Security and Privacy Issues of Medical Systems in Wireless Sensor Networks: A Survey

Muhammad Hunain Memon[1], Aakash kumar[1,] Muhammad Hammad Memon[2], Syeda Munazza Marium[3], Jalaluddin Khan[2]
[1]School of Information Science and Technology, University of Science and Technology of China, Hefei, China
[2]School of Computer Science & Engineering, University of Electronic Science and Technology, Chengdu 611731, China
[3]Computer System Engineering Department Mehran University of Engineering & Technology Sindh Pakistan
Email: hunainmemon@ieee.org, akb@mail.ustc.edu.cn

***Abstract*— For decades, the wireless medical sensor network (WMSN) has shown great prospective in refining health care quality. The vast ranges of medical applications that lead to computer-assisted treatment from all over the health monitoring are based on WMSNs technology. These applications introduce emergency medical response systems with its numerous advantages and facilities. However, these technologies have privacy and security challenges that need to be analyzed to make it preferable and socially acceptable. This survey paper depicts the current state-of-the-art wireless sensor network (WSN) technologies being used in medical applications. In this paper, we have focused on system architecture, routing, security, and privacy issues with various medical applications from various research work.**

Keywords*— *wireless sensors network; medical applications; ubiquitous health monitoring; WSN technologies.

I. INTRODUCTION

Wireless sensor network (WSN) is an emerging technology being researched from the last few decades. WSN is a network with features of reliability, mobility, and deployment [1-10]. It carries vast importance in medical applications, defense, agriculture, transportation, industry, and disaster monitoring [11]. It uses limited resources in any area, with a low cost, more reliable, and devises mobility. The primary focus of WSN is to deploy the number of tiny sensor devices in various regions for data collection and transmit it to its defined destination [12]. In the near future, complete health monitoring of patients will take place remotely through WSN technology by having minimum direct interaction between doctors and their patients [13]. This type of data is further process patient's information at the health care centers and diagnosis centers. There are many types of WSN nodes; some WSN nodes come with wireless medical sensors network, that are portable, small in size, wearable, and consist of a limited tiny-sized battery. Some other forms of WSN include Generic WSN, which are automatic, fixed WSN are reliable with standalone while the WMSN devise human involvement.

Developing a process for wireless healthcare System initiate many challenges, e.g., data transmission reliability, data delivery, management of power, and patient's data security [14]. The state-of-art research shows that WMSN has some flaws which have to be discussed and need to resolve. WMSN are upward towards innovative procedures in healthcare applications. Various projects have been initiated through different scientists and research scholars who provide the monitoring of the patient in a continuous manner at the hospital, clinic, or even at home. This survey paper discusses some WMSNs of medical systems and their applications with their pros and cons and comparison of one system to other systems.

II. NETWORKS OF MEDICAL SYSTEMS

A. *Codeblue*

Codeblue [15] is a wireless medical sensor network in which they have used sensors that can sense the patient's body, analyze the parameters and transmit the data wirelessly to the user's device, e.g., personal digital assistant (PDA) for analysis. In this project, a doctor queries the patient data from the sensors, then the recorded data of the patient is being resent to the doctor's PDAs. The WMSNs publishes data to the channel, and the user uses this channel by using PDAs or handheld device. There are particular goals, which include hospital care and emergency care. This project is composed of software and hardware parts. These parts related to the wireless vital sign sensors

- Wireless two-lead electrocardiogram (EKG)
- Electromyogram (EMG), accelerometer as well as sensor gyroscope, using a stroke to monitors the patients.
- Codeblue software platform

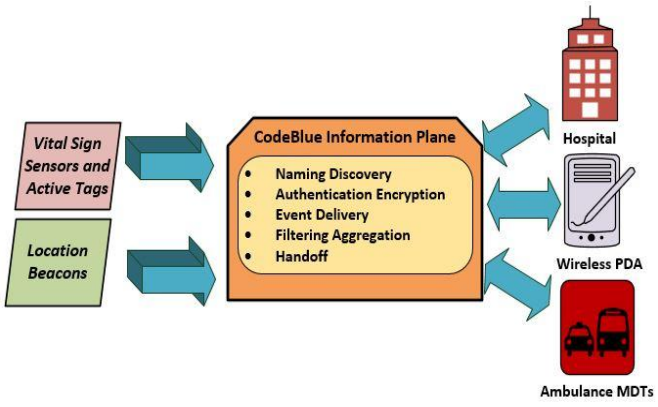


Fig. 1. Codeblue Architecture [15].

