INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

AUTHENTICATION IN HEALTH CARE APPLICATION USING WIRELESS MEDICAL SENSOR NETWORK: A SURVEY

Ghasem Farzaneh[1], Ali Rahnamaei[1]

[1]*Department of Computer Engineering, Ardabil Branch, Islamic Azad University, Ardabil, Iran*
Author Correspondence: ghasemfarzaneh2008@yahoo.com

Abstract: - Healthcare applications are considered as promising fields for wireless sensor networks, where patients can be monitored using wireless medical sensor networks (WMSNs). Current WMSN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. This paper discusses the authentication security and privacy issues in healthcare application using WMSNs. We highlight some popular healthcare projects using wireless medical sensor networks, and discuss their security. Our aim is to instigate discussion on these critical issues since the success of healthcare application depends directly on patient security and privacy, for ethic as well as legal reasons. In addition, we discuss the issues with existing security mechanisms, and sketch out the important security requirements for such applications. In addition, the paper reviews existing schemes that have been recently proposed to provide security solutions in wireless healthcare scenarios. Finally, the paper ends up with a summary of open security research issues that need to be explored for future healthcare applications using WMSNs.

Keywords: Healthcare, Wireless Medical Sensor Networks, Authentication, Security, Privacy

1. Introduction

Wireless sensor networks (WSNs) are an emerging technology in existing research and have the potential to transform the way of human life (i.e., make life more comfortable). A wireless sensor is the smallest unit of a network that has unique features, such as, it supports large scale deployment, mobility, reliability, etc. WSNs are not limited to science and engineering, but they are also included in other popular applications such as the military, water monitoring, infrastructure monitoring, government security policy, habitat monitoring, environment monitoring, and earthquake monitoring, are few examples. A sensor network consists of a discrete group of independent nodes with low cost, low power, less memory, and limited computational power that communicate wirelessly over limited frequencies at low bandwidth [1]. The main goals of WSNs are to deploy a number of sensor devices over an unattended area, and collect the environmental data and transmit it to the base

station or remote location. Later, the raw data is processed online or offline for detailed analysis at the remote server according to the application requirements.

1.1 Background

In the 21st century, the healthcare industry has seen the drastic improvements due to the involvement of wireless medical sensor networks (WMSNs) in healthcare applications. A few decades ago WSNs were a topic of science/movie fiction for healthcare industries, and now they have become a reality and provide much quality-of-care. As the world's aging population is increasing at an unprecedented rate in the developed and developing countries. According to the "An Aging World: 2008" report [2], in 2008 the number of aging people worldwide (i.e., 65 years and older) was estimated at 506 million, and by 2040, that number will touch 1.3 billion. Thus, in just over three decades, the percentage of older age people will increase two times from 7% to 14% of the total world population [2]. Although the aging population signifies, a human success story of increased longevity, the steady, sustained growth of the older population also poses health challenges. As more and more people will be entering an elder age, the risk of developing certain chronic and debilitating diseases is significantly higher. For example, Alzheimer disease symptoms typically first appear after age 60 [3], Heart disease and stroke rates rise after age 65 [4], diabetes, like those of many other conditions (e.g., blood pressure, blood glucose levels etc.). Further, if aged populations prefer to live alone they do however require long-term monitoring for better independent life [5]. Thus the aging population desperately demands independent life and good quality-of-care without disturbing their comfort, while reducing their care costs. In this context, wireless sensor technology could provide highly useful tools for elderly people health monitoring and patients who need continuous monitoring. Consequently healthcare using wireless sensor networks constitutes an exciting and growing field for scientific investigation. In fact the future of modern healthcare in an aging world will need ubiquitous monitoring of health with least actual interaction of doctor and patients [6]. Recently, a term wireless medical sensor network (WMSN) has coined to bring many researchers together from interdisciplinary areas (bioengineering, electronics, computer, medicine), as shown in Figure 1.

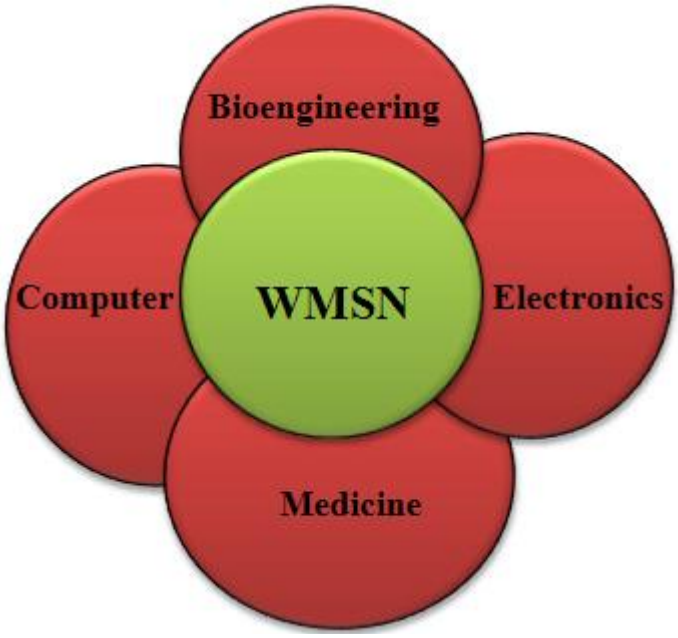

Figure 1: Interdisciplinary research of WMSN.

