# Social Issues in Wireless Sensor Networks with Healthcare Perspective

Moshaddique Al Ameen and Kyung-sup Kwak
Graduate School of IT and Telecommunications, Inha University, Korea

**Abstract:** *The recent advances in Wireless Sensor Networks have given rise to many application areas in healthcare. It has produced new field of Wireless Body Area Networks. Using wearable and non-wearable sensor devices humans can be tracked and monitored. Monitoring from the healthcare perspective can be with or without the consent of the particular person. Even if it is with the consent of the person involved, certain social issues arise from this type of application scenario. The issues can be privacy, security, legal and other related issues. Healthcare sensor networks applications have a bright future and it is a must to take up these issues at the earliest. The issues should be carefully studied and understood or else they can pose serious problems. In this paper we try to raise and discuss these issues and find some answers to them.*

**Keywords:** *Wireless sensor networks, healthcare systems, social issues, privacy, security, and legal issues.*

*Received November 27, 2008; accepted February 25, 2009*

## 1. Introduction

As the cost and size of sensor devices are decreasing fast, the application areas of wireless sensor networks have also expanded rapidly. The major application domains [2, 10] are home and office, control and automation, logistics and transportation, environmental monitoring, healthcare, security and surveillance, tourism and leisure, education and training and entertainment. Typical possible application scenarios may include digitally equipped homes, manufacturing process monitoring, vehicle tracking and detection, and monitoring inventory control.

Wireless sensor devices that can be used to actively monitor human activities have garnered great research interest in recent years. Demand of wearable wireless devices has been on the rise recently. A new concept of 'people centric' and 'urban' wireless sensor networking has been a hot research area [1]. Applications of wireless sensor networks focused on monitoring the health status of patients have been in demand and various projects are in the development and implementation stages [4, 6, 9]. A simple sensor networks in healthcare application scenario is shown in Figure 1. Sensor networks are being researched and deployed in wide range of applications in healthcare. Typical application scenarios could be monitoring of heart beats, body temperature, body positions, location of the person, overall monitoring of ill patients in the hospital and at home and so on. Sometimes this domain area is referred to as wireless body area sensor networks or Wireless Body Area Networks (WBAN).

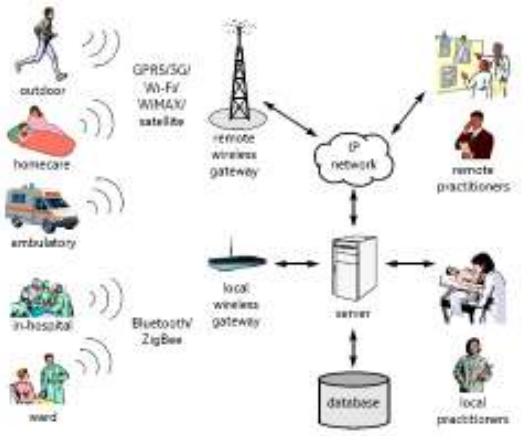


Figure 1. Typical architecture of wireless sensor networks in healthcare applications [11].

Wireless sensor networks applications are going to revolutionize the healthcare system. As shown in Figure 2, the growth of WSN is rapid and fast. The projected sales of sensors are going to be very high. Similarly Figure 3 shows the world revenue forecast and growth rate. We can see that sensor networks have a great future ahead with tremendous growth rate.

In [11], the authors have discussed some potential medical applications. These includes, real-time, continuous patient monitoring by which pre-hospital, in-hospital, and ambulatory monitoring can be possible thereby helping to replace expensive and cumbersome wired telemetry systems.

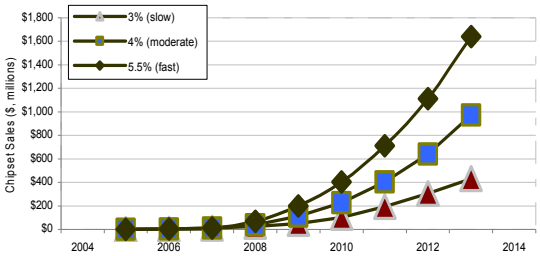


Figure 2. WSN chipset sales and projections [25].

