# A Survey on Security and Privacy Issues in the Use of Wireless Sensor Networks for Health Care Monitoring

[1]Aleburu Deborah, [2]Omotosho, O.O, [3]Joshua Jonah
[1, 2, 3]Computer Science Department, Babcock University, Ilishan-Remo, Ogun State, Nigeria
Email address: [1]debbyaleburu@yahoo.com, [2]omotoshoo@babcock.edu.ng, [3]joshuaj@babcock.edu.ng

***Abstract***— *Development in wireless sensor Networks (WSNs) has led to the increase in its applications in healthcare. Wireless Sensor Network application in health care is divided into two (2) wearable and implantable sensor devices. These devices allows for the monitoring and tracking of patients' health status. Security and privacy are issues that arise from the use of these applications. The use of sensor networks for healthcare monitoring has a lot of benefits; so therefore, it is of necessity that these issues are addressed. This paper gives a survey on the security and privacy issues faced with the use of WSNs for healthcare monitoring.*

## I. INTRODUCTION

Recent advances in wireless networks and electronics have led towards the emergence of Wireless Sensor networks (WSNs). WSNs are regarded as probably the most important technologies which could alter the near future [1].

Wireless Sensor Networks (WSNs) can be defined as "a self-configured and infrastructure-less wireless networks to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location or sink where the data can be observed and analyzed" [2]. A sink or base station acts as an interface between users and the network. It is possible to retrieve required information from the network by putting instructions and gathering results from the sink. Typically a wireless sensor network contains thousands of sensor nodes. Sensor nodes communicate with each other using radio signals. A wireless sensor node provides for sensing and computing devices, radio transceivers and power components. Each nodes in a wireless sensor network (WSN) are usually resource constrained, that is, they have limited processing speed, storage capacity, and communication bandwidth. Once the sensor nodes are deployed, they are responsible for self-organizing a suitable network infrastructure often with multi-hop communication with them, then the onboard sensors begins to gather information. Wireless sensor devices also reply to queries sent from a "control site" to carry out specific instructions. The functional mode of these sensor nodes could be either continuous or event driven. Global Positioning System (GPS) and local positioning algorithms allows for obtaining location and position information. Wireless sensor devices are sometimes designed with actuators to "act" upon certain conditions. These networks are sometimes more specifically referred as Wireless Sensor and Actuator [2].

## II. APPLICATION OF WSN TO HEALTHCARE

Healthcare is often considered an important concern because it involves the total well-being of an individual. It's usually better to prevent a sickness than to take care of it, so individual monitoring is essential as a periodic activity.

Conventionally, health monitoring is carried out on a periodic basis, in which patients must remember its symptoms; the physician carries out some tests and comes up with a diagnostic, then monitors the patients' response to treatment. However, some symptoms manifest themselves once in a while, where an individual may experience some pain or discomfort. WSNs applied to healthcare provides for in-home assistance, smart nursing homes, patient monitoring, etc. In-home healthcare is necessary for health conditions like Parkinson or Alzheimer which helps to provide memory enhancement with the use of medicine reminders, mental stimulation through the use of sounds and images, control of home appliances, emergency situations and lot more [3].

WSN for healthcare is divided into two: wearable and implanted devices. Wearable devices are those which can be used on the body surface of an individual (that is they can be worn) or just at close proximity of the user. Examples of these wearable medical devices and applications are: Temperature measurement, Respiration monitor, Heart rate monitor, Pulse Oximeter, Blood pressure monitor, pH monitor, Glucose sensor etc. The implantable medical devices are those that are put inside the body of an individual. Examples of these devices are: Cardiac arrhythmia monitor/recorder, Brain liquid pressure sensor, Endoscope capsule etc [4].

Since manual tracking of patients' status is very tedious, sensor networks applications in healthcare have potential for large impacts [18] and these can be realized through real-time, continuous vital monitoring to always relay alerts of changes in patient status. This data can also be transmitted to the patients' record in the hospital which could be used for future diagnosis; this data could also be relayed to a physician who can provide for long-term care and trend analysis. It can also reduce length of hospital stay. Manual tracking of patient status is difficult. The clinical data collected over a long period of time can be used in making future diagnosis [4].

