Wireless Body Area Network for Remote Healthcare Monitoring

Prasad S P
Assistant Professor, Department of ISE,
City Engineering College,
Bangalore -560 061
prasadsp.prakash@gmail.com

Deepa P
Assistant Professor, Department of ISE,
City Engineering College,
Bangalore -560 061
palanisamy.deepa@gmail.com

Abstract- A case study of security risk analysis of a wireless body area network for remote health monitoring as a after measure for deploying security and privacy features is introduced in this paper. The target system has a scalable platform that requires minimum human interaction during setup and monitoring. The core components of the system include: (i) biosensor/transceiver pairs, (ii) hardware modules to automatically setup the wireless body area network, (iii) data delivery mechanism to an internet sever, and (iv) automatic data collection, profiling and reporting. As the system contains personal health records that require high level of security when the records are being shared and transferred to health professionals and service providers. We assess security risk based on this critical needs of acknowledged risks and threats in the real time remote health monitoring system.

Keywords- *Wireless body area network; sensor network; remote health monitoring system; security threats; risk assessment*

I. INTRODUCTION

A. Motivation

According to Department of Health and Human Services, in 2007, about one in every seven, or 14.3% of the population is an older American [1]. The older population (65+) will continue to grow significantly in the future. The motivation of an inexpensive pervasive monitoring of people as they continue their daily routines was developed by the University of Texas at Dallas research team. Specifically, utilizing technology in the care of elderly people has attracted a lot of attention due to its potential in increasing the quality of life and reducing the cost. While many research works are reported in the literature and some commercial products and services are offered, the state of the art is still far from maturity. Specifically, platforms that are fully-wireless, can provide high-rate data processing and are scalable to remote monitoring of large population are highly in demand. In this paper, authors bring motivation of preliminary assessment of security risks in wireless body area network for remote health monitoring. Prior to the real world deployment of the remote healthcare monitoring system, security and privacy features should be assessed for privacy and security of client health data.

B. Prior work in body area networks (BAN)

Biosensors and body area networks (BAN) are expected to be used in many applications including health care, sport and entertainment. Among those, the health care applications require a series of miniature biosensors, a data transmission media (e.g. wired or wireless) and a collection/processing node. While one can build an experimental platform easily using the current technologies, there are many challenges to make it robust, secure and scalable. These challenges include the size/power consumption of sensor -transmitter, the data rate, the scalability in terms of number of biosensors and also number of patients. Today's Bluetooth and Zigbee radios have provided experimental platforms for researchers for their investigations. However, they cannot be used in low-power applications in which less than 100μ W power consumption is expected [2]. Another challenge is to provide users with secure and private features into wireless body area network and, accordingly, into the remote healthcare monitoring which is mandatory prior to launching service in real world. In this paper, authors discuss about risk analysis of security threats, enabling technology of security and privacy, and its relevant cryptographic algorithms.

This paper is organized as follow. Section 2 describes the related work in security of health monitoring. Section 3 describes the main elements, their functionalities and the system architecture. Section 4 discusses the working scenario with software modules and the key optimization algorithms. In Section 5, we present our implementation with non-security features using the off-the -shelf components for ECG monitoring and Section 6 discusses the security risk assessment. Finally, concluding remarks are in Section 6.

II. RELATED WORK IN SECURTY OF HEALTH MONITORING

Security and privacy issues are raised automatically when the data is created, transferred, stored and processed in information systems [23]. Especially, data transfers for the medical and healthcare purposes should be secure, safe and reliable [12][13]. Previous work on monitoring human body signals guides us the place where we should put security and privacy features [24][28]. With the advance of computer and networking technology convergence trends, pervasive computing is regarded as key technology to assist real time medical and healthcare information service with the help of deploying different kinds of sensors, communicating with wireless sensor networks, interpreting sensor data and developing large number of medical and healthcare service

rule sets cooperated with medical professionals [26][27].

