International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Design an Algorithms for Body Sensor Network Architecture for Dynamic WBAN Scenarios

Mr. Dhiraj Sanjay Kalyankar [1], Dr. Ajay R. Raundale [2]

Submitted: 10/01/2024 **Revised**: 16/02/2024 **Accepted**: 24/02/2024

Abstract: Data security and reliable transmission are both complicated by the ever-changing nature of WBAN settings. The goal of this study is to develop and test algorithms for safe and dependable data transfer in the ever-changing settings of WBANs. The research examines the relevance of the most important security needs across a variety of use cases, such as data confidentiality, authentication, integrity, and freshness. In this study, we compare and contrast five distinct cryptographic algorithms developed for different use cases: hybrid encryption, erasure coding, trust-based routing, blockchain-enhanced transmission, and cognitive radio networks.

Keywords: *WBAN, environments, scenario, application, cryptographic algorithms*

1. Introduction

Since WBAN seems to be the wave of the future for wireless personal networks, it is one of the most researched topics in wireless communication. The nodes of WBAN are small biological sensors that may be implanted in the body or worn by the user to keep tabs on their health and wellness at all times. There are several possible applications for WBANs, such as in the medical area, physical rehabilitation, the entertainment industry, and the military. Because of this diversity of applications, Quality of Service (QoS) is especially crucial in terms of data throughput, dependability, energy usage, latency, etc. In addition, the peculiar channel characteristics and complicated deployment circumstances make it seem that maintaining transmission reliability in the context of WBAN systems is more challenging than in conventional Wireless Sensor Networks (WSNs). Additionally, battery capacity and Specific Absorption Rate (SAR) impose considerable constraints on power consumption and transmission power. There are several problems that develop as a consequence of all these factors, including transmission reliability and energy efficiency. In order to simulate the WBAN channel, various research have focused on developing analytical formulations.

In the dynamic WBAN scenarios investigated for this thesis, however, the complexity of the environment and the presence of the human body may make the use of mathematical models to create WBAN channels impractical or incorrect. In order to round out the study, it is essential to characterize and simulate the WBAN channel in a way that is both realistic and practical. Since wireless channels in WBANs are inherently dynamic and QoS requirements vary widely among applications, a static design for the transmission system is insufficient. To combat transmission issues in WBANs, several adaptive transmission solutions have been proposed in recent years.

These adaptive methods take into account the state of the channel or the requirements of the application to improve crucial transmission properties including transmission power level, duty cycle, and slot scheduling. In the same vein, Network Coding (NC) technology is getting a lot of attention since it has the potential to revolutionize the industry by fully capitalizing on the broadcast nature of wireless networks. Thanks to NC technology included in nodes, packets (or symbols) may be encoded or mixed before being sent. In recent years, a plethora of alternative NC approaches for WBANs have been introduced. Despite NC's success in other areas, its implementation in WBANs is still in its infancy, with most current research focusing on modifying existing NC schemes designed for generic WSNs rather than establishing new techniques that take into account the unique limits and nuances of WBANs.

Ambulatory wireless patient monitoring is the gold standard for preventive medicine. Mobile therapy is becoming in prominence, especially for the hypothetical cardiac patient. Thanks to developments in ICT and a thorough grasp of the body's physiology, rapid improvement is on the horizon in both diagnosis and therapy. The state of the art has the potential to enhance outpatient care. There may be substantial cost benefits to providing patient care outside of a hospital. Online/real-time surveillance may give the same degree of protection as permanent hospital isolation for victims to avoid future health hazards [1]. The need of prompt and timely inspection to protect the autonomy of the elderly is growing as the population of individuals over 65 continues to rise. Thanks to ongoing online monitoring, specialists can react rapidly to any emergencies or changes in the

[1] *Dr. A. P. J. Abdul Kalam University, Indore, M. P ,India*
ORCID ID : 0009-0006-0590-7818
[2] *Dr. A. P. J. Abdul Kalam University, Indore, M. P ,India*
ORCID ID : 0000-0000-0000-0000
* *Corresponding Author Email: dhiraj.kalyankar50@gmail.com*

victim's condition. Care that may be provided online, lasts for a long time, and is wirelessly targeted is of critical importance for cardiac patients. The data it offers may be particularly useful for long-term valuation and preventive diagnostics, two areas that put a premium on observable trends and signal patterns.