Wireless medical sensors may be wearable, implantable or portable, and integrated on various kinds of wireless communication motes (such as, Mica2, MicaZ, Telos, etc.). A typical Mica2 mote has a 7.3 MHz Atmel ATmega128L CPU with 128 KB of ROM, and 4 KB of RAM for data [7]. The radio operates at 76.8 Kbps bandwidth at a range of a few meters. Moreover, a sensor node typically has a limited battery power (e.g., AA-batteries), which is just enough for communication (e.g., unicast, multicast and broadcast) and computation [7]. Furthermore, WMSNs are different from generic WSNs. The main differences are summarized in Table 1.

Table 1: Difference between generic WSN and WMSN.

Generic WSNs	WMSNs
Automatic and standalone	Human involvement
Scalability (*i.e.*, large scale)	Scalability (*i.e.*, small scale)
Fixed or distributed deployment	Mobility
Reliability (data rate depend on applications)	Reliability (high data rate)

As we can see from the Table 1, generic WSNs are automatic and standalone, deployed at a large scale in either a fixed or distributed manner, and their data rates depend specifically on the applications, whereas WMSNs have direct human involvement (i.e., patient, doctor, nurse, etc.), are deployed at a small scale (i.e., depending on usability), must support mobility (a patient can carry the devices), and WMSNs requires high data rates (e.g., ECG data is normally sampled at a rate of 250 Hz and blood pressure at 100 Hz [8]), with reliable communication and multiple recipients [9]. Wireless medical sensor motes are deployed on a patient's body, and are used to closely monitor the physiological condition of patients. These medical sensors sense the patient's vital body signs and transmit the sensed data in a timely fashion to some remote location without human intervention. A doctor can use these medical sensor readings and gain a broader assessment of a patient's health status. The patient's vital signs may include heart beats, temperature, blood pressure, motion/acceleration, pulse-oximetry etc. Thus patients could benefit for continuous long-term monitoring after returning home from the hospital.

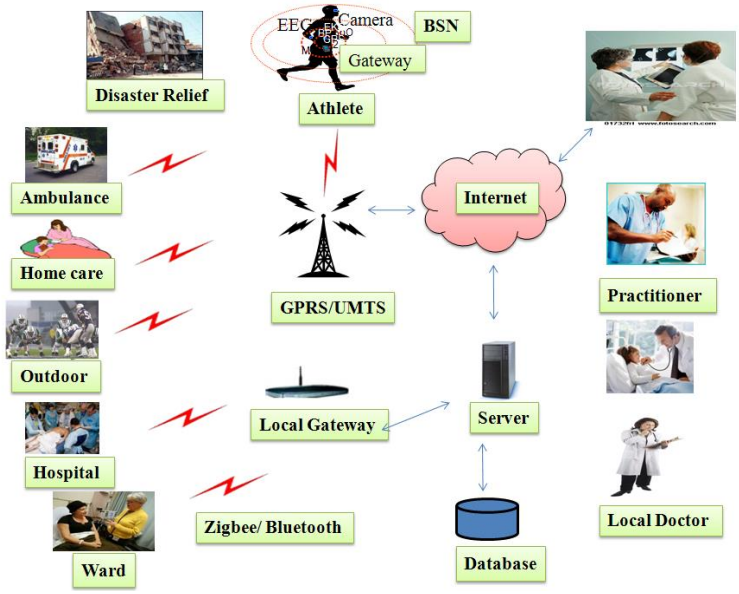

Figure 2: Healthcare application using wireless medical sensor networks.

As shown in Figure 2, WMSNs carry the promise of quality-of-care across wide variety of healthcare applications (e.g., ambulatory monitoring, vital sign monitoring in-hospitals, elderly peoples' at home care monitoring, monitoring in mass-casualty disasters, clinical monitoring, etc.). In addition, other applications that also benefit from WMSNs include sports-person health status monitoring [10], and patients' self-care (i.e., a BAN network on a diabetic patient could be helpful to auto inject insulin though a pump, as soon as their insulin level declines). So far several research groups and projects have started to develop health monitoring using wireless sensor networks, for example, CodeBlue [7], LiveNet [11],

MobiHealth [12], Alarm-Net [13], UbiMon [14], ReMoteCare [15], MobiCare [16,17], Lifeguard [18], AID-N [19], CareNet [20], ASNET [21], WiMoCa [22], SAPHIRE [23], THE-MUSS [24]. Thus, healthcare systems are the most beneficial applications using wireless medical sensor technology that can perform patient care within homes, hospitals, clinics, disaster sites and the open environment.

1.2 Problem Statement

The development of a wireless healthcare application offers many novel challenges, such as, reliable data transmission, node mobility support and fast event detection, timely delivery of data, power management, node computation and middleware [25-32]. Further however, deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable [8,33-36]. For instance, the patient's physiological vital signals are very sensitive (i.e., if a patient has some embarrassing disease), so any leakage of individual disease data could makes him/her embarrassed. In fact sometimes revealing disease information can result in a person losing his/her job, or make it impossible for him/her to obtain insurance protection [37]. Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, and activity monitoring in health-clubs, location tracking for athlete, etc. Consequently, WMSNs share individual data with physicians (in a doctor-patient relationship), insurance companies (as insurance protection), and health-coaches (as sports team trainers) or with family (as relatives' support) [38]. Therefore unauthorized collection and use of patient data by potential adversaries (such as insurance agents, for political reasons, rival coaches, personal enemies etc.) can cause life-threatening risks to the patient, or make the patient's private matters publically available [37]. For example, in a simple scenario, a patient's body sensors transmit his/her body data to a nurse/caregiver; it may happen that an attacker is also eavesdropping the patient data while the data is transmitting, and consequently the patient's privacy is breached. Later that attacker can post the patient data on s social site (Facebook or Twitter, etc.), and thus pose risks to the patient's privacy, as depicted the Figure 3. Indeed wireless healthcare can offer many advantages to patient monitoring, but the physiological data of an individual are highly vulnerable, so security and privacy become some of the big concerns for healthcare applications, especially when it comes to adopting wireless technology. More importantly, a healthcare provider is subjected to strict civil and criminal penalties (i.e., either fine or imprisonment) if HIPAA rules [39] are not followed properly. Thus a patient security and privacy is the central concern in healthcare applications.

