Applications of Wireless Sensor Networks in Healthcare: An Overview of the Areas of Implementation and Related Challenges

Bhaskarjyoti Paul[1]

[1]*Graduate, Department of Electrical and Instrumentation Engineering, Assam Engineering College, Assam, India*

Abstract: *The healthcare domain has seen promising applications of wireless sensor networks. With rapid advances in the development of biomedical sensors, low power electronics and wireless communications, a new generation of wireless sensor networks known as wireless body area networks has emerged. Current wireless medical sensor network healthcare trends focus on patient reliable communication, mobility and energy efficient routing. However, as most of the devices and their applications are wireless in nature, security and privacy concerns, coupled with scarcity of available resources are becoming major areas of concern, which may restrict people from taking advantage of the full benefits of the system. In this paper, some of the established and emerging healthcare applications enabled by wireless sensor networks have been discussed, along with the existing issues and challenges to their successful implementation.*

Keywords: Wireless medical sensor networks, Healthcare, Security.

1. INTRODUCTION:

The application of wireless sensor networks in various domains have allowed for sampling of physical, psychological, physiological, cognitive and behavioural process in both personal as well as large scale spaces [1]. This has resulted in various sensory information based healthcare applications. The advances in the development of cheap, miniature and high quality sensors have enabled for complex medical conditions to be inferred from sensory information, while also allowing caregivers to timely disseminate these sensory information, thanks to the emergence of pervasive internet connectivity.

Let us take a look at some of the successful implementations of wireless sensor networks in the field of healthcare applications.

1.1 Vital sign monitoring in hospitals:

Continuous and benign monitoring of patients and more physiological functions in clinical settings, especially hospitals, is one of the areas where the implementation of wireless medical sensor networks has become increasingly important. The implementation of new biomedical wireless networks with a common architecture and the capacity to handle multiple sensors, monitoring different body signals with different requirements have shown to provide several advantages as compared to traditional wired systems. Wireless medical sensor networks (WMSN) provide ease of application; reduce risk of infections and failures.

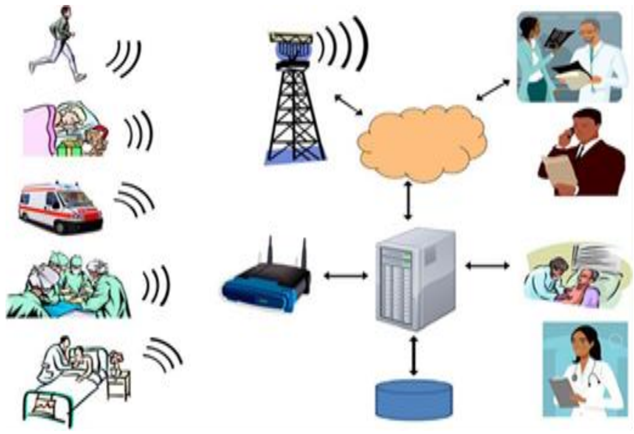

Fig 1: Wireless sensor network architecture.

Biomedical wireless sensor networks have also been shown to reduce the cost of delivery, in addition to enhancing mobility and efficiency. The Biomedical sensor networks developed and implemented at the Interventional Center, Oslo University Hospital has helped facilitate aggressive and early patient ambulation [2]. Implemented using a commercial sensor integration platform from Imatis, it has been successful in overcoming several challenges, such as sensor synchronisation and noise handling, while on the other hand providing for unrestricted mobility. Using Crossbow MICAz motes, a biomedical wireless sensor network has been designed at the University of Texas at Dallas for monitoring patient vital sign data with a mesh network that routes data to a remote base station within the hospital [2]. The nodes of the network are self-powered and get its energy from overhead 34 W fluorescent lights using solar panels. The network nodes can be interfaced to different vital sign sensors like electrocardiograms (ECGs), blood pressure (BP), and pulse oximeters. The hospital faculty can access the patient's data at any point in time without the need to be present in the room. A graphical user interface (GUI) has been designed to store and display data on the base station computer. Such examples provide concrete evidence to believe that the implementation of wireless medical sensor networks have and will lead to reduced hospitalization time, as well as improved documentation, leading to better diagnostic, observation and patient treatment.

