Security in Wireless Body Sensor Network

Subjects: Computer Science, Information Systems

Contributor: Najm Us Sama , Kartinah Zen , Mamoona Humayun , NZ Jhanjhi , Atiq Ur Rahman

Wireless body sensor network (WBSN) is a wireless communication that might enable 24/7 patient monitoring and health findings through the Online platform. Although BSN design is becoming simpler, building a secure BSN seems to be more challenging than designing conventional solutions.

Body sensor network Security mechanisms Security solutions

1. Introduction

Because individuals worldwide are concerned about their health, the body sensor network assists with collecting essential body details of the individual through sensing devices. Although the wireless body sensor network (WBSN) has greatly interested in environmental and medical applications, safety and privacy are still significant issues [1]. Because it is distant, there are possibilities for various challenges such as a lack of energy, a degraded platform's capability, and fake concern. Furthermore, the data shared through the wireless body sensor network (WBSN) is subject to various harmful threats [2].

While the patient's status is transferred between the physician and the patients, any intruder can intercept incoming packets between traversing via wireless signals and rebuild the results. This could put the patients' lives in danger. Any patient with a socially unacceptable condition should have their details handled carefully. As a result, people must ensure that the confidentiality and anonymity of any type of information are protected and transmitted securely. As a result, different intrusion prevention techniques are needed to protect against these assaults. The guarantee of the security and safety of the information obtained has been critical. According to experts, BSN has been the target of numerous assaults in recent decades, ranging from specific functions to the overall network. As a result, experts continually develop new adaptations and combinations of traditional security procedures to defend against such assaults. Security is a significant issue for BSNs, according to surveys. Similarly, several studies [3][4][5] have revealed a general shortage of studies in BSN protection.

2. Security in Wireless Body Sensor Network

A patient’s medical state can be monitored using telemonitoring systems. The rising expense of medical services, the increasing elderly population, and the rise in chronic disease patients worldwide are driving up demands for alternatives in the healthcare sector. Because of these challenges, conventional health care cannot achieve the needed flexibility. As a result, high-performance, low-cost, and appropriate care solutions are required. The Wireless Body Sensor Network (WBSN) is a wireless platform that allows sensors attached to a patient’s body to communicate to monitor the body's essential parameters and surroundings. The use of wireless sensor nodes in public healthcare tracking opens doors for delivering superior patient care. For example, at-risk individuals with a background of heart problems or aged individuals who live independently can be monitored using various sensors. These sensors allow physicians to diagnose diseases more efficiently by providing ongoing, long-term tracking in an invisible manner [6]. A body sensor network, or BSN, is a collection of sensors placed on the person's body to gather physiological signals [7].

In recent research and industry, the design and implementation of such WBSN approaches to health monitoring have gotten a lot of interest. This focus is primarily driven by the high cost of health care and recent advances in the manufacturing of micro health applications and new technologies like the Internet of Things (IoT), contributing to the 5G's main obstacles. An explicit approach to handling the basic software design and validation should be advantageous for building and maintaining such systems. At various spots, the sensors observe and compare the circumstances. Environmental (e.g., pollution levels, weather, and moisture) and essential human functions are typical examples (e.g., heart and brain signals). A WSN can sense, process, and communicate. To acquire data on the centralized environment, diverse WSN-based monitoring apps have been created in many application sectors. Defense applications [7], global warming tracking applications [8], apps in submarine networking [9], and apps in health monitoring [10] are only a few examples.

Regardless of these applications, security has become a significant challenge. The system must ensure the security and privacy of the collected individual health data. Decomposing activity results in an increase in the platform's flaws and renders it more complex to implement the security architecture. This has resulted in a slew of BSN privacy discussions, the most important of which are discussed and taken in context hereunder [11].

The developers [12] suggested a secure platform based on heart rate frequency. They used the measurements of the inter-pulse periods to build binary patterns from the beats. In 8 seconds, they generated a 128-bit sequence using ECG records from the MIT-BIH Arrhythmia dataset. As a result, they could minimize the time it took to generate a random sequence of bits. The fundamental issue with employing a heartbeat as a security measure is inconsistent over time. The person's health records should be protected to avoid information misuse, and the patients should be able to reach the practitioner at the appropriate time and without delay. SEKBAN (Secure Key Management in WBAN) is an innovative approach that addresses security issues at three stages. By constructing keys relying on the ECG signal, this suggested technique protects the data's privacy [13].

Depending on the ECG monitor, the researchers offer [13] a body sensor network encryption and user authentication (BSN-EUA) approach. The BSN-EUA method provides fingerprint recognition for identity verification, and all of a person's health-related activities are logged on the handset. The descriptive properties of the electrocardiogram (ECG) are employed as a recognized fingerprint feature all through the access control mechanism. When modest alterations are required to modify the cryptography technique on the sensor's side, rapid social security protocols are given across all approved sensors. The research results reveal that the proposed method meets the required privacy standards. The authors in [14] presented a symmetric security technique for WBAN that uses the ECG wave to produce and deliver the secret key. WBAN nodes should sense the ECG data using a synchronization approach to make the security key. The suggested method's stability is demonstrated using formal and informal security assessments.

