Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 86 (2015) 35368-35371

ISSN: 2229-712X

A Survey of Security Requirement Issues in E-Healthcare Applications Using Wireless Mobile Sensor Networks

I.Bremnavas[1,*], I.Raja Mohamed[2], N.Shenbagavadivu[3] and S.Kother Mohideen[1]

[1]College of Computer Science & Information Systems, Jazan University, Saudi Arabia.

[2] Department of Physics, B.S.Abdur Rahman University, Chennai, Tamilnadu,India.

[3] Department of Computer Applications, Anna University – BIT Campus, Trichy.

ARTICLE INFO

Article history:

Received: 20 August 2015;

Received in revised form:

23 September 2015;

Accepted: 29 September 2015;

Keywords

E-Healthcare applications,
Healthcare security issues,
Patient privacy,
Wireless medical sensor networks,
Wireless sensor network.

ABSTRACT

The e-healthcare applications are considered as a promising field in wireless sensor networks, where patients can be monitored using wireless medical sensor networks (WMSN). Recent research in WMSN healthcare is focused on patient reliable communication, patient mobility, and energy-efficient routing. Deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. This paper will discuss on various security mechanism, privacy issues and requirement of e-healthcare applications.

Introduction

A wireless sensor networks technology has opened up new opportunities in e-healthcare systems. Wireless sensor is the smallest unit of a network. It is low cost, less memory and limited computational power that communicates wirelessly; it supports large scale deployment and mobility. It's also included in various applications such as healthcare monitoring, military, government security policy and earthquake monitoring. This wireless sensor networks which is distributed and self-organized to supervise an e-healthcare monitoring system [1].

The medical technological system can be benefits more from wireless sensor networks are in smart nursing homes and in-home assistance. Figure-1 illustrates the depiction of a body area network with its supporting information infrastructure.

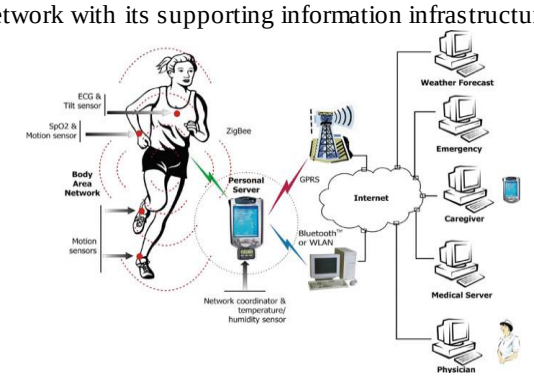

Figure 1. Body area network with its supporting information infrastructure

Now a days the healthcare environment has seen the drastic developments due to the contribution of wireless medical sensor networks (WMSN) in e-healthcare applications. Recently, a term WMSN to bring many other area researchers together from interdisciplinary areas (bioengineering, electronics, computer, medicine), as shown in Figure-2.

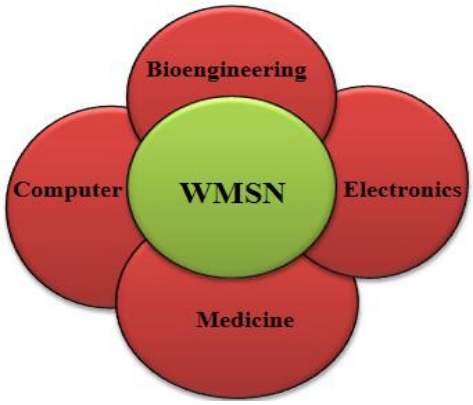

Figure 2. Interdisciplinary research of WMSN

In few decades ago, WMSN is a topic of science and movie fiction for healthcare industries. Now they have provides much quality-of-care in healthcare applications. Especially the development of a wireless e-healthcare, this application offers many innovative challenges, such as, data transmission reliability, mobility of node support, timely delivery of data and power management [2-9]. Figure-3 illustrates a comprehensive design framework of an intelligent wireless patient-monitoring system.

