J Med Syst (2012) 36:93–101
DOI 10.1007/s10916-010-9449-4

ORIGINAL PAPER

Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications

Moshaddique Al Ameen · Jingwei Liu · Kyungsup Kwak

Received: 18 December 2009 / Accepted: 16 February 2010 / Published online: 12 March 2010

Abstract The use of wireless sensor networks (WSN) in healthcare applications is growing in a fast pace. Numerous applications such as heart rate monitor, blood pressure monitor and endoscopic capsule are already in use. To address the growing use of sensor technology in this area, a new field known as wireless body area networks (WBAN or simply BAN) has emerged. As most devices and their applications are wireless in nature, security and privacy concerns are among major areas of concern. Due to direct involvement of humans also increases the sensitivity. Whether the data gathered from patients or individuals are obtained with the consent of the person or without it due to the need by the system, misuse or privacy concerns may restrict people from taking advantage of the full benefits from the system. People may not see these devices safe for daily use. There may also possibility of serious social unrest due to the fear that such devices may be used for monitoring and tracking individuals by government agencies or other private organizations. In this paper we discuss these issues and analyze in detail the problems and their possible measures.

Keywords Wireless sensor networks · BAN · Healthcare systems · Security · Privacy

Introduction

Sensor networks are being used in a wide range of application areas. 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. Sensor devices that can be used to monitor human activities have garnered great research interest in recent years. The application areas can be divided into two major categories—medical use, non-medical use. The medical applications can be of two types: wearable and implanted. Wearable devices are those that can be used on body surface of a human or just at close proximity of the user. Some of the wearable medical devices and applications are: Temperature measurement, Respiration monitor, Heart rate monitor, Pulse oximeter SpO2, Blood pressure monitor, pH monitor, Glucose sensor etc. The implantable medical devices are those that are inserted inside human body. These devices and their applications are: Cardiac arrhythmia monitor/recorder, Brain liquid pressure sensor, Endoscope capsule etc. The non-medical devices and their applications can be real-time video streaming using mp4 video player and real-time audio streaming using mp3 player etc. There can also be scope for remote controlled applications, data file transfer, and sports and gaming applications. Besides the above typical application scenarios of monitoring, there are applications such as measuring body positions and location of the person, overall monitoring of ill patients in hospitals and at homes and so on.

A new concept of 'people centric' and 'urban' wireless sensor networking has been proposed and gaining momentum day by day [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]. Sensor networks in healthcare application scenario are shown in Fig. 1.

M. Al Ameen (✉) · J. Liu · K. Kwak
Graduate School of IT & Telecommunications, Inha University,
Incheon, South Korea
e-mail: m.ameen@hotmail.com