1.2 At-home and mobile aging:

CODEBLUE:

With the potential for enormous impact of sensor networks on the various aspects of medical care, CAREER project has overseen the development of a robust, scalable software platform for medical sensor networks, called CODEBLUE, which provides protocols for device discovery; publish/subscribe multihop routing, and a query interface allowing caregivers to request data from groups of patients [3]. Addressing the robustness and scalability of large networks of Wireless medical sensors intertwines a variety of other challenges, starting from limited radio bandwidth and highly variable data rates to a broad range of reliability requirements. CODEBLUE includes new communication mechanisms to allow wireless sensors to rapidly and reliably relay information on the patient status to a command post or a smartphone. This also carefully manages wireless communication of the sensors to ensure that high quality data can be collected over long periods of time.

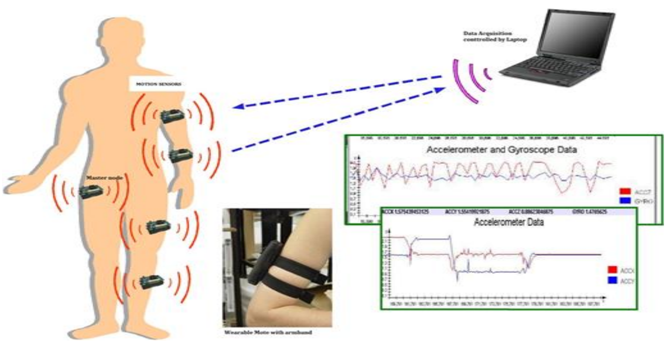

Fig 2: CODEBLUE use in clinical settings.

HEALTHGEAR:

HealthGear is a real-time wearable system for monitoring, visualizing and analysing physiological signals [4]. HealthGear consists of a set of non-invasive physiological sensors wirelessly connected via Bluetooth to a cell phone which stores, transmits and analyses the physiological data, and presents it to the user in an intelligible way.

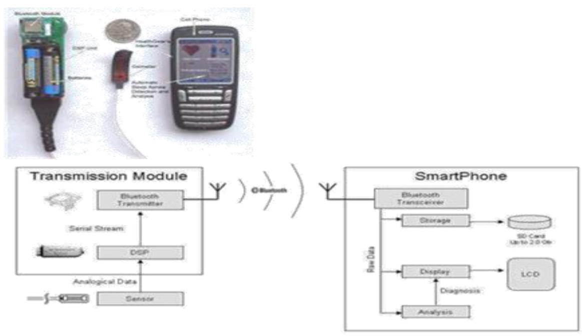

Fig 3: HEALTHGEAR architecture

AMON:

AMON is a wearable medical monitoring and alert system targeting high-risk cardiac/ respiratory patients [5]. The system includes continuous collection and evaluation of multiple vital signs, intelligent multi-parameter medical emergency detection, and a cellular connection to a medical centre. By integrating the whole system in an unobtrusive, wrist-worn enclosure and applying aggressive low power design techniques, continuous and long-term monitoring can be performed without interfering with the patient's everyday activities and restricting their mobility.

1.3 Assistance with motor and sensory decline:

WEMU:

Conventional epilepsy diagnosis and treatment rely on seizures recording through fixed monitoring systems only available in a hospital setting. Often times the patient's seizures are not recorded on account of limited accessibility of these fixed systems, leading to suboptimal diagnosis and treatment. In order to help monitor and diagnose epilepsy with a greater degree of accuracy and reduce diagnostic time, Bioserenity, a French medical device company, in collaboration with a British epilepsy organisation (Epilepsy Action), and a French epilepsy organisation (Efappe) designed WEMU [6], a first of its kind smart clothing system. With embedded dry sensors that constantly monitor the patient's cardiac, muscle and brain activities, the data is transmitted to a smartphone app through low energy Bluetooth, which analyses the received data and allows it to the visualised by the patient or even remotely by an healthcare professional. WEMU system also allows for acquisition of more accurate information which is valuable for research on the occurrence of seizures by the epilepsy research community.