Home monitoring applications for chronic and elderly patients which can be used to collect periodic or continuous data and be uploaded to a physician and can allow long-term care and trend analysis. It can also reduce length of hospital stay. Manual tracking of patient status is difficult. Sensor networks in healthcare can replace the current systems based on paper and phone. Collection of long-term databases of clinical data can be used in future diagnosis. Sensor networks applications have potential for large impacts. It can be used in real-time, continuous vital monitoring and give immediate alerts of changes in patient status. They also can relay data to the hospital or correlate with patient records and so on.

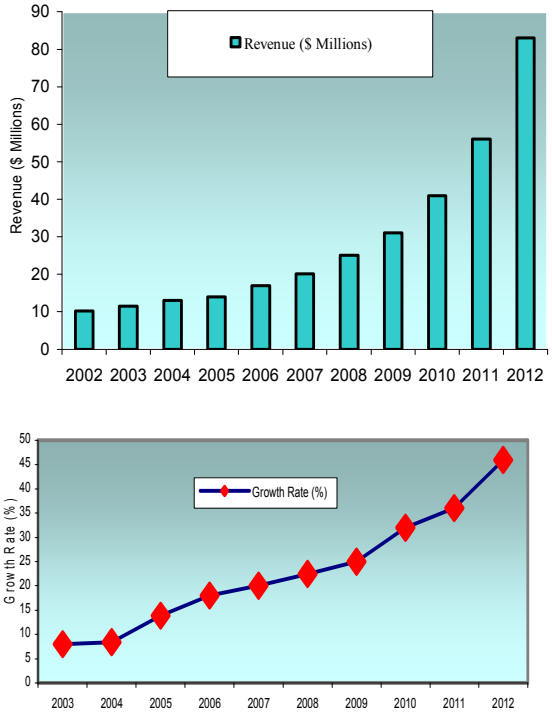


Figure 3. Wireless sensors and transmitters market: revenue forecast and growth for healthcare, medical and biometrics (world), 2002-2012 [18].

Since WBAN and other healthcare sensor networks applications are related directly to humans, they are certainly going to affect the life around us. Due to the impacts of these applications, it is certain that they will influence the social life of a person. Thus, certain typical social issues related to these applications must arise. It is well known that any wireless system has some inherent technical vulnerabilities and limitations. Hence before sensor networks applications in healthcare become a widely accepted concept, psychological, socio-political and a number of challenging system design issues should be taken care of. If resolved successfully, these systems will open a whole range of possible new applications that can significantly influence our lives [4].

The social issues that are directly related to the above mentioned application scenarios can be categorized into three major areas – security, privacy and legal issues. Besides these, there can be more issues such as economic and political issues. In this paper, we discuss the social issues of wireless sensor networks application within healthcare perspective.

This paper has been further organized in the following manner. In section 2, we discuss some projects and related works. In section 3, we discuss the security issues. In section 4, we discuss the privacy issues. In section 5, we discuss the legal issues. In section 6, we discuss other related issues such as economic and political issues and then finally in section 7, the conclusion.

## 2. Some Projects and Related Works

Much research time is being devoted to the area of wireless healthcare systems lately. A number of recent projects have focused on wearable health devices [15]. These projects have been undertaken by government agencies and other private organizations. These projects cover many areas in healthcare viz. ECG monitoring, glucose level monitoring, stress monitoring, cancer detection, elderly people monitoring and so on. Some of the major indoor/outdoor application projects that are going on around the world are mentioned here.

### 2.1. Real Life Projects and Applications

HealthGear [12] is a product of Microsoft Research. It consists of a set of physiological sensors connected via Bluetooth to a cell phone. It is basically a wearable real-time health system for monitoring and analyzing physiological signals.

MobiHealth [24] is a mobile healthcare project funded by the European Commission. It allows patients to be fully mobile while undergoing continuous health monitoring by utilizing UMTS and GPRS networks.

Ubimon [26] is from the Department of Computing, Imperial College, London. The aim of this project is to address the issues related to using wearable and implantable sensors for distributed mobile monitoring. Two areas under consideration are the management of patients with arrhythmic heart disease and the follow-up monitoring of post operative care in patients who have had surgery.