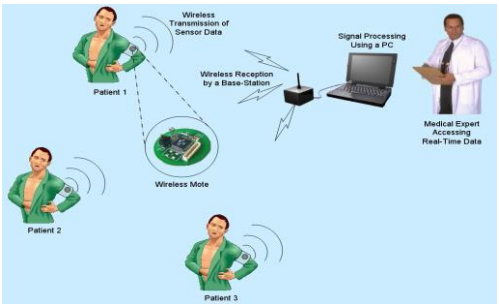

Figure 3. Conceptual demonstration of WMSN

Tele:
E-mail addresses: jmcnavas@gmail.com

In this connection, the new applications are deploying in e-healthcare system predominantly considering the patient privacy and security [10-14]. As shown in Figure-4, WMSN carry the promise of quality-of-care across wide variety of healthcare applications (eg., ambulatory monitoring, vital sign monitoring in-hospitals, elderly peoples at home care monitoring, monitoring in mass-casualty disasters, clinical monitoring, etc.,).

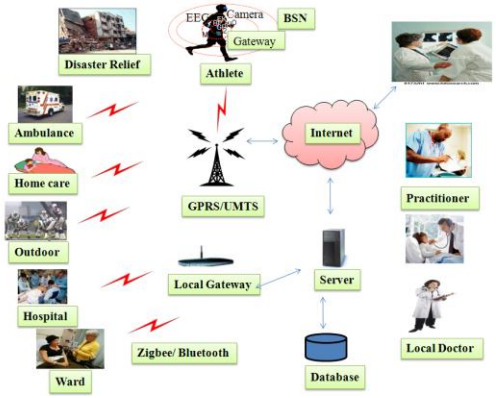

Figure 4. Healthcare application using WMSN

Existing Security Mechanisms

Security mechanisms are used to detect, prevent and recover from security attacks.

Cryptography Security Mechanism

WMSN deals with sensitive physiological information, strong cryptographic functions such as encryption, integrity and authentication. They are considered to be important requirements for developing any safe e-healthcare application. These cryptographic security functions provide privacy and security of patient against many malicious attacks. Strong cryptography security function requires wide computation and resources, therefore picking appropriate cryptography security functions a challenging task. Asymmetric cryptographic security systems are often too expensive for medical sensors and symmetric crypto systems are not versatile enough [15]. However energy, execution time and memory are the basic considerations of medical sensor to apply the various security mechanisms.

Key Management

Key management protocols are essential requirements to develop any secure application. Key management protocol to set up key to the nodes and distribute in the network [16,17].

Secure Routing

Routing and message forwarding is a vital service for end-to-end communication for home care or disaster scenarios. Sensor devices might require sending their data to other devices outside their immediate radio range [18]. Numerous routing protocols have been proposed for sensor networks, but none of them have been designed with strong security [19,20]. Mobility is also considered to be one of the important tasks of wireless sensor networks but most of other proposals; mobility has not been taken into consideration. In e-healthcare applications, mobility needs to be supported by routing protocols. Designing secure routing protocols in mobile networks for WMSN is a complex task.

Secure Localization

WMSN facilitate real time patient access such as the mobility for patient's comfort. Estimation of patient location is needed for the achievement of healthcare applications. Physiological data of an individual, send a patient report to a remote server when medical sensor's sense the patient's location. At the end of this process, medical sensors have to be aware of patient location, i.e., called localization.

Security and Privacy Requirements of e-healthcare Applications

The scenarios on the e-healthcare application, security issues and regulatory laws point out the paramount security and privacy requirements for healthcare using WMSN. Figure-5 shows the healthcare information technology threats, attacks and security concerns.

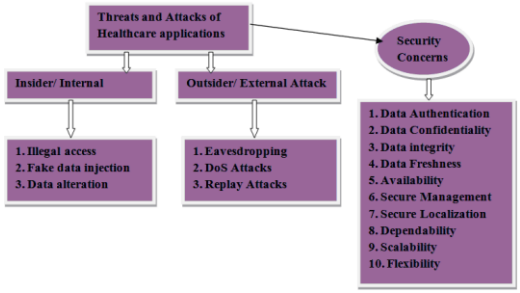

Figure 5. Healthcare information technology, threats, attacks and security concerns

Data Confidentiality

Patient health report information is normally under legal and ethical commitments of confidentiality. These patient health report information should be confidential and available only to the concern doctors or caregivers. Thus, it is important to keep the individual patient health information confidential, so that an adversary cannot eavesdrop on the patient's information. Therefore, data confidentiality is an important requirement of e-healthcare applications using WMSN.

Data Authentication

Authentication is to provide authorization for both medical and non-medical applications. In WMSN e-healthcare applications, authentication service is needed for every medical sensor. The base-station is used to verify that the data were sent by a trusted sensor or not.

