Security and Privacy Issues in Wireless Sensor Networks for Healthcare

Vivek Agrawal(✉)

Norwegian Information Security Laboratory (NISLab), Gjøvik Univeristy College, Gjøvik, Norway
vivek.agrawal@hig.no

Abstract. *Background* –The design and development of wearable sensors enable user to monitor physiological data using wireless sensor networks (WSNs) in healthcare. *Problem* –healthcare applications based on WSNs are not addressing security and privacy issues. *Effect* –A healthcare system using a sensor network can subject to the privacy breach of the patients as the sensitive data may be exposed to a malicious party. Serious security threats might compromise the healthcare service, disabling patients to avail healthcare facilities. *Contribution* –(a) An overview of the status of security requirements in various WSNs healthcare application. (b) An overview of potential security and privacy threats that can compromise the normal functionality of a WSNs healthcare system. (c) We also present a study on the existing security mechanisms to safeguard WSNs healthcare system.

Keywords: Healthcare applications · Patient privacy issues · Security threats · Security mechanism · Wireless sensor network

1 Introduction

The main components of a healthcare monitoring system are –Hardware, software, System Interfaces, Data, services and people. The sensor data being collected by the WSNs contains information about the health status of the patient and stored in a database. Health status data commonly include information of blood pressure, heart rate, distance traveled through walking/ running, playing activities, and surroundings (e.g. room temperature). We are mainly focusing on the medical data as an important asset in this report. The security requirements, threats and mechanism are proposed in the context of protecting Health data. This review report addresses the security challenges in WSNs for healthcare systems. Section 2 discusses major security requirements to protect user's health related data in the most important and widely employed wearable system to monitor physiological data of the user. Section 3 presents a list of possible threats on the security and privacy of user's data. Section 4 proposes various mechanism to counter security threats identified in the Sect. 3. Section 5 offers some concluding thoughts and reflection on the findings of this study.

R. Giaffreda et al. (Eds.): IoT360 2014, Part I, LNICST 150, pp. 223–228, 2015.
DOI: 10.1007/978-3-319-19656-5_32

2 Security Requirements in a WSNs Healthcare System

Data Confidentiality: The health data should be confidential and available only to the authorized doctors or other caregivers. A sensor network should not leak sensor readings to neighboring networks. **Data Integrity:** It must be ensured that content of the messages must remain unchanged throughout the process of data recording to data storage and manipulation. **Data Availability:** In many sensor network deployments, keeping the network available for its intended use is essential. **Data Authentication:** In WSNs 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. **Data Freshness:** Data freshness implies that the patient physiological signs are captured in recent time, and thus, an adversary has not replayed the old messages. **Consent & Privacy:** A User's consent/ permission is needed when a healthcare provider is sharing his/ her health records to another healthcare consultant. Health information should not be distributed without patient authorization. Persons are entitled to access and amend their health records.

We considered some well-known wireless sensing healthcare applications to analyze the status of security and privacy. It can be seen in the Table 1 that there is low awareness of security and privacy in the wireless healthcare application. **UbiMon**, **LifeGuard** not even raised the issue of privacy violation while developing their system. Authors did not consider any security requirements for this application. They did not even address the importance of security or their intention to implement any in the future. **CodeBlue** and **AUBADE** discussed the importance of data privacy but didn't mention any mechanism to ensure it. Authors of **SATIRE** made a weak assumption that the use of internet can guarantee proper availability without any adoption of secure mechanism. Authors of **AMON** project [1] claimed to implement a mechanism to secure confidentiality, integrity, authentication and privacy in their system. However, the technical report does not mention anything explicitly about the security measures. The entries in the Table 1 consist of: NA: the requirement is not acknowledged in the report, NI: no mechanism is enforced to implement the security requirement, I: a mechanism is used to implement security requirement, A: the requirement is acknowledged in the report as a current/ future work.

Table 1. An overview of the status of security requirements in healthcare applications

Projects	Confidentiality	Integrity	Availability	Authentication	Consent &Privacy	Freshness
UbiMon [2]	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI
LifeGuard [3]	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI
AMON [1]	A-I	A-I	A-NI	A-I	A-I	NA-NI
CodeBlue [4]	A-NI	A-NI	NA-NI	A-NI	A-NI	NA-NI
AUBADE [5]	A-NI	A-NI	A-NI	NA-NI	A-NI	NA-NI
SATIRE [6]	A-NI	A-NI	A-I	A-NI	A-I	NA-NI

3 Security and Privacy Threats

This section describes potential security and privacy issues associated to a WSNs healthcare application. These issues may impose severe threats in the absence of proper security counter-measure. Private information of the user/ patient can be leaked to the malicious party.

Eavesdropping or Snooping: This is a passive form of security attack, suggesting simply that some entity is listening to (or reading) communications or browsing files or system information. **LifeGuard** project uses 802.11b (IEEE wireless local area network standard) over the internet to a central server. 802.11 provides no protection against attacks that passively observe traffic [7]. Frame headers of the traffic messages are sent without any encryption and visible to everybody with a wireless network analyzer. **CodeBlue** Technical report does not mention whether the framework employs some cryptographic methods in the upper layers of network.