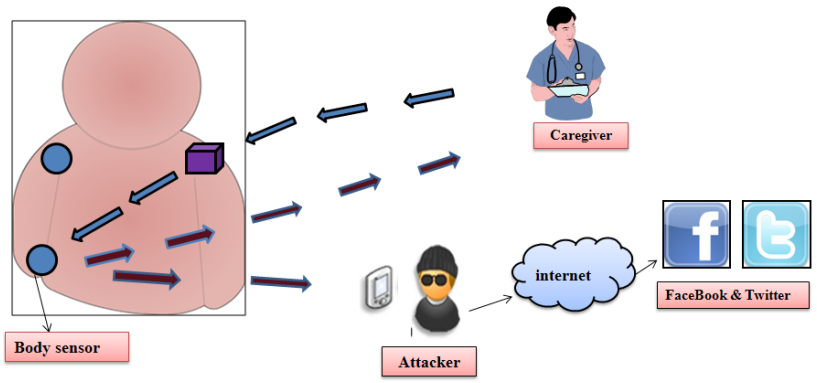

Figure 3: Risks to patient privacy.

2. Authentication and Healthcare Projects Using Wireless Medical Sensor Networks

The advancement of WMSNs in healthcare applications have made patient monitoring more feasible. Recently, several wireless healthcare researches and projects have been proposed, which aim to provide continuous patient monitoring, in-ambulatory, in-hospital, in-clinic, and open environment monitoring (e.g., athlete health monitoring). This section describes few of the popular research projects about healthcare systems using medical sensor networks. CodeBlue [7,44] is a popular healthcare research project based on a medical sensor network developed at the Harvard Sensor Network Lab. In this architecture, several medical sensors (e.g., pulse oximeter, EMG, EKG, and SpO2 sensor board onto the Mica2 motes [45]) are placed on the patient's body. These medical sensors sense the patient body data and transmit it wirelessly to the end-user devices (PDAs,

laptops, and personal computers) for further analysis. The basic idea of CodeBlue is straightforward, a doctor or medical professional issues a query for patient health data using their personal digital assistant (PDA), which is based on a publish and subscribe architecture. The medical sensors publish their relevant data to a specific channel and end-user subscribes the channel by using their hand-held devices (e.g., PDA and laptop). A TinyADMR routing component is used that is based on an adaptive demand-driven multicast routing (ADMR) protocol. TinyADMR facilitates node mobility, multicast routing and minimal path losses. Further, the CodeBlue architecture facilitates RF-based localization (i.e., called MoteTrack [46]), which is accurate enough to locate a patient's or medical professional's position. More importantly, CodeBlue's authors acknowledge the need of security in medical applications, but until now security is still pending or they intentionally left the security aspects for future work, although, in [44] the authors suggested that elliptic curve cryptography (ECC) [47] is a good candidate for the key generation, and TinySec [48] is good for symmetric encryption in CodeBlue project. Further, Kambourakis et al. [49] have sketched-out some security threat and attacks on the CodeBlue project such as denial-of-service attacks, snooping attacks, modification attacks, routing loop attack, grey-hole attack, Sybil attack and masquerading attacks. They address suitable countermeasures for CodeBlue security; for details reader may refer to [49]. CodeBlue is anticipated for deployment in pre-hospital and in-hospital emergency care, stroke patient rehabilitation and disaster response. We assumed that the authors have left security work for future. A heterogeneous network architecture named Alarm-Net was designed at the University of Virginia [13]. The research is specifically designed for patient health monitoring in the assisted-living and home environment. Alarm-net consists of body sensor networks and environmental sensor networks. Three network tiers are applied to the proposed assisted-living and home environment, as shown in Figure 4. In the first tier a resident wears body sensor devices such as ECG, accelerometer, SpO2 (i.e., a MicaZ boards [50]) which sense individual physiological data; and in the second tier environmental sensors such as temperature, dust, motion, light (i.e., MicaZ boards) are deployed in the living space to sense the environmental conditions. In the third tier an internet protocol (IP)-based network is used which is comprised of Stargate gateways called AlarmGate. The idea of Alarm-net is very simple, body sensors broadcast individual physiological data using single-hop to the nearest stationary sensor (i.e., second tier). Thereafter, the stationary emplaced sensor nodes forward the body data using multi-hop communication (i.e., shortest-path-first routing protocol) to the AlramGate. The AlarmGate is a gateway between the wireless sensor and IP networks, and is also connected to a back-end server.

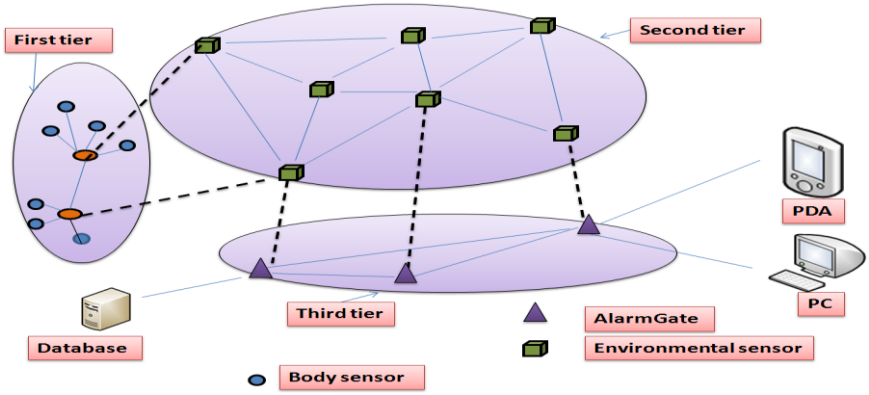

Figure 4: ALARM-NET architecture.