However, it is difficult to develop relevant level of security and privacy features in the pervasive computing environment for healthcare purposes [22][25]. Especially, the computing power is extremely limited because of embedded properties of pervasive computing and the requirements of security and privacy are relatively stronger than any other applications of pervasive computing [15]. With the contradiction of the environments and needs, a number of theoretical and technical approaches showed us feasibility of resolving the restrictions [17][19][21][33]. Some approaches stressed on privacy [15][17][18][21][22] and the other approaches focused on security for healthcare in pervasive computing [16][19][20][26], respectively. The framework approach also showed us the directions to the ideal balance of security and privacy [12][26][32]. Outcomes of mobile and wireless communication research provide us with the streamlined and balanced approach to the specific security applications of the data transfer in monitoring human body signals [30][31][34][35][36][37][38].

For real world experimentation of assessing security risk, we select the remote heart monitoring system of the University of Texas at Dallas's remote healthcare monitoring system. Coronary heart disease is the single largest cause of death in US and one in every five deaths are attributed to it alone [3]. An estimated 60 billions dollars are spent each year for the treatment and prevention of heart attacks. Due to the advancements in pathological research and related technologies; the number of deaths due to heart disease has decreased in the last decade. Still the fact remains that it is the world's number one killer. Most of these deaths are caused by cardiac arrhythmias resulting in sudden death (deaths occurring within one hour after the first symptoms were felt by the patient).

Ventricular Fibrillation, usually caused by Ventricular Tachycardia, is the most severe and life threatening arrhythmias which stops the pumping action altogether and if normal rhythm is not restored within three to five minutes, causes the patient to suffer brain and heart damage and die. Implantable Cardioverter-Defibrillator (ICD) devices are put inside the body to constantly monitor heart rhythm and quickly detect any abnormality and administer the therapy when needed. Since this is an invasive technique requiring surgery with potential complications and associated high cost; it is only a recommended solution for high risk patients. For most of the potential heart disease patients, abnormal cardiovascular symptoms such as chest pain, faints and shortness of breath can be detected before the occurrence of the fatal cardiac arrhythmia.

Therefore, it is important to have an effective measurement and reporting system for providing patients with preventive measures of deaths caused by heart attacks as one of emergency and immediate medical aids. Several wireless Electrocardiograph (ECG) monitoring systems have been proposed [4][5][8][9]. These systems use 802.15.4 (Zigbee) [4][8][9] or Bluetooth [5] as the radio interface for the ECG sensors to communicate with a hand held device. Neither radio interface was originally designed for real-time, high-speed, low-power continuous data transfer applications. To address some of these limitations, a flexible experimental platform of wireless biosensor monitoring was designed and developed. Authors aim at this platform to preliminary assess security risks in patient's data privacy, security, and service reliability.

II. SYSTEM ARCHITECTURE

The architectural block diagram of the system is described in Figure 1. Each biosensor will include a short-range transceiver that transfers data in a secure channel to a small BAN gateway. The gateway, in turn, would process data and resends it through a secure channel to a wireless modem/router for internet delivery. Each main unit is briefly explained as follows.

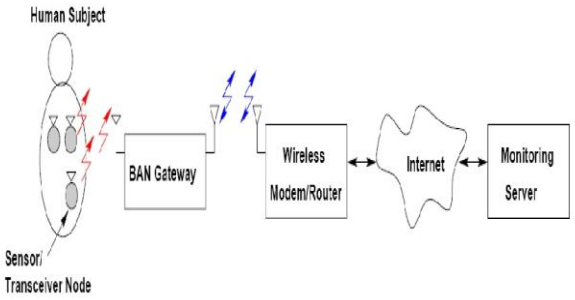

Figure 1. Overall architecture

- **Biosensor-Transceiver Pair**: Wide range of biosensors can be found in the market. Examples are sensors for heart rate, temperature, falling, bending, etc [6][7]. Each sensor needs to be paired and packaged with a miniature low-power transceiver. As a matter of practicality, it would be much easier to use if the sensor-transceiver pair is packaged as a patch.
- **Gateway:** The gateway, would be responsible for data collection, processing and overall BAN network management. Having enough memory and processing power (a mid-size microprocessor) is inevitable. The gateway also includes two types of wireless communication: (i) a receiver to get data from biosensors and (ii) a wireless Ethernet adapter to communicate with the standard wireless router/switch.
- **Monitoring Server**: Monitoring server runs powerful back-end software to collect, analyze profile and make decisions. It is well understood that bio metrics of each individual are very much unique. Thus, for effective processing a personalized profile should be "learned" automatically by the server. This is a crucial step to minimize (and even achieves zero-level of) false positive (i.e. raising alarm for non-critical situations) and false negative (i.e. missing a critical, perhaps life-threatening situation). To do so, a combination of innovative learning and reasoning algorithms are required to interpret data properly during monitoring.