2. Literature Review

Subramanian, Kanaga Suba Raja et.al (2012). A malicious user on a WBAN might potentially reveal private information about patients, such as their vitals and identification numbers, by exploiting security flaws like wormholes and spoofing. Power and mobility issues, which might result in frequent changes to network design, further complicate efforts to ensure reliability. Most of the publications in the state-of-the-art WBAN literature focus on reliability without considering security. In this study, we provide a consolidated approach to ensuring the integrity and dependability of data transfers in WBAN. The proposed architecture includes a body area network (BAN) coordinator in addition to direct and relay nodes. The BAN coordinator and nodes may safely exchange data thanks to encryption and Message Authentication Code (MAC) keys. Whether a sensor node sends data directly to the BAN coordinator or goes via a relay node depends on its battery life and signal-to-noise ratio. The process of selecting the node to act as a relay is also secure. Using simulation findings, we show how the new technique is more reliable than the present strategy.

Elias, Jocelyne et.al (2013). In this study, we provide a robust topology design and provisioning approach for Wireless Body Area Networks (named RTDP-WBAN) that takes patient mobility into account while still providing the robust data transmission essential to suit the needs of healthcare applications. To do this, we first propose a three-dimensional coordinate system for pinpointing relay-sensor node positions independently of the user's position or orientation. A digital spine is constructed using a 3D model of a human body and a carefully planned placement of nodes linked by robust communication connections. The next topic we'll cover is how different body orientations and movements impact the optimal location for relay nodes and the most trustworthy data routing. We employ an Integer Linear Programming (ILP) model to find the optimal location of relay nodes and the most energy-efficient route for data to go from sensors to relays and on to the sink, therefore minimizing the cost of initial network setup and maximizing energy efficiency. We next solve the model under dynamic WBAN (Stand, Sit, and Walk) conditions in order to compare its performance to that of other relaying schemes. When compared to the results obtained in the literature, our realistic and dynamic WBAN design method was shown to dramatically improve reliability, energy-consumption, and the number of relays placed on the body in the experiments.

Liu, Lifei et.al (2018). Wireless body area networks (WBANs) have the potential to collect data on many physiological indicators from the human body. Each sensor extends its own useful life by conserving energy. The three most pressing concerns in WBANs are flexibility, power, and safety. As a remedy for these problems, we propose a secure and flexible data transport method in this research. Approaches such as semi tensor compressive sensing (CS), hash functions, Arnold scrambling, and chaotic scrambling are proposed. Our method uses semi tensor CS to encrypt multiple signals of differing dimensions, therefore resolving the adaptiveness problem. The semi tensor measurement matrix is generated using a chaotic sequence. Since we are just broadcasting a small number of chaotic factors, we can get away with sending less data, which is helpful. However, because the measurement matrix is very small, the computational burden may be kept to a minimum. The proposed method takes security into consideration by bolstering encryption using a combination of Arnold scrambling and logistic scrambling. To prove our methodology works, we give numerical simulations and safety analyses. Adjacent pixels have a correlation of less than 0.004 in absolute value, and there are around 2 of them. In comparison to the traditional CS approach, which needs 524 288 bytes of storage space, the proposed solution only utilizes 2048 bytes. Our method provides a much higher peak signal-to-noise ratio than the other three approaches when the compression ratio is less than 0.7.

