

A Survey: Security Issues and Design Challenges in Healthcare Monitoring System using Wireless Sensor Network

Lilly Roseline Mary J ¹, Buvana M ²

P.G. Student, Dept. of Computer Engineering, PSNA Engineering College, Kothandaram Nagar, Dindigul, India¹

Associate Professor, Dept. of Computer Engineering, PSNA Engineering College, Kothandaram Nagar, Dindigul, India²

ABSTRACT: Wireless sensor network has undergone development in the last one decade. Healthcare monitoring are considered as promising fields for wireless sensor networks. Healthcare monitoring system are traditionally complex system involving not only collecting the data collection using wireless sensor network, but also the security is the major concern of the healthcare monitoring system, mainly in the patient privacy. If the patient have the sensitive disease, then the security and privacy is more important to secure the sensitive data of patient. In this paper, we discuss about some security issues and challenges in healthcare monitoring system using the wireless sensor network..

KEYWORDS: Healthcare Application, Wireless Sensor Network, Security And Challenges Issues.

I. INTRODUCTION

Wireless sensor network is a spatially distributed self-organizing devices using sensor to monitor physical or environmental condition. Wireless sensor network are deployed depends upon the application. In that we have to consider the healthcare application for monitoring the patient's body condition. The monitored data from the body of the patient is very sensitive. That sensitive data are heartbeat, temperature, pressure, blood sugar etc. The healthcare monitoring systems provide useful methods to remotely obtain and monitor the physiological signals without disturbing the patient's normal life. These system not only beneficial to the patient but also the family members of the patient. In this system there are many possibility to misuse and modification of sensitive data. so it can have some security issues and challenges in the health care monitoring.

Manual tracking of patient status is difficult to maintain. Sensor networks in healthcare can replace the current systems based on paper and phone. Collection of long-term previous databases of clinical data can be used in future analysis. Sensor networks applications have potential for great impacts. It can be used in real-time, continuous vital monitoring and give immediate alerts of any changes in patient status. They also can engaged data to the hospital or correlate with patient records and so on.

The paper's aims is to discuss the WSN security issues from a healthcare application perspective with consideration of the typical usage scenarios. The discussions are supplemented by identifying various security issues, design challenges and attacks on WSN in healthcare monitoring.

The contributions of this paper are as follows: we present the state of the art in WSN healthcare application that have been introduced over the last decade and discuss their security flaws. We broadly explore the possible security threats that can have the risk in the healthcare applications, including patient's privacy issues..

The remaining of the survey is organized as follows: Section 2 gives an overview of healthcare application. Section 3 discuss the security and privacy issues for healthcare monitoring applications and Section 4 discusses the design challenges in healthcare monitoring using wireless sensor network and Section 5 conclusions are drawn for wireless sensor network in healthcare applications.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

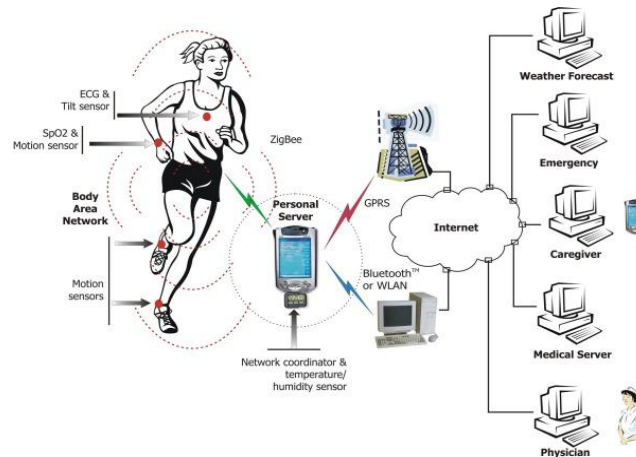


Figure 1. healthcare application using wireless sensor network

The Figure 1 tells about the application of wireless sensor network in dynamic healthcare application in the sports person health monitoring.

