IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 2 (Sep. - Oct. 2013), PP 41-46
www.iosrjournals.org

Security in Body Sensor Networks for Healthcare applications

Mamalisa Nayak[#], Nitin Agrawal[#]
 # NRI institute of information science &technology

Abstract: *This paper offers a depth review of numerous Wireless Sensor/detector Systems. Healthcare applications are considered as talented fields for Wireless Sensor Networks, where patients can be watched using wireless medical sensor networks (WMSNs). Present WMSN healthcare research trends center on patient mobility, patient reliable communication and energy-efficient routing. But, installing new technologies in healthcare applications without considering security and safety makes patient privacy in danger. Furthermore, the physiological data of an individual are extremely sensitive. So, security is a supreme requirement of healthcare systems, particularly in the case of patient privacy. This paper discusses the privacy and security issues in healthcare application using WMSNs*
Keywords: *WMSN, ECIES, Identity Based Encryption, sensor networks,*

I. Introduction

Wearable health-monitoring systems (WHMS) have gained a lot of consideration from the research community and the industry during the last decade as it is pointed out by the numerous research and development efforts [1]–[3]. The aging population in many developed countries and the rising costs of health care have activated the introduction of new technology-driven developments to present health care practices. For example, current advances in electronics have allowed the development of small and intelligent (bio-) medical sensors which can be implanted in the human body.

As healthcare costs are rising and the world population is ageing [4], there has been a requirement to monitor a patient's health status while he/she is out of the hospital in his private environment. To tackle this demand, a variety of commercial products have been formed which aim at providing real-time advice information about one's health condition.

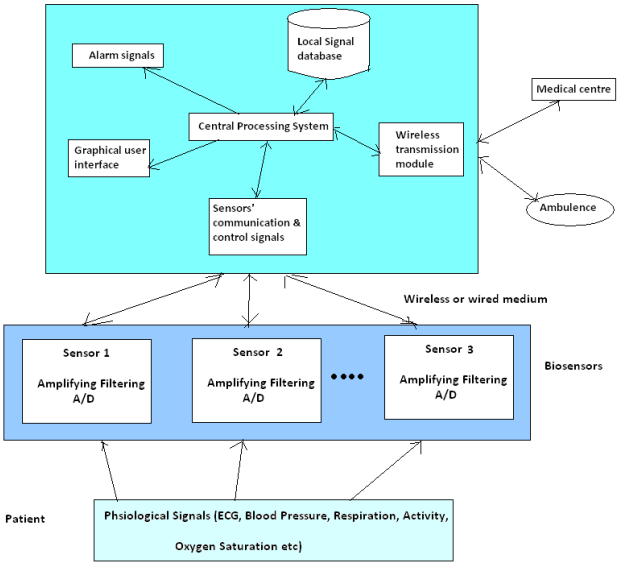
Wearable systems for health care monitoring consist various types of small sensors.These biosensors are capable of determining major physiological parameters like blood pressure, heart rate, body and skin temperature, electrocardiogram, oxygen saturation, respiration rate, etc. The obtained measurements are communicated either via a wireless or a wired link to a central node, for example, a Personal Digital Assistant (PDA) or a microcontroller board.

Present and important applications of sensor networks include: physical security, military sensing, traffic surveillance , air traffic control, video surveillance, environment monitoring industrial and manufacturing automation, distributed robotics, and building and structures monitoring.

The sensors in these applications may be minute or big, and the networks may be wired or wireless. A sensor network consists of a distinct group of independent nodes with little cost, small power, fewer memory, and restricted computational power that communicate wirelessly over limited frequencies at low bandwidth. The main objectives of WSNs are to organize a number of sensor devices over an unattended area, and gather the environmental data and transmit it to the remote location or base station. Afterward, the raw data is processed online or offline for thorough analysis at the remote server as per the application requirements.

As per the U.S. Bureau of the Census, number of elderly over age 75 is expected to double from 36 million to nearly 72 million by 2025 when the youngest Baby Boomers retire [21]. This inclination is global, so the worldwide population over age 75 is expected to more than double from 357 million in 1990 to 761 million in 2025. These statistics underscore the need for more scalable and more affordable health care solutions.