Codeblue's developers realize the necessity of security and safety in medical applications; nonetheless, it is also in the development phase, which advancing its features day by day [16, 17]. The developers of Code Blue suggest that for key generation elliptic curve cryptography is better, and the tiny Sec technique is effective for symmetric encryption within this study. Fig. 1. Shows the architecture of the Code Blue.

B. Alarm-Net

Alarm-Net [18], a medical sensor network for healthcare, developed at the University of Virginia. This project has been designed for the health monitoring of patients living in a home-based environment. It involves environmental sensor networks and body sensor networks. It is 3 tier architecture based on:

- Body sensor devices which sense and collect the patient's body data.
- Environmental sensors are deployed in environments spaces.
- Internet protocol-based network which have gateways and alarm gate.

The idea behind the body sensors is that it transmits data using single hop to the environmental sensors. They forward the data to the alarm gate sensor. The alarm gate is a communication gateway between IP and wireless sensors, and the gate is further connected to the backend server. Fig. 2. Shows the system design of Alarm-Net.

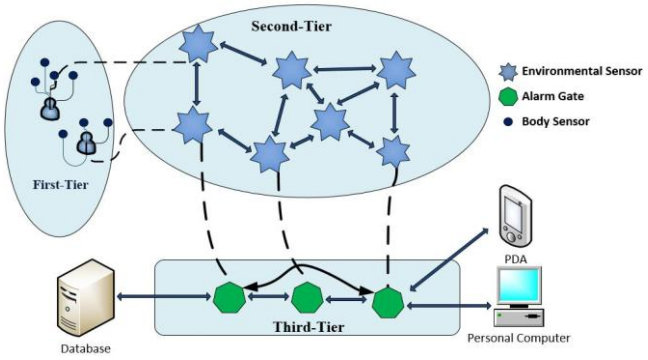


Fig. 2. System Design of Alarm-Net [18]

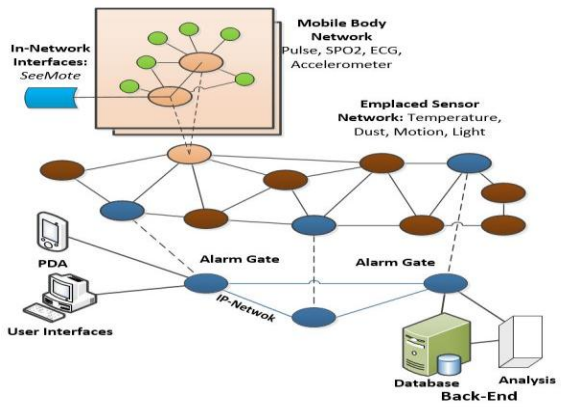


Fig. 3. Alarm-NET architecture components and logical topology [18].

The architecture of the alarm net includes various devices in single architecture (wearable body networks, wireless sensors, and IP-network elements). This architecture is described by grouping devices, based on their platform as well as role within the system. Further alarm net needs data security for the data privacy concern of the patients. Only authenticated and authorized users use the sensors network while the IP network is secured through the password. The WSN is used with layer security setups. Sensors use built-in cryptosystems. Fig. 3. Shows the Alarm-NET architecture components and their logical topology[18].

C. Mobihealth

Mobihealth [10] is a generic platform for house medical management, and this project is initiated by Europeans. This home healthcare project works by using the sensors' body area network (BAN), which is based on wireless technology. It is using general packet radio service GPRS communication technology and wireless technology for transmitting data. Mobihealth has the capability to measure the medical parameters and transfer the measured outcomes. This research provides the feasibility to use BAN to deliver a facility-based platform for medical professionals and patients. It has lightweight sensors that are used on or attached to the human body. It has the capability of mobility for monitoring or observing patients. Fig. 4. shows the healthcare BAN architecture of Mobihealth.

