2011 International Conference on Advancements in Information Technology
With workshop of ICBMG 2011
IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore

Security in Wireless Body Area Networks: A survey

M. Somasundaram[+] and R. Sivakumar
Professor,Department of Computer Science and Engineering (CSE),
R.M.K. Engineering College, Kavaraipettai 601206, Tamilnadu, India,

Abstract : Wireless Body Area Networks (WBAN) has emerged as a key technology to provide real-time health monitoring of a patient and diagnose many life threatening diseases. Among the various research issues required to be addressed to implement this technology effectively, security issue is one of the key issues. This paper surveys the issues related to security and possible solutions taken to address them in the research and the forthcoming IEEE standard. The survey brings out that the current proposed solutions in security are still having limitations needing further research and hence the survey also highlights further areas of research being proposed in the literature.

Keywords : Wireless Communication and Mobile Computing, Wireless Sensor Networks, Computer and network security, Wireless Body Area Network (WBAN), eHealthcare

1. Introduction

Wireless Body Area Networks (WBAN) has emerged as a key technology to provide real-time health monitoring of a patient and diagnose many life threatening diseases. WBAN operates in close vicinity to, on, or inside a human body and supports a variety of medical and non-medical applications. IEEE 802 has established a Task Group called IEEE 802.15.6 for the standardization of WBAN. The purpose of the group is to establish a communication standard optimized for low-power in-body/on-body nodes to serve a variety of medical and non-medical applications. [1]. This paper presents a survey of the security features of the proposed standard including current limitations and proposes the area of future work.

2. Status of the IEEE Standard

The IEEE 802.15 Task Group 6 (BAN) is developing a communication standard optimized for low power devices and operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics / personal entertainment and others. IEEE 802.15 TG6 was formed in November 2007 and begun operations as TG6 in January 2008 in Taipei. It had received 34 proposals, which were merged into a single candidate proposal. A draft of the standard was developed in March 2009. It has undergone significant editing and underwent five Letter Ballots. The last was Letter Ballot #79 which was completed on July 13, 2011. On July 22, 2011, the draft was approved to start Sponsor Ballot. It is expected to be finalized in November 2011 in the TG6 meeting in Atlanta, USA. [2]

3. Target Applications

The WBAN applications targeted by the IEEE 802.15.6 standard are divided into medical and non-medical applications as given in Fig. 1. Medical applications include collecting vital information of a patient continuously and forward it to a remote monitoring station for further analysis. This huge amount of data can be used to prevent the occurrence of myocardial infarction and treat various diseases such as gastrointestinal tract, cancer, asthma, and neurological disorder. WBAN can also be used to help people with disabilities. For

[+] Corresponding author. Tel.: +91 (44) 2792 5338; fax: +(44) 2792 5193.
E-mail address: mss.cse@rmkec.ac.in.

example, retina prosthesis chips can be implanted in the human eye to see at an adequate level. Non-medical applications include monitoring forgotten things, data file transfer, gaming, and social networking applications. In gaming, sensors in WBAN can collect coordinates movements of different parts of the body and subsequently make the movement of a character in the game, e.g., moving soccer player or capturing the intensity of a ball in table tennis. The use of WBAN in social networking allows people to exchange digital profile or business card only by shaking hands. A WBAN architecture for medical applications is as given in the Fig.2. [3]

