Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2555-2563

http://www.ripublication.com

Energy Efficiency and Security Requirements of Wireless Medical Sensor Network

Dr. T. Lalitha
Asso. Prof/MCA
Sona College of Technology, Salem-5,Tamilnadu, India.

U. Sridevi
Research Scholar
SSM College of Arts and Science, Komarapalayam, India.

Dr. K. Kamaraj
Professor/Comp.Sci
SSM College of Arts and Science, Komarapalayam, India.

Abstract

The use of WMSN in health care appliance is a potentially very useful.Recent advances in wireless networks and electronics have led to the emergence of Wireless Sensor networks (WSNs). Healthcare applications are measured as promising fields for wireless sensor networks, where patients can be examined using wireless medical sensor networks (WMSNs) .Wireless sensor networks have standard considerable attention from both the academic and industry communities for many years, since these networks are the vital component for realizing next generation networking and computing. Moreover, this rapidly growing sensor networks technologies and their operation in mobile healthcare systems might create many unseen security and privacy threats. These threats might affect the helpful working environment of a healthcare organization, patient's safety and privacy, confidentiality and reliability of healthcare data, and etc. Hence, it is very important to develop original methods and policies that make certain the secure acquisition, management, and replace of healthcare data in highly effective and secure ways at the same time promoting its interoperability, sharing, integrity, and confidentiality.

Keywords: Energy Efficiency, Wireless Sensor Network, Health Monitor, Security

1. INTRODUCTION

With ageing of the people, existing medical property cannot assure future healthcare demands of seniors and patients. Resources are limited and it is impossible for most patients to meet the expense of long-term hospital stays due to economic limitations, work, and other reasons, even though their health status must be examined in a real-time or short periodic time mode. As a result, wireless monitoring medical systems will become part of mobile healthcare centers with real-time monitoring in the future.

"WSNs are collected of individual embedded systems that are capable of

1. interacting with their environment through various sensors,
2. processing information locally, and
3. communicating this information wirelessly with their neighbors.

A sensor node (embedded system) usually consists of three components which are

- Wireless modules or motes – key components of the network which consists of a Microcontroller, transceiver, power source, memory unit, and may contain few sensors. Examples: Mica2, Cricket, MicaZ, Iris, Telos, SunSPOT, and Imote2.
- A sensor board which is mounted on the mote and is embedded with multiple types of sensors. Examples: MTS300/400 and MDA100/300.
- A programming board (gateway board) – provides multiple interfaces including Ethernet, WiFi, USB, or serial ports for connecting different motes to an enterprise or industrial network or locally to a PC/laptop. These boards are used to program the motes or gather data from them. Example: M1B510, M1B520, and M1B600.

2. CHALLENGES FOR WSN

2.1 Characteristics requirements

The following characteristics with new mechanisms is the major challenge of the vision of wireless sensor networks.

- Type of service
- Quality of Service
- Fault Tolerance
- Lifetime

- Scalability
- Wide range of densities

Wireless Sensor Networks mainly consists of sensors. Sensors are :

- low power
- limited memory
- Energy constrained due to their small size.
- Wireless networks can also be deployed in extreme environmental conditions and may be prone to enemy attacks.

3. REQUIRED MECHANISMS OF WSN

Handling such a wide range of application types will hardly be possible with any single realization of a WSN.Some of the mechanisms that will form typical parts of WSNs are:

Multihop Wireless communication: While wireless communication will be a core technique,a direct communication between a sender and a receiver is faced with limitations.In particular,communication over long distances is only possible using prohibitively high transmission power.The use of intermediate nodes as relays can reduce the total required power.Hence,for many forms of WSNs,so called multihop communication will be a necessary ingredient.Energy-Efficient operation: To support long lifetimes, energy-efficient operation is a key technique. Options to look into include energy-efficient[1] data transport between two nodes or, more importantly, the energy-efficient determination of requested information.Auto-Configuration: A WSN will have to configure most of its operational parameters autonomously, independent of external configuration-the sheer number of nodes and simplified deployment will require that capability in most applications.Nodes should be able to determine their geographical positions only using other nodes of the network. Data-centric: Traditional communication networks are typically centered around the transfer of data between two specific devices, each equipped with one network address.In a WSN, where nodes are typically deployed redundantly to protect against node failures or to compensate for the low quality of a single node's actual sensing equipment.

