AN INVESTIGATION OF MEDICAL APPLICATIONS OF INTEGRATED SENSOR NETWORKS

Dr. S.R.Boselin Prabhu[1], Dr. E.Gajendran[2]
[1]Assistant Professor, Department of Electronics and Communication Engineering,
SVS College of Engineering, Coimbatore, India.
[2]Professor, Department of Information Technology,
St.Martin‟s Engineering College, Hyderabad.
E-mail: eben4uever@gmail.com[1], gajendrane@gmail.com[2]

Abstract

The security and privacy protection of the collected data is a major unsolved issue, with challenges coming from the stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. In this paper, we propose a lightweight and secure system for MSNs. The system employs hash-chain based key updating mechanism and proxy protected signature technique to achieve efficient secure transmission and fine-grained data access control. Furthermore, we extend the system to provide backward secrecy and privacy preservation.

Index Terms: Medical sensor networks, access control, data transmission and security.

1. INTRODUCTION

The medical applications of sensors can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure. Recently, with the rapid development in the wearable biosensor and wireless communication technologies, wireless medical sensor networks (MSNs) have emerged as a promising technique which will revolutionize the way of seeking healthcare at home, hospital, or large medical facilities [1], [2]. Instead of being measured face-to-face, with MSNs, patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, insurance companies, and patients. Through this way, healthcare processes, such as clinical diagnosis and emergency medical response, will be facilitated and expedited, thereby greatly increasing the efficiency of healthcare.

2. LITERATURE SURVEY IN THE VICINITY OF RESEARCH

Ad hoc network facilitates creation of network of medical devices on the fly (Sensor network) thereby supplementing the resources at hand by providing features like reconfiguration and reallocation similar to HAM radios in use today. The devices use minimal power and are robust which decrease their dependence on available infrastructure (resources like electricity supply, communication infrastructure like telephone lines etc., which are target of insurgents or are destroyed by natural disaster) and this makes them an attractive alternative.

However this technology has a limitation as the ranges of these devices are fixed and to enable the services to be extended to large geographical areas like ambulances and patient premises requires this infrastructure to interoperate with

other wireless networks like GSM /CDMA mobile networks. Thus, we are looking at a new technology which is born as a result of fusion of medical sensors and mobile technology. This technology promises to reduce the number of visits required by patients for health checkup by allowing the doctors to remotely monitor the patients and advise them. Life insurance companies can collect the data from the database to settle the medical claims. With all this discussion of wireless applications, healthcare providers such as hospitals, insurance agencies and the government are becoming interested in investing in this area.

Cost saving is one of the main factors because medical errors by doctors bring in law suits and patient and hospital management and be very expensive too. This has drawn a lot of attention of both researchers and industry. Sensor networks, a new class of devices, have the potential to revolutionize the capture, processing and communication of critical data for use by first responders. Sensor network consists, of small low power and low-cost with limited computational and wireless communication capabilities.

They represent the next step in wireless communication's miniaturization, and their power and size make it feasible to embed them. In our aging society, an increasing number of people have chronic medical conditions such as diabetes and heart disease. If these people's health conditions could be monitored [3-11].