II. HEALTHCARE APPLICATION

Wireless network sensors enable dense spatio-temporal sampling of physical, physiological, psychological, cognitive, and behavioral processes in spaces ranging from personal. Such dense sampling across spaces of different scales is resulting in sensor information based healthcare monitoring applications. sophistication of sensing has increased ultimately with the advances in cheap and minuscule, but high quality sensors for home and personal use. we introduce a list of healthcare monitoring applications:

Monitoring in Mass-Casualty Disasters: While casualties for emergency medical services already exist. Their effectiveness can quickly damage with increasing number of victims. Moreover, there is a need to improve the assessment of the first responders' health status during such mass-casualty disasters. In that application that increased portability, scalability, and rapidly deployed in the nature of wireless sensing systems can be used to automatically report the causal levels of many victims and constantly track the health status of first responders at the disaster scene more effectively.

Vital Sign Monitoring in Hospitals: Wireless sensor network helps to address the various drawbacks associated with wired sensors that are used in hospitals and emergency rooms to monitor the patients. The familiar jumble of wires attached to a patient is not only sore for patients leading to restricted mobility and more concern, but is also hard to manage for the staff. Quite common are conscious of sensors by tired patients and failures to reattach sensors properly as patients are moved around in a hospital. Wireless sensor hardware that are less noticeable and have constant network connectivity to back-end medical record systems help reduce the difficulties of using the wires and patient concern, while also reducing the occurrence of errors.

At-home and Mobile Aging: As people of old age, they experience a variety of cognitive, physical, and social changes that challenging their health, independence and quality of life. Diseases such as diabetes, asthma, congestive heart failure, and memory beg off are challenging to monitor. These diseases can affect the patients from an active role in the monitoring process. Wireless networked sensors embedded in people's living spaces or carried on the person can collect information about personal details, physiological, and behavioral states and patterns in real-time. Such data can also be associated with social and environmental circumstance. From such living records are useful inference about

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

health and wellbeing can be drawn. WSN can be useful for self-awareness and individual analysis to assist in making behavior changes, and to share with caregivers for early detection and intercession. At the same time such procedures are effective and economic ways of monitoring age-related illnesses.

Assistance with Motor and Sensory beg off: Another application of wireless networked sensing is to provide active assistance and guidance to the patients for coping with waning sensory and motor capabilities. We are seeing the emergence of new types of intelligent devices that make use of information about the patient's physiological and physical state from sensors that are worn or implanted on the person, and embedded in the surroundings. These intelligent devices can not only modify their response to individual users and the current context, but also provide the user and the caregivers crucial feedback for longer-term training. Traditional devices such as canes, crutches, walkers, and wheel chairs preserve information from incorporated and external sensors to provide the users with frequent personalized comment and guidance towards the correct usage of the devices. Such devices can also adapt the physical characteristics of the device with respect to the context and a approved training or rehabilitation treatment. Furthermore, wireless networked sensing enables the new sensor devices for way-finding for the visually impaired.

III. SECURITY ISSUES

Security issues in healthcare monitoring applications of sensor networks have been always part of active research. Security issues in wireless sensor networks are a major area of research in recent years. Similarly many people have particularly addressed security issues with respect to healthcare monitoring applications.

Monitoring and Eavesdropping on Patient Vital Sign: Patient's vital signs and medical records captured by health sensors are transferred via different wireless connections and through Internet. This involves plenty of security and privacy risks for the patients. An attacker can eavesdrop on wireless channel to listen or to modify user's private health data with malicious intent. The captured message may contain the physical location of the patient, allowing an attacker to locate the patient's position and physically harm the person. In addition, an rival can also detect the message contents together with message-ID, timestamps, source address, destination address and other relevant information.

Denial of Service Threats:

Denial of service attack produces the accidental failure of nodes or malicious action. Dos attack is meant not only for the adversary attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability. Table 1: There are several types of Dos attacks in different layers might be performed.

