Review of Key Management Technique for Wireless Body Area Networks

Nahid.Kittur[1], P. Meena Priya Dharshini[2]

[1] M.Tech Student, Department Of ECE, CMRIT, Institute of Technology, Bangalore, India
[2] Associate Professor, Department Of ECE, CMRIT, Institute of Technology, Bangalore, India

---***---

Abstract - *As there is an increasing need for the medical facilities improvement and day by day there is an attempt to bring the hospital facilities at the door of the common people so as to help the patients. One such popular attempt is through Wireless Body Area Networks. WBAN technology gives the main advantage of mobility to the user and at the same time the health of the user is monitored. The main research challenges in BAN design is personal health security, also transmitting amounts of valuable and confidential data between WBAN nodes through wireless channel puts the data at serious risk of theft, sabotage, exploitation and manipulation. This paper provides a survey of different authentication techniques which are suitable for WBAN and also the level of security acquired depending on their characteristics.*

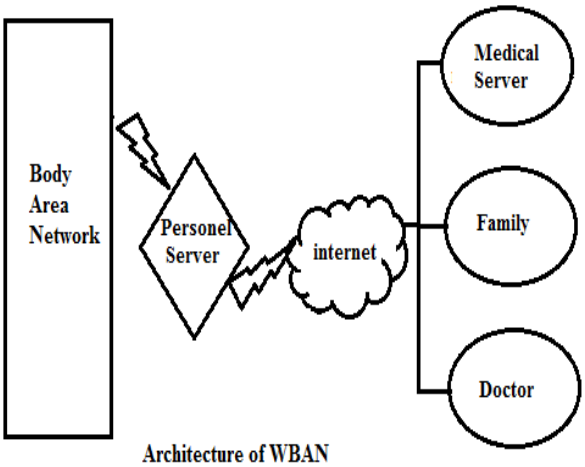
Key Words: Security, Authentication, WBAN

1. INTRODUCTION

Wireless Body Area Network (WBAN) has emerged as a technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques [1]. This network uses wireless sensors which are wearable, which enables prevalent, separated, and real-time health care for the patient [3]. These small wearable or implantable sensor nodes are placed in, on or around a patient's body, which are capable of sensing, storing, processing and transmitting data via wireless communications. A Controller is like a hand-held device, is associated with the same patient and send the collected data to the upper tier of the network for healthcare records [2]. Energy effectiveness for sensors placed on the WBAN is to improve the sustainability of the network, and give the limited power source available at each sensor [3].

And then, this patient's health-related data can be accessed by other users or organizations such as researchers, government agencies and insurance companies. Through such technical renovation, the diagnosis accuracy rate will be improved, the emergency medical response will be expedited and the efficiency of healthcare will be greatly increased [4].

The main research challenges in BAN design is personal health security along communication over the wireless link and stringent resource constraints (i.e., low power, low computational capability and small storage space). [6]. Also transmitting amounts of valuable and confidential data between WBAN nodes through wireless channel puts the data at serious risk of theft, sabotage, exploitation and manipulation [5].



Architecture of WBAN

Wireless networks always have more complications than wired networks towards approach of efficient security system. Security is a high priority in most WBAN networks. Due to the easy accessible way due to the wireless channel there are many security issues which come in the way of the progress of WBAN. The sensor nodes are monitoring and transmitting vital and sensitive medical data. It is a challenge to implement security mechanism in lightweight WBANs since they are limited in both computational and communication resources [5].

So, the security protocols are used to achieve security requirements which are confidentiality, integrity and authenticity in sensor networks and use few symmetric keys for data encryption and to compute the Message Authentication Code (MAC) [7].

Some security risks surrounding WBANs are,

- Eavesdropping
- Data modification
- Impersonation attack
- Replaying
- Denial of service etc [5].

However, WBANs security has some following limitations:

- Users might not trust the keys preloaded.
- Expensive public key techniques due to the limited computation resources.
- Require different manufactures for global Public Key Infrastructure [7].

