A Review on WBAN Security Application to Ensure Confidentiality and Integrity

Ashish Kumar[1], Akhilesh Bansiya[2]
[1]MTech Scholar, [2]Assistant Professor
[1]Department of Computer Science Engineering, Vedica Institute of Technology, Bhopal, India
[2]Department of Computer Science Engineering, Vedica Institute of Technology, Bhopal, India
[1]ashu07128@gmail.com [2]akhilesh2483@gmail.com

* Corresponding Author: Ashish Kumar Manuscript Received: Manuscript Accepted:

Abstract: Wireless Body Area Network (WBAN) is a new technological trend which provides remote monitoring and collection mechanism for healthcare record data of patients using wearable sensors. A high level of system safety and privacy is widely recognised as an important part of protecting these data when used by health professionals and during storages to ensure that the records of patients are kept safe from the risk of the intruder. This study provides a cryptographic survey on framework for WBANs implementations. Hence there is an important interest to address security and privacy problems in WBANs.

1. Introduction

A body area network (BAN) is a network of wireless sensors mounted in, on and across the body that is short-range. It offers short distance data communication, limited to a few metres range. The basic concept is shown in figure 1 below. This new network type uses electronically implanted and wearable circuits. It performs very useful functions and features in comfortable, discreet configurations which operate at incredibly low energy and offer truly outstanding safety.

The number of computing devices used by a user, a desktop, desk, Smartphone, mobile phone and a person using more products daily has risen noticeably. The figures have increased substantially. Certain devices are inserted in citizens to evaluate different body and symptoms and the climate.

The sensor nodes are located directly on or under the person's body to measure such parameters such as, body activity, electrical cardiogram (ECG), temperature, blood glucose, blood pressure, biosensor, pulse rate and breathing rate speeds. The sensor nodes are mounted directly under or at the body. This sensors are designed to satisfy the specifications of ends for particular purposes. An EEG tracker, for instance, was intended for brain electric activity control. Another example is the ECG sensor developed for cardiac activity control.

The IEEE 802.15.6 proposed WBAN nodes taxonomy based upon their implementation in the enterprise and their position in the network.

Each node could be categorised according to the form in which it is implemented:

- Implant node: This node type is planted below the skin or within the tissue of the body.
- Body Surface Node: is located either on the surface of the body, or is 2 cm from the body.
- • Remote Node: Not in contact with the human body but a few centimetres to five metres out from the human body. According to their position as the network coordinator, there are three node forms in WBANs; this node serves as a portal to the outside, another WBAN and a trust hub. The WBAN coordinator, the PDA, is able to connect with all other nodes.
- End Nodes: These types of nodes are limited to the programme, but are not capable of sending signals to several endpoints. Relay: These domains serve medium nodes and are known as relays. A relay network comprises of nodes and relay messages from parents and children. When a network is at the base, all information submitted to be transmitted through other checkpoints and is required before it enters the PDA. These node forms may also feel information from sensors.

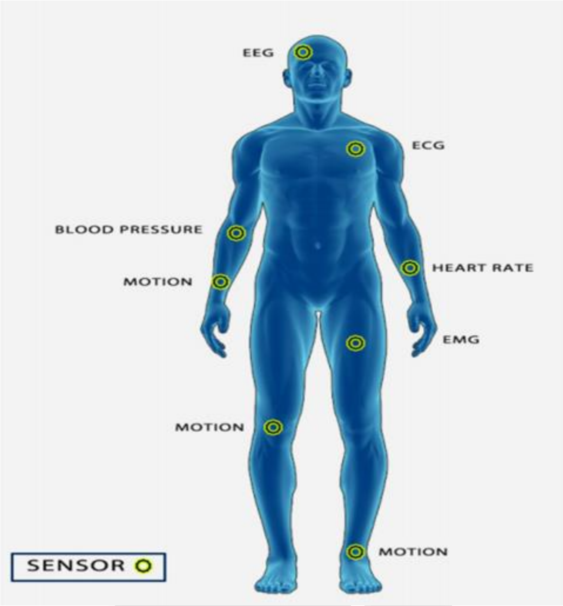

Figure 1: WBAN sensors

The location of the sensors interacting via a WBAN is normally seen in Figure 1. It can also be used in a range of other areas and technologies such as emissions monitoring, physiological and wellbeing monitoring, contact with human machine, education and entertainment [5] [6].

2. BAN Applications

User Authentication for Notebook Computers

A BAN may be used to authenticate a Notebook Computer owner in order to secure property and privacy. A small gadget with an embedded BAN feature is worn by the operator as a 'smart watch.' As the user hits the device touch pad, the ID data is retrieved by the integrated controller in the touchpad and the access control information is checked, allowing login.