Routing Attack: Kambourakis et al. [8] mentioned that **CodeBlue** is prone to Sybil attack when it is operated in ad-hoc mode. In the case of *Sybil* attack [9], a single node duplicates itself and presented in the multiple locations. The attacking node acting as a publisher could advertise through its multiple false identities that he has medical data to send. In the case of **CodeBlue**, an attacker can alter the header of the ADMR packets changing one or more of the address fields (senderAddr, destAddr, originAddr, groupAddr).

Masquerading or Spoofing: Masquerading is an impersonation of one entity by another. **AUBADE** uses IEEE 802.11b for transmitting all the bio-signals obtained from the sensors of the wearable. AUDABE system can be a subject to spoofing as 802.11 networks do no authenticate frames. Attacker can modify the sender address in ADMR packets in **CodeBlue** devices and camouflage its device to make the others believe that s/he is someone else. A proper implementation of 'authentication services' counter this threat.

Denial-of-Service (DoS) Threats: Denial of Service is some occasion that diminishes or eliminates a network's capacity to execute its expected function. In the physical layer the DoS attacks could be network-jamming and node-tampering. At link layer, collision, exhaustion can be executed to produce DoS attack. Similarly, Network layer can be affected with misdirection, black holes. This attack can jam the network in **LifeGuard**, **CodeBlue**, etc. and disrupt the normal service of the system.

Privacy Issues: The definition of privacy, which is adopted in this report, is defined by North Carolina Healthcare Information and Communication Alliance, Inc. It defines privacy as *"'An individual's right to control the acquiring, use or release of his or her personal health information"'* [10]. **CodeBlue**, **AUBADE**, **LifeGuard**, **UbiMon** neither address not implement any mechanism to protect the privacy of the user. Authors in [11] discussed several questions related to privacy of medical data. The questions raised in [11] are (a) Who has the authority to delete, add and edit information to health data? (b) What type of data,

and how much data, should be stored? (c) Where should the health data be stored? (d) Who can view a patient's medical record? (e) To whom should this information be disclosed to without the patient's consent?

As we have seen in the above section, there are potential security and privacy threats exist in healthcare system. Each and every healthcare application is to security and privacy threats. It is obvious that extensive security and privacy research is needed in wireless healthcare application, which can fill the security gaps that we have discussed in the above section.

4 Security Mechanism

A wireless sensor network consists of a large number of tiny sensor nodes deployed over a geographical area. These nodes have *limited processing* capability, *low-storage* capacity and *constrained communication* bandwidth. Therefore, a set of appropriate security mechanisms is proposed and analyzed by many researchers in order to suit the requirements of medical WSNs. Consequently, the security gap between the above security measures are still needs to be explored for healthcare applications.

Encryption: Encryption can be used to ensure the confidentiality of the data and prevent eavesdropping/ snooping. In sensor networks, **TinySec** [12] is proposed as a solution to achieve link-layer encryption and authentication of data. Authors of **SATIRE** project [6] indicated the use of TinySec to ensure security and privacy in their system.

Secure Routing: Karlof & Wagner [9] argued that sensor network routing protocols are not designed with security as a goal. Ferng et al. [13] proposed an energy-efficient secure routing protocol for WSNs. Their protocol addresses issues of delivery rate, energy balancing, and routing efficiency. It also includes authentication and encryption mechanism in the data delivery. The μ**TESLA** (Timed Efficient Stream Loss-tolerant Authentication) protocol [14] can be used for the authentication of broadcast messages with minimal packet overhead. μTESLA is a routing protocol which provides authenticated broadcast for severe resource-constrained environments.

Secure Authentication: Authentication mechanism can be used to ensure the data/ requests are coming from the valid entity it is claiming to be. Guo et al. [15] has proposed a certificate-less authentication scheme without bilinear pairing while providing patient anonymity. Yu et al. [16] proposed password-based user authentication scheme for the wireless healthcare system. The proposed scheme consists of four phases, namely the registration phase, the pre-computing phase, the authentication phase and the password change phase.

Freshness Protection: Perrig et al. proposed **SPINS** protocol [14] to ensure data freshness in a WSN. Their protocol achieves both weak freshness –required by sensor measurements, and strong freshness –is useful for time synchronization within the network. SPINS uses nonce to achieve message freshness.

Regulation and Laws: United States law mandates that medical devices meet the privacy requirements of the 1996 Health Insurance Portability and

Table 2. Security risks and corresponding security requirements

Security Threats	Security Requirements	Security Solutions
Eavesdropping/ Snooping	Data Confidentiality	Data Encryption
Routing attacks	Data Confidentiality, data integrity, data availability	Secure Routing
Masquerading/ spoofing	Data Authentication	Secure Authentication
Privacy	User's Consent	Law & Regulation
Data Replay	Data Freshness	Freshness protection
Denial-of-service	Data availability	Secure routing

Accountability Act, **HIPAA**. The rule gives patient's rights over their health information, including rights to examine and obtain a copy of their records, and to request corrections. The European Union Directive **2002/58/EC** [17] taking care of the privacy of sensitive medical and health data. It mandates to erase traffic data or to make such data anonymous when it is no longer in use.