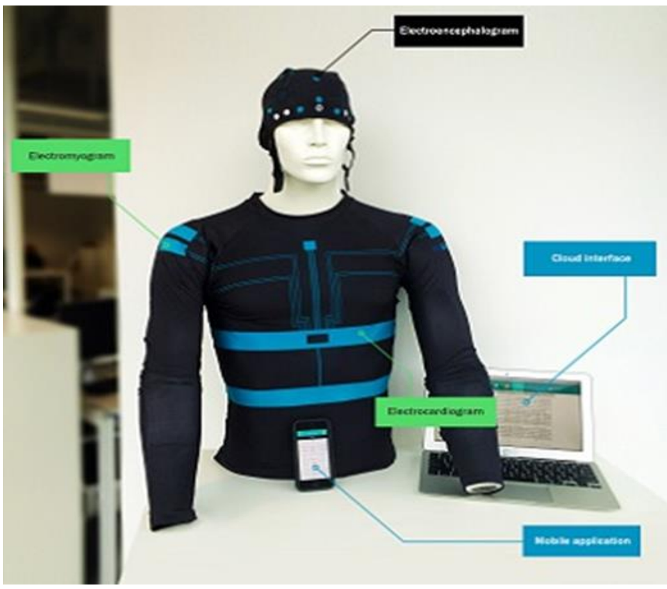

Fig 4: WEMU architecture.

WEALTHY (Wearable Health Care System):

The WEALTHY system [7] has been successfully tested on cardiac patients during rehabilitation and on soldiers during trials where extreme stressful environment conditions have been simulated. Implemented using integrating computing techniques, smart sensors, portable devices and telecommunications, together with local intelligence and a decision support system, the WEALTHY system presents many innovations:

- "Smart" garment fabrics have been developed, where sensing is done through textile materials and pre-processing steps are done on the portable electronic device, thus increasing the mobility and safety of the user, and limiting the amount of data to be transferred
- Direct wireless communication over the public network: Real-time data transfer will be made possible from anywhere the patient is located, and not limited to home or hospital
- Intelligent decision support system: User-friendly interfaces that help the interpretation of physiological signals by medical staff and assist them taking the right decisions

2. CHALLENGES OF WIRELESS BODY AREA NETWORKS

A. Physical Layer Challenges

The physical layer suffers from a number of challenges when it comes to implementing wireless body area networks. Bandwidth limitation is one of the major challenges faced by the physical layer. However, using low data rates and transmitting multiple pulses per bit, bandwidth limitations of current narrowband systems can be overcome. Some of the challenges include receiver complexity, higher power consumption in dynamic condition, and distance limitation between transmitter and receiver antennas. [8][9]

B. MAC Layer Challenges

For health monitoring applications, Quality of Service (QoS) requirements for emergency traffic should be explored. Indeed, under emergency conditions, the delivery of data with a reasonable delay should be guaranteed. Accordingly, emergency data prioritization mechanisms should be developed and fairness among different situations should be considered [8][9].

C. Network Layer Challenges

One of the open research challenges of wireless healthcare monitoring systems is the capability of these networks to reduce the energy consumption of computing and communication infrastructure. In fact, the convergent traffic inherent in wireless sensor networks may cause a choke effect at the node closer to the base station. Consequently, load balancing routing protocols need to be developed. In addition, congestion avoidance and rate control issues become significant when multimedia traffic is encountered. For better utilization, these techniques should as well be integrated with data compression techniques [8] [9].