Room Entry Control

If you have a BAN communication system, no key or pass code is required to reach a restricted access area. The banner transmits the person's ID information to a network bridge linked to the button while their hand is positioned close or touching the door buckle. After this, the information is passed to the access control system and authentication server. Then the machine unlocks the door lock such that the authorized person enters the room correctly.

Fitness Monitoring

When a Body Area Network acts as a pulse sensor during exercises, wellbeing and protection are improved. A detector surface of the skin follows the heartbeat of the human and sends the data to the intelligent rear watch. By watching the watch monitor, the user will check the pulse rate in real time.

3. Security Issues In WBAN

The following define the main protection and privacy criteria for the protection of a WBAN device and its thorough adoption by its users:

Data Confidentiality

Confidentiality of data refers to the security of sensitive exposure data, which is regarded in a WBAN as the main issue. Given that WBAN nodes used in medical contexts are meant to relay delicate and confidential knowledge regarding the state of the welfare of the patient, their details must also be shielded from unwanted, life-threatening access to the patient. These critical data, which can be transported "overheard," can harm the user, the provider or even the device itself during transmission. Encryption will enhance security of this sensitive data by exchanging a mutual key between protected WBAN nodes and their coordinators on a secured communication channel.

Data Integrity

User authentication is the security, authenticity and continuity of the content of a message. It refers both to individual messages and to messages streams. Data security does, however, not shield information from external changes so data can be altered illegally if data is passed to an unprotected WBAN as an opponent that can quickly manipulate knowledge of the client before meeting the system manager.

In particular, amendments can be made by merely integrating a few fragments, modifying data in a packet and forwarding the packet to the PS. This interception and alteration will lead in severe cases to serious health issues and death. Acquiring authentication protocols must also not allow the details available and modified by a possible adversary.

Data Correctness

Information correctness strategies can efficiently ensure that data privacy and secrecy are safeguarded against an opponent's capturing and replay of older information and mislead the WBAN coordinator. It guarantees the non-recycling of old data and that the frames are correct. There are actually two forms of data freshness: solid delay guarantees in addition to frame order; and weak freshness, restricted to frame orders, but without any warranty for delay. For synchronization strong freshness is required when the beacon is sent to the WBAN coordinator, and for WBAN nodes with a low-flow duration weak freshness is used.

Data Authentication

Data authentication may be essential for medical and non-medical applications. Nodes within WBAN must also be able to check that the knowledge is distributed from an established confidence centre rather than from an imponer. The messaging authentication code (MAC), by exchanging an unknown key, is then determined by Network and coordinator nodes for all details. Check the MAC code correctly, guarantees that the message is carried by a trustworthy node to the network coordinator.

Accountability

It is important to protect patient privacy records for healthcare professionals in the area of medicine. If a contractor does not protect or worse, it violates its duty, so he or she must be kept liable to avoid future abusses.

Flexibility

The versatility to designate AP medical data controls in a WBAN is required. For example, a person who does not necessarily have authorization may be allowed, on request, to interpret patient data in the event of an emergency.

4. Related Work

Altaf et al. [1] proposed a lightweight and secure searching scheme over encrypted data for e-Health environment. We make use of hybrid encryption scheme including symmetric encryption and optimized identity-based encryption (IBE) scheme to ensure data confidentiality over communication channel and for enhancing cloud privacy.

Jiang et al. [2] presented an optimal heart rate-based key agreement scheme to ensure secure communication between legitimate devices. The proposed key optimization scheme uses a fuzzy commitment with low latency in extracting features. In addition, the parameter optimization algorithm (PDPO) based on physiological distribution is proposed to adaptively determine the optimal protocol parameters for individuals, which ensures not only excellent and stable performance, but also safety. of the diagram. Finally, we prototype our protocol and conduct experiments on various topics to evaluate its safety and performance. Our results show that the proposed protocol negotiates the key safely and quickly, has low energy consumption and is suitable for practical applications.

Ivanciu et al. [3] proposed an original solution to protect the transmission of recorded data from sensors in a body wireless network using the ECG signal and named data networks. Our contribution is twofold: first, we use the features inherent in these networks to safely transfer sensitive health-related data (of a normal patient or driver) to the cloud, then we pass it on to stakeholders such as these such as doctors. Second, our approach uses the characteristics of the ECG signal (robustness against attack, universality and vitality detection) to encrypt this data and provide a simple and fast authentication mechanism between devices in the body area network.

Kim et al. [4] proposed a secure and lightweight mutual authentication and key establishment scheme using wearable devices to resolve the security shortcomings. The proposed scheme can be suitable to resource-limited environments.