IV. WORKING SCENARIO

Figure 2 pictures the main modules running on the backend software. A brief explanation of the main modules follows.

• **Setup:** Initial signal setup interface checks for the reception of wireless signals, network setup and resolves various difficulties that may arise.

This module makes sure that the BAN and wireless networks are alive and handshake properly.

- **Registration:** Patient's information is fed in this module and stored in the server. This module includes a graphical user interface (GUI) that simplifies data entry and retrieval. Additionally, the module keeps track of patient's biosensor data and records all information needed.

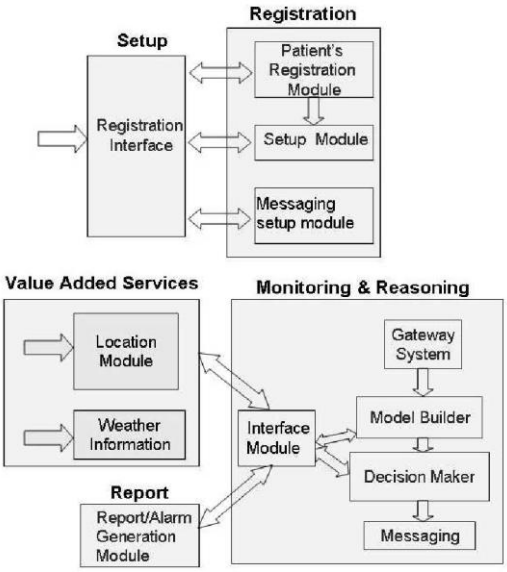

Figure 2. Components of working scenario

If any critical situation occurs, the system behaves based on the patient's pre-defined data and requests (e.g. notifying the relatives) and the severity of the situation (e.g. notifying a hospital).

- **Monitoring & Reasoning:** It keeps track of the patient's health status and depending on his health status, a decision regarding the patient's treatment is made. This is by far the most important module of system as making decisions through logical reasoning using limited number of sensors (e.g. ECG, blood pressure/Oxygen/Glucose) is quite challenging. In general, this is done by building a dynamic model (historical profile) for each individual and use learning/reasoning algorithms to evaluate and grade the severity of each and every significant change. More importantly, this module will be responsible to set off the alarm while achieving almost-zero false positive and false negative.
- **Value Added Services:** This module provides extra information such as geographical location of patients and close hospitals, availability of doctors in region, weather, etc. Such services may be desirable for certain group of patients with special needs or requests.
- **Report:** It is responsible for communicating (exchange messages) with the outside components, e.g. producing/sending an alarm or a report to a health-care provider.

V. IMPLEMENTATION

A. *Block Diagram*

To prove the concept and understand the challenges, we focused on an experimental platform for ECG monitoring. We acknowledge that various ECG monitoring devices (e.g. belts, wrist-watches, etc.) are commercially available in the market. However, our intention was to design a platform as an experimental vehicle to show the concept, evaluate its scalability and effectiveness of various hardware and software components. ECG monitoring requires relatively large volume of data, synchronization, dealing with noise, various types of signal conditioning and processing. Our platform not only does all of these but also hooks the patient to the internet for real time remote monitoring. In this platform, we use all off-the shelf products to show the concept. The block diagram of our system is pictured in Figure 3. Due to lack of space, we will not explain the technical details. Instead, the main configuration of the preliminary system and the challenges ahead will be highlighted.