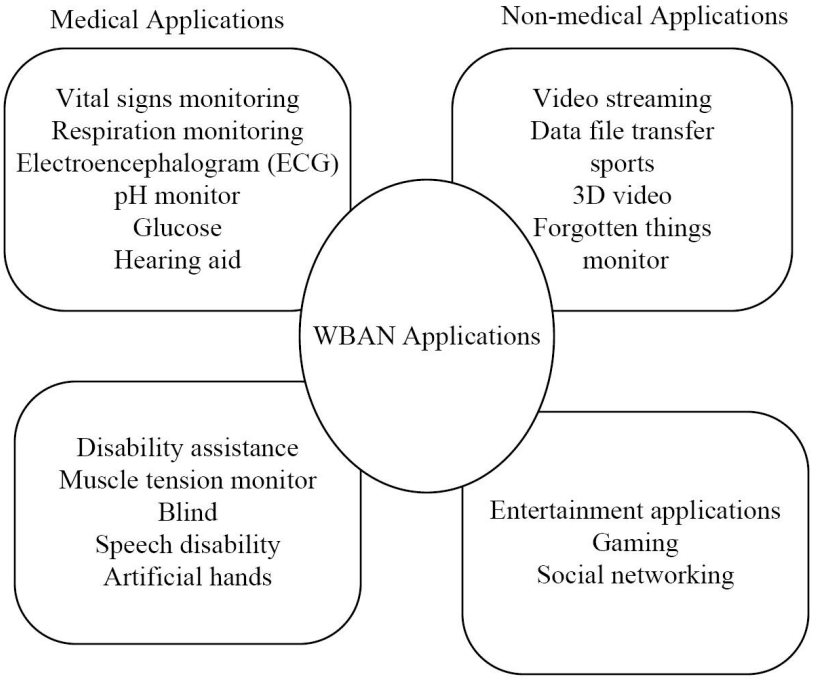

Fig 1 : WBAN Applications targeted by IEEE 802.15.6

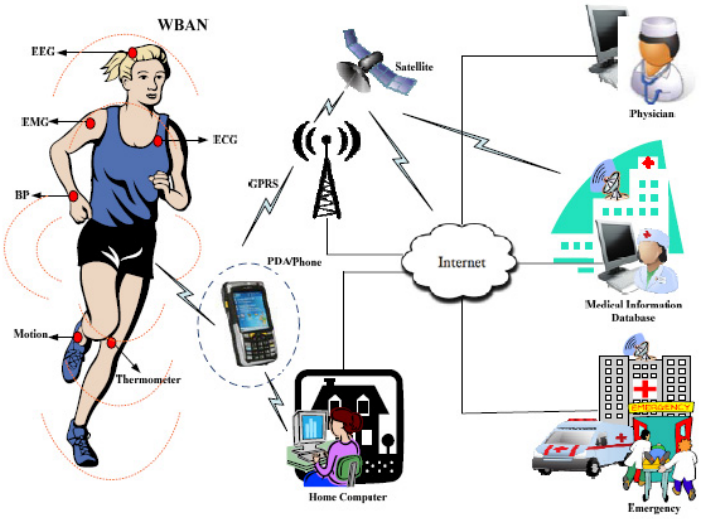

Fig. 2. WBAN Architecture of medical applications

4. WBAN Security Issues and Requirements

WBAN brings forward several research issues that need to be taken into account in the design of radio frequency (RF) wireless systems. Issues are frequency band selection, channel modelling, antenna design, PHY protocol design, energy-efficient hardware, MAC protocol design, QoS and reliability, real time connectivity over heterogeneous networks, regulatory compliance, and security and privacy. Such issues [9]

especially the security issues [10] have been analysed in detailed and are being addressed by various emerging candidate technology solutions with merits and demerits.

The key security requirements in WBANs are discussed below. [3]

Data Confidentiality: Like WSNs, Data confidentiality is considered to be the most important issue in WBANs. It is required to protect the data from disclosure. WBANs should not leak patient's vital information to external or neighbouring networks. The use of symmetric key encryption is the most reliable for WBANs since public-key cryptography is too costly for the energy-constraint sensor nodes.

Data Integrity: Keeping the data confidential does not protect it from external modifications. An adversary can always alter the data by adding some fragments or by manipulating the data within a packet. This packet can later be forwarded to the coordinator. Lack of data integrity mechanism is sometimes very dangerous especially in case of life-critical events (when emergency data is altered). Data loss can also occur due to bad communication environment.