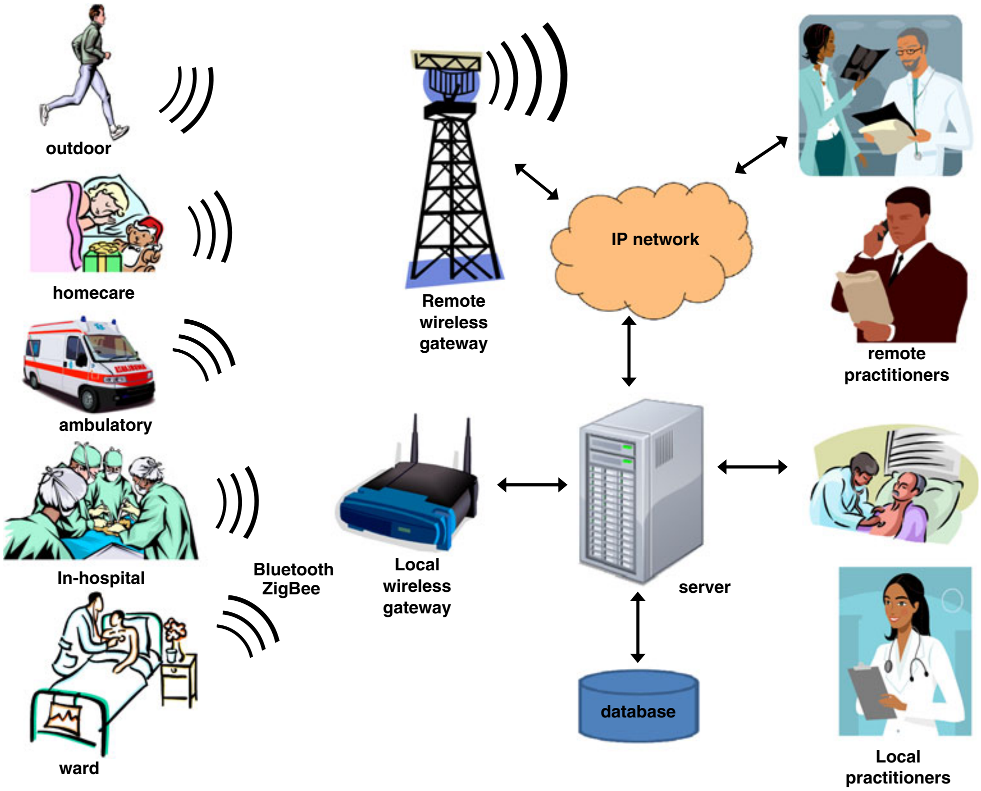


Fig. 1 Typical architecture of wireless sensor networks in healthcare applications [11]

As seen in Fig. 2, the growth of WSN is rapid and fast. The projected sales of sensors are going to increase rapidly. Similarly Fig. 3 shows the world revenue forecast and growth rate for healthcare, medical and biometrics markets. We can see that sensor networks have a great future ahead with tremendous growth rate.

Sensor networks applications in healthcare have potential for large impacts [18]. These can be realized through real-time, continuous vital monitoring to give immediate alerts of changes in patient status. The data can also be relayed to the hospital or correlate with patient records and so on. 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. Collection of long-term databases of clinical data can be used in future diagnosis.

Human lives are directly involved in these application scenarios. The impacts will certainly influence the life of a person. It is well known that any wireless system has some inherent technical vulnerabilities and limitations. Many of the sensor networks applications in the healthcare are heavily relied on technologies that can pose security threats like eavesdropping and denial of services. There are concerns of health hazards for the implanted sensor devices. The above concerns have far reaching social implications. The social implications and 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. 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].

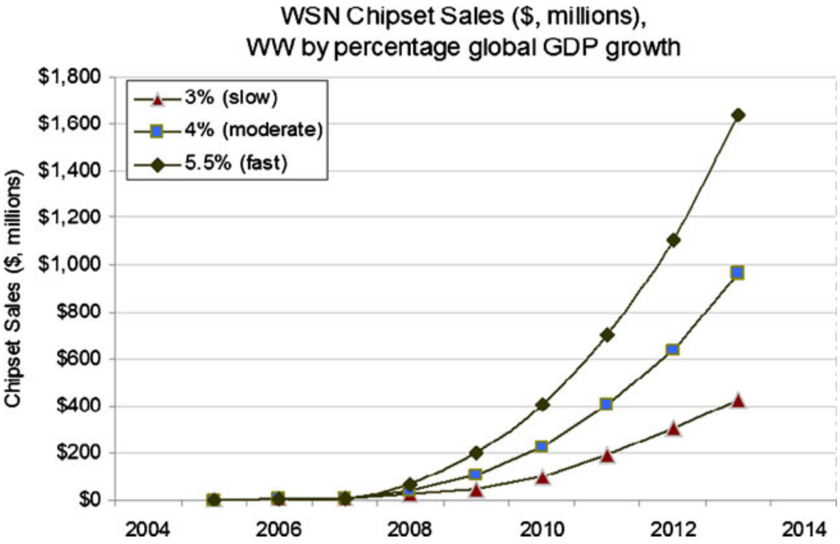
In this paper, we discuss the security and privacy issues of wireless sensor networks application within healthcare perspective. Table 1 shows the Comparison between medical BAN and general WSN [27].