2. PROPOSED METHODOLOGY

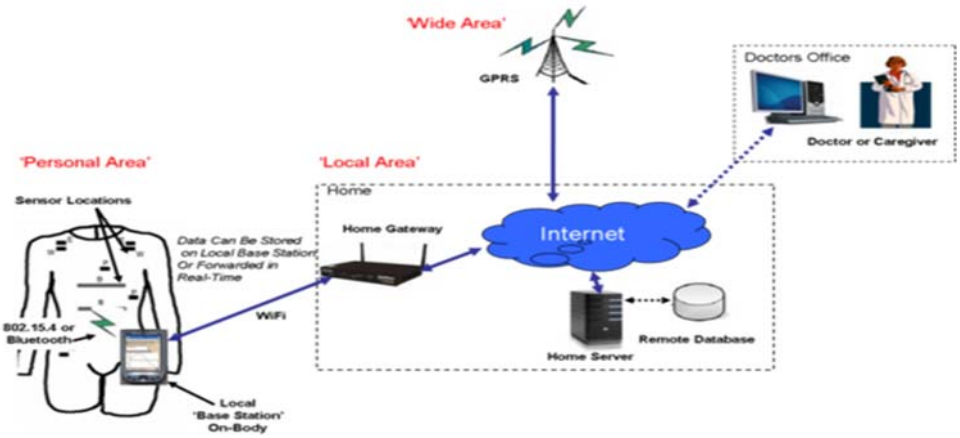

Figure 1: System Architecture

Verifiers validate proxy signatures only with the public key of after a user registers to the network server, he/she is allowed to issue commands to access the collected PHI or control the biosensors according to his/her privilege. To achieve this goal, proxy protected signature by warrant (PSW) [19] is introduced into our system. This technique is a special digital signature. There are two kinds of participants, i.e., an original signer and proxy signers. The original signer gives the proxy signer a warrant, which specifies the identity of the proxy signer, the identity of the original signer, the expiration time of the delegation of signing power, etc. The proxy signer generates proxy signatures only with the proxy signature key given by the original signer. The original signer and pay attention to the legality of the warrant. The detailed information about applying the PSW technique into the proposed system is given as follows. The network server.

4. SYSTEM REQUIREMENTS

In this section, we present several criteria that represent desirable characteristics in a secure and lightweight system for MSNs.

Lightweight: Every PAN often consists of low-end sensor nodes, which rely on battery energy [1]. Furthermore, emergency situations in an MSN require the capability for fast medical reaction without disabling security functions. For example, secure PAN setup in emergency situations must be carried out in less than 1 s and the maximum allowable latency for electrocardiogram transmission is 250 ms, communication, and storage overhead on the

sensors. Hence, cryptographic algorithms must be as fast as possible in order to satisfy these requirements and be invulnerable to DoS attacks [12-21].

Fine-grained data access control: Access control needs to be enforced for the patient-related data in the whole MSN so that private information will not be obtained by unauthorized users. More importantly, a secure system should provide different privileges for different network users.

Scalability: The system should be efficient even in a large scale MSN with many users and many PANs [1].

Flexibility: The access policy should be adapted dynamically to contexts, such as time, location, or certain events related to patients. Note that in MSNs, the access policy should be defined by both patients and healthcare units. For example, on demand authorization to read a patient's PHI can be given temporarily to an available doctor who is not on the access list when a medical emergency happens. Obviously, inability or irresponsiveness in adapting the access rules may threaten a patient's life [1].

Confidentiality: In order to prevent the patient-related data from leaking, the data need to always be kept confidential at a node or local server (i.e., the network server). Data confidentiality should be resistant to device compromise attacks (e.g., node compromised and controller compromised attacks). That is, compromising one node helps the adversary to gain nothing or little from the data stored at that node.

Data integrity assurance: In MSNs, the patient-related data are vital, and modified data would lead to disastrous consequences. Therefore, data integrity shall be protected all the time.

Forward secrecy: It means that even if an adversary obtains the current secrets of a node, it cannot decrypt (or forge authentication tags for) those data collected and encrypted (or authenticated) before compromise [22-26].

Backward secrecy: It means that even an adversary has compromised (and then released) a node, it cannot decrypt (or forge authentication tags for) those data collected and encrypted (or authenticated) by the node after releasing.

Strong contextual privacy preservation: We divide privacy issues in MSNs into content-oriented privacy and contextual privacy. Here we just focus on contextual privacy, since the content-oriented privacy has been considered in Requirements 5, 7, and 8. Contextual privacy means an adversary has the ability to link the source and the destination of a message. In an MSN, if an adversary can link the patient with a specific physician, then the patient's privacy will be lost. Thus, it is very important to protect contextual privacy, which includes sensor identity privacy and PAN identity privacy of every collected data, and each user's privilege content privacy in addition to the privacy of every user command content. For example, if an adversary searches the whole MSN for a specific parameter, protecting the privacy of sensor identity of every collected data is desirable. Similarly, if an adversary searches the whole MSN for a specific patient, protecting the privacy of PAN identity of every collected data is desirable. In addition, we illustrate the importance of user privilege content privacy by considering the following two scenarios. One is that often each user's privilege content indicates the user identity information and the relation between the user and some patients (i.e., the owner of some PAN), thus exposing the patients' privacy. The other is that with the knowledge of some user privileges, an adversary can seek the important users and then launch attacks on the MSNs.

5. UNIQUE FEATURES OF MSNS

MSNs are different from MANETs and WSNs in the following aspects [2].

