Wireless Body Area Network (WBAN): Security and Authentication Methods

Munir Hussain
Institute of Computing, Kohat University of Science & Technology, 26000 Kohat, Pakistan.
munirhabib2016@gmail.com

Abstract

The demand for WBAN has increased for last few years because it is useful network to monitor and improve various health conditions of human being. Information's exchanges among different entities are very sensitive, so it is vital to keep this information's secure from unauthorized access in order to avoid unpleasant incidents. Security and privacy are the most critical issues. Security is the important issue for any network and especially in WBANs its proper management is very crucial otherwise biomedical data collected by sensor nodes should be mixed with other user's data. Also, patients do not want their personal data to be misused and WBAN should provide the privacy to prevent eavesdropping. Mutual authentication is also a key challenge in WBAN, and patients' data originality and integrity are important for their treatment diagnosis etc. Development of the new mutual authentication schemes in healthcare applications without considering security makes patient privacy vulnerable. In this paper, we discuss communication technologies, possible attacks and recently most used popular authentication methods in WBANs.

Keywords: WBAN, Communication Technologies, Security, Authentication, Privacy

Article Number: IOARP-JCN04-005
IOARP Journal of Communication and Networks
Volume 4, Issue 1, June 2024
Appeared on Digital Library: 15 July 2024

1. Introduction

Wireless Body Area Networks (WBANs) can be used for measuring various characteristics of the human body such as it can be used to monitor the blood pressure of a person on regular basis. These networks are consisting of small low power biomedical sensor nodes which can be used to monitor health fundamentals characteristics. WBAN is sub-branch of Wireless Sensor Network (WSN) and it improves the quality of life of a person by regularly observing imperative signs of the human body such as monitoring blood pressure, heartbeat rate and blood sugar level etc in order to avoid unpleasant health issues in advance by passing sensitive information's collected by different implanted or wearable sensor nodes to the local doctor/hospital to assist a patient. Generally, WBAN architecture is divided into 3-tiers communications [1] as shown by figure 1. The tier-1 (Intra-BAN) communication is consisting of different sensor nodes those may be implanted or wearable around the human body to monitor various vital signs of the body. The function of sensor nodes is not only simply collecting vital human body information's but also do some process and communication with each other in order to passed collected information's to a central sensor node known as a master node. In tier-2 (Inter-BAN) communication takes place between the master node and a personal central device known as local processing unit (LPU) or personal server (PS) which can be Smartphone, laptop and PDA etc. As we know that sensor nodes have limited memory therefore captured valuable information's by the sensor nodes are passed to the LPU before their memory gets full. Inter-Ban communication architecture can be divided into two types. Infrastructure based architecture communication is generally used in limited space e.g. it can be used in hospital waiting room, office or home. This architecture utilizes huge bandwidth capacity and use a centralized point known as Access Point (AP). Other type is ad-hoc based architecture uses multiple APs which assist sensor nodes to forward information's to various medical centres. To forward receive information's to the central server, LPU uses 2G, 3G and GPRS mobile phone or WLANs technologies to arrive at an internet AP or home gateway. The functions of LPU are generally data collection, processing, aggregation and communication. Finally, tier-3 (beyond-BAN) connects a LPU to the internet. A communication gateway is used to make a wireless connection between tier-2 and tier-3. The important component of teir-3 is the medical database that retains users' profile and medical history, and doctors use this database to get various information's about patients. In the case of any abnormality occurred, an alarm is notified to the doctor or patient through live call, SMS or email and an immediate response is taken place by doctor or other caretaker contacting the person via videoconferencing, email, SMS or uses other source of communication available facility to diagnose the health issue. In the case of ambulance is needed, a ambulance is sent to the desired location, patient is taken out of that particular location and meanwhile the emergency personal may access all the important required data from the central medical database in order to treat the patient.

The rest of paper is organized as follows: Section 2 describes different WBAN technologies. Section 3 gives the overview of common security attacks in WBAN. Section 4 is the important section of the paper which discusses different authentication methods and make security features compassion shown by table 1 and Section 5, the final section concludes our work.