Table 1 Denial-of-Service attack at each layer

Layers	Attacks
Physical Layer	Jamming, Tampering
Link Layer/medium access control	Collision, exhaustion, and unfairness
Network layer	Neglect and greed, homing, misdirection, spoofing, replaying, routing protocol traffic or clustering messages
Transport layer	Flooding and De-synchronization
Application layer	Reprogramming attack

Routing threats:

The attacks which performed on the network layer are called routing threats. The following are the attacks:

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

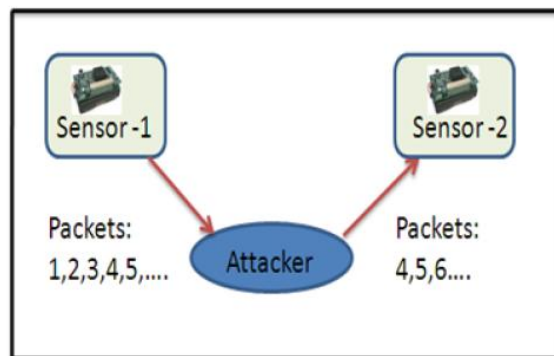
Attack on Information in Transit:

In a sensor network, sensors monitors the changes of specific parameters or values and report to the sink according to the requirement .while sensing the report the information is transit may be altered, spoofed or vanished. As a wireless sensor network is vulnerable to the eavesdropping, any attack can monitoring the traffic flow and get into the action to interrupt, intercept, modify or fabricate packets.

Selective Forwarding:

selective forwarding attack Figure (2) is the one of the insider attack. A more subtle from this attack is when the adversary selectively forwards packets. The adversary is able to create routing loops that attack or repel network traffic. They also can be extend or shorten source routers, generate false message and attempt to drop the sensitive information. A malicious node can refuse to forward the packets randomly. For this reason, base station does not receive the entire message.

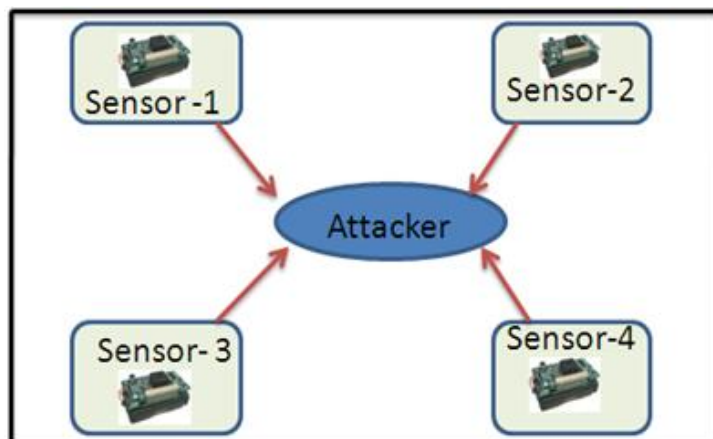
Figure 2. Selective Forwarding



Black hole/Sinkhole Attack:

In Sinkhole attack Figure (3) an attacker tries to attract all neighboring nodes to establish routes through a malicious node. Figure 3 illustrates a sinkhole attack. once the attacker is successful in the sinkhole attack, then the network is also open to other attacks. for example, eavesdropping or selective forwarding. Sinkhole attacks are very hard to detect. Therefore, requesting nodes assume that routing discovery process is completed and ignore the information.