Jiang et al. [5] proposed an optimized system for deep distributed learning which includes a cloud server and several smartphones with IT functions. Each device is used as a personal mobile data hub to enable mobile computing while protecting data protection. The proposed system stores private data locally on smartphones, shares the settings formed and creates a global consensus model. The feasibility and usability of the proposed system are assessed through three experiments and the related discussion. Experimental results show that the proposed distributed deep learning system can reconstruct the behaviour of centralized training. We also measure the network traffic accumulated in different scenarios and demonstrate that the partial parameter sharing strategy not only preserves the performance of the trained model, but can also reduce network traffic.

Pandey et al. [6] presented a state-of-art survey about various features of BAN specifically communications, sensors, applications, requirements, standards & protocol, and security aspects.

Meng et al. [7] proposed a new anonymous mutual authentication and key agreement scheme, with untraceability and session key forward secrecy. The scheme uses as few hash functions and XOR operations as possible for authentication and key agreement. It is officially proven to be correct through BAN logic, and its security has been verified by using the Automated Validation of Internet Security Protocols and Applications (AVISPA) as well.

Nezhad et al. [8] proposed an approach for faulty measurements detection in order to make alarming of emergency situations more precisely. The proposed approach is based on decision tree, threshold biasing and linear regression. Our objective is to detect single and multiple faults in order to reduce unnecessary healthcare intervention. The proposed approach has been applied to real healthcare dataset. Experimental results demonstrate the effectiveness of the proposed approach in achieving high Detection Rate and low False Positive Rate. The ability of this algorithm to detect single and multiple anomalies make it more reliable for medical emergency use.

Shim et al. [9] showed that L-OOCLS is entirely broken: anyone can forge certificateless signatures on any messages for any identities from only publicly known information. Thus, the scheme is trivially insecure against the type I adversary who can replace user public keys and the type II adversary who knows the master secret key. Our result shows that their security proofs are also flawed.

Shanthapriya.R et al. [11] ECG-Based Secure Healthcare Monitoring System in Body Area Networks. Polynomial based curve is generated and steganography technique has been used for secure health monitoring which provides data confidentiality and authentication to maintain the privacy of a patient.

5. Conclusion

The Wireless Body Area Network is an uprising future in healthcare sector. In WBAN scenario, data security and privacy is a serious issue of concern. In this paper, secure frameworks are surveyed that are used to provide secure access control and for ensuring integrity is employed for scalability and low computation cost. Hence, current research efforts will direct in future for implementation of secure framework for WBAN.

References

[1] F. Altaf, M. Aditia, E. Saini, B. Rakshit and S. Maity, "Privacy Preserving Lightweight Searchable Encryption for Cloud Assisted e-Health System," 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 2019, pp. 310-314.

[2] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen and D. Wu, "Optimized Fuzzy Commitment based Key Agreement Protocol for Wireless Body Area Network," *IEEE Transactions on Emerging Topics in Computing*, 2019.

[3] I. Ivanciu, L. Ivanciu, D. Zinca and V. Dobrota, "Securing Health-Related Data Transmission Using ECG and Named Data Networks," *IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, Paris, France, 2019, pp. 1-6.

[4] M. Kim, J. Lee, S. Yu, K. Park, Y. Park and Y. Park, "A Secure Authentication and Key Establishment Scheme for Wearable Devices," *International Conference on Computer Communication and Networks (ICCCN)*, Valencia, Spain, 2019, pp. 1-2.

[5] H. Jiang, J. Starkman, Y. Lee, H. Chen, X. Qian and M. Huang, "Distributed Deep Learning Optimized System over the Cloud and Smart Phone Devices," *IEEE Transactions on Mobile Computing, 2019*.

[6] I. Pandey, H. S. Dutta and J. Sekhar Banerjee, "WBAN: A Smart Approach to Next Generation e-healthcare System," *International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2019, pp. 344-349.

[7] X. Meng, J. Xu, W. Liang and K. Li, "An Anonymous Mutual Authentication and Key Agreement Scheme in WBAN," *Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Washington, DC, USA, 2019, pp. 31-36.

[8] M. M. Nezhad and M. Eshghi, "Sensor Single and Multiple Anomaly Detection in Wireless Sensor Networks for Healthcare," *Iranian Conference on Electrical Engineering (ICEE)*, Yazd, Iran, 2019, pp. 1751-1755.

[9] K. Shim, "Universal Forgery Attacks on Remote Authentication Schemes for Wireless Body Area Networks Based on Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9211-9212, Oct. 2019.

[10] Shanthapriya.R, Vaithianathan.V, “ECG-Based Secure Healthcare Monitoring System in Body Area Networks”, *International Conference on Biosignals, Images and Instrumentation (ICBSII)*, 2018.