Security and Privacy Issues in Wireless Sensor Networks for Healthcare

Vivek Agrawal

Accepted in HealthyIoT 2014 Conference (Springer)

Agenda

- Introduction
- Healthcare Monitoring System
- Security Requirements
- Security and Privacy Threats
- Security Mechanism
- Conclusion

Introduction

- 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 can subject to the privacy breach, compromise the healthcare service, disabling patients to avail healthcare facilities.

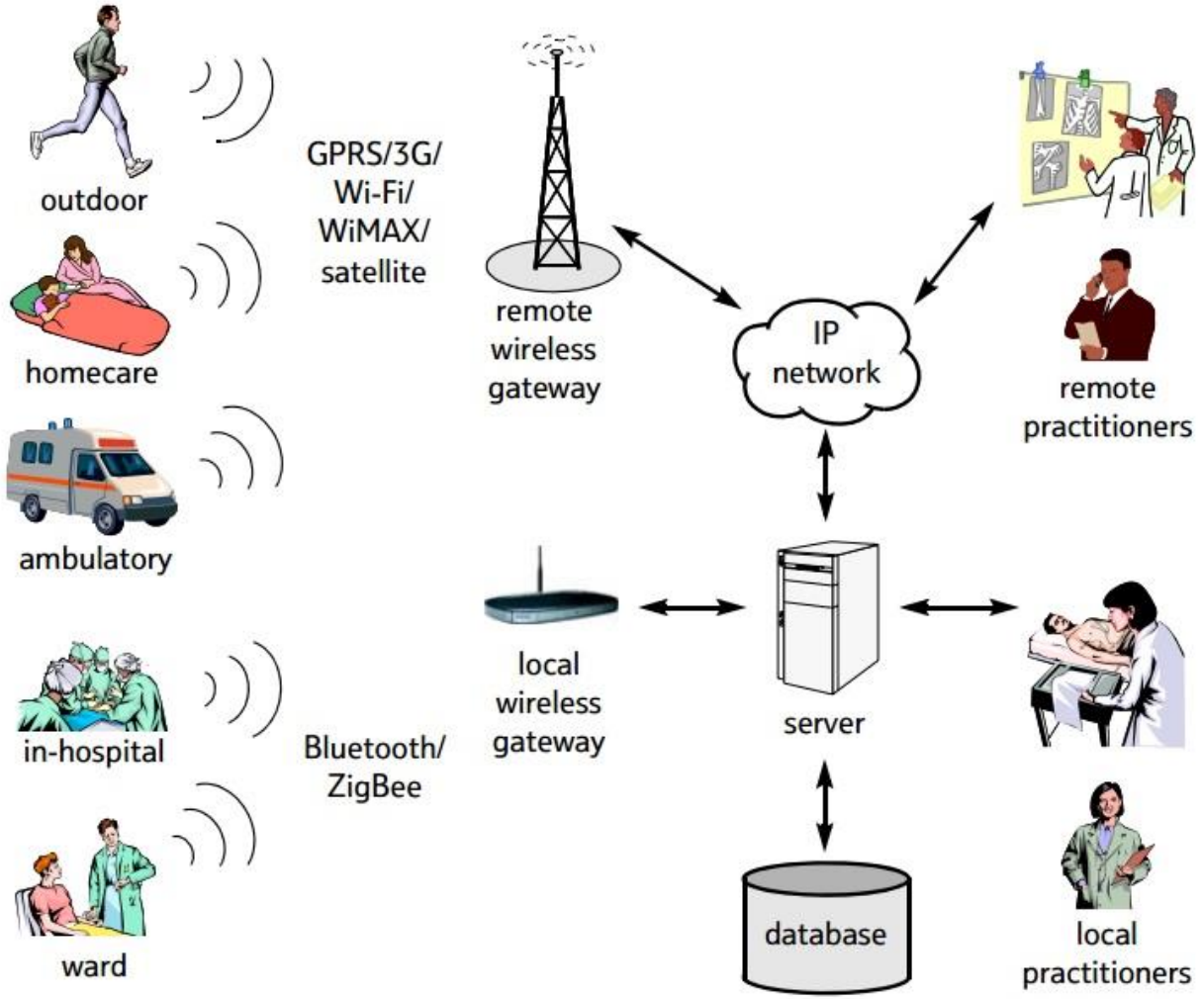
Contribution

- An overview of the status of security requirements in various WSNs healthcare application.
- An overview of potential security and privacy threats that can compromise the normal functionality of a WSNs healthcare system.
- We also present a discussion on the existing security mechanisms to safeguard WSNs healthcare system against several security and privacy threats.