Figure 3. Sinkhole Attack



International Journal of Innovative Research in Science, Engineering and Technology

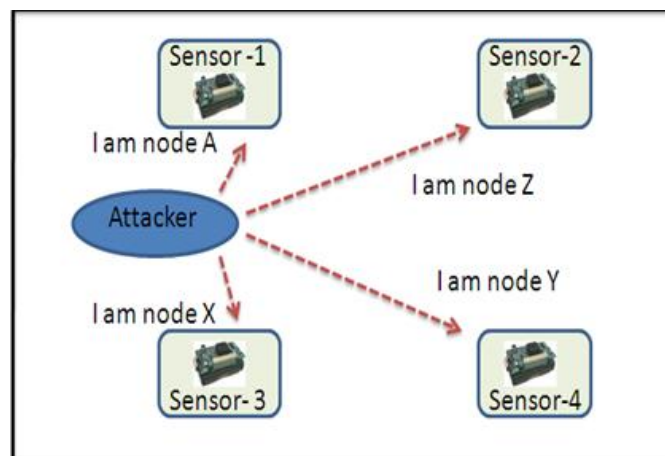
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

Sybil Attack:

In the attack, Figure (4) a compromised node presents multiple fake identities to other neighboring nodes in the network. Figure 4 illustrates how the multiple fake identities of a compromised node are sent to other neighboring node, when it operates in an ad-hoc manner. The Sybil attack poses a significant threat in geographic and multipath routing protocol, because the compromised node may appear in more than one place. Further, more routing attacks in the context of healthcare applications using sensor networks.

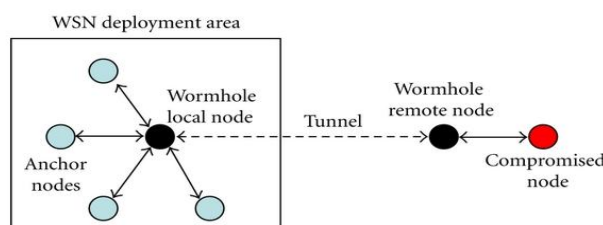
Figure 4. Sybil Attack



Wormhole Attack:

A Wormhole attack Figure (5) requires two(or) more conflict. These conflictions have better communication resources than normal node and can establish better communication channels. The attack changes the network topology and changing the normal message stream. It is commonly involve in two distant malicious nodes collude to minimize their distance from each other by transmitting packets along an out-of-bound channel available only to the attacker. An attacker could persuade nodes who would normally be multiple hops from a base station.

Figure 5. Worm hole Attack



Hello flood Attack:

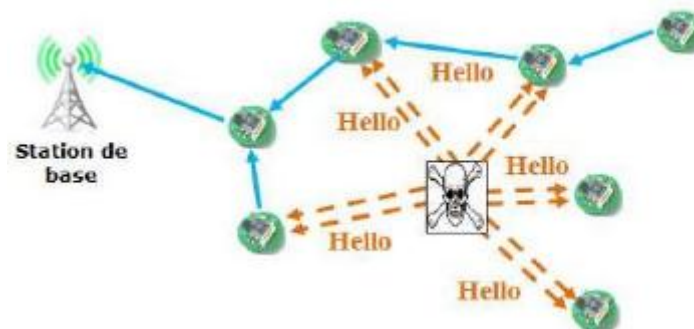
Hello flood attack Figure (6) is the main attack in network layer. It can be caused by a node which broadcasts a Hello packet with large power consumption, so that a large number of nodes even far away in the network choose it as the parent node. All messages to be routed multi-hop to this parent, which increases delay. Hello messages are broadcast to a large number of nodes in a large area of the network. These nodes are then transformed that the attacker node is their neighbor, all the nodes will respond to the Hello message and waste their energy.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

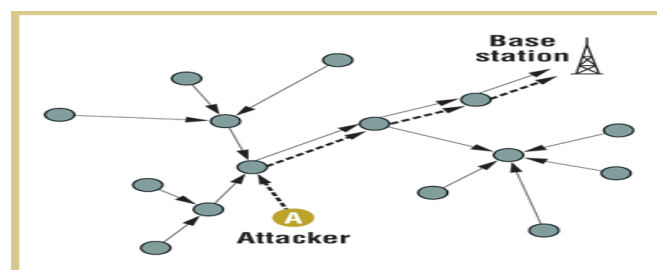
Figure 6. Hello flood Attack



Replay attack:

A replay attack Figure (7) is a one of the network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the creator or by an attacker who intercepts the data and retransmits it and possibly as part of a masquerade attack by IP packet swap (such as stream cipher attack). An attacker copies a forwarded packet and future the attacker sends out the copies repeatedly and continuously to the victim in order to exhaust the victim's power supplies, or to base stations and access points in order to degrade network performance. In addition, the replayed packets can collapse poorly designed applications or exploit vulnerable holes in poor system designs.