CodeBlue [20] is a research project at Harvard University, US. It integrates sensor nodes and other wireless devices into a disaster response setting. It is designed to work across various network densities and a wide range of wireless devices. From a tiny small sensor mote to more powerful devices such as PDSs, PCs can be combined in CodeBlue.

eWatch [7] is a wearable sensor and notification platform developed for context aware computing research. It fits into a wrist watch form making it highly available, instantly viewable, and socially acceptable. eWatch provides tactile, audio and visual notification while sensing and recording light, motion, sound and temperature.

The Vital Jacket [21] mobile device is an intelligent wearable garment that is able to continuously monitor electrocardiogram (ECG) waves and Heart Rate for different fitness, high performance sports, security and medical applications. Here data can be sent via Bluetooth to a PDA and stored in a memory card at the same time.

All these projects aim to provide affordable continuous monitoring of a person's health related issues. The major focus is on the cost effectiveness and power consumption of these devices. Although these devices are for a novel cause, they have serious social issues related to security, privacy and legal aspects. For example, some of these applications are heavily relied on Bluetooth-like technologies. These technologies can pose security threats like eavesdropping and denial of services. They also have to meet the concerns of health hazards for the implanted devices. As our discussion is of the social impacts of these applications, we will present the major issues related to them in the next sections.

### 2.2. Related Works

There are some works authored by people that address the issues related to sensor networks. But social issues as a whole for application scenarios such as wireless body area networks or in healthcare perspective have not yet been covered extensively. Many authors have suggested these issues as important. But we have found that most of these works are for either some stand alone applications or the issues are not covered as a whole. One of the papers [5] discussed these issues in the e-Health monitoring applications. Authors in [9] also have discussed some of these issues for personal health monitoring. We have found that most published works address the security issues for sensor networks applications. These include works such as [6, 11]. We have mentioned the works done by various authors related to particular issues in the subsequent sections of this paper.

## 3. Security Issues

Security is an inseparable part of any system. Different people have defined security in different ways. Wikipedia [19] states that security is the condition of being protected against danger or loss. In a general sense, security is a concept similar to the safety of the system as a whole. The US Department of Commerce site [23] defines security as a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

However what way we may think or define security, it is common fact that security is always of great importance. Due to the wireless nature of communications in sensor networks applications in healthcare, various security threats may occur. These threats and attacks could pose serious problems to the social life of an individual who is using the wireless sensor devices. In some cases such as tracking the location of the subject if compromised may lead to grave consequences. Security issues in healthcare applications of sensor networks have always been a part of active research. Security issues in general wireless sensor networks are a major area of research in recent times. Some works include [16, 17]. Similarly, many people such as [5, 8, 11] have specifically addressed security issues with respect to healthcare applications. We attempt to highlight and discuss some threats and attacks in the following section along with some counter measures.

### 3.1. Threats and Attacks

There is always chance of a security breach in healthcare applications of sensor networks. The threats and attacks [11] can be broadly classified in to two major categories – passive and active. Passive attacks can occur while routing the data packets. The attackers may change the destination of packets or make routing inconsistent. Here, the attackers can also steal the health data by eavesdropping to the wireless communication media. The active threats are more harmful then their passive counter parts. Criminal minded people may find the location of the user by eavesdropping. This may lead to life threatening situations. The normal trend of sensor device design is that they have little external security features and hence are prone to physical tampering. This increases the vulnerability of the devices and poses tougher security challenges. Similarly vital data transmission from WBAN networks through GPRS or similar networks can be stolen by eavesdropping.

The authors in [5] have mentioned few types of attacks in health monitoring in more detail manner viz. eavesdropping on medical data, modification of medical data, forging of alarms on medical data, denial of service, location tracking of users, activity

tracking of users, physical tampering with devices and jamming attacks.

Furthermore the attackers and hence, the threats may be both internal and external. External attackers are not part of the system hence they are hard to deter. The primary purpose of attacks is to steal valuable personal data. Since wireless media is always more vulnerable than wired media, attackers find it easier. Once they are aware of the value of the personal health data, they may try to steal it by using both internal and external attacks.