D. Transport Layer Challenges

Reliable data delivery is one of the most important requirements of a wireless healthcare network since it deals with life-critical data. Thus, a lost frame or packet of data can cause an emergency situation to be either totally missed or misinterpreted. As a result, a cross layer protocol must be designed in order to ensure reliable delivery of different types of traffic [8] [9].

E. Application Layer Challenges

Since the application layer is at the top of the stack, it is expected to have a coordinating mission. In this context, the organization of data is critical and requires efficient machine learning algorithms to allow self-learning and autonomous system replacing [8] [9].

3. Security Threats to Wearables

The security threats present in wearable sensor networks can be placed under three categories:

1) Confidentiality threats 2) Threats to Integrity 3) Threats to Availability.

3.1 Threats to confidentiality: Threats to confidentiality involve scenarios in which the attackers get unauthorised access to information using various techniques such as eavesdropping and traffic analysis among others. [9]

3.1.1 Eavesdropping Attacks:

Eavesdropping is the unauthorized real-time interception of a private communication and these attacks are significant security threats to wearable systems as they can expose user's personal information to an attacker. Also, they may end up being entry points for other forms of attacks. Most of the existing wearables do not have a proper implementation of the MAC address randomisation defined in the BLE specification as a privacy preserving provision. These implementations enable adversaries to eavesdrop on the wireless channel and follow the advertisement packets to track a BLE device easily. [9] [10]

3.1.2 Traffic Analysis Attacks

In the context of wearables, traffic analysis attacks are the processes of monitoring traffic exchanged between wearables and its base and/or server and make inferences from patterns of the communication.[10]

3.1.3 Information Gathering Attacks

As mentioned previously under Eavesdropping Attacks and Traffic Analysis Attacks, passive monitoring of data transmissions on wearable devices allows adversaries to collect information exchanged between a wearable and its hub [9]. Consequently, such collected information can be used to conduct serious information gathering attacks such as breaking the key exchange in BLE wearable device pairing or to collect information about user's other devices such as smartphones. [9][10]

To summarise, majority of the reported vulnerabilities are due to the inadequate implementation of security measures by the devices manufactures rather than fundamental security limitations in Bluetooth LE. As happened in the smartphone domain the next generation of the consumer wearable products are likely to address these security vulnerabilities. However, the resource against security trade-off will still be there and effective countermeasures to protect confidentiality in wearable communication are essential [10].

3.2 Threats to Integrity:

Integrity is an important security requirement for information systems especially for wearable systems where collected data is usually sensitive and private. It is important to make sure that data is not altered in transit and being received by authorised parties only. Potential vulnerabilities with respect to data integrity are discussed below

3.2.1 Modification Attacks:

As data transmission between wearable devices is typically wireless in nature, it is prone to be modified or altered. In these types of attacks, the adversaries after either intercepting the traffic exchange of wearable devices or gaining access to the information can modify the content of exchanging packets or change the timestamp of data packets. Accurate timestamps of medical data is crucial for medical practitioners and insurance providers and attackers/malicious users might attempt to modify the timestamps to obtain monetary benefits. [10] [11]

3.2.2 Replay Attacks:

In replay attacks [10], attackers obtain a copy of the valid data packet uploaded by the wearable device to the server and replay it with the objective such as impersonation or data corruption. It has been demonstrated that by conducting a possible replay attack in a commercially available insulin delivery system consisting of a glucose meter, an insulin pump, a remote control and a Universal Software Radio Peripheral (USRP), the attackers are able to determine the packet format and learn the device type, its PIN, the therapy or glucose level, and medical condition of the patient [9].

3.3 Threats to Availability

The major type of attack against availability is Denial of Service attacks that attempt to interrupt the communications of wearables and their base or inject huge useless information to flood the wearable device's storage capacity. Similar to the other threats explained above, current attacks denying service is possible only because of implementation shortcomings by the manufactures and can be expected to be resolved in next generation of products. Nonetheless, it is essential to continuously look for such vulnerabilities in wearable products, especially the health related products such as insulin pumps which can't accommodate downtimes.