3.1. Applications of Wireless Sensor networks

The applications can be divided in three categories:applications can

1. Monitoring of objects.
2. Monitoring of an area.

3. Monitoring of both area and objects.

3.2 Medical sensor network Application

Sensor networks have been applying in various aspects of medical care . By equipping patients with tiny, wearable vital sign sensors, physiological status of patients can be obtained easily. In emergency or disaster scenario, sensor networks can be used to track healthcare personnel and patient status as well as location continuously in real-time mode. Figure 1 illustrates a medical sensor network application.

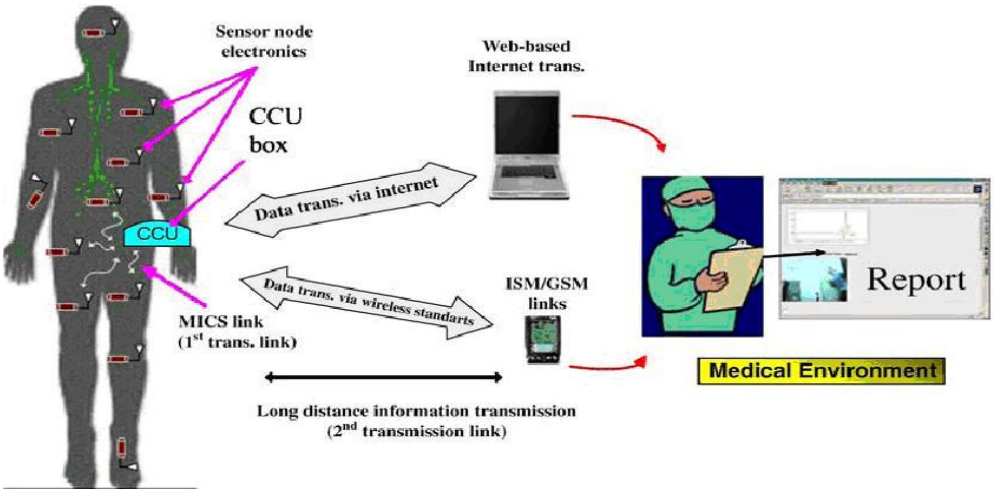

Figure 1: A medical sensor network application

Cellular systems (2.5G, 3G and beyond 3G) have the potential to greatly improve telemedicine services by extending the range of healthcare system, improve the flexibility and heterogeneous network with an end-to-end telemedicine framework. The system consists of a cellular network platform, which gathers the information from wearable sensors, monitoring devices and server platform, which receives, stores, processes collected patients' vital data and forwards them to the existing information systems.

4. ENERGY CONSUMPTION OF SENSOR NODES

4.1. Power Consumption

The main consumers of energy are the controller,the radio front ends,to some degree the memory,and depending on the type, the sensors.To use such a battery to power a node even only a single day,the node must not consume continuously more than 1/(24.60.60) Ws/s≈11.5µw.No current controller,let alone an entire node,is able to work at such low-power levels.one important contribution to reduce power

consumption of these components comes from chip-level and lower technologies:Designing low-power chips is the best starting point for an energy-efficient sensor node.Introducing and using multiple states of operation with reduced energy consumption in return for reduced functionality is the core technique for energy-efficient wireless sensor node.

At time t1,the decision whether or not a component is to be put into sleep mode should be taken to reduce power consumption from P_{active} to P_{sleep}.If it remains active and the next event occurs at time t_{event},then a total energy of $E_{active}=P_{active}(t_{event}-t_1)$ has be spent uselessly idling.Putting the component into sleep mode,on the other hand,requires a time τ down until sleep mode has been reached:as a simplification,assume that the average power consumption during this phase is $(P_{active+} P_{sleep})/2$.Then,Psleep is consumed until t_{event}.In total,$\tau_{down}(P_{active+} P_{sleep})/2+(t_{event}-t_1-\tau_{down)}$Psleep energy is required in sleep mode as opposed to $(t_{event}-t_1) P_{active}$ when remaining active.The energy saving is thus

$$E_{saved}=((t_{event}-t_1) P_{active}- \tau_{down}(P_{active+} P_{sleep})/2+(t_{event}-t_1- \tau_{down)}P_{sleep}).$$

Once the event to be processed occurs,howeverman additional overhead of

$E_{overhead}= \tau_{up(}(P_{active+} P_{sleep})/2.$

is incurred to come back to operational state before the event can be processed,again making a simplifying assumption about average power consumption during makeup.This energy is indeed an overhead since no useful activity can be undertaken during this time.Clearly,switching to a sleep mode is only beneficial if Eoverhead < Esaved,or,equivalently,if the time to the next event is sufficiently large:

$$(t_{event}-t_1)>1/2 \ \frac{(\tau_{down+}(P_{active+} P_{sleep}) \ \tau_{up}}{P_{active+} P_{sleep}}$$