### 3.2. Countering the Attacks and Measures

Any design of healthcare applications for sensor networks, security issues must be resolved first hand or else they may give rise to serious social problems as discussed earlier. To counter the major threats two broad level security measures can be applied– encryption and authentication mechanisms. Any communication of personal health information and data over the networks must be encrypted. Furthermore as mentioned by the authors in [5], preventing unauthorized modifications of data while at the same time ensuring that only legitimate devices can create and inject data to the network prevents many of the previously discussed attacks. Authentication mechanisms can be used to ensure the data is coming from the person/entity is claiming to be from [14].

In a WBAN scenario, where a person wears various devices, we can use a centralized control device for data transmission from in and out of the network. This device can also act as the gateway between the internal network and outside world communication. Security measures such as authentication, firewalls and other checks can be applied at the controller level to monitor the traffic as shown in Figure 4.

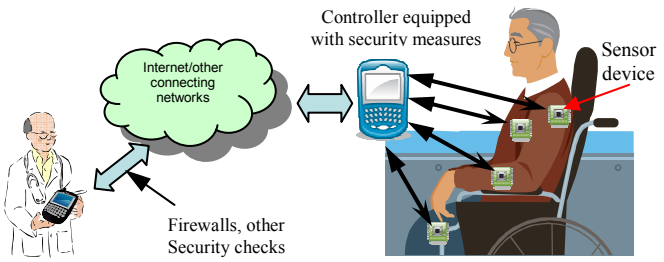


Figure 4. Security measures at controller/gateway in wireless body area networks.

Security in sensor networks applications in health care can not be compromised. Carefully constructed measures are necessary in this regard. We feel that security safeguard measures may be applied in three levels – Administrative, physical and technical.

- Administrative level security: at this level, security measures should be to check the security breaches by the staff or people responsible for system operation. A well defined user hierarchy along with strong authentication measures may prevent security breaches. Hence these important security measures must include various types of access mechanisms so that only authorized users can access the data. Similarly, it may also be a case where data forwarding may be only to the place or people which are previously authorized.
- Physical level security: at this level, measures may include controlling access to physical devices and data in the system for supposed stealing or tampering. As mentioned earlier, devices may be vulnerable from both people with malicious minds or from natural causes such as wear and tear. Hence, careful designing of devices to make them tamper proof is also necessary. But it is also understood that avoiding physical tampering of devices is hard to achieve. Another preventive measure can be that only authorised people should be allowed to physically handle the devices while in operation. Users must be strongly advised regarding these types of security measures.
- Technical level security: technical level, security checks are necessary for wireless communications and propagation of information. If the network is such that data is sent to central servers, server based security measures be used at the server side and client based security at the user side. This may again increase load on sensors at the user side and thereby increase the overall cost. So we also must take care of this aspect. It is also likely that more powerful motes will need to be designed in order to support the increasing requirements for computation and communication [16]. Securing the routing of data can also be applied as a security measure. Wireless networks are very much susceptible to intrusion. Intrusion detection and prevention techniques are hence a must in these networks. Due to the sensitive nature of healthcare applications, extra measures such as encryption of data, and constant monitoring of the network is necessary. While monitoring may not be a cost effective measure, encryption and creation of secure user groups can be effective as well as cost saving. Routing is another area where technical level security is required. If the data is sent to some remote host (e.g., doctors or some other hospital computers), routing is necessary. Attackers may cause routing inconsistencies resulting in wrong destinations and receiving of wrong data. Hence proper routing protocol and management is necessary to prevent such attacks.

At the end, it must be noted that end to end security is a must to make the wireless sensor networks in healthcare applications usable and acceptable by the common people. Threats such as tampering with data, Denial of Service (DoS), physical tampering,

eavesdropping and others need far more special attention than any other common networks.