This paper has been further organized in the following manner. In section II, we discuss related works. In section III, we discuss the security issues. In section IV, we discuss the privacy issues and then finally in section V, the conclusion.

Related works

Research in healthcare applications of sensor devices are being under progress all over the world. Many projects are developed or in developing stage. A number of recent projects have focused on wearable health devices [15]. These projects are funded by both government agencies and private organizations.

Fig. 2 WSN chipset sales and projections [25]



Real life projects and applications

Some of the major indoor/outdoor application projects are mentioned here. These applications work on both real time and non-real time modes.

HealthGear [12] It 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] It 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] It 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] It 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.

Fig. 3 Wireless sensors and transmitters market: growth rate and revenue forecast for healthcare, medical and biometrics (World), 2002–2012 [19]

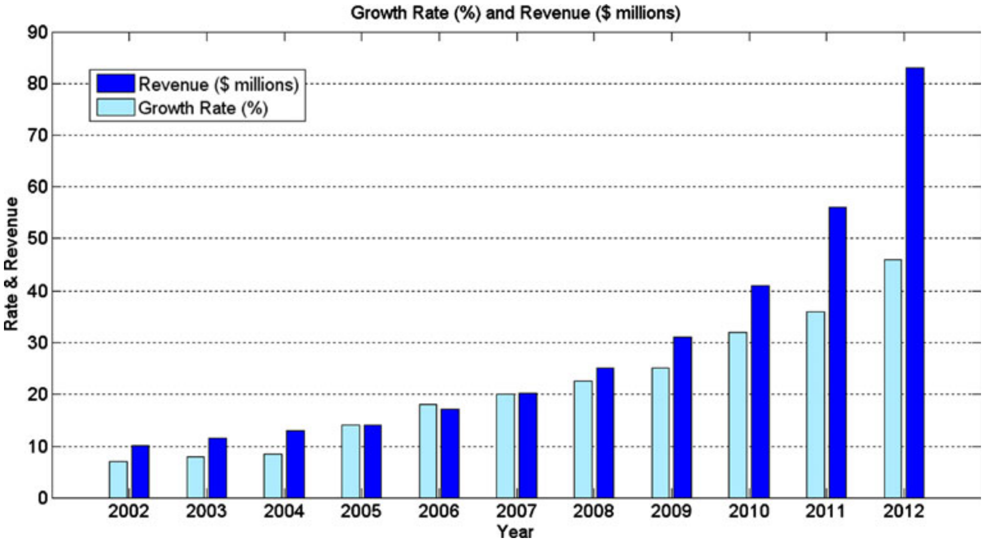


Table 1 Comparison between medical BAN and general WSN

	Medical BAN	General WSN
Common features	Limited resources: battery, computation, memory, energy efficiency Diversity coexistence environment low/modest data rate, low/modest duty cycle Dynamic network scale, plug-and-play, heterogeneous devices ability, dense distribution	
Sensor/ actuator	Single-function device	Multi-function device
	Fast relative movement in small range device lifetime, days, <10 years (implant sensor)	Rare or slow movement in large range network lifetime and device lifetime, months, <10 years
	Safe (low SAR) and quality first	Cost sensitive
Dependability	Reliability (first), guaranteed QoS	Expected QoS, redundancy-based reliability
	Strongly security (except emergency)	Required security
Networking	Small scale star network	Large scale hierarchical network redundant distribution
	No redundancy in device	Random node distribution
	Random node distributionDeterministic node distribution	
Traffic	Periodical real time (dominant), burst (priority)	Burst (dominant), periodical
	Uni-directional traffic	Uni-directional or bi-directional traffic
	M:1 communication	M:1 or point-point communication
channel	Specific medical channel, ISM band	ISM band
	Body surface or through body	Obstacle is unknown

eWatch [7] It 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] A mobile device which 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.