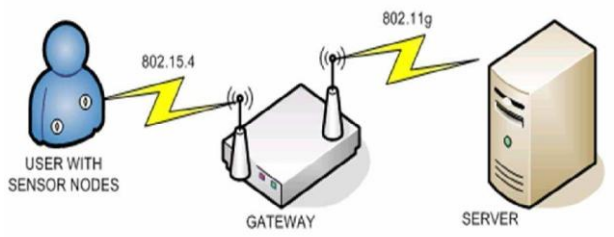

Figure 3. Experimental platforms of working scenario

B. *Experimental Results*

We have used all off-the -shelf components to implement this experimental platform for pervasive wireless ECG monitoring. Our system consists of three main devices:

1) Sensor Nodes: Each sensor node, shown in Figure 4, consists of a commercial ECG electrode patch, an analog front-end and a Micaz board [10].

2) Gateway Node: The gateway node, shown in Figure 5, consists of: (i)Micaz based board, (ii) Altera FPGA [11] board for various signal processing and (iii) an 802.11 module for wireless connection.

3) Server: The server carries the proper storage, database and application softwares. It is intended to be highly available (i.e. 24/7) and be scalable for monitoring a large number of patients. The server runs real-time analysis of sensor's data, provides user access to the database at various levels (e.g. patients, relatives, physicians, etc.) and generates alarm in case of emergencies.

Figure 6 show the ECG signal before and after noise filtering. The top curve is the noisy signal picked up by sensors. This signal is amplified, converted to digital on the Micaz board and quantized at a sampling frequency of 200 Hz. The Micaz board then transmits this data (i.e. 20 samples per packet and 10 packets per second) to the gateway where the signal is further processed in the FPGA. The gateway further conditions the signal by eliminating the hum noise using notch filter and band -limit it to 0.5 Hz to 100 Hz. The band-pass filter also provides a gain of 16 in two cascaded stages. The processed signal is then sent to the server using TCP/IP connection for analysis and storage. All required signal processing is accomplished using software running in the gateway and the server. The final result is shown in the bottom curve in Figure 6.

Figure 4. Components of Sensor Node

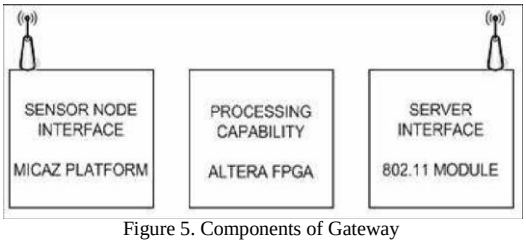

Figure 5. Components of Gateway

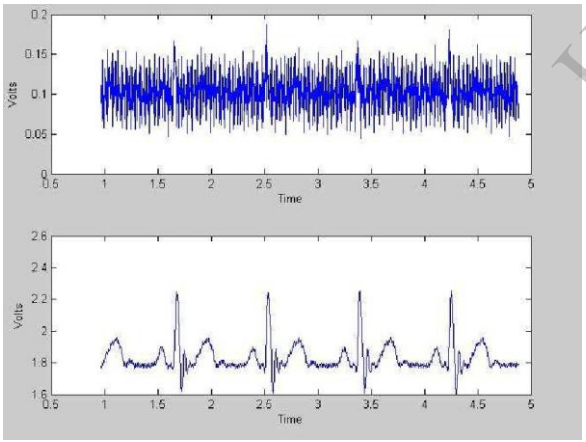

Figure 6. ECG signals: read by sensors (top curve) and recovered after transmission and processing (bottom curve).

C. Challenges Ahead

The preliminary ECG monitoring platform has taught us many valuable lessons that highlighted our direction toward a full-fledge system. We hope to address these challenges in near future.

- **Sensor Node**: (a) Miniaturization of this node (to reduce the cost and enhance its wearability), (b) effective noise removal (to improve bit error rate and indirectly data rate and reliability); and (c) dynamic/programmable power management (to fit in various environments/cases) are the main tasks.
- **Gateway Node**: The key challenges here include: (i) Customizing the two *transceivers* (to reduce cost and power), (ii) a customized network protocol for sensor identification and communication, (iii) an encryption unit for security of transmitted data; and (iv) memory management for store-and-forward operation as well as for backup possibility.
- **Server**: The three vital tasks here are: (a) Minimizing the probabilities of false positive and false negative (e.g. below 0.01), (b) an intelligent context learning methodology that automatically profiles and monitors massive data collected for large number of individuals and sensors; and (c) a multi-level hierarchical graphical user interface allowing patient, doctor and selected individuals (e.g. relatives) see part of the information and exchange data for comfort, monitoring, diagnosis and urgent/non-urgent response action.

