An Energy Efficient Key Management Scheme for Body Sensor Network

Ankita Torawane
University Of Pune,
PG Student,
Department of Computer Engineering,
Nashik-422213

Amitkumar Manekar
University of Pune,
Assistant Professor,
Department of Computer Engineering,
Nashik-422213

ABSTRACT

The distributed systems like Body Sensor Networks(BSNs) where biosensor nodes are distributed in different positions to collect health data from the human body and deliver the information to a remote medical center. As per the medical data regulations, security of BSNs is very important. The operational resources are very restricted of the biosensor nodes which are located in BSNs and traditional security technologies are not directly applicable to BSNs. Time synchronization and low-energy communication are two challenging problems for BSNs because of the characteristics of biosensors. A fuzzy commitment technology with weak time synchronization mechanism for keys negotiation is developed, with a multihop route key management scheme proposed for efficient energy consumption management, which includes an energy-based multihop-route-choice method. The Security analysis and performance evaluation is provided to validate the proposed scheme.

Keywords:

Body sensor network, e-health, fuzzy commitment, security

1. INTRODUCTION

Development of health monitoring systems called body sensor networks (BSNs). BSNs are composed of some biosensor nodes which are microscale electronic equipments integrated with biosensors and wireless transceivers [1].The biosensor nodes are worn on or implanted in the human body, which are designed to measure diverse physiological values including blood pressure (systolic and diastolic), Electrocardiogram (ECG), blood oxygen level (SpO2), activity recognition and so on [16][17][19].Thus, two conveninient services are provided by BSNs[3], a wireless micro network formed by biosensor nodes, which are: one is automated, continuous human monitoring; and the another one is intelligent treatment, such as drug delivery that can execute accurate injection of drug automatically. The security requirements of BSNs include confidentiality, integrity, authentication, and nonrepudiation. These all requirements depend on appropriate cryptographic key management. Thus, designing the efficient key management scheme for BSNs is the base of BSNs' [6][20] security and is also to focus of this paper.

Contributions

1. A hybrid multihop network structure is proposed which is suitable for BSN-based applications such as health monitoring and drug delivery, which is also useful in realizing the delivery of key materials and protected data with low energy consumption.

2. As per the above proposed structure, an energy-based multihop-route-choice is established to optimize the mechanism and a biometrics synchronization mechanism based on weak time synchronization. The energy of all transmission paths, can also leverage by the former and prolong the lifetime of the BSN.[9][10][12][14] and[15] Energy consumption in negotiating shared session keys between biosensor nodes can reduce later.

3. It can also validate the effectiveness of the proposed scheme, which is developed for simulating to compare it with existing schemes.

2. RELATED WORK

BSNs are basically used in two e-health application scenarios: one is monitoring and collecting health data of the human body, and delivering the data to remote medical center in time [2]the another one is executing intelligent treatment automatically through the cooperation of various biosensor nodes. According to these two scenarios, biosensor nodes in BSNs are structured in one of two basic layouts as shown in Fig. 1[8]:

2.1 Star Structure

A centralized architecture requires star structure where medical data collected by biosensor nodes is collated by a central node,which normally called the personal digital assistant (PDA). The PDAs are superior in terms of operational resources, such as computational capability, storage, and energy[12] . The exchanging medical data with remote medical center by wireless technologies is in charge of PDA(2G, GRPS, and 3G), which helps the doctors to make timely decisions. The star structure has an extension of, cluster structures which are also used where some biosensor nodes act as cluster heads in collecting data, and forwarding them to PDA.

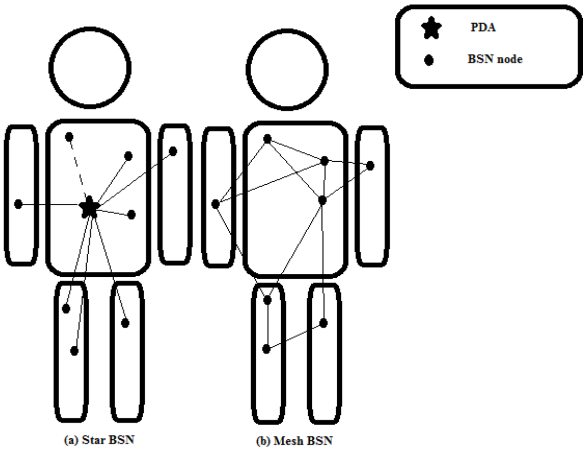

Fig 1:-Two Structures of BSNs

2.2 Mesh Structure

A distributed peer-to-peer network without a central processing unit refers as mesh structure. In this structure, biosensor nodes are distributed algorithms which mainly aim at securely integrating and anonymizing multiple data sources. This research mainly focuses on the scalability issue of TDS anonymization, and therefore, is orthogonal and complementary to them.