IEEE 802.15.6 also known as Task Group 6 (or TG6) was formed in November 2007 to address the issues and standardize WBAN. The call for proposal was issued in January 2009 and heard till May 2009. The standard intends to address both medical/healthcare applications and other non-medical applications with diverse requirements [5]. The MAC layer in the standard intends to define short range, wireless communication in and around the body area. The standard aims to support a low complexity, low cost, ultra-low power and highly reliable wireless communication for use in close proximity to, or inside, a human body (but not limited to humans) to satisfy an evolutionary set of entertainment and healthcare products and services. The project will also address the coexistence issue with other WBAN and similar networks [5].

The major focus of these projects is to provide affordable services as well as cost effectiveness and power consumption of the devices.

Related works in security and privacy

The concerns for privacy and security have been investigated by some authors. The focus is normally on security related issues in general wireless sensor networks. But these issues as a whole for application scenarios in healthcare perspective have not yet been covered extensively. Many authors have suggested these issues as important. Authors in [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 by authors such as [6] and [11]. Security issues are major concern raised by most authors. Privacy issue or other social implications are not discussed extensively regarding this field. We have mentioned the works done by various authors related to particular issues in the subsequent sections of this paper.

Security issues

Security is one of the most important aspects of any system. People have different perspective regarding security and hence it is defined in many ways. In general words, security is a concept similar to safety of the system as a whole. The US department of commerce site [23] has defined 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.

The communications in sensor networks applications in healthcare are mostly wireless in nature. This may result in various security threats to these systems. 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 a patient or person if compromised may lead to grave consequences. People with malicious intent may use the private data to harm the person.

Security issues in healthcare applications of sensor networks have been always 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 have tried to highlight and discuss some threats and attacks in the following section along with some counter measures.

Threats and attacks

Security breach in healthcare applications of sensor networks is a major concern. It is also worth to mention that since healthcare applications of sensor networks are almost similar to WSN application environment, most of the security issues are also similar and hence comparable. The security issues can be divided into two broad levels: system security and information security. We have discussed these in the subsection of this discussion. Authors in [11] classified the threats and attacks [11] into two major categories—passive and active. A passive attack may occur while routing the data packets in the system. The attackers may change the destination of packets or make routing inconsistent. The attackers may also steal the health data by eavesdropping to the wireless communication media. Active threats are more harmful than their passive counter parts. Criminal minded people may find the location of the user by eavesdropping. This may lead to life threatening situation.

The normal trend of sensor device design is that they have little external security features and hence prone to physical tempering. 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.

Authors in [5] have mentioned attacks in health monitoring in detail manner viz. eavesdropping and modification of medical data, forging of alarms on medical data, denial of service, location and activity tracking of users, physical tampering with devices and jamming attacks. People with bad intent may use the information for harmful activities. The attacks which can occur in any healthcare system using wireless sensor networks are shown in Table 2.

a. *Data modification*—The attacker can delete or replace part or all of eavesdropped information and send the modified information back to original receiver to achieve some illegal purpose. Health data are vital. Modifying them may result in system failure and cause disaster for a person.
b. *Impersonation attack*—If an attacker eavesdrops a wireless sensor node's identity information, it can be uses to cheat the other nodes.
c. *Eavesdropping*—For the open features of wireless channel used by sensor networks, any opponent can intercept radio communications between the wireless nodes freely and easily. Data stole may be used for malicious acts.
d. *Replaying*—The attacker can eavesdrop a piece of valid information and resend it to original receiver after a while to achieve same purpose in different case.

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 these attacks is to steal valuable personal data. Since wireless media is always 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.