2. Related Works

Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang [8] have summarized cryptography and authentication in WBAN innovating a biometric-based approach for the authentication of message which is a piratical solution and can be simply implemented in the resource constrained biomedical sensors and a novel key-agreement scheme is developed to allow communication parties to share the same key without much overheads also a framework for the security and energy efficiency analysis of the proposed approach.

Krishna K. Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S. Gupta, [6] have proposed a key management scheme known as physiological-signal-based key agreement (PSKA) for ensuring safe and secure communication within a BAN in a plug-n-play manner. The nodes communicate agreeing to symmetric key using the physiological signals which are obtained from the patients and no initialization or pre-distribution is required and hence there is low latency and distinctiveness is achieved.

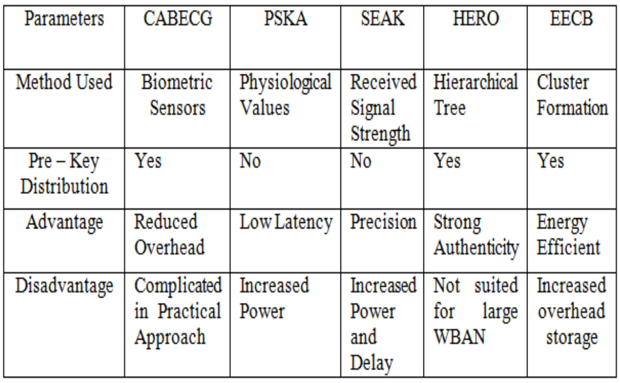
Chitra Javali et al [9] have presented a secure light-weight device pairing protocol for WBAN based on RSS which is obtained by dual-antenna transceivers utilizing spatial diversity. With spatially separated antennas, the RSS values from a nearby device are large and distinct, as opposed to those from a far-away device. SeAK exploits this effect to accomplish authentication and shared secret key generation.

Boushra Maala and Yacine Challal and Abdelmadjid Bouabdallah [10], have proposed a scheme HERO hierarchical key management protocol for heterogeneous wireless sensor networks is based on a random key pre distribution to construct a hierarchical tree which decreases the key storage overhead. The key pre-distribution is done using a large pool and based on child-parent relationship method is employed. The goal of HERO is to construct a secure path between very node and the end point (sink) which is in common for all nodes. Hence all the authenticated nodes are known if any new node is added its path to the sink is calculated.

Aftab Ali and Farrukh Aslam Khan [11], have valuated an key management scheme for WBANs which is energy-efficient that mainly considers the resources available for a node during the complete life cycle of key management. The cluster-based hybrid security structure that deals with both intra-WBAN and inter-WBAN communications is proposed in this scheme.

The electrocardiogram (EKG) based key agreement scheme itself is used by the cluster formation process. The proposed technique is hybrid as it uses both physiological value-based generated keys and preloading of keys. Energy-efficiency can be ensured by using multiple clusters.

TABLE I. COMPARISION OF KEY MANAGEMENT SCHEMES



Parameters	CABECG	PSKA	SEAK	HERO	EECB
Method Used	Biometric Sensors	Physiological Values	Received Signal Strength	Hierarchical Tree	Cluster Formation
Pre – Key Distribution	Yes	No	No	Yes	Yes
Advantage	Reduced Overhead	Low Latency	Precision	Strong Authenticity	Energy Efficient
Disadvantage	Complicated in Practical Approach	Increased Power	Increased Power and Delay	Not suited for large WBAN	Increased overhead storage

3. Problem Identification

The authors in [9] have proposed a physical layer based efficient, light weight, close proximity secure device paring protocol for WBAN which performs authentication and shared secret key generation simultaneously. Only one of the antennas will be selected from the application layer for transmission and receiving of packets. The antenna RSSI (RSS Indicator) threshold value is set for each antenna distance. If the RSSI difference is greater than the RSSI threshold because of antenna distance, which difficult for key generation and affects beam forming attack. Also it increased the power and delay of each antenna based on CU.