## 4. Privacy Issues

Privacy has been always a concern in wireless sensor networks with regard to healthcare applications. Sending data out from a patient through wireless media can pose serious threats to the privacy of an individual. Concerns regarding privacy have been raised by some authors such as [3]. They have emphasized that if the issues associated with privacy are not honestly debated in a reasoned and open ways there is a risk that there will be a public backlash which will result in mistrust and consequently the technology will not be used for the many valuable applications where it can provide significant benefits. Whether the data are obtained with the consent of the person or without it due to the need by the system (for example emergency data from a patient), misuse or privacy concerns may restrict people from taking advantage of the full benefits from the system.

Authors in [8] have also raised a few questions regarding guarding the privacy of an individual. For example, where should the health data be stored, who can view a patient's medical record, and to whom should this information be disclosed to without the patient's consent. These are among several important issues that should be resolved in order to protect privacy as well as to some extent the security of the information.

Applying regulations regarding privacy is a must. In normal circumstances there are only few kinds of users of the data, the physicians, nurses and some other clinical staff thereby limiting the number of users in the system. Well defined and firm guidelines regarding use of data by these users may limit the concerns in privacy. But it should also be noted that in some cases such as emergency, disasters or remote patient monitoring may necessitate disclosure of information to other people in order to serve the patient in need. So the system must be flexible enough and users should be made to accept or compromise to some extent. Still procedures must be placed to make the users of the private healthcare data accountable for their actions or else these people may not care about the privacy concerns of an individual which may lead to bad implications on the social life of the person concerned. Authors in [24] have argued that without appropriate privacy safeguards the information may go into the public domain straight away, which is potentially undesirable for a number of reasons. People may not want some personal data be available in public domain. For example, early stage pregnancy, the details of certain medical conditions, may be made freely available to close family members and friends, but may not be appropriate for the general public. It is also important that these data should not fall into the hands of people with malicious intent and hence managing these types of data is very important in order to maintain the privacy of the person.

Besides those mentioned above, some other measures may include:

- All communications over wireless networks and Internet are required to be encrypted to protect the user's privacy. Some countries have added this type of clause in their existing legal acts or enacted new laws. For example, the US Federal law HIPAA 1996 has this provision in it [22].
- It is also necessary that, specific users should not be identified unless there is a need.
- Another important measure is to create awareness in general public. It can be extremely beneficial if people are educated regarding security and privacy issues and their implications. It has been observed by authors in [3] that common people do not understand the technology and therefore may not be in a position to make balanced judgments concerning the extent to which it may have a negative impact on their own standards of privacy. Therefore educating the common people will greatly help in this regard.

The role of wireless infrastructure in healthcare applications is expected to become more prominent with an increasingly mobile society and with the deployment of mobile and wireless networks [13]. Hence it is always a better idea to be ready for such situations before the time comes for it. Educating people about the future ahead can make them more relaxed as well.

## 5. Legal Issues

As the data in wireless sensor networks for healthcare systems will be sent to different people at different places, legal issues must arise. The most natural question is 'who will have the responsibilities and liabilities for the data collected from a person'. Some other most obvious questions that may arise are, who will be responsible to enforce regulations and who can have access rights to use these data? In the case of misuse who will be accountable? The data generated from a person could be used for illegal purposes. This may lead to problems to the person whose data are being opened to other people. He/she may subject to blackmailing and other problems in life such as discrimination. A person who's certain secrets about healthcare are known may face discrimination at work. As discussed earlier, one major question is about onus of the healthcare data generated from a person. Who will take the responsibility for it? Normally personal medical data are sent to the doctor directly or to the hospital database. It may be possible that due to negligence of the doctor or the person in charge of the database, it might fall into the wrong hands. In such a case can the doctor be prosecuted? The question of

'who owns the data' is particularly troublesome and unsettled. It has been the object of recurrent, highly publicized lawsuits and congressional inquiries [8].

The legal issues in the computing world fall under 'cyber crime'. Countries around the world such as the US, European Union, Japan, Korea, Australia and India, have enacted strict laws to deal with cyber crimes. It is now needed that these laws be extended to healthcare sensor networks applications too.