Any real-time data queries about physiological or environmental data are originated by the user that contains the source address, ID, and sensor type. For a single-shot query, the sensors sample the requested data and respond a single report to the query originator, and hence complete the query. In addition, authors have developed a circadian activity rhythms program to aid context-aware power management and privacy policies. Further Alarm-Net facilitates network and data security for physiological, environmental, behavioral parameters about the residents. Only authenticated users can access the Alarm-Net and can query the sensor networks. The IP-network is secured by secure remote password (SRP) protocol for user authentication. The wireless sensor networks are enabled with Link-layer security suites. Sensors (i.e., MicaZ [20] and Telos [21]) use built-in cryptosystems, i.e., an advanced encryption system (AES) for cryptographic operations. AES security modes supported are: none, CBC-MAC authentication-only, CTR mode encryption-only, and CMM combines with authentication and encryption [13]. The major drawback of the built-in cryptosystem is that it does not offer

AES-based decryption, by which means the encrypted data cannot be accessed by an intermediary node during communication, if needed. Further, hardware based built-in cryptosystem makes the application highly platform dependent. More notably, Pai et al. have pointed out some confidentiality infringement scenarios on Alarm-NET, such as the fact it is susceptible to adversarial confidentiality attacks, which can leak resident's location; refer to [22] for details. UbiMon (Ubiquitous monitoring environment for wearable and implantable sensors) [14] is a BSN (Body Sensor Network) architecture composed of wearable and implantable sensors using an ad hoc network. The aim of the project is to provide continuous monitoring of an individual's physiological states and capture transient as well as life threatening abnormalities that can be detected and predicted.

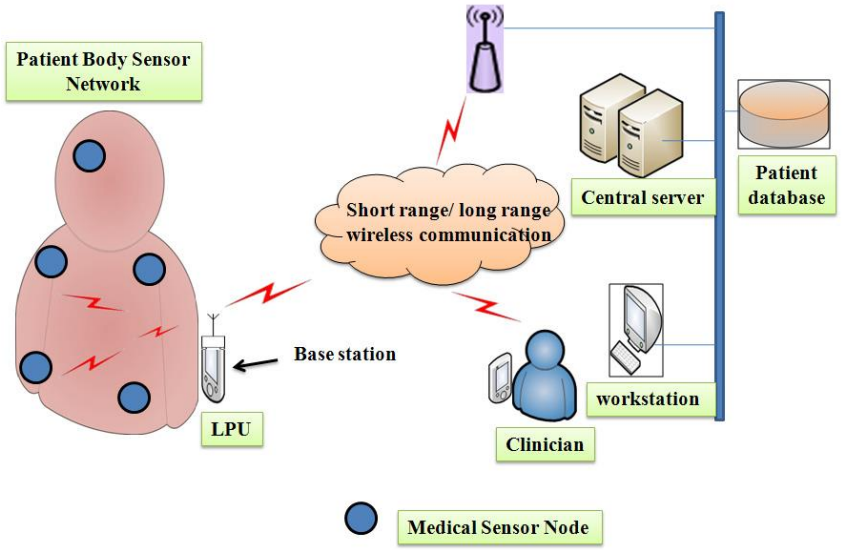

Figure 5: UbiMon system architecture.

As shown in the Figure 5, the UbiMon architecture consists of the following: (i) BSN node: Each node is integrated with bio-sensors (ECG, SpO2, temperature). (ii) LPU (Local Processing Unit): LPUs can be portable devices (PDAs, laptop, etc.) used to the gather data from BSNs, and are known as the base station. They detect the patient's abnormalities and provide immediate warning to the physician. Apart from this function, the LPU works as a router between BSN nodes and the central server using wireless communication (for short range Bluetooth/Wi-Fi and long-range mobile networks such as 3G/GPRS). (iii) CS (Central Sever): A CS feeds the patient data to the PD (Patient Database), and can analyze the patient's data on the basis of patient's condition, and detect potential life-threatening abnormalities. (iv) WS (Work-station): The WS is the patient's data monitoring terminal (PC/laptop), which is used by the physician. Although Ng et al. proposed and demonstrated the ubiquitous healthcare monitoring architecture, it is widely accepted that without considering security for such applications they are often vulnerable to security attacks. So the authors did not consider security for wireless healthcare monitoring, which is a paramount requirement of healthcare applications, according to government laws [39].

2. Security and Privacy Issues for Authentication

Wireless sensor networks in healthcare are used to determine the activities of daily living (ADL) and provide data for longitudinal studies. It is then easy to see that such WSNs also pose opportunities to violate privacy. Furthermore, the importance of securing such systems will continue to rise as their adoption rate increases. The first privacy challenge encountered is the vague specification of privacy. The Heath Insurance Portability and Accountability Act (HIPPA) by the U.S. government is one attempt to define this term [1]. One issue is that HIPPA as well as other laws define privacy using human language (e.g., English), thus, creating a semantic nightmare. Nevertheless, privacy specification languages have been developed to specify privacy policies for a system in a formal way. Once the privacy specifications are specified, healthcare systems must enforce this privacy and also be able to express users' requests for data access and the system's policies. These requests

should be evaluated against the predefined policies in order to decide if they should be granted or denied. This framework gives rise to many new research challenges, some unique to WSNs, as we describe in the paragraphs that follow.