Data Rate: Events monitored by MANETs and WSNs usually occur at irregular intervals. On the contrary, MSNs are employed to monitor humans' physiological activities, which more or less may occur periodically. As a result, data streams of applications exhibit relatively stable rates. All nodes are assumed to have loosely synchronized clocks with the help of some existing secure time synchronization scheme.

Mobility: Relatively, there is no movement between sensors as they are all in the same patient. Movement between controllers and sensors is due to mobility of patients, which is very low.

Efficiency: The sensed signals can be efficiently processed by biosensors to obtain estimates of physiological information. Also, the power consumption on biosensors is low, and thus, batteries can last longer

5.1 Network Model: All the biosensor nodes in an MSN have limited power supply, storage space, and computational capability. Due to the

constrained resources, computationally expensive and energy intensive operations such as the public key cryptography are not favorable for such nodes. We assume that the network server is secure. That is, the network server is equipped with a tamper resistant component for storing the keying materials. According to the data rate feature of an MSN described in Section III-A, we assume that time is divided into equal and fixed collection rounds and each biosensor collects a single data item per round. The sensor nodes may be placed in, on, or around the patient's body. Although there is no consensus on the communication technologies in PANs, the communication ranges of off-the-shelf technologies (e.g., Zigbee) are larger than 3 m. Thus, according to the mobility feature of an MSN described in Section III-A, we assume that all sensor nodes in a PAN can directly communicate with the controller; thus, a star topology is assumed.

5.2 Adversary Model: We assume that an adversary can behave as both outside and inside attackers. Outside attackers can drop messages by jamming the communication channel, eavesdrop messages, modify messages, inject forged messages, or replay old messages. Insider attackers can compromise a number of biosensor nodes, controllers, and network users to obtain their data and keying materials. Considering the special features of an MSN, a powerful mobile adversary

5.3 Implementation and Experimental Setup: In order to investigate the feasibility of the proposed system on the biosensor nodes, same as the existing studies [4]–[11] on securing MSNs, we choose two common resource limited sensor nodes, i.e., Telos B and Mica Z motes. The Telos B mote is equipped with an 16-bit, 8-MHz MSP430 microcontroller, 10-kB RAM, 48-kB ROM, 1024-kB flash and an 802.15.4/Zig- Bee radio. Also, the Mica Z mote features an8-bit, 8-MHzAtmel microcontroller with 4-kB RAM and 128-kB ROM. Our implementation has the network server, controller, network user, and sensor node side programs. The protocols operated by the first entities have been implemented i n C (using Open SSL [22]) and executed in laptop PCs (with 2-GB RAM) under Ubuntu 11.04 environment with different computational power. In addition, the sensor node side programs are written in nesC. Our motes run TinyOS [23] 2.x. Throughout this paper, unless otherwise stated, all experiments on laptop PCs and sensor nodes were repeated one thousand times for each measurement in order to obtain accurate average results. Additionally, for one-way hash function h (), we have selected SHA-1, thus the output size is 160 bits.

6. CONCLUSION AND FUTURE WORKS

The security and privacy protection of the collected data is a major unsolved issue, with challenges coming from the stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. In this paper, we have identified the security challenges facing an MSN for wireless health monitoring and then proposed a novel and lightweight system to achieve secure data transmission and access control for MSNs. The security analysis has demonstrated that our system can achieve the requirements of the protocol of this kind. We have implemented the protocols on real mobile devices and sensor platforms with limited-resource. Experimental results have shown that our approaches are feasible for real-world applications.

REFERENCS

[1] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, S. Moulton, and M. Welsh, "Sensor networks for emergency response: Challenges and opportunities," IEEE Pervas. Comput., vol. 3 , no. 4, pp. 16–23, Oct. 2004.

[2] Hamid Ali Abed Al-Asadi, "Temperature dependence of the lasing characteristics of vertical cavity surface emitting lasers," Engineering Journal of Technology University, Vol. 145, 1994.

[3] Boselin Prabhu S.R. and Sophia S., "Environmental monitoring and greenhouse control by distributed sensor Network", International Journal of Advanced Networking and Applications, 5(5), 2014.

[4] Boselin Prabhu S.R. and Sophia S., "Greenhouse control using wireless sensor network", Scholars Journal of Engineering and Technology, 2(4), 2014.