VI. SECURITY RISK ASSESSMENT

Currently, the following two risks were identified. A few more risks will be added later as the system is deployed and services are delivered in a full scale.

A. Qualitative Security Threats Assessment

As the system is in laboratory scale implementation and testing, we conduct risk assessment with the assumption of user's activities of daily living while the user is using the device for the remote healthcare monitoring service consisting of data collection, processing, transmission, storing and sharing. Two of the major security threats are caused by the user's daily use and data sharing. Typically, we can find the most vulnerable points of security threats in the system those are sensor transmission nodes, wireless body area network (gateway), remote web portal system, and users who transmit their health data in the web portal system. The communication links of IEEE 802.15.4, IEEE 802.11g, and Internet protocol are also regarded as vulnerable points of security threats.

When the user has a wireless device in his/her Wireless Body Area Network (WBAN), the vital signals are being sensed by the sensor transmission node, the vital signals can be targeted when intruders synchronize the wireless bandwidth using IEEE 802.15.4 bandwidth as an unauthorized source. It causes a confidentiality issue and an availability issue. When the intruders alter the vital signals in the sensor transmission node, it will cause misinterpretation of the user's vital signals by the automated analysis software tool in the remote web portal system and/or by the health professionals as it causes an integrity issue. When the health professionals access users' health monitoring data, the professionals might be one of target points as the intruders easily acquire unauthorized access by way of social engineering. At the beginning of system design and implementation, considerations of security features and user needs of security and privacy had not been discussed yet. It might cause severe counter measures on integrity, confidentiality, and availability issues of patients' remote healthcare monitoring records. It will also cause more cost and time in assessing, designing and deploying relevant security features of the system after system implementation.

B. Proposed Security Features

The features for security and privacy in transferring data consists of monitoring human body signals needs authentication, integrity, access control, non-repudiation and

encryption features. For the security features of the system, we need to adopt the concept of scalability and compatibility by adopting the Elliptic Curve Cryptographic algorithm, Mutual Authentication and Group key Agreement protocols. We also need to consider security features for privacy of accessing and sharing clinical data stored at the remote web portal system by updating role-based access control or task-based access control. It should include the security features integrated into the cryptographic protocol and the data structure. The verification of security features in the system will also have to assess power consumption and computing resources.

C. Enabling Technology Resolving Security Threats

We reviewed security perspectives for the remote health monitoring system which offers an inexpensive, yet flexible and scalable, wireless platform to deliver, train and monitor data provided by biosensors. For the proof of concept, we have implemented a preliminary ECG monitoring system using off-the-shelf components. Additional requirements to achieve a high level of security and privacy of patients' information including remote health monitoring data, and to deploy full-fledge biosensor technology for remote monitoring will have to be carefully reviewed. A large number of applications, particularly in health care sector, can benefit from such platform because it is expected to significantly lower the cost. For sustaining the high level of security in all the applications in the system, we consider importing cryptographic functions with a plug-and-play (PnP) gadget that can be setup quickly by a non-professional and the pervasive monitoring becomes possible without interruption in patient's daily routines. The security threats while offering a few technical innovations including efficient signal conditioning, ubiquitous connection to internet and a powerful back-end software that performs data acquisition, profiling, reasoning and decision making are required to verify in the forthcoming research.

To sustain high level of security in the real time remote health monitoring system, we need to include security and privacy needs from the starting point of system design and implementation. This will reduce cost and time of deploying the security features. For the strong level of security, we need to implement Advanced Encryption Standards (AES) 128 cryptographic algorithm in the hardware accelerator of the user's sensor node module [38]. There is a new block cipher suitable for low resource device in the research community and one of them is HIGHT (aka high security and light weight) block cipher with 64-bit block size and 128 bit key size [39].
For the cryptographic algorithm of TinyOS, elliptic curve cryptographic algorithm, ECIES, and key distribution protocol, ECDH, and digital signature algorithm, ECDSA, have been introduced [40]. With these cryptographic algorithms, we need to investigate and perform feasibility research on real world implementation and field testing of security features in the remote health monitoring system.