As the loss of data to criminal-minded person may cause havoc to the user, we feel that insurance policies and reimbursements issues should be strictly defined under the current legal frame works. We also feel that responsibilities such as ownership of the data and legal liabilities should be explicitly defined. Legal regulation will be necessary to regulate access to person-identifiable information. It is a high time that strict regulations and policies should be drafted and made in to laws. The access to all kinds of information generated through sensor networks applications in healthcare should be regulated. Tougher laws under clear legal frameworks are the need of the hour. It is also necessary to enact rules aimed at increasing the efficiency of the wireless sensor networks healthcare system by creating standards for the real use of health care information. Authors in [3] suggested that although external legislation may be more desirable, regulations developed by a group of users can be very effective, especially if there are penalties which can be imposed for noncompliance. In this scenario, authorities which are self-regulating, such as government departments or agencies are rather less attractive as a prospect.

As mentioned many countries have laws related to cyber crime or similar kind of laws to address legal issues arise due to use of computing devices. But conflicting regulatory frameworks may hamper the course of justice. Authors in [8] have raised such concerns regarding US federal law HIPAA and laws in different sates. They have also suggested that there is a need to have cohesive policies to protect sensitive personal health information as it becomes available electronically in wireless or other media. As the attackers can be from anywhere in the world, we feel the need of some kind of global standards and laws be in place. Problems still exist in the lack of awareness of these laws in the general public. Hence it is essential that Governments and the law enforcement agencies should take actions to generate public awareness of such laws. Common people should be aware of these things. Mass media can play a great role in this direction.

## 6. Other Related Issues

In this section we discuss the issues that do not exactly fit into the above mentioned categories. These can be political, economical and psychological issues.

These issues are related more or less with the mass implementation of wireless sensor network devices in healthcare. People may be hesitant to use these devices not only for the major issues discussed in earlier sections but also for the above mentioned factors. For example, the law enforcement agencies can be made to monitor individuals to get political leverage which can be exploited and use for malicious purposes.

Another big issue is regarding implantable sensor devices inside human body. These devices can become an unwanted burden on the privacy of a person and thereby put psychological pressures on the mind of an individual. The cost of maintaining these devices may also put an extra financial burden on the person and on the Government. This can always lead to fear in the minds of common people. Unless properly addressed, it would be difficult to use sensor networks on a mass level.

## 7. Conclusions

The future has been predicted when wearable sensor devices would be an integrated part of daily life activities. In fact some people already have implanted sensor devices inside their bodies. This is already having tremendous effects on normal human life. The impact of these networks would be considerable and cover many aspects of daily life. The applications will not only lead to convenience but also lead to far reaching implications. Social issues related to these systems include privacy, security and legal. Also trade-offs between security, privacy and other issues with services have to be handled carefully. So it has become the utmost necessity to raise and address the issues related to the social life which would be caused by the advent of wireless sensor networks in healthcare. General public awareness is vital and a must for the success of these applications. In this paper we discussed these social issues and tried to answer to some possible impacts.

## Acknowledgment

This research was supported by the Ministry of Knowledge Economy, Korea, under the Information Technology Research Centre support program, supervised by the Institute of Information Technology Assessment IITA-2008-C1090-0801-0019.

## References

[1] Campbell T., Eisenman B., Lane D., Miluzzo E., Peterson A., Lu H., Zheng X., Musolesi M., Fodor K., and Ahn G., "The Rise of People Centric Sensing," *Computer Journal of IEEE Internet Computing*, vol. 12, no. 4, pp. 12-21, 2008.