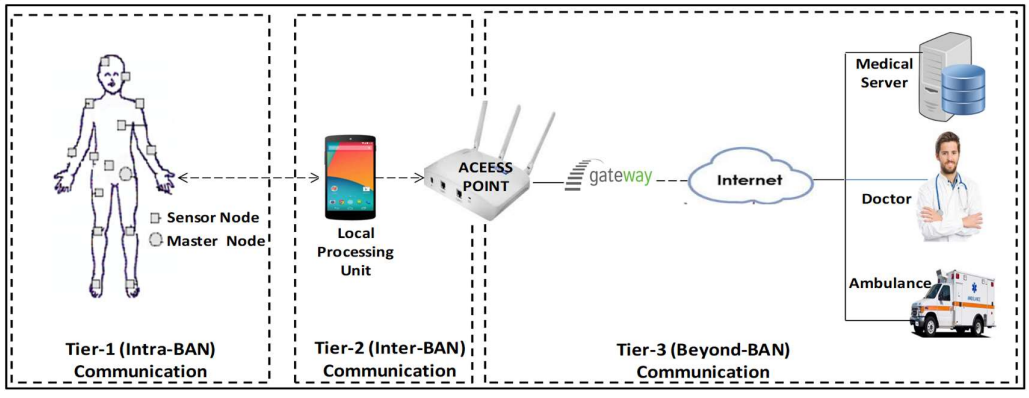

Figure 1: WBAN 3-tiers architecture

2. WBAN Technologies

Various technologies are used at various tiers or levels in WBAN to provide various functions and some of the main technologies are as follow [2, 3].

2.1. Bluetooth

It is more secure short range wireless communication technology, and each device has the ability to make a connection with seven other devices at the same time within single piconet. In a single piconet one device is working as master and other is working as slaves. The master device is used for synchronizing slaves by using system clock. Bluetooth technology allows different Bluetooth enabled devices of different vendors to connect and freely share simple, voice and video data. It supports frequencies from 2.4 to 2.485 GHz band using frequency hopping among 79 1MHz channels at the rate of 1600 hops per second and covers about distance of 30 feet (10 meters). Today many versions of this technology are available in the market. The initial versions of this technology have speed below 1Mbps, and the new versions are capable of supporting speed up to 25Mbps.

2.2. Bluetooth low energy (BLE)

BLE is more suitable wireless communication technology for health-monitoring applications because it consumes very little amount of power by using low duty cycle operations. It was originally intended for wireless connection among small devices to mobile terminals. It is expected that this technology will provide speed up to 1Mbps. BLE is utilizing smaller number of channels for pairing devices, synchronization is very fast and takes only few milliseconds as compared to Bluetooth which normally takes few seconds. It is useful for critical WABN applications such as emergency response and alarm generation etc. The features like small energy consumption, low latency and normal speed makes it suitable choice to be used between sensor nodes and AP.

2.3. ZigBee and 802.15.4

This is simple and less expensive wireless communication technology for low power devices than Bluetooth technology and it is intended to meet the requirements of remote monitoring and control, and sensor networks. ZigBee technology is based on physical and medium access control (MAC) layers described by IEEE 802.15.4 for low data rate. The major advantages of using this technology are ease of installation, reliable data transfer, extremely low cost, short-range operations, and support a long lasting battery power etc while utilizing an uncomplicated and flexible protocol. ZigBee is high data rate technology, can support speed maximum up to 250 Kbps and that is enough to meet individual's needs. This technology can be divided into two parts. The first ZigBee association designates application layers, defines application software, network and security layers. The second is IEEE 802.15.4 standard describes the physical and MAC layers. ZigBee enabled devices can operate in 868MHz, 915MHz and 2.4GHz bands. ZigBee is inappropriate choice for real time health-monitoring applications because it has very low speed that is just 250Kbps. Another issue of this technology when operating in 2.4GHz frequency band for health-monitoring applications is interference with WLAN transmission.