Agenda

- Introduction
- Healthcare Monitoring System
- Security Requirements
- Security and Privacy Threats
- Security Mechanism
- Conclusion

Architecture of a WSN for Healthcare



WSN based Healthcare monitoring system

- Components: Hardware, software, System Interfaces, Data, services and people.
- 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, and surroundings (e.g. room temperature).
- We are mainly focusing on the medical data as an important asset in this report.

Summary of Selected Projects

Project	Description	Application
UbiMon	Ubiquitous Monitoring Environment for Wearable and Implantable Sensors	General remote health monitoring
LifeGuard	is a multiparameter wearable physiological monitoring system for space and terrestrial observation device	Medical monitoring in extreme environments
AMON	Advanced care and alert portable telemedical monitor	High-risk cardiac-respiratory patients
CodeBlue	combined hardware and software platform for medical sensor networks.	Real-time physiological status monitoring with wearable sensors
AUBADE	an integrated platform built for the effective assessment of individuals	Evaluation of the emotional state of an individual at environments where subjects operate at extreme stress conditions.
SATIRE	a wearable personal monitoring service transparently embedded in user garments	Records the owner's activity (activity patterns, such as walking, sitting, or typing) and location

Agenda

- Introduction
- Healthcare Monitoring System
- Security Requirements
- Security and Privacy Threats
- Security Mechanism
- Conclusion

Security Requirements in a WSNs Healthcare system

- Data Confidentiality: authorized doctors or caregivers.
- Data Integrity: Data recording-> Storage-> manipulation
- Data Availability: Keep the network available
- Data Authentication: trusted sensor or not?
- Data Freshness: patient's data is new
- Consent and Privacy: data should not be distributed without patient's authorization.

Security requirements in healthcare application

Projects	Confidentiality	Integrity	Availability	Authentication	Consent & Privacy	Freshness
UbiMon	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI
lifeguard	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI	NA-NI
AMON	A-I	A-I	A-NI	A-I	A-I	NA-NI
CodeBlue	A-NI	A-NI	NA-NI	A-NI	A-NI	NA-NI
AUBADE	A-NI	A-NI	A-NI	NA-NI	A-NI	NA-NI
SATIRE	A-NI	A-NI	A-I	A-NI	A-I	NA-NI

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.

Agenda

- Introduction
- Healthcare Monitoring System
- Security Requirements
- Security and Privacy Threats
- Security Mechanism
- Conclusion

Eavesdropping or snooping

- 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. 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

- CodeBlue is prone to Sybil attack when it is operated in ad-hoc mode.
- In 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

- 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.

Denial-of-service (DoS)

- 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

- “An individual's right to control the acquiring, use or release of his or her personal health information”.
- CodeBlue, AUBADE, LifeGuard, UbiMon neither address not implement any mechanism to protect the privacy of the user.
- 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?

Agenda

- Introduction
- Healthcare Monitoring System
- Security Requirements
- Security and Privacy Threats
- Security Mechanism
- Conclusion

Encryption

- Tiny sensor nodes have limited processing capability, low-storage capacity and constrained communication bandwidth.
- In sensor networks, TinySec is proposed as a solution to achieve link-layer encryption and authentication of data. Authors of SATIRE project indicated the use of TinySec to ensure security and privacy in their system.

Secure Routing

- Karlof & Wagner argued that sensor network routing protocols are not designed with security as a goal.
- Ferng et al. 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 μTESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol 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. has proposed a certificate-less authentication scheme without bilinear pairing while providing patient anonymity.
- Yu et al. 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 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 & Laws

- 1996 Health Insurance Portability and Accountability Act, HIPAA.
- Patients can ask for a copy of their electronic medical record (EMR) in electronic form.
- Penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation
- The European Union Directive 2002/58/EC 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.

Agenda

- Introduction
- Healthcare Monitoring System
- Security Requirements
- Security and Privacy Threats
- Security Mechanism
- Conclusion

Discussion and Conclusion

- advantages of sensor applications can be exploited effectively if the desired level of security and privacy can be ensured.
- Almost all the WSNs healthcare applications lack a measure to counter security and privacy challenges.
- IEEE 802 has established a Task Group called IEEE 802.15.6 (in year 2012) for the standardization of wireless sensor healthcare service.

Discussion and Conclusion

Security threats	Security Requirements	Security mechanism
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.

Thank You!

Questions?