[2] Dohler A., "Wireless Sensor Networks: The Biggest Cross Community Design Exercise to Date," *Computer Journal of Recent Patents on Computer Science*, vol. 1, no. 2, pp. 9-25, 2008.
[3] Hanna L. and Hailes S., "Privacy and Wireless Sensor Networks," University College, London, www.petsfinebalance.com/docrepo/privacy_and_WSN.PDF, Last Visited 2010.
[4] Jovanov E., Milenkovic A., Otto C., and de Groen C., "A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation," *Computer Journal of Neuro Engineering and Rehabilitation*, vol. 2, no. 6, pp. 124-127, 2005.
[5] Kargl F., Lawrence E., Fischer M., and Lim Y., "Security, Privacy and Legal Issues in Pervasive eHealth Monitoring Systems," in Proceedings of *7th International Conference on Mobile Business*, pp. 296-304, 2008.
[6] Kouvatsos D., Min G., and Qureshi B., "Performance Issues in a Secure Health Monitoring Wireless Sensor Network," *in Proceedings of 4th International Conference on Performance Modelling and Evaluation of Heterogeneous Networks*, UK, pp. 1-6, 2006.
[7] Maurer U., Rowe A., Smailagic A., and Siewiorek P., "eWatch: a Wearable Sensor and Notification Platform," *in Proceedings of International Workshop on BSN, Wearable and Implantable Body Sensor Networks*, pp. 144-145, 2006.
[8] Meingast M., Roosta T., and Sastry S., "Security and Privacy Issues with Health Care Information Technology," *in Proceedings of 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5453-5458, 2006.
[9] Milenkovic A., Otto C., and Jovanov E., "Wireless Sensor Network for Personal Health Monitoring: Issues and an Implementation," *Computer Journal of Computer Communications*, vol. 29, no. 5, pp. 2521-2533, 2006.
[10] Munir A., Yu B., Ren B., and Ma M., "Fuzzy Logic Based Congestion Estimation for QoS in Wireless Sensor Network," *in Proceedings of Wireless Communications and Networking Conference*, pp. 4336-4341, 2007.
[11] Ng S., Sim L., and Tan M., "Security Issues of Wireless Sensor Networks in Healthcare Applications," *Computer Journal of BT Technology Journal,* vol. 24, no. 2, pp. 138-144, 2006.
[12] Oliver N. and Flores F., "HealthGear: A Real-Time Wearable System for Monitoring and Analyzing Physiological Signals," *International Workshop on Wearable and Implantable Body Sensor Networks,* pp. 3-5, 2006.
[13] Varshney U., "Using Wireless Technologies in Healthcare", *Computer Journal of International Journal of Mobile Communications*, vol. 4, no. 3, pp. 354-368, 2006.
[14] Vaudenay S., *A Classical Introduction to Cryptography: Applications for Communications Security*, Springer, 2006.
[15] Wolf L. and Saadaoui S., "Architecture Concept of a Wireless Body Area Sensor Network for Health Monitoring of Elderly People," *in Proceedings of Consumer Communications and Networking Conference 4th IEEE*, pp. 722-726, 2007.
[16] Yong W., Attebury G., and Ramamurthy B., "A Survey of Security Issues in Wireless Sensor Networks," *Computer Journal of IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, pp. 2-23, 2006.
[17] Zia T. and Zomaya A., "Security Issues in Wireless Sensor Networks," *in Proceedings of International Conference on Systems and Networks Communications*, pp. 40-40, 2006.
[18] www.researchandmarkets.com, Last Visited 2009.
[19] http://en.wikipedia.org/wiki/Security, Last Visited 2009.
[20] http://fiji.eecs.harvard.edu/CodeBlue, Last Visited 2009.
[21] http://limserver.com/vitaljacket/index.php, Last Visited 2009.
[22] http://www.cms.hhs.gov/, Last Visited 2009.
[23] http://www.its.bldrdoc.gov/, Last Visited 2009.
[24] http://www.mobihealth.org/, Last Visited 2009.
[25] http://www.the-infoshop.com, Last Visited 2009.
[26] http://www.ubimon.net/, Last Visited 2009.

**Moshaddique Al Ameen** received the M Tech (CS) from India. He is currently a PhD student in telecommunication engineering in Inha University, South Korea. His research interests include wearable sensor devices for wireless body area networks, theory and applications of Wireless communications, and sensor networks. Research emphasis is on the development of new QoS model and standard for the body area networks in healthcare applications.

**Kyung-sup Kwak** received BS degree from the Inha University, Inchon, Korea in 1977, and the MS degree from the University of Southern California in 1981 and the PhD degree from the University of California at San Diego in 1988, under the Inha University Fellowship and the Korea Electric Association Abroad Scholarship Grants, respectively.