Resource Scarcity

In order to enable small device sizes with reasonable battery lifetimes, typical wireless sensor nodes make use of low-power components with modest resources [12]. The extremely limited computation, communication, and energy resources of wireless sensor nodes lead to a number of challenges for system design. Software must be designed carefully with these resource constraints in mind. The scant memory necessitates the use of lean, event driven concurrency models, and precludes conventional OS designs. Computational horsepower and radio bandwidth are both limited, requiring that sensor nodes trade off computation and communication overheads, for example, by performing a modest amount of on-board processing to reduce data transmission requirements. Finally, application code must be extremely careful with the node's limited energy budget, limiting radio communication and data processing to extend the battery lifetime. While smartphone-based systems typically enjoy more processing power and wireless bandwidth, the fact that they are less flexible compared to customizable mote platforms limits their capability to aggressively conserve energy. This leads to shorter recharge cycles and can limit the types of applications that smartphones can support. Another consideration for low-power sensing platforms is the fluctuation in the resource load experienced by sensor nodes. Depending on the patient's condition, the sensor data being collected, and the quality of the radio link, sensor nodes may experience a wide variation in communication and processing load over time. As an example, if sensor nodes perform multihop routing, a given node may be required to forward packets for one or more other nodes along with transmitting its own data. The network topology can change over time, due to node mobility and environmental fluctuations in the RF medium, inducing unpredictable patterns of energy consumption for which the application must be prepared.

4. CONCLUSION

In this paper, an overview of the wireless sensor network applications in healthcare has been presented. The overview focused on current healthcare applications using wireless sensor networks and the requirements for a successful implementation. It further discusses the challenges present, including security and privacy concerns, interoperability, scarcity of resources, as well as a need for reliable communication. The latest advances in both hardware and software provide enough evidence to suggest wireless sensor networks will result in significant developments in healthcare practise and research.

REFERENCES:

1) Jeonggil Ko, Chenyang Lu, Mani B. Srivastava, John A. Stankovic, “Wireless sensor networks for healthcare”

2) Dr. Afsaneh Minaie, Dr. Ali Sanati-Mehrizy, Paymon Sanati-Mehrizy, Dr. reza Sanati-Mehrizy, “Applications of wireless sensor networks in healthcare system”

3) Matt Welsh, “Code Blue: A wireless Sensor Network for medical care and disaster response”

4) Nuria Oliver and Fernando Flores-Mangas, “HealthGear: A Real time Wearable System for Monitoring and Analysing Physiological Signals”

5) U. Anliker, J.A Ward, P. Lukowicz, G. Troster, F. Dolveck, M. Baer, F. Keita, E. Schenker, F. Catarsi, L. Coluccini, A.Belardinelli, D. Shklarski, M. Alon, E. Hirt, R. Schmid and M. Vuskovic, “AMON: A wearable multiparameter medical monitoring and alert system”.

6) https://www.medgadget.com/2014/08/wemu-smart-clothing-for-epilepsy-monitoring-and-diagnosis-video.html

7) http://www.smartex.it/en/research/111-european-projects/268-wealthy-en

8) Hadeel Elayan, Raed Shubair and Asimina Kiourti, “Wireless Sensors for Medical Applications: Current Status and Future Challenges”

9) Pardeep kumar and Hoon-Jae Lee, “Security Issues in Healthcare Applications using wireless medical sensor networks: A survey”

10) Suranga Seneviratne, Yining Hu, Tham Nguyen, Guohao Tan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, Aruna Seneviratne, “A survey of wearable Devices and Challenges”

11) Moshaddique Al Ameen and Jinqwei Liu and Kyungsup Kwak, “Security and Privacy issues in Wireless Sensor networks for Healthcare Applications”

12) I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey”.