5 Discussion and Conclusion

The potential of Wireless sensor networks has been widely accepted in the healthcare system. However, advantages of sensor applications can be exploited effectively if the desired level of security and privacy can be ensured. It is found in our study that almost all the WSNs healthcare applications lack a measure to counter security and privacy challenges. Researchers are either ignoring the security aspects or keeping it aside for the future works. This has created a major security gaps in the existing healthcare solution. We presented a list of potential threats to manifest the importance of proper acknowledgment of security and privacy issues in the healthcare system. We also discussed possible mechanisms to counter threats and ensure privacy of user's data. The relationship among various security requirements, attacks and countermeasures, discussed in this study, can be presented using Table 2. This table serves as a guideline to understand the associated security requirement with each security threats and how can it be mitigated using a security mechanism. Consequently, general public awareness is a vital mechanism that must be given proper importance to address various security and privacy issues. It can be extremely useful if people are educated regarding security, privacy issues, existing laws and regulations.

References

1. Anliker, U., Ward, J., Lukowicz, P., Troster, G., Dolveck, F., Baer, M., Keita, F., Schenker, E., Catarsi, F., Coluccini, L., Belardinelli, A., Shklarski, D., Alon, M., Hirt, E., Schmid, R., Vuskovic, M.: Amon: a wearable multiparameter medical monitoring and alert system. IEEE Trans. Inf. Technol. Biomed. **8**(4), 415–427 (2004)

2. Ng, J.W.P., Lo, B.P.L., Wells, O., Sloman, M., Peters, N., Darzi, A., Toumazou, C., Yang, G.Z.: Ubiquitous monitoring environment for wearable and implantable sensors (UbiMon). In: UbiComp 2004 - The Sixth International Conference on Ubiquitous Computing, Poster Proceedings. UbiComp 2004 (2004)
3. Mundt, C., Montgomery, K., Udoh, U., Barker, V., Thonier, G., Tellier, A., Ricks, R., Darling, B., Cagle, Y., Cabrol, N., Ruoss, S., Swain, J., Hines, J., Kovacs, G.T.A.: A multiparameter wearable physiologic monitoring system for space and terrestrial applications. IEEE Trans. Inf. Technol. Biomed. **9**(3), 382–391 (2005)
4. Shnayder, V., Chen, B.r., Lorincz, K., Jones, T.R.F.F., Welsh, M.: Sensor networks for medical care. In: Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems SenSys 2005, pp. 314–314. ACM, NY, USA (2005)
5. Katsis, C., Ganiatsas, G., Fotiadis, D.: An integrated telemedicine platform for the assessment of affective physiological states. Diagn. Pathol. **1**(1) (2006)
6. Ganti, R.K., Jayachandran, P., Abdelzaher, T.F., Stankovic, J.A.: Satire: A software architecture for smart attire. In: Proceedings of the 4th International Conference on Mobile Systems, Applications and Services. MobiSys 2006, pp. 110–123, ACM, NY, USA (2006)
7. Gast, M.: The Top Seven Security Problems of 802.11 Wireless. Technical report, May 2002
8. Kambourakis, G., Klaoudatou, E., Gritzalis, S.: Securing medical sensor environments: the codeblue framework case. In: ARES 2007 The Second International Conference on Availability, Reliability and Security, pp. 637–643, April 2007
9. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier's AdHoc Netw. J. **1**(2–3), 293–315 (2003). Special Issue Sensor Network Applications Protocols
10. Information, N.C.H., Communication Alliance, I.: Glossary of Top 45 Security & Privacy Terms June 2014
11. Meingast, M., Roosta, T., Sastry, S.: Security and privacy issues with health care information technology. In: EMBS 2006, 28th Annual International Conference of the IEEE, Engineering in Medicine and Biology Society, pp. 5453–5458, August 2006
12. Karlof, C., Sastry, N., Wagner, D.: Tinysec: A link layer security architecture for wireless sensor networks. In: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems. SenSys 2004, pp. 162–175. ACM, NY, USA (2004)
13. Ferng, H.W., Rachmarini, D.: A secure routing protocol for wireless sensor networks with consideration of energy efficiency. In: Network Operations and Management Symposium (NOMS), pp. 105–112. IEEE, April 2012
14. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: Spins: security protocols for sensor networks. Wirel. Netw. **8**(5), 521–534 (2002)
15. Guo, R., Wen, Q., Shi, H., Jin, Z., Zhang, H.: An efficient and provably-secure certificateless public key encryption scheme for telecare medicine information systems. J. Med. Syst. **37**(5), 1–11 (2013)
16. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., Chung, Y.: A secure authentication scheme for telecare medicine information systems. J. Med. Syst. **36**(3), 1529–1535 (2012)
17. Directive 2002/58/ec concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002)