2.4. IEEE 802.11

Wi-Fi is short for "Wireless Fidelity" is based on IEEE 802.11 and the big advantage of this technology is its high-speed internet connections. Today devices like tablets, Smartphone and laptops have built-in Wi-Fi technology and it is good choice for transferring large amount of data wirelessly because it provides high speed connectivity, and it permits voice call, videoconferencing and video streaming. The only demerit of this technology is the high energy consumption.

2.5. IEEE 802.15.6

It is short-range, vastly consistent, support different data rates and low power wearable WBAN communication standard and it is the first WBAN standard which can support both medical and non-medical applications by using various frequency bands for data exchanging. IEEE 802.15.6 can support 256 sensor nodes per WBAN and sensor nodes have various priorities from high to low according to the

application requirements. The various kinds of Communication supported by IEEE 802.15.6 are ultra-wideband utilizes 3.1 to 11.2GHz, narrowband (NB) uses 400, 800, 900MHz and 2.3GHz and 2.4GHz bands, and human body communication (HBC) using the frequencies range inside 1050MHz. CSMA/CA or slotted Aloha access method is used for channel accessing and it provides great level of security because it defines three types of security schemes. Sometimes it speeds close to 10Mbps while at very low energy consumption. Although IEEE 802.15.6 standard can support many WBAN applications, but it may not be able to support applications those needed high quality video or voice communications.

2.6. Ultra-wideband (UWB)

UWB is a radio technology uses 3.1 to 11.2GHz frequencies bands for short range communication and it can provide high bandwidth. It is unlike spread spectrum technology because it transmits signals in a way that never allows interference with other transmission technologies when both using the same frequency at the same time. UWB can be useful for hospitals because it provides reliable mechanism for tracking users' locations. However, UWB cannot be suitable technology for wearable applications devices because of their complexity.

2.7. ANT

ANT protocol is low power and low speed proprietary wireless radio technology for E-health sensor networks, and it is open-source technology for mobile devices. It almost covers all kinds of topologies from plain peer-to-peer to very complex type of mesh topology. ANT is a good choice when lower power battery consumption is needed, and it can operate in 2.4GHz band provides speed of 1Mbps and using TDMA method to solve medium access or interference issues.

2.8. Zarlink

It is an ultra-low power radio technology. Zarlink technology has data speed up to 800Kbps and works in ISM (from 433 to 434MHz) and MICS (from 402 to 405MHz) frequencies bands. It is also an appropriate technology for E-health implant applications because it uses an ultra-low power, low frequency and has low data speeds.

2.9. Rubee

Rubee is similar to Bluetooth, Wi-Fi and ZigBee technologies but it supports low data rates and provides more security in harsh atmospheres because it does not need the line-of-sight communications for their functions. It can exchange data packet of size 128 bytes within a LAN region by using long wave magnetic (not radio frequency) signals and works in 131 KHz band. The main characteristics of Rubee are ultra-low power consumption, high level security, efficient transmission coverage (cover distance up to 50 feet) and long battery lifetime. Due to these characteristics, it is suitable option for WBANs applications.

2.10. Sensium

It is an ultra-power technology for E-health chronic disease supervision applications, and it is a competent technology for supporting ultra-low power monitoring of critical health parameters like blood glucose level, PH levels and ECG signals. Sensium technology can work in 900MHz frequency band and has data speed of 160Kbps.

Other WBAN technologies like ANT+, Z-Wave, Insteon, Wavenis, BodyLAN, Dash7, ONE-NET, EnOcean and Intra-Body Communication (IBC) are also available for different WBANs applications. Bans applications.

3. Common Type of Security Attacks in WBANs

Security is protecting data or other network resources from unauthorized access. The most important feature of a network is the security, and it is important for all kinds of networks to maintain a proper strategy for security in order to make it safe against various types of attacks. In this section I am discussing some important common security attack in WBAN [4].

3.1. Offline password guessing attack

An attacker needs a physical access to the system or device which has stored password file, first steal password contains file by copying the password file and then he/she finds the correct password.

3.2. Impersonation attack

In this type of attack, legal identity information is used by an attacker to cheat different WBANs participants.

3.3. Replay attack

Information's or data packets exchanged between two participants are intercepted by an attacker and after sometimes captured information's or data packets are sent back in the original form to the desired receiver.