2.3 Problem Analysis

The low-energy problem in key management for BSNs, a key management scheme is called "BARIþ" was proposed . This scheme used a timestamp and key management schedule for distributing key management responsibility among all nodes in BSNs, which also could decrease energy consumption of the PDA (denoted by "PS") and balance the energy dissipation of the whole BSNs.

3. SECURITY ANALYSIS

The analysis of security in terms of protocols and keys. This analysis is the core assumption that legal nodes will act in according with predesigned protocols. This assumption is based on two factors:

1) Biosensor nodes are under surveillance, then suppose that biosensor nodes cannot be captured or compromised; and

2) Biosensor nodes often run automatically without human intervention.

Security protocols, should avoid a mistake while designing: misuse of cryptographic services. Which means, a cryptographic algorithm is used in a protocol provides an incorrect protection so that the needed protection is absent, which will lead to various attacks. For example, protecting the freshness value using cryptographic confidentiality service is wrong, and the correct service is data integrity which must be provided to integrate the once and the principals' identifiers [9]. Thus, "providing correct cryptographic services to messages" is a principle that must be held in designing security protocols. The protocols designed strictly comply with the above principle. Because tampering of health data will cause serious consequences, it also provide integrity not only for freshness values and entities identifiers, but also for the time values and cipher text.

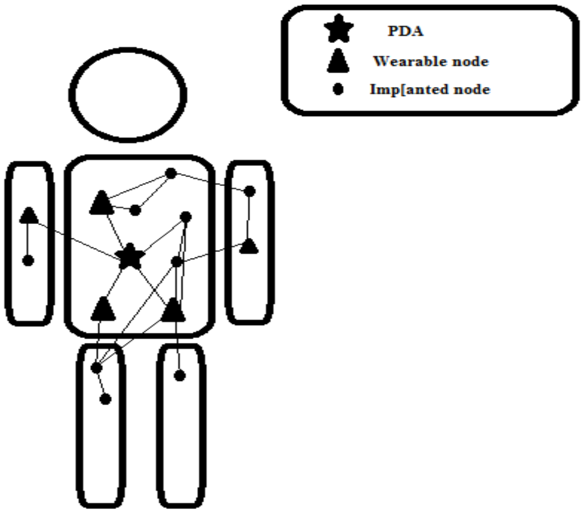

Fig 2:-The Multiphop structure of BSN

3.1 Security of Keys

The same keys are use frequently will give the adversary a good chance to break them. Security associations are established by K1 and K2, the derived keys are used to protect the following exchanged data which will give the adversary chance to analyze the two initial keys. And to protect derived keys, update them periodically by mechanisms. For an eligible key, the high degree randomness is important. In a BSN, many biosensor nodes collect time variant biometrics as good candidates for keys, and an adversary cannot reliably predict them[17].

4. PERFORMANCE ANALYSIS

I surveyed the performance of scheme in terms of keys storage and efficiency of security protocols.

4.1 Key Storage

All biosensor nodes should store K1 and K2 to establish security associations with existing nodes and new nodes. Additionally, each type of nodes will store various keys. Here, two assumptions are considered [15]:

1) The length of each key is 128 bits; and

2) Each biosensor takes part in one type of intelligent treatments.

4.2 Protocol Efficiency

One of the simplest method of distributing cluster keys is predistribution. It has the following drawback: the distance between an implanted node and its cluster head may be beyond one-hop of the implanted node. In this, the implanted node has no specific route to deliver its data to its cluster head though they have a shared cluster key. The only way it can do so is to broadcast its data and ask all intermediary nodes that are hearing its data to forward them to its cluster head. This method will consume a large amount of energy[7][8]. To address the problem, an implanted node broadcasts its data and build a multihop path to its cluster, which is helpful in energy saving. The energy consumption is closely related to the number of bits transmitted and received. An identifier is 128 bits, a fresh number and the time value are 32 bits, and the between a cluster head and its biosensor is one hop

5. CONCLUSION

The security of BSNs is an important part of e-health systems, and its core problem is key management. As some serious limitation of operational resources, a low-energy key management scheme is necessary for BSNs. An energy efficient key management scheme for BSNs is proposed based on a hybrid multihop network structure. Here two new mechanisms are used, energy-based multihoproute- choice and biometrics synchronization mechanism based on weak time synchronization are used to balance energy of routes and reduce the energy consumption in transmission. The performance of simulation and security analysis show that the proposed scheme can be used to build an efficient secure system for BSNs.