- Since context can affect privacy, policy languages must be able to express different types of context from the environment such as time, space, physiological parameter sensing, environmental sensing, and stream based noisy data. Moreover, most of the context must be collected and evaluated in real-time. Since context is so central it must also be obtained in a secure and accurate manner.
- There is a need to represent different types of data owners and request subjects in the system as well as external users and their rights when different domains such as assisted living facilities, hospitals, and pharmacies interact. One of the more difficult privacy problems occurs when interacting systems have their own privacy policies. Consequently, inconsistencies in such policies may arise across different systems. For this reason, on-line consistency checking and notification along with resolution schemes are required.
- There is a need to represent high-level aggregating requests such as querying the average, maximum, or minimum reading of specified sensing data. This privacy capability must be supported by anonymizing aggregation functions. This need arises for applications related to longitudinal studies and social networking.
- There is a need to support not only adherence to privacy for data queries (e.g., data pull requests), but also the security for push configuration requests to set system parameters (e.g., for private use or configuring specific medical actuators).
- Because WSNs monitor and control a large variety of physical parameters in different contexts, it is necessary to tolerate a high degree of dynamics and possibly even allow temporary privacy violations in order to meet functional, safety or performance requirements. For example, an individual wearing an EKG might experience heart arrhythmia and the real-time reporting of this problem takes precedence over some existing privacy requirements. In other words to send an emergency alert quickly it may be necessary to skip multiple privacy protections. Whenever such violations occur, core healthcare staff members must be notified of such incidents.

In addition this section discusses: (i) which would be the possible threats to a wireless healthcare application without implementation of proper security; and (ii) privacy issues. Before discussing the security issues in wireless healthcare applications, it is worthwhile to assume the scale of deployment of healthcare applications using WMSNs. In this regards, we have considered three wireless healthcare scenarios, namely, a nursing home, in-home monitoring, and in-hospital monitoring, as shown in Figure 6.

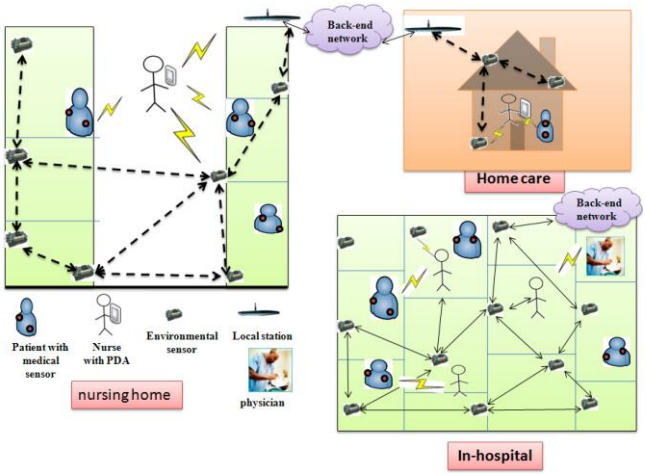

Figure 6: Application scenarios for a nursing home, home care, and in-hospital.

The wireless healthcare applications use medical sensors (i.e., as per patient appropriateness) and environmental sensors (ES), mobile devices (i.e., PDA, laptop or iPhone), and more especially wireless communication (i.e., IEEE 802.11, IEEE 802.15.4, Bluetooth etc.) protocols. Further, a back-end server is used for physiological healthcare information (PHI) storage, and for offline analysis of PHIs. According to the nursing home scenario

Figure 8 (left), medical sensors are placed on a patient's body and sense the physiological data of an individual and transmit it in a timely way to the PDA that may be held by a nurse. A nurse can query the patient's sensors and analyze the real-time patient data conditions. Later she can send patient data to the central server either using Internet or a wireless medium. Many ES are deployed in nursing homes that can form a wired or wireless network, sense the environmental parameters (e.g., ward temperature, humidity, etc.) and transmit the data to either a nurse or a remote center. In addition, the environmental sensors may forward an alarm to the remote server in an emergency situation (e.g., supposing a severe condition is detected), should one occur. In the home scenario (Figure 8, upper right), medical sensors are planted on a patient's body and capture the health data from an individual and transmit it in a timely fashion to a PDA held by a nurse or family member. In addition, environmental sensors are required when a patient is usually alone at home. The environmental sensors are placed at the corners of rooms, collecting the environmental conditions (e.g., room temperature, humidity, etc.), and patient movement data. Later they automatically send collected environmental and patient abnormal conditions to the PDA, which is held by either a nurse or a responsible family member. The home local station can directly communicate with environmental sensors using Zigbee modules. To analyze the patient physiological data an application program will be implemented at the back-end network. In the In-hospital scenario (Figure 8, bottom right), the same deployment and sensing scenario (i.e., as in the nursing home and homecare scenarios) is now applicable to the hospital environment, where groups of patients are temporarily monitored using a wireless medical sensor network by nurses or physicians using their PDAs; for more details the reader may refer to [36].