Access Control

In e-healthcare application many users such as doctors, pharmacists, insurance companies, lab staff, etc., are directly involved with the patient's physiological data. So, it is highly desirable that a role-based access control mechanism. It should be implemented in real time e-healthcare applications, which can restrict the access of the physiological information, as user's roles.

Data Availability

Data availability ensures that the required information and services can be accessed at any time. Medical sensor node ensures that the patient's data are constantly available to the authorized doctor or the caregiver. If a sensor node is captured by an intruder, then its data availability will be lost. Thus it is required to maintain always-on in the case to avoid loss of availability.

Patient Permission

As a legacy and law enforcement the patient's permission is needed when an e-healthcare provider is disseminating his/her health history information data to another e-healthcare consultant such as medical researcher, insurance company, etc.,

Design Requirements for WMSN

The important design requirements for WMSN are

Reliability and Robustness

For medical diagnosis process and treatment, sensors should give sufficient reliability and must be vigorous to yield high confidence data [21].

Wearability

To attain non-invasive health monitoring, wearable systems detecting physiological signs placed on patient without discomfort, with capability of continuous real time recording. This wearable system should be equipped with wireless communication to transmit signals, although sometimes it is fitting to extract locally relevant variables, which are transmitted when needed.

Real time data acquisition and analysis:

Real time data acquisition, analysis, efficient communication and examination are essential of patient. In e-healthcare applications these are all the requisite of event ordering, time-stamping, synchronization, and rapid response in emergency circumstances.

New Node Architectures

The unification of diverse sensors, RFID tags and back channel is extended haul networks require new and modular node architectures.

Enabling Technology for WMSN

Recently, the WMSN technology is widely used. As shown in Figure-6, wireless medical sensor networks carry the promise of caretaking across wide variety of e-healthcare applications such as ambulatory monitoring, elderly people at home care monitoring and clinical monitoring, etc.,

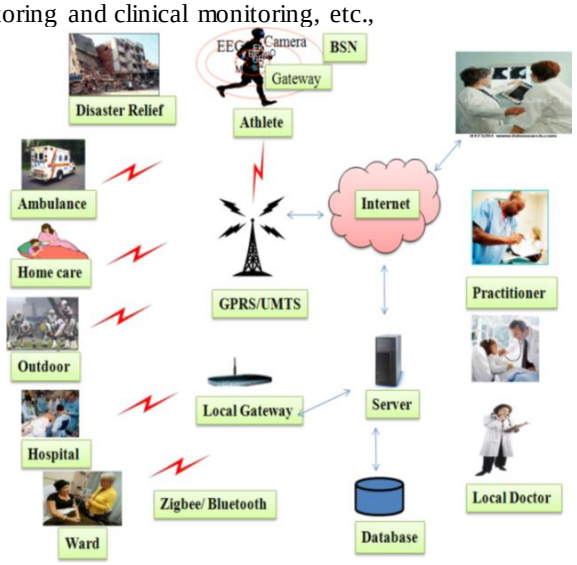

Figure 6. Healthcare Application using WMSN

WBAN (Wireless Body Area Network)

One of the most promising e-healthcare applications that wireless medical sensor networks pioneers thought to be fit to wireless medical sensor technology. Easy to conceive where the patients carry a sensor that can detect health related parameters such as heart rate, glucose level and monitor the patient continuously via a wireless network.

RFID (Radio Frequency Identification)

RFID technology is a hot in recent days. The RFID tags are used in hospitals to keep track of equipment and also planted on patient's body. The doctor's can easily identify the location of the patients with the help of RFID tags. It's a low powered radio device.

WIMAX

Based on the IEEE 802.16 standards, so-called WiMAX which has strong-security wireless data transmission over long distance, up to 50km. WiMAX has with high data rate, up to 70 Mbps, and high mobile capability, up to 150km/hour.

ZIGBEE

Based on the IEEE 802.15.4 so called, ZiGBee specification defines a standard for low-rate, low-power wireless personnel area networks that are well suited for body area and home networking applications such as home automation and security. In 2000, the ZigBee Alliance and the IEEE 802 working group came together to build the specifications for low-rate Personnel Area Networks (PAN) [22].

Challenges in designing wireless sensor networks for e-healthcare applications

Technical challenges in designing wireless sensor networks for e-healthcare applications are a wide range of topics, from core computer systems themes such as reliability, efficiency and scalability.