Data Authentication: It confirms the identity of the original source node. Apart from modifying the data packets, the adversary can also change a packet stream by integrating fabricated packets. The coordinator must have the capability to verify the original source of data. Data authentication can be achieved using a Message Authentication Code (MAC) (to differentiate it from Medium Access Control (MAC), the Message Authentication Code (MAC) is represented by bold letters) that is generally computed from the shared secret key.

Data Freshness: The adversary may sometimes capture data in transit and replay them later using the old key in order to confuse the coordinator. Data freshness implies that the data is fresh and that no one can replay old messages. There are two types of data freshness: weak freshness, which guarantees partial data frames ordering but does not guarantee delay, and strong freshness, which guarantees data frames ordering as well as delay.

Secure Localization: Most WBAN applications require accurate estimation of the patient's location. Lack of smart tracking mechanisms allow an attacker to send incorrect reports about the patient's location either by reporting false signal strengths or by using replaying signals.

Availability: Availability implies efficient availability of patient's information to the physician. The adversary may target the availability of WBAN by capturing or disabling a particular node, which may sometimes result in loss of life. One of the best ways is to switch the operation of a node that has been attacked to another node in the network.

Secure Management: Secure management is required at the coordinator to provide key distribution to the nodes for encryption and decryption operation. In case of association and disassociation, the coordinator adds or removes the nodes in a secure manner.

5. Possible Security Threats and Attacks in WBAN

A WBAN is vulnerable to a considerable number of key attacks. These attacks are conducted in different ways, i.e., Denial of Service (DoS) attacks, privacy violation, and physical attacks. Due to restrictions on the power consumption of the sensor nodes, protection against these types of attacks is a challenging task. A powerful sensor can easily jam a sensor node and can prevent it from collecting patient's data on regular basis. Attacks on WBAN can be classified into three main categories as follows: [3]

Layers	DoS attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proof, hiding
Link	Collision	Error correcting code
	Unfairness	Small frames
	Exhaustion	Rate limitation

Network	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization monitoring
	Black holes	Authorization, monitoring, redundancy
Transport	Flooding	Client Puzzles
	De-synchronization	Authentication

6. Adopting IEEE 802.15.4 Security Framework for WBAN

The above security structure has been taken from IEEE standard 802.15.4 with modifications. The IEEE 802.15.4 standard is a low-power standard designed for low data rate applications. It intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) focusing on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end-user oriented approaches, such as Wi-Fi) [3]

The IEEE 802.15.4 is considered very close to WBAN due to its quick implementation, reliable security mechanism, and support of low data rate applications with low cost of power consumption. The table as below lists different security suites defined in the IEEE 802.15.4 standard [6]. The security suits in the IEEE 802.15.4 are broadly classified into null, encryption only (AES-CTR), authentication only (AES-CBC-MAC), and encryption and authentication (AES-CCM) suites.

- In AES-CTR, confidentiality protection is provided using Advance Encryption Standard (AES) block cipher [4] with counter mode. Rijndael is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits. The design strategy provides resistance against linear and differential cryptanalysis. In the strategy, the round transformation is divided into different components, each with its own functionality. Rijndael is a very fast block cipher. It can be implemented very efficiently on a Smart Card or such devices with a small amount of code, using a small amount of RAM and taking a small number of cycles. Some ROM/performance trade-off is possible. It is easy to make the implementation of the cipher resistant to timing attacks. The variable block length allows the construction of a collision-resistant hash function with Rijndael as compression function. The most important disadvantage is the fact that the inverse cipher is different from the cipher. The inverse cipher is typically 1.5 to 2 times slower on Smart Card (or takes more ROM).
- In AES-CBC-MAC, security including integrating protection is provided using CBC-MAC [5]. The Cipher Block Chaining Message Authentication Code (CBC MAC) specifies that an m-block message x = x1 ….. xm be authenticated among parties who share a secret key a for the block cipher. This method is a pervasively used international and U.S. standard.
- The AES-CCM provides high-level security that includes both data integrity and encryption. [7] [8]. CCM is a new mode of operation of a block cipher that combines the existing Counter (CTR) and CBC-MAC modes.