Any breach would not only harm the patients' security, but it might also put their lives at risk. For example, providing physicians with a misleading ECG sensor readout may result in inappropriate actions that are potentially hazardous to patients. When a mechanical insulin pump gets a faulty or corrupted signal, it may deliver an excessive amount of insulin into the patient's veins. WBAN is vulnerable to a wide range of assaults, from interior to exterior, passive to active.

In terms of addressing potential security issues, all of the studies listed above reference security measures that range from conventional security mechanisms like encryption and authentication to Intrusion Detection Systems (IDSs) and Trust Management Solutions (TMSs). For WBANs to be a success and be widely adopted, developers must focus on security solutions and authentication mechanisms for data and services.

3. Conclusions

EHealth is becoming a popular issue not only in the science community, but also in the manufacturing and commercial worlds. Information and communication technologies, which are both new, have a lot of capability to make the public healthcare platform better. There are a few problems with a digitalized healthcare system, like security worries, system unscheduled downtime, and loss of security for patient information. With the aid of technology, WBSN clients can get to their body sensor data and other resources from all over the world. It will assist reduce the cost of diagnosis, improve services, give better analytical reports, and speed up the process of getting care. But although there are a range of advantages, data security and privacy were still major concerns.

But there is still a big necessity to find better and more creative ways to deal with the growing sophistication due to rapid development and advancement of wireless sensor networks used in vital applications now and in the coming decades.

References

1. Oleiwi, S.S.; Mohammed, G.N.; Albarazanchi, I. Mitigation of packet loss with end-to-end delay in wireless body area network applications. Int. J. Electr. Comput. Eng. 2022, 12, 460.
2. Liu, Q.; Mkongwa, K.G.; Zhang, C. Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. SN Appl. Sci. 2021, 3, 1–19.
3. Karchowdhury, S.; Sen, M. Survey on attacks on wireless body area network. In International Journal of Computational Intelligence & IoT, Forthcoming; SSRN: Rochester, NY, USA, 2019.

4. Roy, M.; Chowdhury, C.; Aslam, N. Security and privacy issues in wireless sensor and body area networks. In Handbook of Computer Networks and Cyber Security; Springer: Berlin/Heidelberg, Germany, 2020; pp. 173–200.
5. Asam, M.; Ajaz, A.; Jamal, T.; Adeel, M.; Hassan, A.; Butt, S.A.; Gulzar, M. Challenges in wireless body area network. Int. J. Adv. Comput. Sci. Appl. 2019, 10.
6. Yoo, J.; Cho, N.; Yoo, H.-J. Analysis of body sensor network using human body as the channel. In Proceedings of the ICST 3rd International Conference on Body Area Networks, Princeton, NJ, USA, 13–15 March 2008; CiteseerX: Princeton, NJ, USA, 2008.
7. Tan, C.C.; Wang, H.; Zhong, S.; Li, Q. Body sensor network security: An identity-based cryptography approach. In Proceedings of the First ACM Conference on Wireless Network Security, Alexandria, VA, USA, 31 March–2 April 2008.
8. Pahuja, R.; Verma, H.; Uddin, M. A wireless sensor network for greenhouse climate control. IEEE Pervasive Comput. 2013, 12, 49–58.
9. Mansour, A.; Leblond, I. Ecosystem monitoring and port surveillance systems. AIAAS Adv. Appl. Acoust. 2013, 2, 91–111.
10. Reyer, M.; Hurlebaus, S.; Mander, J.; Ozbulut, O.E. Design of a wireless sensor network for structural health monitoring of bridges. In Wireless Sensor Networks and Ecological Monitoring; Springer: Berlin/Heidelberg, Germany, 2013; pp. 195–216.
11. Oh, S.-R.; Seo, Y.-D.; Lee, E.; Kim, Y.-G. A comprehensive survey on security and privacy for electronic health data. Int. J. Environ. Res. Public Health 2021, 18, 9668.
12. Pirbhulal, S.; Zhang, H.; Wu, W.; Mukhopadhyay, S.C.; Zhang, Y.-T. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. IEEE Trans. Biomed. Eng. 2018, 65, 2751–2759.
13. Sivasangari, A.; Ajitha, P.; Gomathi, R. Light weight security scheme in wireless body area sensor network using logistic chaotic scheme. Int. J. Netw. Virtual Organ. 2020, 22, 433–444.
14. Sammoud, A.; Chalouf, M.A.; Hamdi, O.; Montavont, N.; Bouallegue, A. A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. Comput. Secur. 2020, 96, 101838.