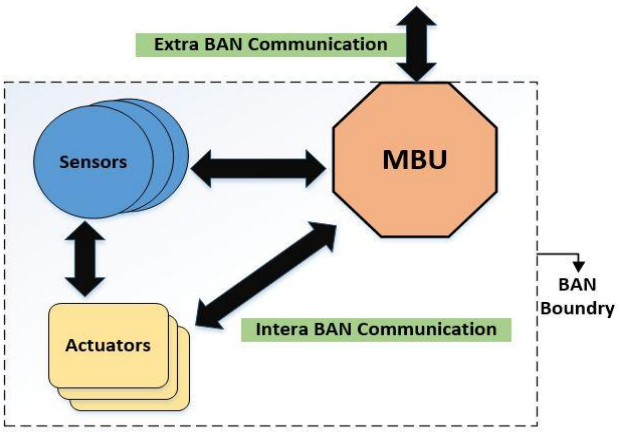


Fig. 4. Healthcare BAN Architecture [10].

D. MEDiSN

MEDiSN [12, 19], a medical sensor network about healthcare, it is based upon research which is presented and developed at Johns Hopkins University. It is composed of physiological monitors (PM) with powered batteries and medical sensors for collecting patient's information. The PMs stores the temporary data and transmits it to the relay points (RP) of stationary RPs. It has a bidirectional routing tree; moreover, the MEDiSN network is connected to the database server, which continuously stores data and presents it to the authorized user. There is a limitation in MEDiSN that the authentication protocol for its backend server is unknown, which results in safety breaching and unreliable privacy Fig. 5. Shows the healthcare architecture of MEDiSN.

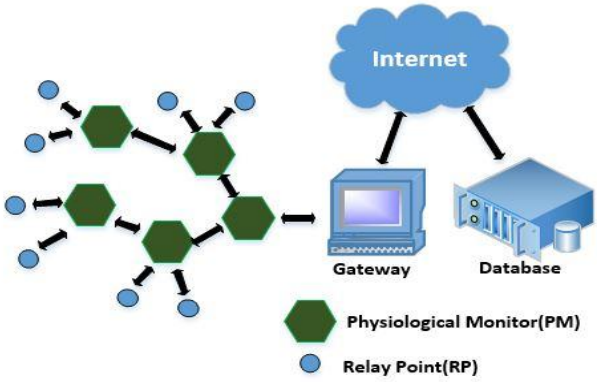


Fig. 5. Healthcare Architecture of MEDiSN [12, 19].

E. MobiCare

A health care project developed by Chakravorty in 2006. The design is based on a wide area network patient monitoring system, that consists of body sensors networks (BSN) wearable sensors, BSN manager, and Mobicare servers. It will timely sense the status of the patient's body and transmits data to the BSN manager. Afterward, in the final stage, it will send the data to the mobicare server. It utilizes the Http protocol, and the post method is used to transmit the data to the server.

Mobicare is an architecture that provides quality health care, Programmable architecture, flexible service, and medical systems integration. Furthermore, health care personnel can monitor the patient's condition globally whenever and wherever they want. These factors remain fruitful in expanding health care and patient monitoring applications. Fig. 6. Shows the Mobicare Architecture [20].

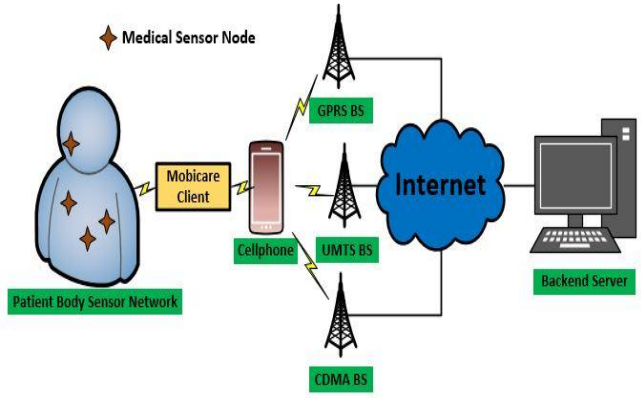


Fig. 6. MobiCare Architecture [20].

III. MEDICAL SYSTEMS COMPARISON

Table I. Shows the comparison of different medical systems discussed in this research paper in terms of the operational environment, supported application, reliability mechanism, a scheme for energy efficiency, routing methodology, and techniques for mobility support.