Name	Description	Access Control	Confidentiality	Frame integrity	Sequential freshness
Null	No security				
AES-CTR	Encryption only, CTR mode	X	X		X
AES-CBC-MAC-128	128 bit MAC	X		X	
AES-CBC-MAC-64	64 bit MAC	X		X	
AES-CBC-MAC-32	32 bit MAC	X		X	
AES-CCM-128	Encryption & 128 bit MAC	X	X	X	X
AES-CCM-64	Encryption & 64 bit MAC	X	X	X	X

AES-CCM-32	Encryption & 32 bit MAC	X	X	X	X

7. Security Paradigm in the IEEE 802.15.6 standard

The IEEE 802.15.6 standard defines the following three levels of security. Each security level has different security properties, protection levels and frame formats. [1] The security structure has been taken from IEEE standard 802.15.4 with modifications

- Level 0 - unsecured communication: This is the lowest security level where data is transmitted in unsecured frames. There is no mechanism for data authentication and integrity, confidentiality and privacy protection, and replay defense.
- Level 1 - authentication only: This is the medium security level where data is transmitted in secured authentication but is not encrypted. The confidentially and privacy is not supported by this mode.
- Level 3 - authentication and encryption: This is the highest security level where data is transmitted in secured authentication and encryption frames. It provides solutions to all of the problems not covered by the level 0 and level 1. The required security level is selected during the association process, i.e., when a node is joining the network. For unicast communication, a pre-shared Master Key (MK) or a new key (established via unauthenticated association) is activated. Then a Pairwise Temporal Key (PTK) is established, which is used once per session. For multicast communication, a Group Temporal Key (GTK) is shared with the corresponding multicast group. The whole security structure is given in Fig. 3.

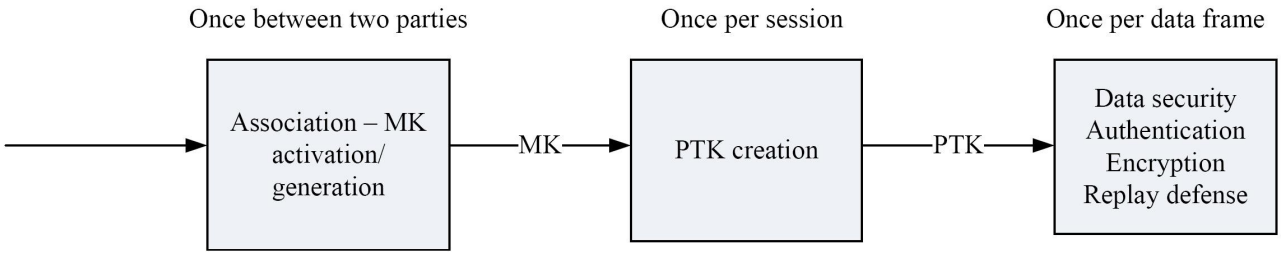

Fig.3. Security structure of IEEE 802.15.6

8. Issues in the Security structure and possible solutions

IEEE 802.15.4 MAC has two operational modes: a beacon-enabled mode and a non-beacon enabled mode. In the beacon-enabled mode, the network is controlled by a coordinator, which regularly transmits beacons for device synchronization and association control. The channel is bounded by a superframe structure as illustrated in Fig. 4. The superframe consists of both active and inactive periods. The active period contains three components: a beacon, a Contention Access Period (CAP), and a Contention Free Period (CFP). The coordinator interacts with nodes during the active period and sleeps during inactive period. There are maximum of seven GTS slots in the CFP period to support time critical traffic. In the beacon-enabled mode, a slotted CSMA/CA protocol is used in the CAP period. In the non-beacon enabled mode, the channel is accessed using unslotted CSMA/CA protocol.

