International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)
(Vol. 02, Issue 01, December 2013)
ISSN: 2347 - 601X
www.ijemhs.com

WBAN and its Applications

Sachin Minocha

M. Tech Student, Vaish College of Engineering, Rohtak, Haryana (India)

Abstract

Wireless Body Area Network (WBAN) is a collection of low-power and lightweight wireless sensor nodes that are used to monitor the human body functions and the surrounding environment. It supports a number of innovative and interesting applications, including ubiquitous healthcare and Consumer Electronics (CE) applications. Since WBAN nodes are used to collect sensitive (life-critical) information and may operate in hostile environments, they require strict security mechanisms to prevent malicious interaction with the system. This paper gives a brief introduction about WBAN, their application and attacks on different layers.

Keyword: *Body Area Network, Wireless Sensor Network, Attacks, Security.*

1. Introduction

A Wireless Body Area Network (WBAN) allows the integration of intelligent, miniaturized, low-power sensor nodes in, on, or around a human body to monitor body functions and the surrounding environment. It has great potential to revolutionize the future of healthcare technology and has attracted a number of researchers both from the academia and industry in the past few years. WBANs support a wide range of medical and Consumer Electronics (CE) applications. For example, WBANs provide remote health monitoring of patients for a long period of time without any restriction on his/her normal activities **[1]**. Generally WBAN consists of in-body and on-body area networks. An in-body area network allows communication between invasive/implanted devices and a base station. An on-body area network, on the other hand, allows communication between non-invasive/wearable devices and a base station **[2]**.

Table 1 : Difference b/w WBAN and WSN

	Wireless Body Area Network(WBAN)	**Wireless Sensor Network(WSN)**
Sensor Nodes	Limited number	Large number
Area of Interest	Small area	Wide area
Range	Limited	Large
Reliability	High	Low
Delay	Low	High
Security Mechanism	Stronger	Lower
Data Rates	Heterogeneous	Homogeneous
Wireless Technology	Low power technology required	Bluetooth, ZigBee, GPRS, WLAN
Power Demand	Small	Large
Node Size	Small is essential	Small is preferred.
Scale	In centi meters/meters	In Meters/kilometers

2. Wireless Body Area Network Applications

WBAN applications are divided into medical and nonmedical applications. 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 **[3]**. WBAN can also be used to help people with disabilities. For example, retina prosthesis chips can be implanted in the human eye to see at an adequate level. In the healthcare sector BANs serve diagnostic purposes and furthermore achieve local independence for monitoring of

patients. As already mentioned, a major role of BANs is to close the feedback loop by adding actors to the network, e.g. a drug delivering medical feedback loop. Such a system, e.g. consisting of a sensor to detect the blood sugar and an insulin-delivering actor, could please the permanent need of insulin by patients suffering from diabetes **[4]**. Continuous monitoring of the glucose level is the prerequisite to imitate the function of the insulin-producing pancreas. An individualized dose is always preferable and avoids under- or overdosing.

Non-medical applications include monitoring forgotten things, data file transfer, gaming, and social networking applications. In gaming **[3]**, 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.

3. Security Applications

A BAN could be very useful in security applications, additionally to the observation of life signs the opportunity of tracking will reduce mistakes. People who are often in hazardous situations like fire-fighters, policemen or paramedics could benefit from monitoring and tracking, but also from an analysis of the surrounding area **[4]**. In the case of fire-fighters the amount of oxygen in the air and the temperature could be values of interest.

4. Requirements for Data Security and Privacy in WBAN

The security and privacy of patient-related data are two indispensable components for the system security of the WBAN. By data security, they mean data is securely stored and transferred, and data privacy means the data can only be accessed by the people who have authorization to view and use it **[6]**. The key security requirements in WBANs are discussed below:

a. **Confidentiality:** In order to prevent patient-related data from leaking during storage periods, the data needs to always be kept confidential at a node or local server **[6]**. Data confidentiality should be resilient to device compromise attacks; that is, compromising one node helps the attacker to gain nothing or little from the data stored at that node or elsewhere.

b. **Dynamic integrity assurance:** In WBANs the patient-related data is vital, and modified data would lead to disastrous consequences. Thus, data integrity shall be dynamically protected all the time. In particular, they will be able to not only detect modification of data at end users, but also check and detect that during storage periods, in order to discover potential malicious modification in advance and alert the user **[6]**.

c. **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 **[2]**. 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.

d. **Secure Localization:** Most WBAN applications require accurate estimation of the patient's location **[2]**. 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.

e. **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 **[3]**. One of the best ways is to switch the operation of a node that has been attacked to another node in the network.

f. **Secure Management:** Secure management is required at the coordinator to provide key distribution to the nodes for

encryption and decryption operation **[3]**. In case of association and disassociation, the coordinator adds or removes the nodes in a secure manner.