VII. CONCLUSION

Non-invasive wireless monitoring of biosensors is highly in demand for various applications. In particular, such system can significantly improve the quality of life and reduce the health care cost especially for elderly and people with various disabilities. In this paper, we discussed a simple yet flexible and scalable framework of a scalable wireless biosensor system tuned for real-time remote monitoring as a case study of security threats assessment. We will expand the specifications of the design with the target data and communication paths where security and privacy are required. We also assess security and privacy threats from the patient's perspective. With the short term assessment of security and privacy threats of the target system, we will also pursue further study with respect to the national and international standards. In the forthcoming study, we will reference procedural and functional requirements being proposed as methodology and criteria to the Health Information Security and Privacy Collaboration (HISPC) and Health Information Technology Standards Panel (HITSP) in American Health Information Society and also to the US Trusted Computer System Evaluation Criteria (TCSEC) and Common Criteria (CC) for Information Technology Security Evaluation.

REFERENCES

[1] Department of Health and Human Services, http://www.aoa.gov, 2007.

[2] J. Rabaey, M. Ammer, J. Silva, D. Patel and S. Roundy, "Picoradio Supports Ad-Hoc Ultra-Low Power Wireless Networking," IEEE Computers, pp. 42-48, July 2000.

[3] American Heart Association, http://www.americanheart .org/presenter.jhtml?identifier=4591, July 2007.

[4] R. Fensli, E. Gunnarson and T. Gundersen, "A Wearable ECG-Recording System for Continuous Arrhythmia Monitoring in a Wireless Tele-Home-Care Situation," Proceedings of the 18th IEEE Symposium on Computer-Based Medical Systems, pp. 407-412, 2005.

[5] Z. Tafa and R. Stojanovic, "Bluetooth-Based Approach to Monitoring Biomedical Signals," Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, pp. 415-420, May 2006.

[6] Questex U.S. Technology Group, http://www.sensorsmag.com, 2007.

[7] Biosensors International, http://www.biosensors.com, 2007.

[8] [illegible]

[9] V. Shnayder, B. Chen, K. Lorincz, T. FulfordJones and M. Welsh, "Sensor Networks for Medical Care," Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2005.

[10] Crossbow Technology Inc., "User Manuals for WSN Development Kit," 2007.

[11] Altera Corporation, "Stratix-II Device Handbook," 2007.

[12] Integrating the Healthcare Enterprise (IHE), "IHE IT Infrastructure Technical Framework: Cross-Enterprise User Authentication (XUA) Integration Profile," White paper, 2006.

[13] Karen Witting, "Healthcare and Life Sciences: Deployment Guide – Setting up an XDS Affinity Domain using IHII Components," IBM Healthcare and Life Science, June, 2006.

[14] Monica Tentori, et.al., "Quality of Privacy (QoP) for the Design of Ubiquitous Healthcare Applications," Journal of Universal Computer Science, Vol. 12, No. 3, pp.252-269, 2006.

[15] Wan-rong Jih, et.al., "Context-aware Access Control in Pervasive Healthcare," EEE'05 Workshop: Mobility, Agents, and Mobile Services (MAM), 2005.

[16] Andreas Görlach, Wesley W. Terpstra, Andreas Heinemann, "Survey on Location Privacy in Pervasive Computing (in: Privacy, Security and Trust within the Context of Pervasive Computing)," Proceedings on Euro mGov 2005, 2005.

[17] [illegible]

Computing," Proceedings on Euro mGov 2005, 2005.

[18] G. Zhang and M. Parashar, "Context-aware Dynamic Access Control for Pervasive Applications," Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004), 2004 Western MultiConference (WMC), Jan., 2004.

[19] David Jea, Ian S Yap, Mani B Srivastava, "Context-aware Access to Public Shared Devices," HealthNet 2007: the First International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, June 2007.

[20] Alastair R. Beresford and Frank Stajano, "Location Privacy in Pervasive Computing," Pervasive Computing, pp.46-55, Jan.-Mar., 2003.