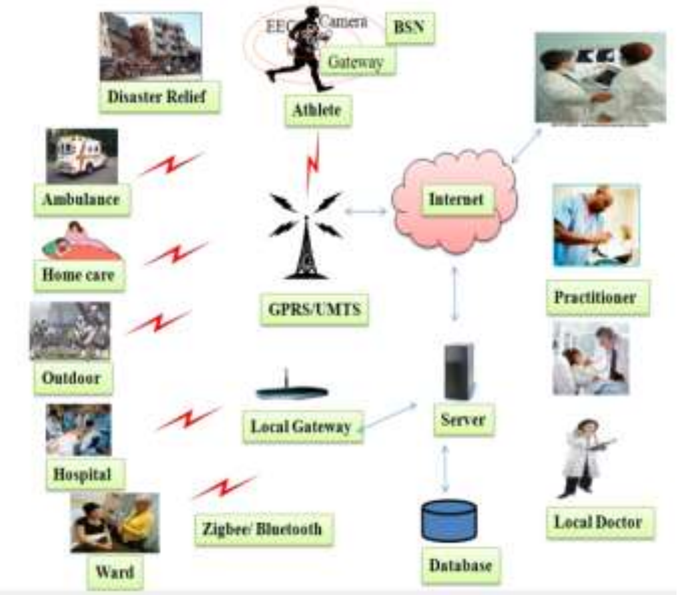

Fig. 1. Healthcare application using wireless medical sensor networks.

As shown in Fig 1, WMSNs provides a high quality-of-care across different healthcare applications such as, ambulatory monitoring, vital sign monitoring in-hospitals, elderly peoples' in-home monitoring, monitoring in mass-casualty disasters, clinical monitoring, etc. Others that also benefit from WMSNs are sports-person for health status monitoring, and patients' self-care for example a BAN network on a diabetic patient could be used to auto inject insulin though a pump, once the level of insulin in the body drops.

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. Also, a back-end server is used to store physiological healthcare information (PHI), as well as for offline analysis of PHIs [5].

## III. Projects on Sensors Applied to Health Care

Researches in the use of sensors for healthcare monitoring are in progress around the world. Many projects have been developed, some are in development stages. Several of these research projects have centered on wearable health devices, these projects are usually funded by both government agencies and private organizations. These applications work in both real time and non-real time modes. Examples of these projects include:

*HealthGear*: This is a product of Microsoft Research. It is made up of a number of physiological sensors connected via Bluetooth to a mobile phone. It is a wearable real time health care system for monitoring and analyzing physiological signals [6].

*MobiHealth*: This is a mobile healthcare project which was funded by the European Commission. It ensures that patients can be mobile while undergoing continuous health monitoring by making use UMTS and GPRS networks [7].

*Ubimon*: This was developed by the Computing Department, Imperial College, London. The main goal of this project is to address the issues regarding the use of wearable and implantable sensors for distributed mobile monitoring. This device has two functions: management of patients with arrhythmic heart disease and follow-up monitoring of post-operative care in patients who have had surgery [8].

*CodeBlue*: This was a research project carried out at Harvard University, US. It combines sensor nodes and various wireless devices into an emergency response setting. It was designed to function across several network densities and numerous wireless devices. From a tiny small sensor mote to more powerful devices such as PDSs, PCs can be combined in CodeBlue [9].

*eWatch*: This is a wearable sensor and notification platform developed for context aware computing research. It is inserted into a wrist watch which makes it highly available, instantly viewable, and socially acceptable. eWatch provides tactile, audio and visual notification while sensing and recording light, motion, sound and temperature [10].

The vital jacket: This is a smart and intelligent wearable garment that has the ability to monitor electrocardiogram (ECG) waves and heart rate for several fitness, sports, security and medical applications. The data is sent via Bluetooth to a PDA and stored in the device memory at the same time [11].

## IV. Challenges of WSN in Healthcare Application

The growth of a wireless healthcare application offers many challenges, such as, reliable transmission of data, support for node mobility, immediate event detection, and timely delivery of data, power management and node computation. The deployment of new technologies in healthcare applications without the consideration of security and privacy often makes patients' vulnerable. Patient's physiological vital signals are extremely sensitive, therefore any leakage of an individual's data could embarrass him/her and in some cases, the revelation of such data could lead to the person losing his/her job or make it impossible for such an individual to receive insurance protection. WMSNs provides data such as physiological data monitoring, and activity monitoring in health-clubs, location tracking for athlete, etc., these data are shared physicians (in a doctor-patient relationship), insurance agencies (as insurance protection), and health coaches (as sports team trainers) or with family (as relatives' support). Therefore unauthorized collection and use of patient data by adversaries can result in life-threatening risks to the patient. For instance, data is transmitted from a patient's body sensors to his/her nurse/caregiver; an intruder might eavesdrop on the patient data while the data is been sent, and thereby the patient's privacy is breached. This intruder might even post these data on social media which can ruin the person. Wireless healthcare offers numerous advantages to patient monitoring, however the physiological data of a person is very sensitive, so security and privacy is a very big concern for its use.

