ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Secret-Key and Public-Key Based Privacy Protection Protocols in Wireless Medical Sensor Networks: A Survey

[1] S. Gayathri , [2] B. Vanaja

[1] PG Student (CSE), Dept. of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

[2] Assistant professor, Dept. of IT, Sri Vidya College of Engineering and Technology, Virudhunagar, Tamil Nadu, India

ABSTRACT: Recently, with the rapid development and implementation of wireless medical sensors has gained increasing popularity. Monitor and record some vital parameters of patients are of importance to know the patient's health condition. But malicious attacks happen occasionally, which may cause the patient-related data being leaked or modified. In this study, we made a survey about some researches in the domain of privacy protection for data security and privacy issues and the privacy of the patient-related information stored in the database of the medical organization systems.

KEYWORDS: Wireless Medical Sensor Networks, Security, Privacy and Medical information system.

I.INTRODUCTION

WSNs deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Sensor Networks have direct human involvement are deployed on a small scale must support mobility (a patient can carry the devices), and WMSNs requires high data rates with reliable communication. Monitoring of vital signs is an essential element in intensive care units, ambulatory monitoring, and emergency rooms. Medical sensors such as pulse oximeters, noninvasive blood pressure monitors, or electrocardiographic devices are currently wired to bedside monitors, which analyze, interpret, and present the patient's vital waveforms, numeric values, and alarm conditions to an interested user. Physiological conditions of patients are closely monitored by deploying Wireless medical sensor motes.

These medical sensors are used to sense the patient's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical sensor readings the doctor can get the details of a patient's health status. The patient's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate [1]. WMSNs carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from WMSNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless sensor networks. Wireless Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc.

Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could makes the patient embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job [2]. Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, activity monitoring in health-clubs, location tracking for athlete are the broad range of healthcare applications. WMSNs share individual data with physicians and insurance companies. Thus unauthorized collection and use of patient data by adversaries can cause life-threatening risks to the patient and make the patient's private matters publically available.

DOI: 10.15680/IJIRCCE.2015. 0311055

For example, In [3] a simple scenario, a patient's body sensors transmit the body data to a nurse, the patient's privacy is breached when some attacker is eaves dropping. Later that attacker can post the patient data on social site and pose risks to the patient's privacy. Indeed wireless healthcare can offer many advantages to patient monitoring, but the medical health data of an individual are highly vulnerable to various threats, so security and privacy become some of the big concerns for healthcare applications, when it comes to adopting wireless technology. A healthcare provider is subjected to strict civil and criminal penalties if Health Insurance Portability and Accountability Act (HIPAA) rules are not followed properly [4]. Thus the security and privacy of the sensed data is the major concern in healthcare applications. A detailed review is presented in the following section.

II.SECRET-KEY AND PUBLIC-KEY BASED PRIVACY PROTECTION PROTOCOLS

S. Dagtas et al. [5] presented a framework for a wireless health monitoring system using wireless networks such as Zig Bee. Vital signals are collected and processed using a 3-tiered architecture. The first stage is the mobile device carried on the body that runs a number of wired and wireless probes. This device is also designed to perform some basic processing such as the heart rate and fatal failure detection. At the second stage, further processing is performed by a local server using the raw data transmitted by the mobile device continuously. The raw data is also stored at this server. The processed data as well as the analysis results are then transmitted to the service provider center for diagnostic reviews as well as storage. The main advantages of the proposed framework are (1) the ability to detect signals wirelessly within a body sensor network (BSN), (2) low-power and reliable data transmission through ZigBee network nodes, (3) secure transmission of medical data over BSN, (4) efficient channel allocation for medical data transmission over wireless networks, and (5) optimized analysis of data using an adaptive architecture that maximizes the utility of processing and computational capacity at each platform.

W. Diffie and M. Hellman [6] examined two kinds of contemporary developments in cryptography. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

D. He, S. Chan and S. Tang [7] proposed 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, the system is extended to provide backward secrecy and privacy preservation. The system only requires symmetric-key encryption/decryption and hash operations and is thus suitable for the low-power sensor nodes. This paper also reports the experimental results of the proposed system in a network of resource-limited motes and laptop PCs, which show its efficiency in practice. To the best of our knowledge, this is the first secure data transmission and access control system for MSNs until now.

F. Hu et al. [8] designed a practical TSN hardware/software platform for a typical U.S. healthcare community scenario (such as large nursing homes with many elder patients) to perform real-time healthcare data collections. On the other hand, due to the radio broadcasting nature of MANET, a TSN has the risk of losing the privacy of patients' data. Medical privacy has been highly emphasized by U.S. Department of Health and Human Services. This research also designs a medical security scheme with low communication overhead to achieve confidential electrocardiogram data transmission in wireless medium.