4.2. Energy Consumption during transmission

The energy consumed by a transmitter is due to two sources: one part is due to RF signal generation,which mostly depends on chosen modulation and target distance and hence on the transmission power P_{tx},that is,the power radiated by the antenna.A second part is due to electronic components necessary for frequency synthesis,frequency conversion,filters,and so on.The transmitted power is generated by the amplifier of a transmitter,ITS own power consumption Pamp depends on its architecture,but for most of them,their consumed power depends on the power they are to generate.A more realistic model assumes that a certain constant power level is

always required irrespective of radiated power,plus a proporational offset:

$$P_{amp}=\alpha_{amp}+\beta_{amp}P_{tx}$$

Where α_{amp} and β_{amp} are constants depending on process technology and amplifier architecture.

The efficiency of the power amplifier $\eta_{pa}=P_{tx}/P_{amp=1Mw/174Mw+5.0.1mW}\approx 0.55\%$

4.3 Energy Efficiency

Energy is a precious resource in wireless sensor networks and that energy efficiency should therefore make an evident optimization goal.It is clear that with an arbitrary amount of energy, most of the QOS metrics defined above can be increased.The most commonly considered aspects are:

- Energy per correctly receive bit
- Energy per reported event
- Delay/energy trade offs
- Network Lifetime
- Network half-life
- Time to partition
- Time to first node death
- Time to loss of coverage
- Time to failure of first event notification

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:

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.

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.

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 [3].

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.

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

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 mechanism should be implemented in real-time healthcare applications that can restrict the access of the physiological information, as user's roles. For example, the HL7 Standard Development Organization uses a role-based access control model

Data availability: Availability ensures that services and information can be accessed at the time when they are required. Thus, medical sensor node availability ensures that the patient's data are constantly available to the caregiver. If a sensor node is captured by an adversary, then its data availability will be lost, thus it is required to maintain always-on the operation of the healthcare applications in the case of loss of availability.

Data freshness: In healthcare applications, data confidentiality and integrity are not enough if data freshness is not considered. Data freshness implies that the patient physiological signs are fresh or resent; and thus an adversary has not replayed the old messages. There are two kinds of freshness: weak freshness, which gives partial message ordering but does not carry time-delay information; and strong freshness,

gives a total order on a request-response pair and allows for delay estimation. ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted towards health care

Table 1: Different networks for healthcare

	WLAN (802.11)	**Bluetooth-based WPAN (802.15.1)**	**ZIGBEE (802.15.4)**
Range	100m	~10-100m	~10m
Cost/complexity	100m	1	0.2
Power consumption	Medium	Low	Ultralow
Size	Larger	smaller	smallest

CONCLUSION

In this paper we discussed advantages of wireless medical devices and challenges involved in this technology. The use of wireless communications technology in Medical Applications is increasing steadily.This technology can have an important contribution in improving lives of patients at the same time as reducing costs.Wireless sensor networks (WSN) are already being deployed in a variety of scenarios including those in the area of medical care. We present deeply wireless technologies used in medical recently. We have also identified standards being used in wireless medical applications and location of wireless network in a healthcare system.

REFERENCES:

[1] Zahra Rezaei, Shima Mobininejad , Energy Saving in Wireless Sensor Networks, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012.

[2]. Saleem S., Ullah S., Kwak K.S. A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks. Sensors. 2011;11:1383–1395.

[3]. Strong User Authentication and HIPAA: Cost-Effective Compliance with Federal Security Mandates. Available online: http://www.techrepublic.com/whitepapers/strong-user-authentication-and-hipaa-cost-effective-compliance-with-federal-security-mandates/2345053 (accessed on 28 May 2011).

AUTHOR BIOGRAPHY

Dr. T.Lalitha is an Associate professor at the department of Master of Computer Application(MCA), Salem. She have 16 years experience in academic field. She completed Master of Computer Application in 2000 and completed M.Phil in Bharathidasan University in 2004.She completed Ph.D Computer Science in 2013.Totally she had 35 International publication and these publications are Scopus indexed and high impact factor. She had 31 International Conference publication. She published a book such as "Problem Solving Techniques"," Open Source System" and "Computer Concepts". She delivered a topic such as "Computer Algorithms", Open Source System" ,"Digital Communication" and "Network Security" in various Organizations. She is a Lifetime member of ISTE.