## V. Security Issues

Security is one of the most important aspects of any system. There a different perspective to which people regard security and therefore it is defined in different ways. Generally, security is a notion just like safety of a system as a whole. Security can be defined “as a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences” [4].

### *Threats to Information When in Transit*

Wireless communication ranges are not confined and are easily vulnerable. Medical sensors gather an individual’s data and send it to the doctor or the hospital server. While data is been sent, it could be attacked, an adversary can intrude into the network and capture the data from the wireless channels. The intruder can change the data and then send the altered data to the doctor or remote server which can endanger the patient. There are two major types of transit attacks: (i) Interception: In this type of attack, the intruder illegally access the sensor node data which includes the cryptographic keys, sensor ID’s, sensor type, etc. (ii) Message Modification: In this type of attack, the intruder captures an individual’s medical data and tampers with it which could mislead the user(s) of the data (e.g doctor, nurse, relation, etc). For example, if a cardiograph sensor transmits normal data to a medical personnel, an intruder can alter the data while in transit and send the altered data to the medical personnel which can result in the medical personnel administering to the patient an under-dose or overdose of the medication. Also, the altered data can trigger a false alarm or can hide the actual condition of the patient. Message modification threatens the message integrity of medical sensor nodes [5].

### *Masquerade and Replay Threats*

In healthcare application, an intruder can easily rogue a wireless relay point while patient data is in transmission. Wireless relay nodes are usually unguarded and an intruder can have unrestricted access to the network. In this type of attack, an illegal relay node (attacker) behaves as a real node in the network. This might lead to false alarms been raised in remotes sites and an emergency dispatch team could commence a rescue operation for a person that does not exist or does not need it, which can defeat the purpose of wireless healthcare. Thus, masquerading nodes is quite dangerous for healthcare applications. Also, if a masquerade relay node hijacks a patient’s data, these hijacked data can cause replay threats to real-time healthcare application. The treatment of a patient relies on freshly received data from medical sensor networks. If masquerade nodes replay previous messages repeatedly, this would result in mistreatment or overtreatment (i.e. overdose) of the patients. Therefore, masquerade and replay threats could endanger patients using WMSNs for healthcare [5].

### *Denial-of-Service (DoS) Threats*

Denial-of-Service (DoS) attack can be defined “is any event that diminishes or eliminates a network’s ability to perform its expected function” [16]. DoS attack is much more disruptive in healthcare applications because these applications need a health monitoring network that is always on. DoS attacks may damage the health monitoring network which can result in the loss of a patient’s life. Thus these (DoS) attacks are harmful especially in mission-critical applications, such as location tracking, ambulance assistance, home care monitoring, etc. [5].

## VI. Privacy Issues

Privacy is among the major concerns in wireless sensor networks regarding healthcare applications. Medical related data should be private in nature. To preserve privacy, patients should possess the rights to choose what data needs be collected, used or disclosed. Any unauthorized collection or leakage of patient data could harm the patient. For instance, a person could illegally use a patient’s data (e.g his/her identity) for their own personal benefit, such as for medical fraud, fraudulent insurance claims, and this could pose life-threatening risks to such patient [12].