4. Existing Security Mechanisms

Security mechanisms are processes that are used to detect, prevent and recover from security attacks. Although there are significant security mechanisms for traditional networks (i.e., wired and ad hoc) they are generally not directly applicable to resource constrained wireless medical sensor networks, so this sub-section discusses the issues concerning existing security mechanisms, as follows:

4.1 *Cryptography*

As wireless medical sensor networks deal with sensitive physiological information, strong cryptographic functions (i.e., encryption, authentication, integrity, etc.) are paramount requirements for developing any secure healthcare application. These cryptographic functions provide patient privacy and security against many malicious attacks. Strong cryptography requires extensive computation and resources, therefore selecting appropriate cryptography are a challenging task for resource hungry medical sensor nodes that can provides maximum security whilst utilizing the minimum resources. Further, the selection of cryptography system depends on the computation and communication capability of the sensor nodes. Some argue that asymmetric crypto systems are often too expensive for medical sensors and symmetric crypto systems are not versatile enough. However, applying the security mechanisms to resource constrained medical sensors should be selected based on the following considerations: Energy: how much energy is needed to perform the crypto functions Memory: how much memory (i.e., read only memory and random access memory) is needed for security mechanisms. Execution-time: how much time is required to execute the security mechanisms.

4.2 *Key Management*

Key management protocols are fundamental requirements to develop a secure application. These protocols are used to set up and distribute various kinds of cryptographic keys to nodes in the network. Generally, there are three types of key management protocols, namely, trusted server, key Pre-distribution and self-enforcing [40]. (i) Trusted server protocols rely on a trusted base station responsible for establishing the key agreement in the network. It is considered that the trusted server protocols are well suited to hierarchical networks in the presence of unlimited resource gateways. Although, trusted server based schemes provide stronger security to hierarchical networks, in a Real-time environment, a trusted server could become a single point for the entire network failure; Hence, they are not suitable for critical applications (e.g., healthcare) [40]. (ii) Key pre-distribution Protocols are based on symmetric key cryptography, where secret keys are stored in the network before the

network deployment. The key pre-distribution protocols are easy to implement, and offer relatively less computational complexity, making them more suitable for resource constrained sensor networks. (iii) Self-enforcing protocols using a public-key infrastructure provide many advantages, such as, strong security, scalability, and memory efficiency. Earlier public key based solutions were thought to be too computationally expensive (i.e., RSA [31] and Diffie-Hellman key exchange [32]) for wireless sensor networks. However, some researchers [33-35] have shown that Elliptic curve cryptographic based schemes are viable on resource constrained networks. In fact, in real-time implementation, the ECC based necessary cryptographic primitives (e.g., signature generation and verification) are still expensive in term of the time complexity.

5. Security and Privacy Requirements of Healthcare Applications

Based on the above application scenarios, security issues and regulatory laws, this section points out the paramount security and privacy requirements for healthcare applications using wireless medical sensor networks, as follows:

1) Data confidentiality: Patient health data are generally held under the legal and ethical obligations of confidentiality. These health data should be confidential and available only to the authorized doctors or other caregivers. Thus, it is important to keep the individual health information confidential, so that an adversary cannot eavesdrop on the patient's information. Data eavesdropping may cause damage to the patient because the adversary can use the patient's data for many illegal purposes and hence, the patient's privacy is breached. Therefore, data confidentiality is an important requirement in healthcare applications using WMSNs.
2) Data authentication: Authentication services provide authorization, which is necessary for both medical and non-medical applications. In WMSN healthcare applications, authentication is a must for every medical sensor and the base-station to verify that the data were sent by a trusted sensor or not.
3) Strong user authentication: The major problem in a wireless healthcare environment is vulnerability of wireless messages to an unauthorized user, so it is highly desirable that strong user authentication should be considered, whereby each user must prove their authenticity before accessing any patient physiological information. Furthermore, strong user
authentication, also known as two-factor authentication, provides greater security for healthcare applications using wireless medical sensor networks.
4) Data integrity: Data integrity services guarantee at the recipient end that the data has not been altered in transit by an adversary. Due to the broadcast nature of the sensor network, the patient's information could be altered by an adversary; this could be very dangerous in the case of life-critical events. To verify the data integrity, one must have the ability to identify any data manipulation done by illegal parties. Thus, proper data integrity mechanisms ensure that the received data has not been altered by an adversary.
5) Key distribution: If two parties exchange information, they must share a session key and that key must be protected from others. A secure session key helps secure subsequent communication and safeguards data against various security attacks. Thus in order to preserve the patient's privacy, an efficient key distribution scheme is a major requirement in wireless healthcare applications.
6) Access control: In healthcare application many users (such as doctors, nurses, pharmacists, insurance companies, lab staff, social workers, etc.) are always directly involved with the patient's physiological data, so it is highly desirable that a role-based access control Authors are expected to conclude their presentation comprehensively in the conclusion. Authors have to freedom to include future research details as part of the conclusion or as a separate section before the conclusion, depending on the appropriateness. Conclusion should not repeat the main text; instead it should try to help the reader to have a strong view on the article's claims. Following a critical approach on own research methods and experiments can show maturity and impartial evaluation, which enhance the quality of your article.

In addition, patient's anonymity is also needed for healthcare applications because medical sensor networks are wireless in nature. Thus anonymity hides the source of a packet (i.e., medical sensor data) during wireless

communication. It is a service that can enable confidentiality. Further, a wireless healthcare application should enable minimum survivability in the presence of power loss, failures or attacks.

6. Conclusions

This survey discussed the security and privacy issues in healthcare applications using medical sensor networks. It has been shown that a well-planned security mechanism must be designed for the successful deployment of such a wireless application. In this respect, we have found many important challenges in implementing a secure healthcare monitoring system using medical sensors, which reflects the fact that if a technology is safe, then people will trust it. Otherwise, its use will not be practical, and could even endanger the patient's life. Consequently, many security and privacy issues in healthcare applications using wireless medical sensor networks still need to be explored and we hope that this survey will motivate future researchers to come up with more robust security mechanisms for real-time healthcare applications.