[5] Hamid Ali Abed Al-Asadi, "Temperature dependence of the noise characteristics of Multiisection semiconductor lasers," Science Journal, vol. 7, No. 3, 2001.

[6] Hamid Ali Abed Al-Asadi, "Linewidth characteristics of vertical cavity surface emitting

lasers due to external optical feedback," Science Journal, vol. 8, 2001.
[7] Boselin Prabhu S.R. and Sophia S., 'Modern cluster integration of advanced weapon system and wireless sensor based combat system', Scholars Journal of Engineering and Technology, 2(6A), 2014.
[8] Boselin Prabhu S.R. and Sophia S., 'A review of efficient information delivery and clustering for drip irrigation management using WSN', International Journal of Computer Science and Business Informatics, 14(3), 2014.
[9] Hamid Ali Abed Al-Asadi, "Linewidth characteristics of vertical cavity surface emitting lasers due to external optical feedback," Science Journal, vol. 8, 2002.
[10] Hamid Ali Abed Al-Asadi, "Theoretical investigation of spectral linewidth properties of double fused 1.3 um MQW-VCA in reflection and transition modes," Tikrit Journal for Pure Science, vol. 8, No. 2, 2002.
[11] Boselin Prabhu S.R. and Sophia S., 'Mobility assisted dynamic routing for mobile wireless sensor networks', International Journal of Advanced Information Technology, 3(3), 2013.
[12] Boselin Prabhu S.R. and Sophia S., 'A review of energy efficient clustering algorithm for connecting wireless sensor network fields', International Journal of Engineering Research and Technology, 2(4), 2013.
[13] Hamid Ali Abed Al-Asadi, "Vertical cavity amplifiers and its cavity length dependence the saturation power and quantum efficiency," Tikrit Journal of Pure Science, vol. 9, No. 2, 2003.
[14] Hamid Ali Abed Al-Asadi, "Effects of pump recycling technique on stimulated Brillouin scattering threshold: A theoretical model," Optics. Express, Vol. 18, No. 21, pp. 22339-22347 Impact factor: 3.88, 2010.
[15] Boselin Prabhu S.R. and Sophia S., 'Variable power energy efficient clustering for wireless sensor networks', Australian Journal of Basic and Applied Sciences, 7(7), 2013.
[16] Boselin Prabhu S.R. and Sophia S., 'Capacity based clustering model for dense wireless sensor networks', International Journal of Computer Science and Business Informatics, 5(1), 2013.
[17] Hamid Ali Abed Al-Asadi, "Brillouin Linewidth Characterization in Single Mode Large Effective Area Fiber through the Co-Pumped Technique," International Journal of Electronics, Computer and Communications Technologies (IJECCT), Vol. 1(1), pp. 16-20, 2010.
[18] Boselin Prabhu S.R. and Sophia S., 'An integrated distributed clustering algorithm for dense WSNs', International Journal of Computer Science and Business Informatics, 8(1), 2013.
[19] Boselin Prabhu S.R. and Sophia S., 'A research on decentralized clustering algorithms for dense wireless sensor networks', International Journal of Computer Applications, 57(20), 2012.
[20] Hamid Ali Abed Al-Asadi, "Analytical study of nonlinear phase shift through stimulated Brillouin scattering in single mode fibre with pump power recycling technique,", Volume 13 Number 10, Journal of Optics. Impact factor: 1.99, 2011.
[21] Hamid Ali Abed Al-Asadi , "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, June 2012.
[22] Boselin Prabhu S.R. and Sophia S., 'Hierarchical distributed clustering algorithm for energy efficient wireless sensor networks', International Journal of Research in Information Technology, 1(12), 2013.
[23] Boselin Prabhu S.R. and Sophia S., 'Real-world applications of distributed clustering mechanism in dense wireless sensor networks', International Journal of Computing Communications and Networking, 2(4), 2013.
[24] Younis, O. and Fahmy, S., "HEED: A Hybrid Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks," IEEE Transactions on Mobile Computing, 2004.
[25] J. Choi, B. Ahmed, and R. Gutierrez-Osuna, "Development and evaluation of an ambulatory stress monitor based on wearable sensors," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 2, pp. 279–286, Mar. 2012.
[26] D.He,C.Chen,S.Chan,andJ.Bu,"DiCode:DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May 2012