Y. M. Huang et al. [9] presented a healthcare monitoring architecture coupled with wearable sensor systems and an environmental sensor network for monitoring elderly or chronic patients in their residence. The wearable sensor system, built into a fabric belt, consists of various medical sensors that collect a timely set of physiological health indicators transmitted via low energy wireless communication to mobile computing devices. Three application scenarios are implemented using the proposed network architecture. The group-based data collection and data transmission using the ad hoc mode promote outpatient healthcare services for only one medical staff member assigned to a set of patients. Adaptive security issues for data transmission are performed based on different wireless capabilities. This study also presents a monitoring application prototype for capturing sensor data from wireless sensor nodes. The implemented schemes were verified as performing efficiently and rapidly in the proposed network architecture.

P. Kumar et al. [10] addressed security requirements of health monitoring using medical sensor networks and proposed a secure framework called “SHM” using wireless sensor networks. SHM provides security services such as confidentiality, authenticity and integrity to patient data at low-cost. To provide confidentiality PingPong-128 stream cipher is used. Authenticity and data integrity is achieved by Ping Pong-MAC (message authentication code). A real-time prototype with ECG and tri-axial accelerometer sensors are designed on Telos-mote for evaluating the proposed secure framework and the results confirm their feasibility.

X. H. Le et al. [11] proposed a secure, lightweight public key - based security scheme, Mutual Authentication and Access Control based on Elliptic curve cryptography (MAACE). MAACE is a mutual authentication protocol where a healthcare professional can authenticate to an accessed node (a PDA or medical sensor) and vice versa. This is to ensure that medical data is not exposed to an unauthorized person. On the other hand, it ensures that medical data sent to healthcare professionals did not originate from a malicious node. MAACE is more scalable and requires less memory compared to symmetric key-based schemes. Furthermore, it is much more lightweight than other public key-based schemes. Security analysis and performance evaluation results are presented and compared to existing schemes to show advantages of the proposed scheme.

X. Lin et al. [12] proposed a strong privacy-preserving Scheme against Global Eavesdropping, named SAGE, for eHealth systems. The proposed SAGE can achieve not only the content oriented privacy but also the contextual privacy against a strong global adversary. Extensive analysis demonstrates the effectiveness and practicability of the proposed scheme.

K. Malasri and L. Wang [13] identified the unique security challenges of such a sensor network and proposed a set of resource-efficient mechanisms to address these challenges. The solution includes (1) a novel two-tier scheme for verifying the authenticity of patient data, (2) a secure key agreement protocol to set up shared keys between sensor nodes and base stations, and (3) symmetric encryption/decryption for protecting data confidentiality and integrity. The proposed mechanisms are implemented on a wireless mote platform, and the results confirm their feasibility.

J. Misic and V. Misic [14] described two algorithms for key distribution. The first algorithm relies on a central trusted security server (CTSS) to authenticate that participants indeed belong to the patient's group and to generate the session key. In the second algorithm, participants authenticate each other using certificates and are largely independent of the central trusted security server (CTSS); this algorithm uses elliptic curve cryptography (ECC) to reduce energy consumption by cryptographic computations. In both cases, the patient's security processor has a lead role in authenticating group membership and the key generation process. Using the data from commercial devices compliant with the IEEE 802.15.4 low data rate WPAN technology that shows this approach can be successfully implemented in networks built with low power motes.

S. Raazi et al. [15] designed key management schemes for WSN are inefficient and unnecessarily complex when applied to WBAN. Considering the key management issue, WBAN are also different from WPAN because WBAN can use random biometric measurements as keys. The differences between WSN and WBAN are highlighted and propose an efficient key management scheme, which makes use of biometrics and is specifically designed for WBAN domain.

R. Rivest et al. [16] presented an encryption method with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: (1) Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intented recipient. Only he can decipher the message, since only he knows the corresponding decryption key. (2) A message can be “signed” using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems. A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret primer numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e * d \equiv 1 (\mathrm{mod}\ (p - 1) * (q - 1))$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

A. B. Waluyo et al. [17] presented a lightweight middleware to be used for wireless medical body area networks. The middleware is designed to reside in mobile devices, and acts as a gateway to receive sensor data as well as to control a set of sensor devices attached to the wearer. The main essence of the middleware is to simplify and accelerate the development of wireless healthcare applications by providing highly reusable codes. The architecture of the middleware including its main functions such as data acquisition, dynamic plug-and-play capabilities, on-the-fly sensor reconfiguration, and resource management (i.e., sensor sleep/wake-up, critical self-wake) will be discussed. A security feature as a means to protect critical sensor data from malicious/unauthorized parties has also been incorporated in the proposed middleware. The prototype system of the middleware has been built and is presented in this paper together with its performance measurements.