TABLE I. MEDICAL SYSTEMS COMPARISON [12, 15, 18, 20, 21]

Parameter	MEDiSN	Codeblue	AlarmNet	MobiCare
Operational Environment	The operational environment constitutes a dedicated wireless sensor network in hospital deployment with RPs and PMs.	Codeblue prototype was validated on 30 node Ad Hoc sensor network test-bed, demonstrating its scalability and robustness.	Scalable and heterogeneous architecture Integrating ESs and PMs in assisted-living and home environment.	A remote wireless patient monitoring Consisting of BSN, Mobi client, and Mobicare Server.
Supported Application	Applied in medical emergency detection for patients monitored in hospitals and disaster scenes.	It has been applied as a medical application for home-based patients.	Patient health monitoring in the assisted-living and home environment.	Wide-area mobile patient monitoring .
Reliability Mechanism	Message-oriented middleware which was JMS-based has been selected to run On the gateway. While the backend server is responsible for storing, routing, and retransmitting messages.	Codeblue was designed to provide for reliable transmission of critical data through content-specific prioritization and dynamic scaling of Transmission power.	Three-tier architecture with mobile body network, emplaced sensor network and IP network.	It has a secure, stable dynamic cryptograph update functionality
Scheme for Energy Efficiency	through duty cycling their radios the distribution enables PMs to use low energy	Codeblue uses Berkeley Mica2 sensor nodes having advantages (low-power, SOC radio) Which utilizes low power sleep state up to 10μA	Uses (COPM) in which some nodes are connected into the wall and operates using batteries.	Propose the use of low-frequency the wireless sensor which enables the property of low power property by using the Berkeley MICA2
Routing Methodology	several-to-single and single-to-single communication between PMs and RPs. also use the collection tree protocol (CTP)	(ADMR) protocol in which sensors transmits data to a respective channel as well as end-user	Single hop at the first tier, multi-hop at the second tier (i.e., shortest-path-first routing protocol)	Application layer standard Http post protocol.
Techniques for mobility Support	During mobility PM transmit its data to the stationed RP that shares the superlative link with it.	Mote tracking system which operates in an entirely decentralized, robust fashion, location accuracy	Emplaced sensors (ES) allows connections with mobile body while in movement	Used always-on wide-area cellular wireless communication Interface.

Recently, several researchers, research-based organizations, and many healthcare medical applications systems have the main focus on the use of wearable sensor devices. Wireless sensor devices having limited capabilities, memory constraints, limited network capacity, and limited power sources, these obstructions caused technical restrictions on their network's functionalities. The upcoming health care system is predicted to raise many issues; these issues can be described as Technical and nontechnical medical applications design issues. (Flowchart 1. Medical Applications Design Issues)

A. Security concerns

Medical sensors are wireless in nature, and these medical sensors are perilous to some attacks, e.g., breach of integrity, breach of confidentiality, and denial of service

attacks. So, numbers of precautions are needed for the safety of health care systems

B. Authentication and authorization of Wireless networks

Authentication and authorization in sensor networks are essential for every single sensor node and healthcare base station. It must verify that only authenticated and authorized users access the data and also validate that either data sent by an authorized user or by an attacker. So, in order to discover adequate security and privacy mechanism, authentication and authorization must be executed for the security of healthcare systems.

C. Data Confidentiality

The process of data protection from the attacker during its transfer is termed as data confidentiality, i.e., and an attacker must be incapacitated to access the data among nodes. If there is an efficient authentication and authorization, then packets of data are secured among nodes.

D. Data Integrity

Data Integrity is a mechanism that verifies the data, which has been transferred, must reach the proper destination in its original form. It makes sure that no packet has been replaced or changed by the attacker.

E. Availability of Data

In medical WSNs applications, to ensure that the data of sensor devices are always accessible even in any case of any attack. Availability confirms the correctness of data being transferred if there is security.