Countering the attacks and measures

Any security issues must be resolved while designing the healthcare applications for sensor networks, or else they may give rise to serious social problems as discussed earlier. Authors in [28] argued that in the light of modern concepts of security, the safety should accompany the availability, scalability, efficiency and the quality parameters of inter-node communication. Hence countering the

Table 2 Security risks to WBAN and corresponding security requirements

Attack assumptions	The risks to WBAN	Security requirements
Computational capabilities	Data modification	Data integrality
	Impersonation	Authentication
Listening capabilities	Eavesdropping	Encryption
Broadcast capabilities	Replaying	Freshness protection

system and information security threats should include all aspects of the network and its applications.

a) *System Security*

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

Security in sensor networks applications in health care cannot be compromised. Outmost measures are necessary in this regards. We feel that security safeguard measures should be applied in three levels—Administrative, Physical and Technical. These also come under the domain of network management with emphasis on security.

i) *Administrative Level Security*

Effective administrative control is necessary to manage the system. Security measures should be applied to check the security breaches by the staff or people responsible for overall system operation. A well defined user hierarchy along with strong authentication measures may prevent security breaches at this level. The security measures must include kind of access mechanisms so that only authorized users can access the data. Similarly, it may be also a case where data forwarding may be only to the place or people which are previously authorized.

A start topology with all devices connected to a centralized system can help minimize overheads in network management. These will also help preventing attacks such as DoS and eavesdropping.

ii) *Physical Level Security*

At this level, measures may include controlling access to physical devices and data in the system for supposed stealing or tempering. The devices are vulnerable from people with malicious intent and from natural causes such as wear and tears. In case of natural disasters, the system may malfunction and may pose serious problems to the overall system operation. Hence, careful designing of devices to make them temper proof is necessary. But it is also understood that avoiding physical tempering of devices is hard to achieve. Another preventive measure can be that only authorized people should be allowed to physically handle the devices while in operation. Users must be strongly advised regarding this type of security measures.

iii) *Technical Level Security*

Technical level security checks are necessary mostly on hardware such as servers, disks, and other such devices. If the network is such that data is sent to central servers, server based security measures should be used at the server side and client based security at the end-user side. This is particularly necessary for safe propagation of information. This may again increase load on sensors at user side and thereby increase the overall cost. Hence some trade-offs between these issues will be necessary. 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 security measure. Wireless networks are very much susceptible to intrusion. Intrusion detection and prevention techniques are a must in these networks. Due to sensitive nature of healthcare applications, extra measures such as encryption of data, and constant monitoring of the network is necessary. While constant 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 destination and receivers of data. Hence proper routing protocol and management is necessary to prevent such attacks.

b) *Information security*

WBAN applications contain not only medical but also personal information. Security and privacy are key concerns of all parts in WBAN. However, placing increasing amounts of valuable and confidential data on WBAN devices puts the data at serious risk to theft, sabotage, exploitation and manipulation. As shown in Table 2, there are several security risks surrounding any healthcare system using sensor networks.

The security mechanism of the system is responsible for providing the following security services on specified biomedical data when requested to do so by the applications.

a. *Data Encryption*—The data is encrypted so that it is not disclosed whilst in transit. Data encryption service provides confidentiality against eavesdropping attacks.
b. *Data Integrality*—Data integrality service consists of data integrity and data origin authentication. With data integrity the recipient can be sure that the data has not been altered or changed. Data origin authentication proves to the recipient that the stated sender has originated the data. It is an efficient method against data modification attack.
c. *Authentication*—Authentication service consists of association process among nodes. It is an efficient method against impersonation attacks.