Figure 7. Replay Attack



IV. DESIGN CHALLENGES

The main requirement in WSN is the size of WSN node must be small. A sensor node has limited processing capabilities and limited amount of energy so that there are many challenges in designing perfect sensor network for various applications. It is very difficult to develop proper routing protocol for guaranteed communication from source to destination. Small size of sensor node puts limits on battery size so that overall system should be energy efficient and this is the great challenge for the design engineers. The section explores some limitations of WSN for medical healthcare application.

1. Accuracy and Reliability:

Reliability proposes high degree of accuracy in the sensors must be able to provide real time accurate information regarding the patient's health. If the patient's information is not accurate then it may result in improper treatment or it can escort to the patient's death. For example, in case of cancer detection application, system failure can lead to the incorrect reports. The sensor devices must be vigorous since they are left with the patients without all time monitoring .

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

2.Context Awareness:

Context-aware healthcare information can be obtained from heterogeneous and distributed sources, including sensors, profile files, and applications. Context means the information which can be used to describe the state of an unit can be a person and physical object. In medical healthcare applications, it demonstrates the significance of associated with physiological activity of the user to the sensed signals of the user. The sensors must modify the behaviors in accord with the user's situation. The context aware sensing algorithm can be able to reduce the effect of noise in the sensor data. For long term persistent systems, new context can added to the system. Therefore, it must automatically update new contexts and remain updated with old context to avoid re-learning.

3.Compatibility and efficient Response:

One of the most important issues is to make the applications comfortable and easy to use. The main purpose of the applications is to improve healthcare services without put any effect on user's daily activities. In the healthcare application response important than others in the healthcare application. patients in the serious condition have the quick response from the caregivers. If there is any laziness in the patient response, then it causes the patient lead to some serious problem in the patient body.

4.Energy Consumption:

Sensor nodes have limited energy. The nodes may drain out while performing the tasks like calculating and transmitting the data in a wireless environment. The lifetime of a sensor node may depend on its battery lifetime. In health care application sensor node are mostly implement in the human body so that recharging or replacement of battery is very difficult. It is observed that communication of data consume more energy as compare to the processing . The continuous monitoring operation of a sensors is essential for healthcare applications so that energy efficient routing protocol is main issue. The transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi-hop routing will obtain less energy than direct communication. However, multi-hop routing introduces considerable overhead for topology management and medium access control.

5. Fault Tolerance:

Sensor nodes on the body of the patient will be co-ordinate for a particular application. Nodes are placed for longer usage in the body. Network must not seize due to failure of nodes hence the network must be fault tolerant. If there is any network or node failure in the network of the healthcare application, then network will accept the failure and sensing the data is usual means the healthcare network is fault tolerance. It is one the major design issues in the healthcare monitoring system in wireless sensor network.

6.Privacy:

Privacy issues obtain from multidisciplinary fields such as computer science, bioinformatics, the social sciences and medical science. These days some pervasive healthcare applications are in development while patients have put other applications into use, therefore users and researchers are also starting to raise privacy issues. For example, before dementia patients agree to use the application, they and their relatives often ask about the privacy policies. This is because they want to ensure that their use either health is taken care of by the healthcare service providers while the privacy of their life is insured. Based on the collected and analysed privacy issues, we have summarized and grouped similar and related issues into six major privacy issues. The six issues identified are medical status misuse, prescription leakage, social implications for the patient, patient difficulties in managing privacy and lack of support in designing privacy-sensitive applications. By doing this grouping, it would be easier for future research to know current issues in healthcare and embark upon the interested privacy issue.