In Fig. 1, a general WHMS architecture is depicted



II. Background Description

A. Medical Sensing

There is a lengthy history of using sensors in medicine and public health. Sensors offer patients and their healthcare providers physiological and physical health states that are serious to the diagnosis, detection, treatment, and management of disorders. Many modern medicine are not cost effective without sensors such as thermometers, blood pressure monitors, glucose monitors, photoplethysmogram (PPG), etc. The capability to determine physiological state is also crucial for devices such as pacemakers and insulin pumps.Medical sensors unite transducers for detecting thermal, electrical, optical, genetic, chemical, and other signals with physiological origin with signal processing algorithms. Sensors ahead of those that directly measure health state have also found use in the medicine. For example, location and nearness sensing technologies [10] are being used for improving the delivery of patient care and workflow efficiency in hospitals [12], following the reach of diseases by public health agencies [13], and monitoring people's health related issues.

B. Wireless Sensor Platforms

Recent years have observed the emergence of a variety of computing platforms that put together storage, processing wireless networking, and sensors. These embedded computing platforms presents the capability to sense physical phenomena at temporal and spatial fidelities. Embedded computing platforms used for healthcare applications varies from smartphones to specialized wireless sensing platforms, known as motes, that have much more severe resource constrictions in terms of available computing power, network bandwidth, memory and existing energy. Existing motes normally use 8- or 16-b microcontrollers with tens of kilobytes of RAM, external storage in the form of Flash memory and hundreds of kilobytes of ROM for program storage. These devices work at a few milli watts while running. Most of the circuits can be powered off, so the standby power can be about 2 _W. If such a device is dynamic for 1% of the time, its average power consumption is just a few microwatts allowing long-term operation with two AA batteries. Motes are generally equipped with low-power radios such as those compliant with the IEEE 802.15.4 standard for wireless sensor networks [15]. Such radios generally transmit at rates between 10 and 250 Kb/s, consume about 20–60 mW, and their communication range is usually measured in tens of meters [14].

IV. Body Sensor Networks

Body Sensor Networks or bodynets or Body Area Networks have the ability to reform healthcare monitoring. These networks consist of wearable devices with attached sensors that can determine various environmental and physiological signals. Bodynet devices converse wirelessly with networked gateways such as computers , mobile phones, and PDAs which accumulate, examine and correspond critical information in real-time. A Bodynet can be designed to instantly alert emergency personnel to a serious situation like a heart attack. Bodynets also help physicians in catching warning signs of a disease earlier or monitor the progress of a improving surgery patient.

The rising field of wireless sensor networks merges computation, sensing, and communication into a single tiny device.
BSN has its own uniqueness compared to wireless sensor networks (WSNs):
 It is a network with tiny-scale structure and short range of communications.
 Its nodes are limited in their computation, power, and communication capabilities, particularly for those implanted into the body.
 It strongly surrounds the body which is biologically and physiologically well-known to contain its own transportation systems.

Security and reliability in body sensor networks (BSNs) for medical applications is mainly important because critical medical information must be protected from illegal usage for personal advantages and fake acts. Data security and privacy can introduce many problems in body sensor network used for health organisations. For example, patient health data can be altered by insurance companies (e.g. in refusing health coverage), corporations (e.g. in deciding promotions), etc.. So healthcare applications must meet the severe requirements of the Health Insurance Portability and Accountability Act (HIPAA) in the US [16].

Bodynet solves these issues with an infrastructure that enables:
(1) Safe data administration with healthcare providers,
(2) Sound network security,
(3) Secure monitoring and sensing devices, and
(4) Stronger patient-provider authentication.

IV. Literature Survey

The growth of sensor networks involves technologies from three different research areas: communication, sensing and computing). As a result, combined and separate advancements in each of these areas have led to research in sensor networks.

A. Early Research on Military Sensor Networks

Defense applications have been a driver for development and research in sensor networks. During the ColdWar, the Sound Surveillance System (SOSUS), a system of acoustic sensors (hydrophones) on the ocean bottom, was used at strategic locations to detect and track quiet Soviet submarines. Over the years, other more classy acoustic networks have been developed for submarine surveillance. SOSUS is now used by the National Oceanographic and Atmospheric Administration (NOAA) for monitoring events in the ocean, e.g., seismic and animal activity [5]. Also during the Cold War, networks of air defense radars were developed and used to defend the United States and Canada. These sensor networks usually agree to a hierarchical processing structure where processing takes place at consecutive levels until the information about events of interest arrives at the user. In most of the cases, human operators play a key role in the system.