6. REFERENCES

[1] S. Cheng and C.Y. Huang, "Coloring-Based Inter-WBAN Scheduling for Mobile Wireless Body Area Network," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 2, pp. 250-259, Feb. 2013.

[2] R. Lu, X. Lin, and X. (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE

Trans. Parallel and Distributed Systems, vol. 24, no. 3, pp. 614-624, Mar. 2013.

[3] H. Zhao, J. Qin, M. Shu, and J. Hu, "A Hash Chains Based Key Management Scheme for Wireless Sensor Networks," Lecture Notes in Computer Science (LNCS), vol. 7672, pp. 296-308, 2012.

[4] P. Judge, "Hack Attacks Warning on Medical Implants," TechWeekEurope warning- on-medical-implants-72025, 2012.

[5] J.K. Hu, H.H. Chen, and T.W. Hou, "A Hybrid Public Key-vInfrastructure Solution(HPKI) for HIPAA Privacy/Security Regulations," Computer Standards and Interface, vol. 32, nos. 5/6, pp. 274-280, 2011.

[6] J.Y. Sun and Y.G. Fang, "Cross-Domain Data Sharing in Distributed Electronic Health Record Systems," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 6, pp. 754-764, June.2010.

[7] K.R.S. Muhammad, H. Lee, S. Lee, and Y.K. Lee, "BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks," Sensors, vol. 10, no. 4, pp. 3911- 3933, Oct. 2010

[8] S. Mesmoudi and M. Feham, "BSK-WBSN-Biometric Symmetric Keys to Secure Wireless Body Sensors Networks," Int'l J. Network Security and Its Applications, vol. 3, no. 5, pp. 155-166, Mar. 2010.

[9] Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park, "Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks," IEEE J. Selected Areas in Comm., vol. 27, no. 4, pp. 400-411, May 2009.

[10] M.M. Haque and A.S.K. Pathan, "Securing U-Healthcare Sensor Networks Using Public Key Based Scheme," Proc. 10th Int'l Conf. Advanced Comm. Technology, pp. 1108-1111, 2008.

[11] W.B. lee and C.D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations," IEEE Trans. Information Technology in Biomedicine, vol. 12, no. 1, pp. 34-41, Jan. 2008.

[12] F. Hu, M. Jiang, M. Wagner, and D.C. Dong, "Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign," IEEE Trans. Information Technology in Biomedicine, vol. 11, no. 6, pp. 619-627, Nov. 2007.

[13] W.D. Yu and M.A. Chekhanovskiy, "An Electronic Health Record Content Protection System Using Smartcard and PMR," Proc. Ninth Int'l Conf. e-Health Networking, Application and Services, pp. 11-18, 2007.

[14] B. Zhou, C. Hu, M.Q.H. Meng, H.B. Wang, and R. Guo, "A Wireless Sensor Network for Pervasive Medical Supervision," Proc. IEEE Int'l Conf. Integration Technology, pp. 740-744, 2007.

[15] D.O. Kang, H.J. Lee, E.J. Ko, K. Kang, and J. Lee, "A Wearable Context Aware System for Ubiquitous Healthcare," Proc. IEEE 28th Ann. Int'l Conf. Eng. Medicine and Biology Soc., pp. 5192-5195, 2006.

[16] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring," J. Mobile Multimedia, vol. 1, no. 4, pp. 307-326, Apr. 2006.

[17] F. Axisa, P.M. Schmitt, C. Gehin, G. Delhomme, E. McAdams, and A. Dittmar, "Flexible Technologies and Smart Clothing for Citizen Medicine, Home Healtcare, and Disease Prevention," IEEE Trans.Information Technologies in Biomedicine, vol. 9, no. 3, pp. 325-336, Sept. 2005.

[18] HIMSS Reports, "Systemic Interoperability Commission Releases Report to Congress and Administration," News item. asp?cid=65448&tid=3 . 2005.

[19] P. Lukowicz, U. Anliker, J. Ward, G. Troster, E. Hirt, and C. Neufelt, "AMON: A Wearable Computer for High Risk Patients," Proc. Sixth Int'l Symp. Wearable Computers, pp. 133-134, 2002.

[20] M.V. Della, "What Is E-Health (2): The Death of Telemedicine?" J. Medical Internet Research, vol. 3, no. 2, p. e22, 2001.

.