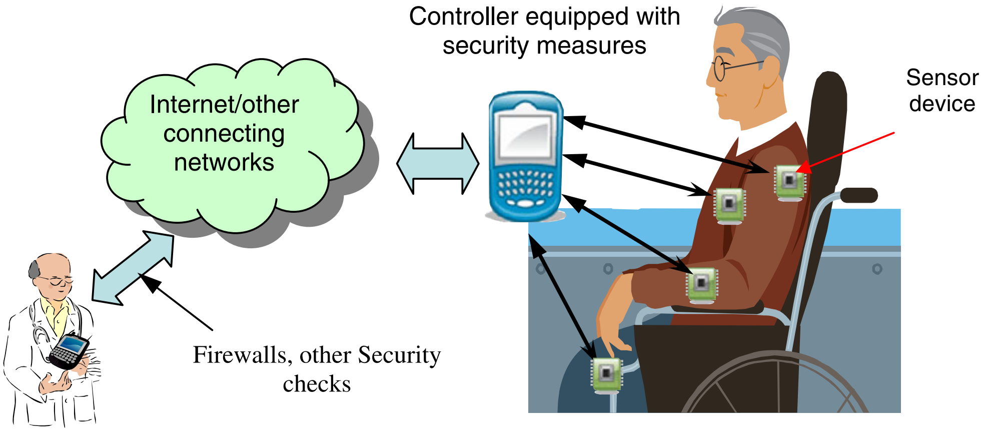

Controller equipped with security measures
Sensor device
Internet/other connecting networks
Firewalls, other Security checks

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

d. *Freshness Protection*—This security service prevents the attacker from replaying the old frames that it eavesdropped by using nonce or time token.

To counter the major threats to information, 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. Authors in [29] proposed an ID-based cryptography and propose a novel secure architecture to enable secure communications in large-scale multi-domain wireless mesh networks. This can be extended easily to the healthcare applications of sensor networks which shows that clients can conveniently gain services securely even when roaming. Furthermore as mentioned by 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 it is claiming to be from [14]. We feel that even if the network is unattended for longer time, security measures should be always in highest priority mode. Authors in [30] discuss unattended network security in detail. It is well argued that adversarial models and defense techniques in prior WSN literature about security are unsuitable for the unattended WSN setting. This can be very helpful for healthcare applications where a person is not subject to constant monitoring or for monitoring elderly patients and illiterate people in remote/underdeveloped areas.

It should be noted that end to end security is must to make the wireless sensor networks in healthcare applications usable and acceptable by the common people. Threats such as tempering with data, denial of service (DoS), physical tampering and eavesdropping need far more special attention than any other common networks. Unless it happens acceptance of wireless sensor networks applications in healthcare will not be easy.

Privacy issues

Privacy is also among major concerns in wireless sensor networks with regard to healthcare applications. The health related data are always private in nature. Privacy issues arise from many reasons. It may be personal belief, social and cultural environment and other general public/private causes. 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.

There are major questions raised by people from time to time. For example, authors in [8] have raised questions regarding guarding the privacy of an individual such as, where should the health data be stored, and who can view a patient's medical record. There are also questions such as to whom should this information be disclosed to without the patient's consent and who will be responsible for maintaining these data in case any problem arise, who will be held accountable. 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.

In normal circumstances there are only few users of the data: the physicians, nurses and some other clinical/technical staffs. This limits the number of users in the system. Well defined regulations and firm guidelines regarding use of data for these users may limit the concerns for 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.

Privacy measures

Besides those mentioned above, some other measures may include:

a) 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].
b) It is also necessary that, specific users should not be identified unless there is a need.
c) 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 from now on. It is mentioned 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.

Conclusion

Sensor networks applications in healthcare being research and deployed all over the world. With the rise of these applications, implications will arise too. In this paper we tried to raise the concerns of major social implications like privacy and security. We have tried to analyze the cause and effects of these two issues. We feel that without taking care of these issues, the necessary growth and development will face major obstacles in coming future. Proper coordination between different government agencies, research institutes and manufactures is necessary to overcome these obstacles and have smooth implementation. General public should also be made aware of the benefits and implications so that they are better prepared. Rules and regulations like that of cyber laws and existing health regulations should be formalized and implemented.