3.4. Insider attack

An attack performed by an authorized user of the network is known as insider attack and this attack is performed by an authorized user for their own benefits.

3.5. Online password guessing attack

In this type of attack, an attacker login into the serve and tried all possible passwords to guess the correct password. Two types of online password guessing attacks are brute force and dictionary.

3.6. Modification attack

Captured data packets are completely or partly changed or removed by an attacker. These data packets modifications are done for illegal achievements and finally, the modified data packets are sent back to the desired receiver.

3.7. Man-in-the-middle attack

This attack allows an attacker to intercept the communication between two participants, the attacker can read and listen the important conversion and it is also possible that he/she can change the communication between two participants who think they are directly doing conversing with each other.

3.8. Denial of service (DoS) attack

This attack is more common and can be easily implemented on different WBAN participants. Generally, these types of attack are performed on limited resource-constrains devices such as it can be performed on sensor nodes in order to destroy their limited available resources like battery power by continuously forwarding malicious data packets.

3.9. Data disclosure attack

An attack performed by an authorized user of the network is known as insider attack and this attack is performed by an authorized user for their own benefits.

4. Important Instructions

Authentication is a procedure or method for verifying the identity of registered user ahead of permitting entry into the protected resources. It is not only important method in tradition networks, but it is equally or more important for E-health applications for maintaining both data confidentiality and integrity to achieve highly level security and privacy of user data. In this section, I will describe the most popular authentication methods use in WBAN.

4.1. Password based authentication method

The very basic and simple form of an authentication is the password-based authentication method. Password based authentication can be simply handled by all entities involved in the authentication

process of the network and this method is in use from very long time due to its easy implementation. F. Wei et al. [5] proposed a provably secure password-based anonymous authentication scheme for WBAN is based on low-entropy password and they have proved their authentication protocol security by using random oracle model. The proposed scheme not only achieves data confidentially and user privacy but also achieves strong anonymity. It is competent in terms of computation power as compared with the related proposed schemes in the paper. Proposed scheme provides features like mutual authentication, client anonymity, user intractability, no verification table, session key establishment, forward secrecy and attack resistance. J. Zhang et al. [6] presented an advance version of password authentication association IEEE 802.15.6 based on pre-shared short password between two parties to authenticate each other. A new master key is created between two parties on basis of pre-shard short password and one positive point of this scheme is that it reduces computational cost burden at the limited resource-constrained sensor nodes. This protocol is secure against security attacks like man-in-the-middle, offline-dictionary, impersonation and forward secrecy.

4.2. Smart card based authentication method

This method of authentication is using a smart card technology for authentication purpose. A smart card has an electronic chip that has microcontroller or other equivalent intelligence abilities with internal memory. Smart card based technology for authentication is most popular authentication technology for modern day's networks due to their storage and computational abilities. A card reader terminal is used to enter and read information's from the smart card and the terminal can be either physically wired or wirelessly connected to a network. N. Radhakrishnan et al. [7] proposed mutual authentication scheme on the smart card based authentication technology for Telecare Medical Information System (TMIS). Similar type of authentication scheme was proposed by Lee et al. for TMIS and claimed that their proposed system is more secure against well-known security attacks. However, according to N. Radhakrishnan et al. it suffers from offline password guessing attack and forgery attack and also claimed that it does not provide mutual authentication, forward secrecy and user anonymity. N. Radhakrishnan et al. have proved the security of their scheme by using well-known random oracle model and claimed that their scheme is more secure against well-known attacks like offline password guessing, replay, man-in-the-middle, forgery, stolen verifier and modification, Insider, and smart card loss. However, the proposed scheme has the disadvantage of using a little bit extra computational cost as compared to describe schemes in the proposed paper. C. T. Li et al. [8] introduced mutual authentication scheme for IoT-based medical applications is based on smart card based technology for authentication purpose. The proposed scheme has removed flaws associated with Liu-Chung's authentication scheme and claimed that Liu-Chung's scheme is suffering from password disclosure, replay, forgery, data disclosure, offline password guessing and stolen smart card attacks. C. T. Li et al. authentication scheme is not only providing user anonymity but also preventing attacks associated with Liu-Chung's scheme and proved the security of their scheme by using random oracle model.