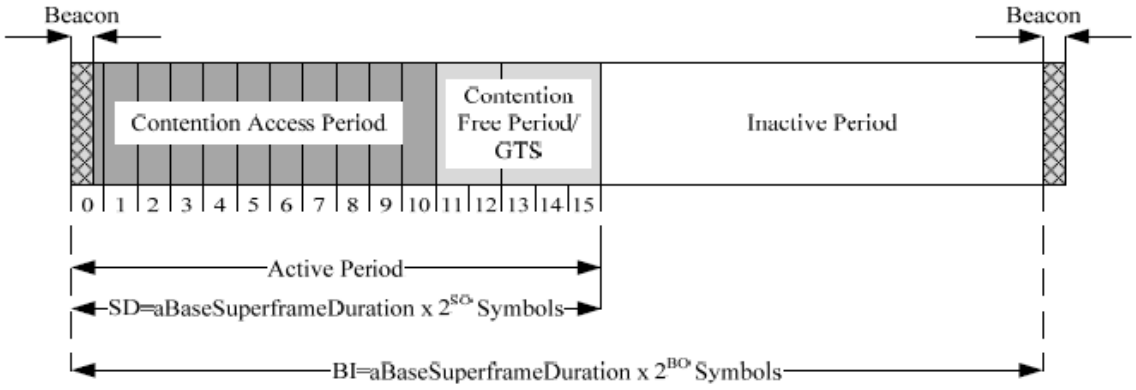

Fig.4. IEEE 802.15.4 superframe structure in a beacon enabled mode

Based on the study done on IEEE 802.15.4 security framework for WBANs by simulating smart, random, and weak attacks, the results showed that the smart attacker(s) has the capability of corrupting an increasing number of GTS slots compared to random and weak attackers. This means that the direct adaption of IEEE 802.15.4 security framework for WBANs is not reliable since most of the traffic in WBANs is carried in CFP period, which is most vulnerable to GTS attacks.

One of the solutions is to implement a sophisticated backoff detection scheme that should successfully detect the backoff attacks. However, the backoff detection scheme may not work for adversaries who have enough knowledge of the scheme. They may try to maximize their throughput and minimize their chances of detection. Another approach is to allow the receiver to assign the backoff window to the sender. In this scheme, the receiver can easily detect any attack and can even penalize the adversaries by increasing their backoff values. A game theoretic approach could also be useful to detect and prevent the attacks by considering that all nodes are selfish. [3].

9. References

[1] Kyung Sup Kwak, Sana Ullah, Niamat Ullah, “An overview of IEEE 802.15.6 Standard”, 3rd International Symposium on Applied Sciences in Biomedical & Communication Technologies (ISABEL2010) in Rome, Italy

[2] IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks : http://ieee802.org/15/pub/TG6.html

[3] S. Saleem, S. Ullah, and K.S. Kwak, A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks, Sensors, vol.11, No.2, pp. 1383-1395, 2011.

[4] Rijmen, V.; Daemen, J. The block cipher Rijndael. In Smart Card Research and Applications; LNCS 1820;, Springer-Verlag: New York, NY, USA, 2000; pp. 288-296.

[5] Bellare, M.; Kilian, J.; Rogaway, P. The security of the cipher block chaining message authentication code. J. Comput. Syst. Sci. 2000, 61, 362-399.

[6] Xiao, Y.; Chen, H.H.; Sun, B.; Wang, R.; Sethi, S. MAC security and security overhead analysis in the IEEE 802.15.4 Wireless Sensor Networks. EURASIP J. WCN 2006, doi:10.1155/WCN/2006/93830.

[7] AES CCM Encryption and Decryption : http://www.inno-logic.com/resourcesEncryption.html#1

[8] Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality : National Institute of Standards and technology (NIST) : http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

[9] Maulin Patel and Jianfeng Wang : Applications, challenges, and prospective in emerging body area networking technologies , Journal IEEE Wireless Communications Volume 17, Issue 1, February 2010, pp 80-88.

[10] Ming Li, Wenjing Lou and Kui Ren , Data security and privacy in wireless body area networks, Journal IEEE Wireless Communications Volume 17, Issue 1, February 2010, pp 51-58.