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

References

1. Campbell, A. T., Eisenman, S. B., Lane, N. D., Miluzzo, E., Peterson, R. A., Lu, H., Zheng, X., Musolesi, M., Fodor, K., and Ahn, G., The rise of people-centric sensing. *IEEE Internet Comput.* 12(4):12–21, 2008.
2. Dohler, A., Wireless sensor networks: The biggest cross-community design exercise to-date. *Recent Patents Comput. Sci* 1:9–25, 2008.
3. Hanna L., and Hailes S., Privacy and wireless sensor networks. University College, London, www.petsfinebalance.com/docrepo/privacy_and_WSN.PDF
4. Jovanov, E., Milenkovic, A., Otto, C., and de Groen, P. C., A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *J. Neuro. Eng. Rehabil.* 2:6, 2005.
5. Kargl, F., Lawrence E., Fischer M., and Lim Y. Y., Security, privacy and legal issues in pervasive ehealth monitoring systems. 7th International Conference on Mobile Business icmb, 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 Int. Conference on Performance Modelling and Evaluation of Heterogeneous Networks (HET-NETs'2006), British Computer Society (BCS), IEE, Ilkley, UK, September 11–13, 2006, pp. WP01(1-6).
7. Maurer U., Rowe A., Smailagic A., and Siewiorek D. P., eWatch: a wearable sensor and notification platform. International Workshop on BSN, Wearable and Implantable Body Sensor Networks. 2006, pp.4–145, 3–5 April 2006.
8. Meingast, M., Roosta, T., and Sastry, S., Security and privacy issues with health care information technology. 28th Annual International Conference of the IEEE Engineering in Medicine

and Biology Society, EMBS '06., vol., no., pp.5453–5458, Aug. 30–Sept. 3 2006.

9. Milenkovic, A., Otto, C., and Jovanov, E., Wireless sensor network for personal health monitoring: issues and an implementation. *Comput. Commun.* 29:2521–2533, 2006.
10. Munir, S. A., Yu, W. B., Ren, B., and Ma, M., Fuzzy logic based congestion estimation for qos in wireless sensor network. Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE, pp.4336–4341, 11–15 March 2007.
11. Ng, H. S., Sim, M. L., and Tan, C. M., Security issues of wireless sensor networks in healthcare applications. *BT Technol. J.* 24 (2):138–144, 2006.
12. Oliver, N., and Flores-Mangas, F., HealthGear: a real-time wearable system for monitoring and analyzing physiological signals. International Workshop on Wearable and Implantable Body Sensor Networks, 2006. BSN 2006, pp. 4 pp.-, 3–5 April 2006.
13. Varshney, U., Using wireless technologies in healthcare. *Int. J. Mobile. Comm.* 4(3):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. Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE , pp.722–726, Jan. 2007.
16. Yong, W., Attebury, G., and Ramamurthy, B., A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* 8 (2):2–23, 2006. Second Quarter.
17. Zia, T., and Zomaya, A., Security issues in wireless sensor networks. In Proceedings of International Conference on Systems and Networks Communications, 2006. ICSNC '06, vol., no., pp.40–40, Oct. 2006.
18. Welsh, M., Malan, D., Duncan, B., Fulford-Jones, T., and Moulton, S., Wireless sensor networks for emergency medical care. GE Global Research Conference, Boston, 2004.
19. www.researchandmarkets.com
20. http://fiji.eecs.harvard.edu/CodeBlue
21. http://limserver.com/vitaljacket/index.php
22. http://www.cms.hhs.gov/
23. http://www.its.bldrdoc.gov/
24. http://www.mobihealth.org/
25. http://www.the-infoshop.com
26. http://www.ubimon.net/
27. Zhen, B., Li, H. -B., and Kohno, R. Networking issues in medical implant communications. International Journal of Multimedia and Ubiquitous Engineering. 4(1), January, 2009.
28. Ashraf, A., Rajput, A., Mussadiq, M., Chowdhry, B. S., and Hashmani, M. SNR based digital estimation of security in wireless sensor networks. In Communications Infrastructure. Systems and Applications in Europe , Vol. 16: 35–45, 2009.
29. Zhu, X., Fang, Y., and Wang, Y., How to secure multi-domain wireless mesh networks. Wireless Networks, July 2009.
30. Ma, D., Soriente, C., and Tsudik, G., New adversary and new threats: Security in unattended sensor networks. *IEEE Netw.* 23 (2):43–48, 2009.