B. Distributed Sensor Networks Program at the Defense Advanced Research Projects Agency

Modern research on sensor networks came into action around 1980 with the Distributed Sensor Networks (DSN) program at the Defense Advanced Research Projects Agency (DARPA). At this time, the Arpanet was very famous, with about 200 hosts at universities and research institutes. The sensor network was understood to have many spatially distributed low-cost sensing nodes that work together with each other but operate separately, with information being routed to whichever node can best use the information. Technology components for a DSN were identified in a Distributed Sensor Nets workshop in 1978 [6]. These included communication (high-level protocols that link processes working on a common application in a resource sharing network [7]), sensors (acoustic), processing techniques and algorithms. Since DARPA was sponsoring much artificial intelligence (AI) research at the time, the workshop also included talks on the use of AI for understanding signals and assessing situations [8].

C. Military Sensor Networks in the 1980s and 1990s

Though previous researchers on sensor networks thought of large numbers of tiny sensors, the technology for tiny sensors was not quite ready. Still, planners of military systems rapidly accepted the benefits of sensor networks, which become a vital component of network-centric warfare [18]. In this, sensors do not belong to weapons or platforms. Instead, they work together with each other over a communication network, and information is transferred to the appropriate "shooters." Sensor networks can improve tracking performance and detection through multiple observations, phenomenological and geometric diversity. The development cost is decreased by utilizing commercial network technology and common network

interfaces. Other military sensor networks consist of audio sensor arrays for antisubmarine warfare such as the the Advanced Deployable System (ADS) and, Fixed Distributed System (FDS) and unattended ground sensors

D. Sensor Network Research in the 21st Century

Current advances in computing and communication have caused a major shift in sensor network research and brought it nearer to achieve the original vision. Tiny and cheap sensors based upon wireless networking , microelectromechanical system (MEMS) [20] technology, and cheap low-power processors permit the operation of wireless ad hoc networks for various applications. Today's networking techniques, developed for voice and data and relying on a fixed infrastructure, will not suffice for battlefield use. Thus, the program developed new networking techniques suitable for highly dynamic *ad hoc* environments. The second thrust was networked information processing, i.e., how to get useful, trustworthy, and timely information from the deployed sensor network. This involves leveraging the distributed computing environment created by these sensors for information and signal processing in the network, and for dynamic and interactive querying Current systems such as the Tactical Automated Security System (TASS) [19] for perimeter security are devoted rather than programmable. They employ technologies based on transmit-only nodes and a long-range detection paradigm. A multitasking feature in the system permits multiple simultaneous users. Finally, since detection ranges are much shorter in a sensor system, the software and algorithms can use the nearness of devices to threats to severely increase the accuracy of detection and tracking.

E. Research in the area of Healthcare applications

There are various protocols implemented for the security of the patient' s private data and also there are several authentication techniques implemented in these wireless devices.

Advanced Health and Disaster Aid Network (AID-N) [9] is developed at the Johns Hopkins University Applied Physics Laboratory. The system facilitates communication between health providers at disaster scene, medical professionals at local hospitals, and specialist available for consultation from distant facilities.

AMON [10] is the advanced care and alert portable telemedical MONitor project financed by the EU FP5 IST program. It is a wearable (wrist-worn) medical monitoring and alert system that targets high-risk cardiac/ respiratory patients.

CodeBlue [4] is a wireless infrastructure intended to provide common protocol and software framework in a disaster response scenario. The architecture was developed at Harvard University which allows wireless monitoring and tracking of patients and first responders.

HealthGear [5] is designed as real-time wearable system for constant monitoring, visualizing and analyzing the user' s SpO2, HR, plethysmographic signals and location information available in the cell phone.

The LifeShirt [11] System by VivoMetrics is a miniaturized, ambulatory version of an in-patient system. The system consists of the data recorder , LifeShirt garment, VivoLogic analysis and reporting software.

Many efforts have been made to solve the problem of setting up safe communications, from symmetric and traditional public-key cryptography through today' s breakthrough technology, Identity-Based Encryption (IBE) [17].