5. Possible Security Threats and Attacks

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 **[7]:**

- **a.** Attacks on secrecy and authentication, where an adversary performs eavesdropping, packet replay attacks or spoofing of packets,
- **b.** Attacks on service integrity, where the network is forced to accept false information **[8]**,
- **c.** Attacks on network availability (DOS attacks), where the attacker tries to reduce the network's capacity.

Table 2 : WBAN OSI layers and DOS attacks/defenses [2]

Layers	**DOS attacks**	**Defenses**
Physical	Jamming	Spread-spectrum, 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

5.1 Physical Layer Attacks

Some of the main responsibilities of physical layer include frequency selection and generation, signal detection, modulation, and encryption **[9]**. Since the medium is radio-based, jamming the network is always possible. The most common attacks are jamming and tampering. Jamming refers to interference with the radio frequencies of the nodes. The jamming source can be powerful enough to disrupt the entire network. Tampering refers to the physical attacks on the sensor nodes **[10]**. However, nodes in WBAN are deployed in close proximity to the human body, and this reduces the chances of physical tampering.

5.2 Data Link Layer Attacks

This layer is responsible for multiplexing, frame detection, channel access, and reliability. Attacks on this layer include creating collision, unfairness in allocation, and resource exhaustion. Collision occurs when two or more nodes attempt to transmit at the same time. An adversary may strategically create extra collisions by sending repeated messages on the channel. Unfairness degrades the network performance by interrupting the MAC priority schemes. Exhaustion of battery resources may occur when a self-sacrificing node always keeps the channel busy.

5.3 Network Layer Attacks

The nodes in WBAN are not required to route the packets to other nodes. Routing is possible when multiple WBANs communicate with each other through their coordinators. Possible attacks include spoofing, selective forwarding, sybil and hello flood. In spoofing, the attacker targets the routing information and alters it to disrupt the network. In selective forwarding, the attacker forwards selective messages and drops the others

[11]. In sybil, the attacker represents more than one identity in the network [12]. The hello flood attacks are used to fool the network, i.e., the sender is within the radio range of the receiver.

5.4 Transport Layer Attacks

The attacks on the transport layer are flooding and de-synchronization. In flooding, the attacker repeatedly places requests for connection until the required resources are exhausted or reach a maximum limit. In de-synchronization, the attacker forges messages between nodes causing them to request the transmission of missing frames.

6. Conclusion

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. This paper presents a survey of WBAN and proposes the area of future work.

References

[1] Ullah, S.; Higgins, H.; Braem, B.; Latre, B.; Blondia, C.; Moerman, I.; Saleem, S.; Rahman, Z.; Kwak, K.S. A comprehensive survey of wireless body area networks: On PHY, MAC, and Network Layers Solutions. J. Med. Syst. 2010, doi: 10.1007/s10916-010-9571-3.

[2] Shahnaz Saleem et. al. , “A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks”, Sensors 2011, 11, 1383-1395; doi:10.3390/s110201383.

[3] M. Somasundaram et. al. ,“Security in Wireless Body Area Networks: A survey”, 2011 International Conference on Advancements in Information Technology With workshop of ICBMG 2011,IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore.

[4] Ann-Kristin Kock et. al. , “Medical Body Area Networks”, Seminar Kommunikations standards in der Medizin, SS 2010.

[5] Saleem, S.; Ullah, S.; Yoo, H.S. On the security issues in wireless body area networks. J. Digital Content Technol. Appl. 2009, 3, 178-184.

[6] Ming li and Wenjing Lou et. al. ,“Data Security And Privacy In Wireless Body Area Networks”, IEEE Wireless Communications, February 2010, 1536-1284/10/$25.00 © 2010 IEEE.

[7] Shi, E.; Perrig, A. “Designing secure sensor networks”. IEEE Wirel. Commun. Mag. 2004, 11, 38-43.

[8] Wood, A.D.; Stankovic, J.A. “,Denial of service in sensor networks”. IEEE Comput. 2002, 35, 54-62.

[9] Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. ,“A survey on sensor networks”, IEEE Commun. Mag. 2002, 40, 102-114.

[10] Wang, X.; Gu, W.; Schosek, K.; Chellappan, S.; Xuan, D. ,“Sensor Network Configuration under Physical Attacks”, Technical Report (OSU-CISRC-7/04-TR45); Department of Computer Science and Engineering, Ohio State University: Columbus, OH, USA, July 2004.

[11] Karlof, C.; Wagner, D. “Secure routing in wireless sensor networks: Attacks and counter measures”, In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, May 2003; pp. 113-127.

[12] Douceur, J. ,“The Sybil attack”. In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS’02), Cambridge, MA, USA, February 2002.