REFERENCES

[1] Ko, B.J.G.; Lu, C.; Srivastva, M.B.; Stankovic, J.A.; Terzis, A.; Welsh, M. Wireless Sensor Network for Healthcare. Proc. IEEE 2010, 98, 1947-1960.
[2] An Aging World. Available online: http://www.census.gov/prod/2009pubs/p95-09-1.pdf (accessed on 2 October 2011).
[3] Alzheimer's Disease. Available online: http://www.nia.nih.gov/NR/rdonlyres/7DCA00DB-1362- 4755-9E87 96DF669EAE20/18196/ADFACTSHEET.pdf (accessed on 7 October 2011).
[4] Aging Heart and Arteries, A scientific Quest. Available online: http://www.nia.nih.gov/ NR/rdonlyres/0BBF820F-27D0-48EA-9820-736B7E9F08BB/0/HAFinal_0601.pdf (accessed on 7 October 2011).
[5] Gaddam, A.; Mukhopadhyay, S.C.; Gupta, G.S. Elder Care Based on Cognitive Sensor Network. IEEE Sensors J. 2011, 11, 574-581.
[6] Chung, W.Y.; Walia, G.; Lee, Y.D.; Myllyla, R. Design Issues and Implementation of Query-Driven Healthcare System Using Wireless Sensor Ad Hoc Network. In Proceedings of 4th International Workshop on Wearable and Implantable Body Sensor Network (BSN 2007), Aachen, Germany, 26–28 March 2007.
[7] Malan, D.; Jones, T.F.; Welsh, M.; Moulton, S. CodeBlue: An Ad-Hoc Sensor Network Infrastructure for Emergency Medical Care. In Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004), Boston, MA, USA, 6–9 June 2004.
[8] Dimitriou, T.; Loannis, K. Security Issues in Biomedical Wireless Sensor Networks. In Proceedings of 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL'08), Aalborg, Denmark, 25–28 October 2008.
[9] Muhammad, K.R.R.S.; Lee, H.; Lee, S.; Lee, Y.K. BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks. Sensors 2010, 10, 3911-3933.
[10] Alonso, J.V.; Matencio, P.L.; Castano, F.J.G.; Hellin, H.N.; Guirao, P.J.B.; Martinez, F.J.P.; Alvarez, R.P.M.; Jimenez, D.G.; Castineira, F.G.; Fernandez, R.D. Ambient Intelligence Systems for Personalized Sport Training. Sensors 2010, 10, 2359-2385.
[11] Chen, B.R.; Peterson, G.; Mainland, G.; Welsh, M. LiveNet: Using Passive Monitoring to Reconstruct Sensor Network Dynamics. In Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor System (DCOSS'08), Santorini Island, Greece, 11–14 June 2008.
[12] Halteren, A.V.; Bults, R.; Wac, K.; Konstantas, D.; Widya, I.; Dokovsky, N.; Koprinkon, G.; Jones, V.; Jerzog, R. Mobile Patient Monitoring: The MobiHealth System. J. Inform. Tech. Healthcare 2004, 2, 365-373.
[13] Wood, A.; Virone, G.; Doan, T.; Cao, Q.; Selavo, L.; Wu, Y.; Fang, L.; He, Z.; Lin, S.; Stankovic, J. ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring; Technical Report CS-2006-01; Department of Computer Science, University of Virginia: Charlottesville, VA, USA, 2006.
[14] Kamalika Chaudhuri and Nina Mishra. When random sampling preserves privacy. In 26th Annual International Cryptology Conference (CRYPTO), 20006.
[15] B. Chen, K.K. Muniswamy-Reddy, and M. Welsh. Ad-hoc multicast routing on resource-limited sensor nodes. In Proceedings of the 2nd international workshop on Multi-hop ad hoc networks: from theory to reality, page 94, 2006.
[16] O. Chipara, C. Brooks, S. Bhattacharya, C. Lu, R.D. Chamberlain, G.- C. Roman, and T.C. Bailey. Reliable Real-time Clinical Monitoring Using Sensor Network Technology. In American Medical Informatics Association Annual Symposium (AMIA), November 2009.
[17] O. Chipara, C. Lu, T. C. Bailey, and G.-C. Roman. Reliable patient monitoring: A clinical study in a step-down hospital unit. Technical Report WUCSE-2009-82, Department of Computer Science and Engineering, Washington University at St. Louis, Dec 2009.
[18] CNN. Death after two-hour ER wait ruled homicide, September 2006.
[19] Coalition for American Trauma Care. Action Needed to Bolster Nation's Emergency Care System, June 2006.
[20] James Coughlan and Roberto Manduchi. Color targets: fiducials to help visually impaired people find their way by camera phone. J. Image Video Process., 2007(2):10–10, 2007.
[21] Foad Dabiri, Alireza Vahdatpour, Hyduke Noshadi, Hagop Hagopian, and Majid Sarrafzadeh. Ubiquitous personal assistive system for neuropathy. In HealthNet '08: Proceedings of the 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, pages 1–6, New York, NY, USA, 2008. ACM.