V. Existing Projects

Haodong Wang et al. [2009] developed IBE-Lite, a identity based encryption suitable for sensors in a BSN.They presented protocols based on IBE-Lite that balanced security and privacy. IBE-Lite,a lightweight IBE, retains the properties of conventional IBE, and yet can be executed on a BSN sensor as needed. The two properties are the ability to use an arbitrary string to produce a public key, and the ability to generate a public key separately from the corresponding secret key. IBE-Lite is built upon elliptic curve cryptography (ECC), a public key primitive suitable for BSN.

Mont *et al.* [24] used IBE in a medical setting to secure the communications in a hospital, and Malasri and Wang [25] developed a security architecture for BSN focusing on the problem of key exchange between a sensor and a base station.

Bao *et al.* [13] proposed a secure system for BSNs using symmetric keys. While symmetric key schemes use less storage space per key and produce a smaller ciphertext, they do not have the asymmetric property of public keys schemes like RSA or IBE-Lite. Another paper by Bao *et al.* [14] uses the variability of a patient's heart rate as a means of person authentication. This paper complements our IBE-Lite encryption since the patient's heart rate can be used as an input string to generate encryption keys.

VI. Conclusion

This paper gives us a depth review of all the security techniques available currently in healthcare organisations. During this study various approaches found to be useful at various places.Use of ECC alongwith IBE has achieved a great success.

For the future task we can take multiple patients into account. We can do the improvement in the existing protocol for data encryption, decryption and transfer between BSN, storage site and doctor with the need for high data rates. In this proposal some saving of encryption and decryption, specially bandwidth of channel and energy consumption of sensor can be achieved. In this thesis, IBE has been used with Elliptic Curve Integrated Encryption Scheme (ECIES) which makes tough public key cryptography system for the point of data encryption and decryption.

VII. Further Reaearch

We can divide the following future research on different areas :

Functionality Enhancement: In the future, the work can be extended from centralized health care to spread remote medication in which patient is treated by a doctor from a distance in case of emergency, but this can need presence of a medical assistant like another doctor or nurse close to patient and interacting with the doctor treating the patient.

Protocol Enhancement*:* Whole new research may be done in this area with the implementation of the protocol to its functionality. It can be developed in sensor, client as well as server side. voice conversation between the doctor and the personnel in the critical situation vehicle. Various ratios like bandwidth requirement and energy consumption for encrypting and decrypting patient record can be observed and as a result the protocol is improved to gather the requirements.

Technology Enhancement: In future there can be the employment of of artificial neural networks for performing context aware sensing and the use of involuntary principles of self-organization, self-healing and self-defence for developing BSN with precious fault tolerance and self-defence. Because of the intrinsic complexities concerned in managing a giant range of wireless sensors, bio-inspired sensing and networking is an important area of study for future BSN study.

Network Channel Allocation Enhancement*:* Future generation wireless networks will know-how huge are the demands from mobile telemedicine applications. Mobile telemedicine enable patients to do their daily events at the connected occasion as they are being monitored endlessly anytime, anywhere. Typical telemedicine applications comprise transmission of ECG(graphical record signals) signals from the patient to the doctor, voice conversation between the doctor and the personnel in the vital situation vehicle, communication of X-rays and medical pictures from the patient to the doctor at the health-care center. These appliances need communication between a mobile patient and a health-care center or central server. But, these applications have to be compelled to cope with the properties of wireless networks such as channel fluctuations , low bandwidth or low information measure, and exposure changes. Furthermore, a single network alone would not be able to collect the information measure needs of applications in the least locations.

References

[1] L. Gatzoulis and I. Iakovidis, "Wearable and portable ehealth systems", IEEE Eng. Med. Biol. Mag., vol. 26, no. 5, pp. 51–56, Sep.–Oct. 2007.

[2] A. Lymperis and A. Dittmar, "Advanced wearable health systems and applications, research and evelopment efforts in the european union," IEEE Eng. Med. Biol. Mag., vol. 26, no. 3, pp. 29–33, May/Jun. 2007.

[3] G. Tr¨oster, "The Agenda of Wearable Healthcare," in IMIA Yearbook of Medical Informatics. Stuttgart, Germany: Schattauer, 2005, pp. 125–138.

[4] Y. Hao and R. Foster, "Wireless body sensor networks for health monitoring applications," Phys. Meas., vol. 29, pp. R27–R56, Nov. 2008

[5] C. E. Nishimura and D. M. Conlon, "IUSS dual use: Monitoring whales and earthquakes using SOSUS," Mar. Technol. Soc. J., vol. 27, no. 4, pp. 13–21, 1994

[6] Proceedings of the Distributed Sensor Nets Workshop. Pittsburgh, PA: Dept. Comput. Sci., Carnegie Mellon Univ., 1978.