Concerns relating to privacy have been raised by researchers, they emphasized that if the problems related to privacy are not honestly debated in a reasoned in an open way, then there is a risk that there might be a public backlash which will lead to mistrust and therefore this technology won’t be utilized for the numerous applications where it can provide significant benefits, misuse or privacy concerns may restrict people from benefitting from the use of these sensor networks for health care monitoring [5]. As medical data are highly sensitive, there are some questions that arise such as: who owns the medical data, who control the access to medical data? Also, in wireless healthcare applications, a large amount of health and life-style data are gathered that requires close awareness about who controls it, what exactly is gathered, who has the right to gain access to the data and where/how/whether that data is stored or not [13]. Similar questions have been raised concerning patient privacy: (i) Who has permission to possess the data; (ii) what kind of medical data, how much, and where should the data be stored; (iii) who has permission to examine the medical data; (iv) to whom should medical data be revealed to without the patient’s consent; (v) who is responsible for maintaining these data if any issue arise; and (vi) who will be held accountable. These questions are important issues that need to be addressed to be able to protect the privacy of patients and their information as well as to some extent the security of the information [14]. Some examples of privacy threats include:

*Monitoring and Eavesdropping on Patient Vital Signs:* This privacy threats is the most commonly encountered threat to the patient privacy. By snooping on patient vital sign, an intruder can easily obtain the patient information from communication channels. Also, if the intruder has an effective receiver antenna, then he/she can easily capture the data sent through the network. The data captured may contain the patient’s geographical location, allowing the intruder to discover the patient’s position and the patient could be physically harmed. Also, the message contents such as message-ID, timestamps, source address, destination address and other relevant information could be detected by the intruder. Therefore, monitoring and eavesdropping can pose a serious threat to patient privacy [17].

*Identity threat:* The loss of an individual's identity can pose serious financial, physical and emotional damage to him/her. An intruder could use this patient identity for his/her personal benefit, for example, using the identity to receive reimbursement (insurance claims) or to medical services [15].

*Location Threats*: Medical sensor networks provides for patient mobility, so the exact patient location is necessary to allow medical staff reach the patient very quickly in the event of any emergency. Location-tracking systems depend on on radio frequency, ultrasound, received signal strength indicator or some technology, if an intruder receives the patients' radio signals regularly and analyses them, then he/she can know the details of such patient's location and that would directly infringe on the persons privacy [5].

## VII. CONCLUSION

In conclusion, the use of sensor in health care monitoring has come to stay, and while it has all its benefits, it also has some issues that need to be considered by the manufacturers of these systems and also by researchers. Privacy is a very important issue in ethics, once the privacy of an individual is lost, it cannot be regained. Therefore, more research needs to be done in this area to ensure that people who use it don't have to worry about their information getting into wrong hands.

## REFERENCES

[1] A. Minaie, A. Sanati-Mehrizy, P. Sanati-Mehrizy, and R. Sanati-Mehrizy, "Application of wireless sensor networks in health care system," *120th ASEE Annual Conference & Exposition*, 2013.

[2] M. A. Matin and M. M. Islam, "Overview of wireless sensor network," *INTECH*, 2012.

[3] Paulo Neves, Michal Stachyra, and Joel Rodrigues, "Application of wireless sensor networks to healthcare promotion," *Journal Of Communications Software And Systems*, vol. 4, no. 3, pp. 181-190, 2008

[4] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, issue 1, pp. 93-101, 2010.

[5] P. Kumar and H. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, issue 1, pp. 55-91, 2011.

[6] N. Oliver and F. Flores-Mangas, "HealthGear: A real-time wearable system for monitoring and analyzing physiological signals," *International Workshop on Wearable and Implantable Body Sensor Networks*, BSN, 3–5, 2006.

[7] http://www.mobihealth.org/

[8] http://www.ubimon.net/

[9] http://fiji.eecs.harvard.edu/CodeBlue

[10] U. Maurer, A. Rowe, A. Smailagic, and D. P. Siewiorek, "eWatch: a wearable sensor and notification platform," *International Workshop on BSN, Wearable and Implantable Body Sensor Networks*, 4–145, 2006.

[11] http://limserver.com/vitaljacket/index.php

[12] A. K. Davenport, Identity Theft that can Kill You, 2006. Available online: http://www.law.uh.edu/healthlaw/perspectives/2006/(KD)IdentityTheft.pdf

[13] I. Brown and A. A. Adams, "The ethical challenges of ubiquitous healthcare," *Int. Rev. Inform. Ethics*, vol. 8, pp. 53-60, 2007.

[14] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with healthcare information technology," in *Proceedings of the 28th IEEE EMBS Annual International Conference*, New York, NY, USA, pp. 5453-5458, 2006.

[15] M. E. Johnson, "Data hemorrhages in the healthcare sector," Available online: http://fc09.ifca.ai/papers/54_Data_Hemorrhages.pdf