[22] T. Das, P. Mohan, V. N. Padmanabhan, R. Ramjee, and A. Sharma. PRISM: Platform for Remote Sensing using Mobile Smartphones. In International conference on Mobile systems, applications, and services (MobiSys), June 2010.
[23] R.P. Dresher and P.P. Irazoqui. A Compact Nanopower Low Output Impedance CMOS Operational Amplifier for Wireless Intraocular Pressure Recordings. In Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, pages 6055–6058, Aug. 2007.
[24] Adam Dunkels, Bj¨orn Gr¨onvall, and Thiemo Voigt. Contiki – a lightweight and flexible operating system for tiny networked sensors. In Proceedings of the First IEEE Workshop on Embedded Networked Sensors (Emnets-I), Tampa, Florida, USA, November 2004.
[25] Emory A. Fry and Leslie A. Lenert. MASCAL: RFID Tracking of Patients, Staff and Equipment to Enhance Hospital Response to Mass Casualty Events. In Proceedings of the AMIA Annual Symposium, page 261265, January 2005.
[26] Raghu Ganti, Praveen Jayachandran, Tarek Abdelzaher, and John Stankovic. SATIRE: A Software Architecture for Smart AtTIRE. In Proc.ACM Mobisys, Uppsala, Sweden, June 2006.
[27] T. Gao, C. Pesto, L. Selavo, Y. Chen, J. Ko, J. Lim, A. Terzis, A. Watt, J. Jeng, B. Chen, et al. Wireless medical sensor networks in emergency response: Implementation and pilot results. In IEEE Int. Conf. Technologies for Homeland Security, 2008.
[28] David Gay, Phil Levis, Rob von Behren, Matt Welsh, Eric Brewer, and David Culler. The nesC Language: A Holistic Approach to Networked Embedded Systems. In Proceedings of Programming Language Design and Implementation (PLDI) 2003, June 2003.
[29] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis. Collection Tree Protocol. In Proceedings of SenSys, 2009.
[30] M.S. Goodwin, W.F. Velicer, and S.S. Intille. Telemetric monitoring in the behavior sciences. Behavior Research Methods, 2007.
[31] A Hanjagi, P Srihari, and AS Rayamane. A public health care information system using GIS and GPS: a case study of Shiggaon. In PC Lai and SH Mak, editors, GIS for Health and the Environment, pages 243–55. Springer, 2007.
[32] Jin He, Huaming Li, and Jindong Tan. Real-time daily activity classification with wireless sensor networks using hidden markov model. Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, pages 3192–3195, Aug. 2007.
[33] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, 12: 55-91, 2012.
[34] Â . Costa, J. C. Castillo, P. Novais, A. Fernández-Caballero and R. Simoes, "Sensor-driven agenda for intelligent home care of the elderly," Expert Syst. Appl., 39: 12192-12204, 2012.
[35] S. Led, M. Martinez-Espronceda, J. Redondo, A. Baquero, L. Serrano, L. Cabezas and M. Niegowski, "Wearable electrocardiogram (ECG) recorder for a mobile point-of-care based on recent interoperability standards," 2013 IEEE Point-of-Care Healthc. Technol., 287-290, 2013.
[36] I. Martíez, J. Escayola, M. Martínez-Espronceda, P. Muñoz, J. D. Trigo, A. Muñoz, S. Led, L. Serrano and J. García, "Seamless integration of ISO/IEEE11073 personal health devices and ISO/EN13606 electronic health records into an end-to-end interoperable solution," Telemed. e-Health, 16: 993-1004, 2010.
[37] B. Latré, B. Braem, I. Moerman, C. Blondia and P. Demeester, "A survey on wireless body area networks," Wirel. Netw., 17: 1-18, 2011.
[38] G. Blumrosen, N. Avisdris, R. Kupfer and B. Rubinsky, "C-SMART: Efficient seamless cellular phone based patient monitoring system," IEEE Int. Symp. World Wirel. Mob. Multimed. Netw., 1-6, 2011.
[39] D. Malan, T. Fulford-Jones, M. Welsh and S. Moulton, "CodeBlue: An Ad hoc sensor network infrastructure for emergency medical care," Proc. Int. Workshop Wearable Implant. Body Sens. Netw., 12-14, 2004.
[40] L. Coluccini, A. Belardinelli, D. Shklarski, M. Alon, E. Hirt, R. Schmid and M. Vuskovic, "AMON: a wearable multiparameter medical monitoring and alert system," IEEE Trans. Inf. Technol. Biomed., 8: 415-427, 2004.
[41] O. Nee, A. Hein, T. Gorath, N. Hulsmann, G. B. Laleci, M. Yuksel, M. Olduz, I. Tasyurt, U. Orhan, A. Dogac, A. Fruntelata, S. Ghiorghe and R. Ludwig, "SAPHIRE: intelligent healthcare monitoring based on semantic interoperability platform: pilot applications," IET Commun., 2: 192-201, 2008.
[42] D. Han, M. Lee and S. Park, "THE-MUSS: mobile u-Health service system," Comput. Meth. Programs Biomed., 97: 178-188, 2010.
[43] P. Kumar and H. J. Lee, "A user authentication for healthcare application using wireless medical sensor networks," 2011 13th Int. Conf. High Perform. Comput. Commun., 647-652, 2011.
[44] J. T. Kim, "Enhanced secure authentication for mobile RFID healthcare system in wireless sensor networks," Commun. Comput. Inf. Sci., 352: 190-197, 2012.
[45] A. K. Das, "Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks," Int. J. Netw. Secur., 14: 1-21, 2012.
[46] X. H. Le, M. Khalid, R. Sankar and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," J. Netw., 6: 355-364, 2011.
[47] H. M. Chen, J. W. Lo and C. K. Yeh, "An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems," J Med. Syst., 36: 3907-3915, 2012.
[48] C. C. Lee, R. X. Chang, T. Y. Chen and L. A. Chen, "An improved delegation-based authentication protocol for PCSs," Inf. Technol. Control, 41: 258-267, 2012.
[49] C. C. Lee, T. H. Lin and R. X. Chang, "A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards," Expert Syst. Appl., 38: 13863-13870, 2011.
[50] J. K. O'Herrin, N. Fost and K. A. Kudsk, "Health insurance portability accountability act (HIPAA) regulations: effect on medical record research," Ann. Surg., 239: 772-776, 2004.