Trustworthiness

In e-healthcare applications are imposed strict requirements on end-to-end system reliability and data delivery. For example, pulse oximetry applications which measures the level of oxygen in a patient's blood, should deliver at least one measurement every 30 seconds. The properties of trustworthiness of the system are the combinations of data delivery and quality properties [23].

Patient security and privacy issues

The patient security and privacy issues mainly discussed on, the possible threats to a wireless e-healthcare application without implementation of proper security. Figure-7 illustrates on three wireless healthcare scenarios, namely, a nursing home, in-home monitoring, and in-hospital monitoring.

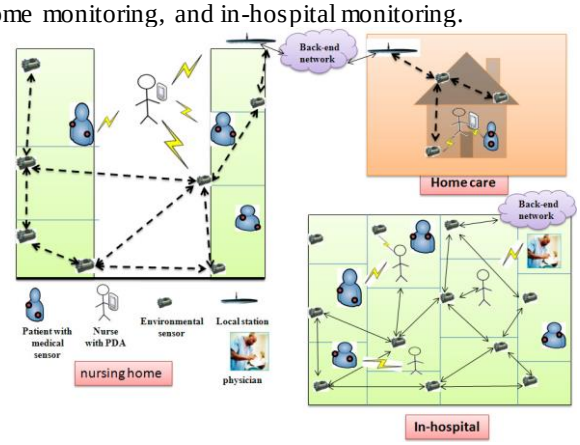

Figure 7. Application scenarios for a nursing home, home care and in-hospital

Resource Scarcity

In order to enable the small device sizes with reasonable battery lifetimes, typical wireless sensor nodes make use of low-power components with modest resources. Extremely limited computation, communication, and energy resources of wireless sensor nodes lead to a number of challenges for system design. Figure-8 illustrates the SHIMMER wearable sensor platform. It incorporates a TI MSP430 processor, a CC2420 IEEE 802.15.4 radio, a triaxial accelerometer, and a re-chargeable Li-polymer battery. The platform also includes a MicroSD slot supporting up to 2 GBytes of Flash memory [23].

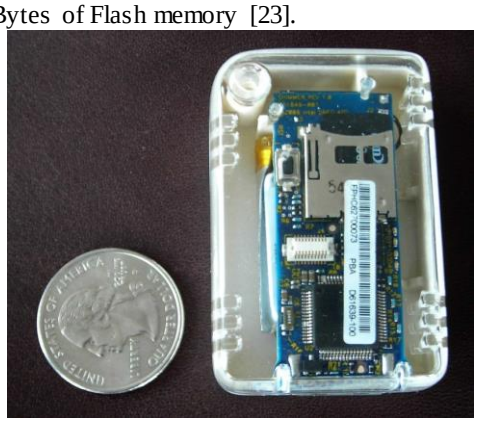

Figure 8. Shimmer wearable sensor platform

Conclusion

In this paper, we discussed about the various security mechanism, security privacy issues and requirement of e-healthcare applications using wireless medical sensor networks. It has been shown that a well-planned security mechanism should be designed for the successful deployment of such a wireless application. This paper will motivate researchers to come up with more robust security mechanisms for real-time e-healthcare applications.

References

[1]. Ko, B.J.G.; Lu, C.; Srivastva, M.B.; Stankovic, J.A.; Terzis, A.; Welsh, M. Wireless Sensor Network for Healthcare. *Proc. IEEE* 2010, *98*, 1947-1960.

[2]. Koch, S.; Hagglund, M. Health Informatics and the Delivery of Care to Older People. *Maturitas* 2009, *63*, 195-199.

[3]. Chung, W.Y.; Yan, C.; Shin, K. A Cell Phone Based Health Monitoring System with Self Analysis Processing Using Wireless Sensor Network Technology. In *Proceedings of 29th Annual International Conference on the IEEE EMBS*, Lyon, France, 23–26 August 2007.

[4]. Gravina, R.; Guerrieri, A.; Fortino, G.; Bellifemine, F. Giannantonio, R.; Sgroi, M. Development of Body Sensor Network Application Using SPINE. In *Proceedings of IEEE International Conference on Systems, Man and Cybernetics (SMC 2008)*, Singapore, 12–15 October 2008..

[5]. Lorincz, K.; Chen, B.; Challen, G.W.; Chowdhury, A.R.; Patel, S.; Bonato, P.; Welsh, M.
Mercurty: A Wearable Sensor Network Platform for High-Fidelity Motion Analysis. In *Proceedings of 7th ACM Conference on Embedded Networked Sensor Systems (SenSys'09)*, Berkeley, CA, USA, 4–6 November 2009.