4.3. Biometric based authentication method

The Biometric based authentication method is more competent authentication method than password and smart card based authentication methods and also it is not important for users to remember password for authentication purpose. This kind of authentication method uses physiological and/or behavioural features of the human body for user verification. Characteristics of human body like fingerprints, facial, voice and iris pattern etc. are used to authenticate a user. A. Arya et al. [9] proposed an improved remote user verification scheme for WBAN is the modified edition of Salam et al. scheme. It is using biometric based authentication method between senor nodes and a sink and thus way it removes flaws like insider, plain-text and stolen card verifier attacks associated Salam et al. authentication scheme for WBAN. The modified authentication edition scheme uses biometric based authentication through the fingerprint verification. R. Ali et al. [10] introduced a remote user authentication scheme for E-health is based on biometric based authentication method. This scheme is the advance version of Li et al. user authentication system for E-health and claimed that Li et al. scheme is vulnerable to some security attacks such as user identity and password guessing, user impersonation, privileged insider attack and smart card

stolen attack. The new proposed scheme is safe against many kinds of cryptography attacks and security is validated by random oracle model and BAN logic.

4.4. Multi-level authentication method

This authentication method is the combination of two or more authentication methods. Due to more than authentication methods, it is more secure method of user authentication and can resist against many types of network attacks. On the other hand, these methods of authentications are more complex and different from domain to domain. Q. Jiang et al. [11] authentication scheme is using the combination of password, smart card and biometrics for user authentication and is based on Islam et al. authentication scheme. Islam et al. claimed that their proposed scheme is more secure than other available scheme but Q. Jiang et al. said that their authentication scheme is still vulnerable to password validation during login issue, impersonation, and biometric template privacy leakage and offline password guessing attacks. X. Li et al. [12] proposed a multi-level authentication protocol for E-health using the combination of password, smart card and biometric based authentication methods. This scheme has examined He et al. proposed authentication protocol and find that their authentication protocol is wrong in session key agreement and authentication phase. Also, the protocol of He et al. may suffer from DoS attack, waste computational and communication costs unnecessarily because there is no wrong password detection method is available. X. Li et al. scheme not only eliminates different flaws associated with The et al. protocol but also it is more secure and efficient in the computation cost.

The security features comparison of authentication schemes of different well-known methods can be shown by table 1 and it is concluded that smart card based and multi-level authentication methods have more security features as compare to other authentication methods.

Table 1: Security features comparison

Security Features	F. Wei et al. [5]	J. Zhang et al. [6]	N. Radhakrishnan et al.[7]	C. T. Li et al. [8]	A. Arya et al. [9]	R. Ali et al. [10]	Q. Jiang et al. [11]	X. Li et al. [12]
	PB	PB	SCB	SCB	BB	BB	M-LB	M-LB
A1			√	√		√	√	√
A2		√				√	√	
A3			√	√		√	√	√
A4			√		√	√	√	√
A5			√	√		√		√
A6	√		√	√		√	√	√
A7	√					√	√	
A8	√		√	√		√		√
A9							√	
A10							√	
A11			√				√	
A12						√	√	
A13		√	√				√	
A14							√	
A15	√		√	√	√		√	√
A16	√	√	√				√	
A17	√							
A18		√						

A19			**√**					
A20			**√**	**√**				**√**
A21			**√**		**√**		**√**	**√**
A22			**√**					**√**
A23				**√**				
A24				**√**				
A25					**√**			
A26								**√**

Legend: Yes (√) , Password Based (PB), Smart Card Based (SCB), Biometric Based (BB), Multi-Level Based (M-LB),A1 resists to identity and offline-password guessing attacks, A2 resists to user impersonation attacks, A3 resists to replay attack, A4 resists to insider attack, A5 resists to smartcard stolen attack, A6 preserves user anonymity, A7 resists to user intractability attack, A8 provides session key establishment/verification, A9 online password guessing attack, A10 biometric template privacy, A11 modification attack, A12 resists to server impersonation attacks, A13 Man-in-the-middle attack, A14 denial of service attack, A15 mutual authentication, A16 perfect forward secrecy, A17 no verification table, A18 offline-dictionary, A19 local password verification, A20 forgery attack, A21 stolen verifier attack, A22 User-friendliness, A23 provision of efficient login phase, A24 data disclosure attack, A25 plain-text attack, A26 wrong password detection attack.