F. Data Freshness

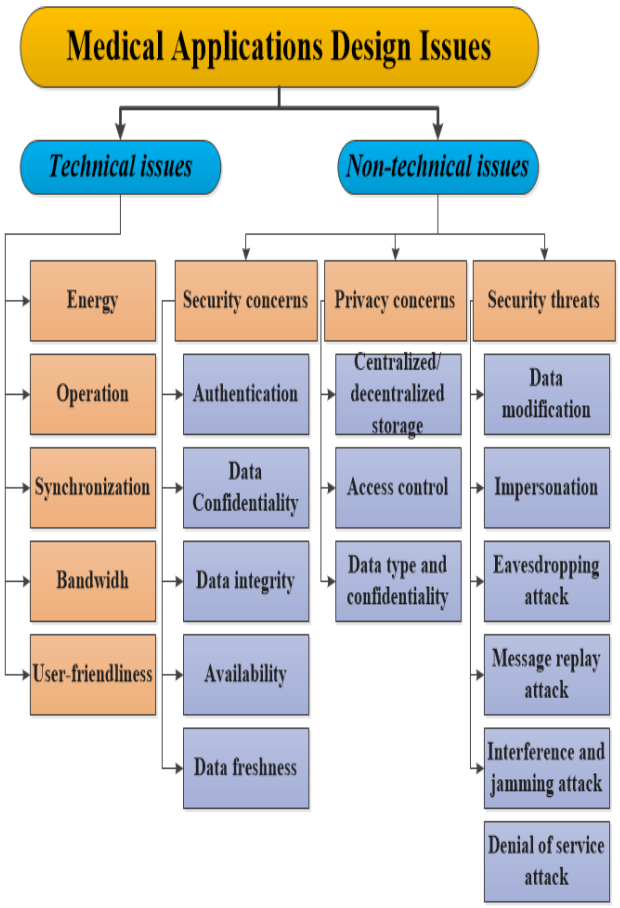
Sometimes attacker attacks in such a way that the message is replied again and again. To ensure the freshness of the data message must not be replied again or repeat many times.

G. Security Threats

Table II. Is representing the attacks and their description with countermeasures for health care sensor networks[22, 23].

TABLE II. ATTACK AND THEIR COUNTERMEASURES [22, 23].

Attack	Description	Countermeasures
Data modification	The assaulter can modify or delete or generate false information which can be the cause of a patient's death	Data security
Impersonation Attack	The assaulter eavesdrops a wireless sensor node's identity information, which causes a delay in the medical data storage process.	Verification
Eavesdropping Attack	The assaulter uses robbed data in performing various evil acts.	Encryption
Message replay Attack	In this type of attack, the attacker sits in the way of communication after breaching the authentication and authorization of the user profile.	Data freshness
Interference	By using an efficient Tx, an assailant can jam sensor radio signals, which causes the delay or loss of data.	interference filters
Denial of service Attack	An attempting will may cause disable of source system which can seriously harm the patient's health	Authentication



Flowchart 1. Medical Applications design issues

H. Privacy Concerns

Privacy is one of the most highlighted and fundamental concerns in WSNs with regard to medical applications. Medical care systems based on wireless technology, which aims to steadily monitor personal information using wireless technology. Therefore, they can have a serious menace to the privacy of a patient or individual patient. There are many privacy issues concerning the use of sensors in health care [22-23].

The first privacy-based issue is that when data stores in the database server, it can be centralized or decentralized, and it may consist of several other local databases in the system. The second privacy-based issue is to give authentic access to the patient's record and his history. There are two ways to access the patient's record. The first way is that users have given rights to read and write in the patient's medical record, such as the physicians and staff members. The other way is that the users have merely given the read-only rights to patients or doctors, staff, etc. In emergency cases that occur to the patient, it is a prerequisite to conserve the patient's privacy, so patient's information can be kept secure from other people. The Third privacy concern is data confidentiality; As the patient may go through multiple medical tests, e.g., pathology tests, psychological tests, x-rays, etc. so it is an obligation to keep tests data secret from others. Those particular records are saved in a database, so it

is suggested that encryption mechanisms should be implemented on them as safety anticipation.

IV. CONCLUSION

WSN has great importance because of its necessity and performance in a variety of applications. This survey paper presents reader knowledge of WMSN projects, their architectures, privacy issues, and security threats to the WSN for medical applications. Also, the comparison among applications is debated. For future research concern, the number of security and privacy issues need to be explored.

