suitable for our purpose. However, in spite of its efficiency, we observe that this scheme has a design weakness, which will cause failure of the proposed protocol. Thus, to ensure that the proposed protocolworks, a feasible approach has been proposed to fix such aweakness.

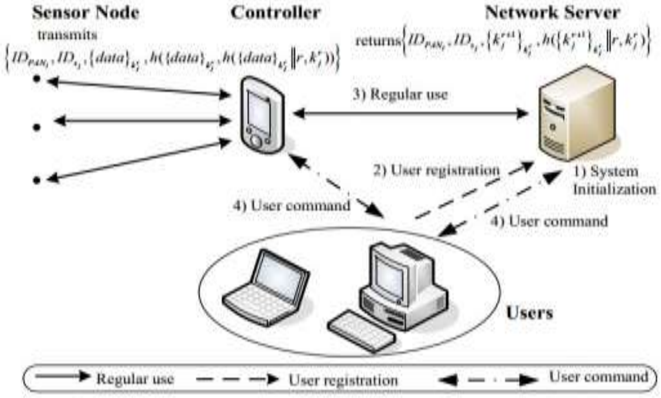
Sensor Node
Controller
Network Server
transmits
$\{ID_{PAN_i}, ID_{s_j}, \{data\}_{k_j^r}, h(\{data\}_{k_j^r}, h(\{data\}_{k_j^r} \| r, k_j^r))\}$
returns $\{ID_{PAN_i}, ID_{s_j}, \{k_j^{r+1}\}_{k_j^r}, h(\{k_j^{r+1}\}_{k_j^r} \| r, k_j^r)\}$
3) Regular use
2) User registration
1) System Initialization
4) User command
4) User command
Users
Regular use
User registration
User command

Figure 2 The flows of security information in the proposed system.

Our system involves four phases. The system initialization phase is performed by the network server to set up an MSN. User joining phase is involved before a user can issue commands to the MSN. During the regular use phase, the data from each biosensor node is securely transmitted to the network server via the controller. In the user command phase, if a network user has a new command, he/she will need to construct the command and the proxy signature and then send them to the network server (or the controller of a target PAN). If the command verification passes, the network server (or the controller of a target PAN) responds to the user's command. Fig. 2 illustrates the flows of security information of the proposed system. More detailed description will be provided in the following subsections.

4.2 CONTEXTUAL PRIVACY PRESERVATION EXTENSION

Note that the current system cannot provide strong contex-tual privacy preservation, i.e., Requirement (9) is not satisfied yet. More exactly, there are four issues about this requirement exist in the system as follows.

(1) Command exposure: The commands from users are transmitted in plaintext in free air.

(2) Warrant exposure: The warrant from a user, which indicates the user privilege, is transmitted in

plaintext in open environment.

5. CONCLUSION

In this paper, we have identified the security challenges facing an MSN for wireless health monitoring and then proposed a novel and lightweight system to achieve secure data transmission and access control for MSNs. The security analysis has demonstrated that our system can achieve the requirements of the protocol of this kind. We have implement-ed the protocols on real mobile devices and sensor platforms with limited-resource. Experimental results have shown that our approaches are feasible for real-world applications.

REFERENCES

[1] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnay-der, G. Mainland, S. Moulton, and M. Welsh, “Sensor networks for emergency response: challenges and opportunities,” IEEE Pervasive Computing, vol. 3, no. 4, pp. 16-23, Oct. 2004.

[2] J. Choi, B. Ahmed, and R. Gutierrez-Osuna, “Development and evalua-tion of an ambulatory stress monitor based on wearable sensors,” IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 2, pp. 279-286, Mar. 2012.

[3] D. He, C. Chen, S. Chan, and J. Bu, “DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks,” IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.

[4] V. Shnayder, B.-R. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsh, “Sensor networks for medical care,” Technical Report TR-08-05, Harvard University, 2005.

[5] Crossbow Solutions Newsletter. Motes for mobile communication and tele-medicine. 2005. [6] K. Malasri and L. Wang, “Addressing security in medical sensor networks,” in Proc. ACM HealthNet, pp. 7-12, 2007.

[7] R. Rajasekaran, V. Manjula, V. Kishore, T. Sridhar, and C. Jayakumar, “An efficient and secure key agreement scheme using physiological signals in body area networks,” in Proc. ICACCI, pp. 1143-1147, 2012.

[8] H. Wang, H. Fang, L. Xing, and M. Chen, “An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN),” in Proc. IEEE ICC, pp. 1-5, 2011.

[9] K. Malasri and L. Wang, “Design and implementation of a secure wireless mote-based medical sensor network,” Sensors, vol. 9, no. 8, pp. 6273-6297, Aug. 2009.

[10] S. Keoh, “Efficient group key management and authentication for body sensor networks,” in Proc. IEEE ICC, pp. 1-6, 2011.

[11] C. C. Tan, H. Wang, S. Zhong, and Q. Li, “IBE-lite: A lightweight identity-based cryptography for body sensor networks” IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 6, pp. 926-932, Nov. 2009.

[12] X. Le, M. Khalid, R. Sankar, and S. Lee, “An efficient mutual au-thentication and access control scheme for wireless sensor network in healthcare,” Journal of Networks, vol. 6, no. 3, 355-364, 2011.

[13] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," sensor, vol. 12, pp. 55-91, 2012.

[14] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3472-3481, Oct. 2011.

[15] W. He, Y. Huang, R. Sathyam, K. Nahrstedt, and W. Lee, "SMOCK: A scalable method of cryptographic key management for mission-critical wireless ad-hoc networks," IEEE Trans. Information Forensics and Security, vol. 4, no. 1, pp. 140-150, Mar. 2009.

[16] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," IEEE Commun. Surveys & Tutorials, vol. 14, no. 2, pp. 380-400, Second Quarter 2012.

[17] D. Ma and G. Tsudik, "Security and privacy in emerging wireless networks," IEEE Wireless Commun., vol. 17, no. 5, pp. 12-21, Oct. 2010.

[18] C. Cordeiro and M. Patel, "Body area network standardization: present and future directions," in Proc. BodyNets '07, pp. 1-2, 2007.

[19] Z. Shao, "Provably secure proxy-protected signature schemes based on RSA," Computers & Electrical Engineering, vol. 35, no. 3, pp. 497-505, May 2009.

[20] Z. Shao, "Proxy signature schemes based on factoring," Information Processing Letters, vol. 85, no. 3, pp. 137-143, 2003. [21] K. C. Barr and K. Asanovi, "Energy aware lossless data compression," ACM Trans. Comput. Syst., vol. 24, no. 3, pp. 250-291, Aug. 2006.

[22] OpenSSL, http://www.openssl.org.

[23] TinyOS: An open-source OS for the networked sensor regime. http://www.tinyos.net/.

[24] J. Lee, K. Kapitanova, and S. Son, "The price of security in wireless sensor networks," Computer Networks, vol. 54, no. 17, pp. 2967-2978, Dec. 2010.

[25] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proc. IPSN, pp. 245-256, 2008.

[26] Software AES, http://tinyos.cvs.sourceforge.net/viewvc/tinyos/tinyos-2.xcontrib/crypto/index.html

[27] A. Milenkovi, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," Computer Communications, vol. 29, no. 13-14, pp. 2521-2533, Aug. 2006.