[21] Monica Tentori, et.al., "Privacy-Aware Autonomous Agents for Pervasive Healthcare," IEEE Intelligent Systems, pp.55-62, Nov.-Dec., 2006.

[22] Munirul Haque and Sheikh Iqbal Ahamed, "Security in Pervasive Computing: Current Status and Open Issues," International Journal of Network Security, Vol.3, No.3, pp.203-214, Nov. 2006.

[23] S.C. Shin, et.al., "Realization of an e-Health System to Perceive Emergency Situations," Proceedings of the 26th Annual International Conference of the IEEE EMBS, pp.3309-3312, Sep. 2004.

[24] Anthony W. March, "System/method for secure storage of personal information and for broadcast of the personal information at a time of emergency," US Patent 6034605, 2000.

[25] Brian K. Hensel, et.al., "Defining Obtrusiveness in Home Telehealth Technologies: A Conceptual Framework," Journal of American Medical Informatics Association, Vol.13, No.4, pp.428-431, Jul-Aug, 2006.

[26] Mashhour Mustafa Moh'dBanh Irbid Amer and Mahmoud Ibrahim Mahmoud Amman Izraiq, "System with Intelligent cable-less transducers for monitoring and analyzing biosignals," European Patent Application, EP 1815784A1, 2007.

[27] Ja'afer AL-Saraireh and Sufian Yousef, "Extension of Authentication and Key Agreement Protocol (AKA) for Universial Mobile Telecommunication System (UMTS)," International Journal of Theoretical and Applied Computer Sciences, Vol.1, No.1, pp.109-118, 2006.

[28] Emmanuel Bresson, et.al., "Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices," The Fifth International Conference on Mobile and Wireless Communications Networks (MWCN '03), October, 2003.

[29] Meeanuel Bresson et.al., "Mutual Authentication and Group Key Agreement for Low-power Mobile Devices," The Fifth IFIP-TC6 International Conference on Mobile and Wireless Communications Networks (MWCN '04), 2004.

[30] Philip Robinson, Harald Vogt, Waleed Wagealla, "Privacy, Security, and Trust Within the Context of Pervasive Computing," SpringerVerlag, ISBN 0387234616, 2005. (book)

[31] Raja Bose, Abdelsalam (Sumi) Helal, Shinyoung Lim and Vishak S Sivakumar, "Virtual Sensors for Service Oriented Environments", The 3rd IASTED International conference on Advances in Computer Science and Technology (ACST) 2007, April, 2007.

[32] Shinyoung Lim, Sangseung Kang, Joochan Sohn, "Modeling Multiple Agent based Cryptographic Key Recovery Protocol", IEEE 19th 2003 ACSAC (Annual Computer Security Applications Conference), pp.119 ~ pp.128, 2003.

[33] Shinyoung Lim, Youjin Song, "Secure Multiple Mobile Payment Protocol", 1st ACNS 2003 (The 1st International Conference on Applied Cryptography and Network Security), pp.169 ~ pp.183, 2003.

[34] Shinyoung Lim, Sangseng Kang, Joochan Sohn, "Secure Communication Protocol for User Authentication of Java Card", 5th ICACT 2003 (The 5th International Conference on Advanced Communication Technology), pp.201 ~ pp.204, 2003.

[35] Shinyoung Lim, Khjong Ho, Juneun Ah, Kangsoo Lee, Specification and Analysis of n-way Key Recovery System by Extended Cryptographic Timed Petri Net, The Journal of Systems and Software, Vol. 58, No. 2, pp.93 ~ pp.106, Sep 2001.

[36] Shinyoung Lim, Youjin Song, "Experience from Mobile Application Service Framework in WIP", EurAsia-ICT (Information & Communication Technology) 2002 Springer Verlag LNCS 2510, pp.907 ~ pp.915, 2002.

[37] CC2420 DataSheet, "C2420, 2.4GHz IEEEE 802.15. 4/ZigBee-ready RF Transceiver," Chip-con, 2006.

[38] Deuko Hong, et al, "HIGHT: A New Block Cipher Suitable for Low-Resource Device," CHES'06, LNCS 4249, 2006.

TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks, Ver 1.0, http://discovery.csc.ncsu.edu/software/TinyECC, 2007.