REFERENCES

[1] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *The Journal of supercomputing*, vol. 68, pp. 1-48, 2014.

[2] H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad, and M. Ismail, "Energy-efficient wireless sensor networks for precision agriculture: A review," *Sensors*, vol. 17, p. 1781, 2017.

[3] X. Yu, P. Wu, W. Han, and Z. Zhang, "A survey on wireless sensor network infrastructure for agriculture," *Computer Standards & Interfaces*, vol. 35, pp. 59-64, 2013.

[4] Y.-C. Du, Y.-Y. Lee, Y.-Y. Lu, C.-H. Lin, M.-J. Wu, C.-L. Chen, *et al.*, "Development of a telecare system based on ZigBee mesh network for monitoring blood pressure of patients with hemodialysis in health care centers," *Journal of medical systems*, vol. 35, pp. 877-883, 2011.

[5] J. Medina-García, T. Sánchez-Rodríguez, J. A. G. Galán, A. Delgado, F. Gómez-Bravo, and R. Jiménez, "A wireless sensor system for real-time monitoring and fault detection of motor arrays," *Sensors*, vol. 17, p. 469, 2017.

[6] C. Alippi, R. Camplani, C. Galperti, and M. Roveri, "A robust, adaptive, solar-powered WSN framework for aquatic environmental monitoring," *IEEE Sensors Journal*, vol. 11, pp. 45-55, 2010.

[7] J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, and M. Á. Porta-Gándara, "Automated irrigation system using a wireless sensor network and GPRS module," *IEEE transactions on instrumentation and measurement*, vol. 63, pp. 166-176, 2013.

[8] J. V. Capella, A. Bonastre, R. Ors, and M. Peris, "In line river monitoring of nitrate concentration by means of a Wireless Sensor Network with energy harvesting," *Sensors and Actuators B: Chemical*, vol. 177, pp. 419-427, 2013.

[9] M. H. Memon, W. Kumar, A. Memon, B. S. Chowdhry, M. Aamir, and P. Kumar, "Internet of Things (IoT) enabled smart animal farm," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 2067-2072.

[10] A. Van Halteren, R. Bults, K. Wac, D. Konstantas, I. Widya, N. Dokovsky, *et al.*, "Mobile patient monitoring: The mobihealth system," *Journal on Information Technology in Healthcare*, vol. 2, pp. 365-373, 2004.

[11] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," *Proceedings of the IEEE*, vol. 98, pp. 1947-1960, 2010.

[12] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *sensors*, vol. 12, pp. 55-91, 2012.

[13] W.-Y. Chung, G. Walia, Y.-D. Lee, and R. Myllyla, "Design issues and implementation of query-driven healthcare system using wireless sensor ad-hoc network," in *4th International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2007)*, 2007, pp. 99-104.

[14] E. Alasaarela, R. Nemana, and S. DeMello, "Drivers and challenges of wireless solutions in future healthcare," in *2009 International Conference on eHealth, Telemedicine, and Social Medicine*, 2009, pp. 19-24.

[15] D. J. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," in *International workshop on wearable and implantable body sensor networks*, 2004.

[16] K. Lorincz, D. J. Malan, T. R. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, *et al.*, "Sensor networks for emergency response: challenges and opportunities," *IEEE pervasive Computing*, vol. 3, pp. 16-23, 2004.

[17] G. Kambourakis, E. Klaoudatou, and S. Gritzalis, "Securing medical sensor environments: the codeblue framework case," in *The Second International Conference on Availability, Reliability and Security (ARES'07)*, 2007, pp. 637-643.

[18] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, *et al.*, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," *University of Virginia Computer Science Department Technical Report*, vol. 2, p. 17, 2006.

[19] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, *et al.*, "MEDiSN: Medical emergency detection in sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 10, pp. 1-29, 2010.

[20] R. Chakravorty, "A programmable service architecture for mobile medical care," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, 2006, pp. 5 pp.-536.

[21] 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, pp. 93-101, 2012.

[22] T.-G. Lupu, I. Rudas, M. Demiralp, and N. Mastorakis, "Main types of attacks in wireless sensor networks," in *WSEAS international conference. proceedings. recent advances in computer engineering*, 2009.

[23] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, 2006, pp. 5453-5458.