5. Conclusion

WBANs providing different healthcare applications are in initial stage of development nevertheless offer important commitments at various levels. This research paper is planned in a manner to discuss some important communication technologies, security concepts and authentication methods, which can be useful for truly understanding of WBANs. Section 2 of the paper discussed different communication technologies, and their understanding might be helpful during the WBANs installation process. During this paper, I also discussed most common WBANs security attacks which might be helpful for developers for introducing new secure and mutual authentication protocols. In the last section, we have reviewed most common authentication methods and popular protocols used in WBANs and finally did the security features comparison of these protocols in order find out the best method of authentication.

References

[1] Nourchène Bradai, Lamia Chaari Fourati and Lotfi Kamoun, "WBAN data scheduling and aggregation under WBAN/WLAN," International Journal on Ad Hoc Networks, vol. 25, no. Part A, pp. 251-262, November 2014.

[2] Rim Negraa, Imen Jemilia and Abdelfettah Belghitha, "Wireless Body Area Networks: Applications and technologies Communications," in The Second International Workshop on Recent Advances on Machine-to-Machine, 2016, pp. 1274-1281.

[3] Mohammad Ghamari, Balazs Janko , R. Simon Sherratt and William Harwin, "A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments," Internation Journal on Sensors, vol. 16, no. 6, p. 831, June 2016.

[4] Shikha Pathania and Naveen Bilandi, "SECURITY ISSUES IN WIRELESS BODY AREA NETWORK," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 1171-1178, April 2014.

[5] Fushan Wei , P. Vijayakumar , Jian Shen , Ruijie Zhang and Li Li , "A provably secure password-based

anonymous authentication scheme for wireless body area networks," International Journal on Computers and Electrical Engineering, vol. 65, pp. 322-331, April 2017.

[6] Jie Zhang, Xin Huang, Paul Craig, Alan Marshall and Dawei Liu, "An Improved Protocol for the Password Authenticated Association of IEEE 802.15.6 Standard that Alleviates Computational Burden on the Node," MDPI submitted to Symmetry, pp. 1-14, November 2016

[7] Niranchana Radhakrishnan and Marimuthu Karuppiah, "An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems," Informatics in Medicine Unlocked, https://doi.org/10.1016/j.imu.2018.02.003, pp. 1-11, February 2018.

[8] Chun-Ta Li, Tsu-Yang Wu, Chin-Ling Chen, Cheng-Chi Lee and Chien-Ming Chen, "An Efficient User Authentication and User Anonymity Scheme with Provably Security for IoT-Based Medical Care System," MDPI Sensors, doi:10.3390/s17071482, pp. 1-18, June 2017.

[9] Aakriti Arya, Chaitanya Reddy and TrupilLimbasiya, "An Improved Remote User Verification Scheme in Wireless Body Area Networks," Procedia Computer Science, vol. 113, pp. 113-120, 2017.

[10] Rifaqat Ali and Arup Kumar Pal, "Cryptanalysis and Biometric-Based Enhancement of a Remote User Authentication Scheme for E-Healthcare System," Arabian Journal for Science and Engineering, https://doi.org/10.1007/s13369-018-3220-4, pp. 1-16, March 2018.

[11] Caffeine Qi Jiang, Fushan Wei, Shuai Fu, Jianfeng Ma, Guangsong Li and Abdulhameed Alelaiwi, "Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy," Nonlinear Dyn, DOI 10.1007/s11071-015-2467-5, pp. 1-17, October 2015.

[12] Xiong Li1, Jianwei Niu, Saru Kumari, Junguo Liao, Wei Liang and Muhammad Khurram Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," SECURITY AND COMMUNICATION NETWORKS, vol. 9, no. 15, pp. 2643-2655, October 2016.