[7] R. F. Sproull and D. Cohen, "High-level protocols," Proc. IEEE, vol. 66, pp. 1371–1386, Nov. 1978.

[8] P. Nii, E. Feigenbaum, J. Anton, and A. Rockmore, "Signal-tosymbol transformation: HASP/SIAP case study," AI Mag., vol. 3, pp. 23–36, Spring 1982

[9] T. Gao, D. Greenspan, M. Welsh, "Vital sign monitoring and patient tracking over a wireless netowrk", Proceeding of 27th annual international conference of the IEEE EMBS, September 2005.

[10] U. Anliker, J. Ward, P. Lukowicz, "AMON: A wearable multiparameter medical monitoring and alert system" IEEE Transactions on information technology in Biomedicine, Vol. 8, No. 4, Pages 415-427, December 2004.

[11] A. Cardenas, R. Pon, R. Cameron, "Management of streaming body sensor data for medical information systems", The 2003 International Conference on METMBS, Las Vegas Nevada, Pages 186-191, June 2003.

[12] E. A. Fry and L. A. Lenert, BMASCAL: RFID tracking of patients, staff and equipment toenhance hospital response to mass casualty events,[in Proc. AMIA Annu. Symp., Jan. 2005, pp. 261–265.

[13] A. Hanjagi, P. Srihari, and A. S. Rayamane, BA public health care information system using GIS and GPS: A case study of Shiggaon,[in GIS for Health and the Environment, P. C. Lai and S. H. Mak, Eds. New York: Springer-Verlag, 2007, pp. 243–255.

[14] Atmel Corporation. AT86RF230: Low power 2.4 GHz transceiver for ZigBee, IEEE 802.15.4, 6LoWPAN, RF4CE and ISM applications. [Online]. Available: http://www.atmel.com/ dyn/resources/prod_documents/doc5131.pdf

[15] IEEE Standard for Information TechnologyVTelecommunications and Information Exchange Between SystemsVLocal and Metropolitan Area Networks, Specific Requirements-Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), May 2003. [Online]. Available: http://www.ieee802.org/ 15/pub/TG4.html

[16] The US Department of Health and Human Services. Summary of the HIPAA Privacy Rule, 2003.
[17] http://www.voltage.com/technology/ibe.htm
[18] T. Gao, D. Greenspan, M. Welsh, "Vital sign monitoring and patient tracking over a wireless netowrk", Proceeding of 27th annual international conference of the IEEE EMBS, September 2005.
[19] J. Corella, "Tactical automated security system (TASS): Air force expeditionary security," presented at the SPIE Conf. Unattended Ground Sensor Technologies and Applications, Orlando, FL, 2003.
[20] J.W. Gardner, V. K Varadan, and O. O. Awadelkarim, Microsensors, MEMS and Smart Devices. New York: Wiley, 2001.
[21]. U.S. Census Bureau, U.S. Interim Projections by Age, Sex, Race, and Hispanic Origin,http://www.census.gov/ipc/www/usinterimproj/, accessed in September 2005
[22]. K. Lorincz , D. Malan, A. Nawoj, G. Mainland, M. Welsh, "Sensor networks for emergency response: challenges and opportunities", IEEE Pervasive Computing, Vol. 3, No. 4, Pages 16- 23, October 2004.
[23] N. Oliver, F. Flores-Mangas, "HealthGear: A Real-time Wearable System for onitoring and Analyzing Physiological Signals" Microsoft Research Technical Report MSR-TR-2005-182. http://research.microsoft.com/ nuria/healthgear/ healthgear.htm.
[24] M. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploiting IBE technology for privacy in health care," in Proc. Int. Workshop Database Expert Syst. Appl., 2003, pp. 432–437.
[25] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in Proc. HealthNet, 2007, pp. 7–12.
[26] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "A new symmetric cryptosystem of body area sensor networks for telemedicine," in Proc. Conf. Jpn. Soc. Med. Electron. Biol. Eng., 2005, p. 654.
[27] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in Proc. IEEE Eng. Med. Biol., 2005, pp. 2455–2458