[6]. Lee, S.C.; Lee, Y.D.; Chung, W.Y. Design and Implementation of Reliable Query Process for Indoor Environmental and Healthcare Monitoring System. In *Proceedings of International Conference on Convergence and Hybrid Information Technology (ICHIT'08)*, Daejeon, Korea, 28–30 August 2008; pp. 398-402.

[7]. Omeni, O.; Eljamaly, O.; Burdett, A. Energy-Efficient Medium Access Protocol for Wireless Medical Body Area Sensor Networks. In *Proceedings of 4th IEEE/EMBS International Summer School and Symposium on Medical Devices and Biosensors*, Cambridge, UK, 19–22 August 2007; pp. 29-32.

[8]. Lamprinos, I.E.; Prentza, A.; Sakka, E.; Koutsouris, D. Energy-Efficient MAC Protocol of Patients Personal Area Networks. In *Proceedings of 27th Annual International Conference of the IEEE EMBS*, Shanghai, China, 1–4 September 2005; pp. 3799-3802.

[9]. Waluyo, A.B.; Pek, I.; Chen, X.; Yeoh, W.-S. Design and Evaluation of Lightweight Middleware for Personal Wireless Body Area Network. *Pers. Ubiquit. Comput.* 2009, *13*, 509-525.

[10] Stankovic, Stanislava, Medical Applications Based on Wireless Sensor Networks, Retrived from:http://internetjournals.net/journals/tir/2009/July/Full%20Journal.pdf#page=20.

[11]. Xiao, Y.; Shen, X.; Sun, B.; Cai, L. Security and Privacy in RFID and Applications in Telemedicine. *IEEE Commun. Mag.* 2006, *44*, 64-72.

[12]. Venkatasubramaniam, K.K.; Gupta, S.K.S. Security for Pervasive Health Monitoring Sensor Applications. In *Proceedings of 4th International Conference on Intelligent Sensing and Information Processing (ICPSIP 2006)*, Bangalore, India, 15–18 December 2006; pp. 197-202.

[13]. 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 (CERMA'09)*, Cuernavaca, Morelos, Mexico, 22–25 September 2009; pp. 125-130.

[14]. Halperin, D.; Benjamin, T.S.H.; Fu, K.; Kohno, T.; Maisel, W.H. Security and Privacy for Implantable Medical Devices. *Pervas. Comput.* 2008, *7*, 30-39.

[15]. Le, X.H.; Khalid, M.; Sankar, R.; Lee, S. An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare. *J. Networks* 2011, *27*, 355-364.

[16]. Ng, H.S.; Sim, M.L.; Tan, C.M. Security Issues of Wireless Sensor Networks in Healthcare Applications. *BT Tech. J.* 2006, *24*, 138-144.

[17]. Shaikh, R.A.; Lee, S.; Khan, M.A.U.; Song, Y.J. L-Sec: Lightweight Security Protocol for Distributed Wireless Sensor Network. In *Proceedings of Personal Wireless Communication*, Albacete, Spain, 20–22 September 2006; pp. 367-377.

[18]. Lorincz, K.; Malan, D.J.; Fulford-Jones, T.R.F.; Nawoj, A.; Clavel, A.; Shayder, V.; Mainland, G.; Welsh, M. Sensor Networks for Emergency Response: Challenges and Opportunities. *Pervas. Comput.* 2004, *3*, 16-23.

[19]. Nasser, N.; Chen, Y. SEEM: Secure and Energy-Efficient Multipath Routing Protocol for Wireless Sensor Network. *Comput. Commun.* 2007, *30*, 2401-2412.

[20]. Chen, X.; Makki, K.; Yen, K.; Pissinou, N. Sensor Network Security: A Survey. *IEEE Communication. Survev. Tutor.* 2009, *11*, 52-73.

[21]. Ming Li and Wenjing Lou, Data Security and Privacy in Wireless Body Area Networks, *IEEE Wireless Communications*, (2010).

[22]. ZigBeeAlliance (2010) Zigbee Alliance. http://www.zigbee.org

[23] ISO 9919:2005 Medical electrical equipment – Particular requirements for the basic safety and essential performance of pulse oximeter equipment
for medical use. Publication of the ASTM F29.11.05 and ISO TC 121 SC3 working group on pulse oximeters, March 2005.