X. Yi et al. [18] proposed a practical approach to prevent from the inside attack by using Sharemind system, developed by Cybernetica to perform computations on input data without compromising its privacy. This paper has two main contributions. One contribution is proposing a lightweight encryption algorithm to protect the communication between the sensor node and the Sharemind system. Another contribution is employing Sharemind system to protect patient data privacy and support medical research.

H. Zhao et al. [19] developed a fuzzy commitment technology with weak time synchronization mechanism for keys negotiation, with a multi hop route key management scheme proposed for efficient energy consumption management, including an energy-based multi hop-route-choice method. Security analyses and performance evaluation have been provided to validate the proposed scheme.

III.CONCLUSION

This survey discussed the security and privacy issues in healthcare applications using medical sensor networks. It has been shown that a well-planned security mechanism must be designed for the successful deployment of such a wireless application. In this respect, we have found many important challenges in implementing a secure healthcare monitoring system using medical sensors, which reflects the fact that if a technology is safe, then people will trust it. Otherwise, its use will not be practical, and could even endanger the patient’s life. Consequently, many security and privacy issues in healthcare applications using wireless medical sensor networks still need to be explored and we hope that this survey will motivate future researchers to come up with more robust security mechanisms for real-time healthcare applications.

REFERENCES

[1] Denis Trcek And Andrej Brodnik, University Of Ljubljana,” Hard And Soft Security Provisioning for Computationally Weak Pervasive Computing Systems In E-Health”, IEEE Wireless Communications August 2013,45-53.

[2] Rongxing Lu, Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE,” SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile- Healthcare Emergency”, IEEE Transactions On Parallel And Distributed Systems, Vol. 12, No. 2, May 2012,452-461.

[3] Pardeep Kumar and Hoon-Jae Lee,” Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey”, Published: 22 December 2011, Sensors 2012, 12, 55-91.

[4] Geoffrey G. Messier and Ivars G. Finvers,” Traffic Models for Medical Wireless Sensor Networks”, IEEE Communications Letters, Vol. 11, No. 1, January 2007,21-30.

[5] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa. Real-Time and Secure Wireless Health Monitoring. Int. J. Telemed. Appl. 2008, doi: 10.1155/2008/135808.

[6] W. Diffie and M. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, 22 (6): 644-654, 1976.

[7] D. He, S. Chan and S. Tang. A Novel and Lightweight System to Secure Wireless Medical Sensor Networks. IEEE Journal of Biomedical and Health Informatics, 18 (1): 316-326, 2014.

[8] F. Hu, M. Jiang, M. Wagner, D. C. Dong. Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign. IEEE Trans. Inform. Tech. Biomed, 11: 619-627, 2007.

[9] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 27: 400-411, 2009.

[10] P. Kumar, Y. D. Lee, H. J. Lee. Secure Health Monitoring Using Medical Wireless Sensor Networks. In Proc. 6th International Conference on Networked Computing and Advanced Information Management, pages 491-494, Seoul, Korea, 16-18 August 2010.

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

[12] X. Lin, R. Lu, X. Shen, Y. Nemoto, N. Kato. SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth System. IEEE J. Select. Area Commun. 27: 365-378, 2009.
[13] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9: 6273-6297, 2009.
[14] J. Misic, V. Misic. Enforcing Patient Privacy in Healthcare WSNs Through Key Distribution Algorithms. Secur. Commun. Network 1: 417-429, 2008.
[15] S. Raazi, H. Lee, S. Lee, Y. K. Lee. BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks. Sensors 10: 3911-3933, 2010.
[16] R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2): 120-126, 1978.
[17] A. B. Waluyo, I. Pek, X. Chen, W.-S.Yeoh. Design and Evaluation of Lightweight Middleware for Personal Wireless Body Area Network. Pers. Ubiquit. Comput, 13: 509-525, 2009.
[18] X. Yi, J. Willemson, F. Nat-Abdesselam. Privacy-Preserving Wireless Medical Sensor Network. In Proc. TrustCom'13, pages 118-125, 2013.
[19] H. Zhao, J. Qin, and J. Hu. An Energy Efficient Key Management Scheme for Body Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 24 (11): 2202-2210, 2013.