1. Medical Information Misuse:

In Healthcare monitoring system, patients are more exposed to privacy risks. A comprehensive monitoring system can be applied at the hospital, home or nursing home. The system can transmit signals from the patient to the healthcare provider when unusual signs are detected to get immediate help. When there is pervasive healthcare, the technology usually involves wireless communication; therefore it is open to all of the wireless threats such as eavesdropping and

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2015

information stealing. The one privacy issue would be the possible misuse of patient medical information by unauthorized personnel who can intercept and manipulate the information.

2. Prescription Leakage:

In a healthcare monitoring system, patient data such as their prescriptions is saved in the database. This personal information is not sufficient to picture whom the exact person is; however if the third party is enthusiastic enough, they could combine the prescription information with other information that might be able on the net to eventually lead them to the exact patient. Finally they can go directly to the patient to promote drugs that might be suitable. The fascinating finding in the paper is that by only asking one colleague if he knew anyone who had been admitted to the hospital recently, and asking for general information such as gender, age and date admitted, the authors did some database searching and eventually found the details of the patient's drugs.

V. CONCLUSION

The technology improvement in wireless sensor network and its networking technology has been resulting in various healthcare applications which making the human life easier and comfortable. The applications of WSN have a great impact on medical healthcare monitoring of the patient's in emergency situations. It have the responsibility to provide pleasant environment to patients at homes. The various security issues and design challenges in WSN are discussed in the article. There are many healthcare applications which can monitor patients and alerts physicians, when the patient is in risk. The small sized wearable sensor devices typically do not affect patient's normal schedule. It very challenging to design suitable sensor network to meet various needs health care applications.

REFERENCES

1. Pardeep Kumar and Hoon-Jae Lee, Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. *Sensors* **2012**, 12, 55-91; doi:10.3390/s120100055.
2. I-Ching Hsu, Member, IACSIT, Wireless Context-Aware Healthcare System Based on Sensor Web 2.0. *International Journal of Innovation, Management and Technology*, Vol. 4, No. 4, August 2013.
3. K. Venkatraman, J. Vijay Daniel and G. Murugaboopathi, Various attacks in wireless Sensor Network-Survey. *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-3, Issue-1, March 2013.
4. Rusyaizila Ramli, Nasriah Zakaria, Putra Sumari, privacy issues in Healthcare Monitoring in Wireless Sensor Network. *World academy of science, engineering and technology* Vol:4 2010-12-23.
5. Dilip Chaudhary, Dr. L.M. Waghmare, Design Challenges of Wireless Sensor Network and Impact on Healthcare Application. *International Journal of Latest Research in Science and Technology*, Volume 3, Issue 2: Page No.110-114, March-April, 2014.
6. M. Souil and A. Bou Abdullah, On QoS Provisioning in Context-Aware Wireless Sensor Networks for Healthcare, in proc of 20th international conference on Computer Communications and Networks (ICCCN), 2011.
7. Genita Gautam, Biswaraj Sen, Survey of different types of attack in healthcare application using wireless sensor network. Genita Gautam et al, / (IJCSIT) *International Journal of Computer Science and Information Technologies*, Vol. 6 (1), 2015, 770-774.
8. Waltenegus Dargie and Christian Poellabauer, "fundamentals of wireless sensor networks", John Wiley & Sons, Ltd, pp.25-30, 2010.
9. Leon, M.D.L.A.C.; Garcia, J.L. A Security and Privacy Survey for WSN in e-Health Application. In Proceedings of Conference on Electronics, Robotics and Automotive Mechanics (ERMA'09), Cuernavaca, Morelos, Mexico, 22-25 September 2009; pp. 125-130.
10. Ameen, M.A.; Liu, J.; Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *J. Med. Syst.* **2010**, doi: 10.1007/s10916-010-9449-4.