4. Proposed Solution

Two fundamental issues in WBAN are authentication and key generation which are usually handled as two different issues. We address these separate issues and propose a common method for the authentication as well as secret key generation. To establish secure channel in the device pairing and association SeAK (Secure Authentication and Key Generation) is used. Here for association process, the device sent association request to CU. When the ack message is received by the device the CU send N packet at a particular time interval between different antennas. The sensor nodes measure RSSI and text probe response of each antenna. For successful authentication both CU and device use RSSI values which are stored during probe exchange. After the measure of RSS we include EKG key management for secure communication among nodes. Here pairwise key used for key management and unique key used for communication between sensor nodes. The calculation of pairwise key is based on required data and IDs of communicating nodes. The sensor node encrypts and decrypts the data with this pairwise key.

Before receiving this message the PS (Personal Server) first calculates pairwise key of nodes by keyed-hash function, if both are equal it will receive the data. Here the communication between PS is done through the ID of PS. Finally due of dynamic and highly random nature of EKG values of the human body PS wishes to refresh the key, so the keys are refreshed at regular time interval by keyref message. It computes the key by EKG value of human body.

5. CONCLUSIONS

In this paper the various key management and authentication schemes have been discussed and their advantages and disadvantages have been stated. To establish a secure channel in wireless body area network a new key management technique is to be proposed which involves the authentication and key generation process. The proposing technique will be compared with the existing technique and performance is to be observed.

REFERENCES

[1] Ming Li, Wenjing Lou and Kui Ren, "Data Security And Privacy In Wireless Body Area Networks", IEEE Wireless Communications, Pages: 51-58, February 2010.

[2] Ming Li, Shucheng Yu, Wenjing Lou and Kui Ren, "Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks", Proceedings IEEE INFOCOM, 2010.

[3] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Green and Sustainable Cyber-Physical Security Solutions for Body Area Networks", Sixth International Workshop on Wearable and Implantable Body Sensor Networks, Pages: 240 - 245, June 2009.

[4] Rong Fan, Ling-Di Ping, Jian-Qing Fu, and Xue-Zeng Pan, "The New Secure and Efficient Data Storage Approaches for Wireless Body Area Networks", International Conference on Wireless Communications and Signal Processing (WCSP), Pages: 1-5, October 2010.

[5] Jingwei Liu and Kyung Sup Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", Second International Conference on Ubiquitous and Future Networks (ICUFN), Page(s): 98 - 103, 2010.

[6] Krishna K. Venkatasubramanian, Ayan Banerjee, and Sandeep Kumar S. Gupta, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 1, Pages: 60-68, January 2010.

[7] Sofia NajwaRamli, Rabiah Ahmad, MohdFaizalAbdollah, and ErykDutkiewicz, "A Biometric-based Security for Data Authentication in Wireless Body Area Network", 15th International Conference on Advanced Communication Technology, Page(s): 998- 1001, ISSN: 1738-9445, January 2013.

[8] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang ECG-Cryptography and Authentication in Body Area Networks IEEE transactions on information technology in biomedicine, vol. 16, no. 6, november 2012

[9] Chitra Javali, Girish Revadigar, Lavy Libman, and Sanjay Jha, Seak: Secure Authentication and Key Generation Protocol based on Dual antenna Wireless Body Area Networks, Pages: 1-12.

[10] Maala, B., Challal, Y. and Bouabdallah, A. HERO: Hierarchical key management protocol for heterogeneous wireless sensor networks, 2008, in IFIP International Federation for Information Processing, Volume 264;
(Boston: Springer), pp. 125–136.

[11] Aftab Ali1 and Farrukh Aslam Khan "energy efficient cluster based security mechanisms for intra WBAN and inter WBAN communications for WBAN and inter-wban communications for applications", Pages: 1-19, 2013.