Subramanian, Kanaga Suba Raja et.al (2015). The growing number of people living sedentary lifestyles and the fast spread of infectious illnesses have increased the urgency of the need for healthcare for everyone. The wireless body area network (WBAN) is one such concept that has potential as a health monitoring gadget. In a WBAN, a person's vital indicators, such as heart rate and blood pressure, are tracked via sensors implanted in various parts of the body. The patient's readings are sent to a doctor so that they may maintain a close eye on their health from afar. The patient may now get therapy without being restricted to a hospital or their home. Privacy and security issues have been raised with relation to WBAN use. Patients will feel more comfortable sharing information if their medical records are sent in an encrypted format. The data collected by sensors must be sent to the relevant healthcare authorities in a safe and secure manner. Another issue is the short battery life of the sensors. If a sensor is overworked by being asked to do an excessive number of computations, it might soon run out of juice. In this study, we propose an energy-efficient method for transferring patient data to healthcare authorities. To improve system dependability, a variant of the ad hoc on-demand distance vector (AODV) protocol called RelAODV (Reliable AODV) was suggested. The proposed method has been shown via computer simulations to reduce energy consumption while simultaneously improving service quality.

Kathuria, Madhumita et.al (2021). Recent studies have shown that dynamic Quality of Service (QoS) is necessary for a Patient Monitoring Wireless Body Area Network (PA-WBAN) to effectively manage a patient's health data throughout its operation. Quality of Service (QoS) must be greatly improved in such a system because of the difficulty of assuring the secure transmission of a large volume of heterogeneous data in a dynamic situation. Sensing or reading data from various parts of the body is just part of what constitutes quality of service in a PA-WBAN; interpreting that data is equally crucial. The information gathered by the patient monitoring system is useless if it cannot be used because it was not made available in a timely manner or in an understandable format. However, this research suggests two strategies for settling this discrepancy. Dynamic quality of service for encrypted packet transmission is introduced here for the first time in any published study. In terms of node- and packet-level resource allocation, queuing, scheduling, retransmission, drop, and delay, it takes a fair and dynamic approach. Using fair queuing and percentile scheduling, it prioritizes packets based on their expected wait time. It also delivers reliability that is specific to the requirements of particular applications via the use of predictive retransmission and loss recovery rules. During the loss recovery phase of transmission, it calculates a retransmission rate for each sensor node and retransmits just that many packets from each sensor node. Dynamic rate adjustment using priority and packet drop rules is used to control congestion. To further mitigate these issues, a time-bound based packet transmission mechanism is presented. The second protocol is tailored to the specifics of the dynamic PA-WBAN in an effort to improve quality of service. To do this, it employs a multi-dimensional Lion Cooperative Hunt Optimization (LCHO) technique. We compare simulation results and theoretical analysis to demonstrate the benefits of the proposed approaches over the current state of affairs.

Body Sensor Network Architecture

Figure 1 shows that there are essentially three different ways that body sensors may be constructed:

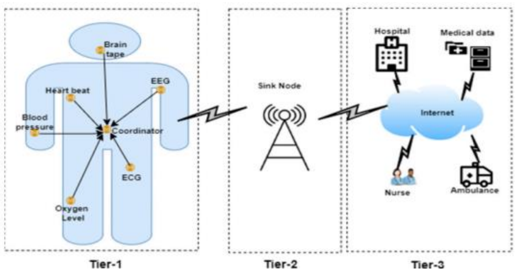

Fig 1. The architecture of wireless body sensor networks

Today, wireless sensor networks are often used to increase the intelligence and coordination of industrial or environmental systems. The use of wireless body sensor networks is growing in significance in the field of human healthcare. This sensor network allows patients or the elderly to continue sending physiological data to hospitals after being discharged. This enables medical professionals and emergency rooms to monitor patients' vitals in near-real time or with a little latency, and respond accordingly. Figure 2 depicts a possible use for the data collected by wireless sensor networks: medical care coordination centers. Multiple routes of communication provide this information to the clinician. Wireless sensor network architecture for the human body.

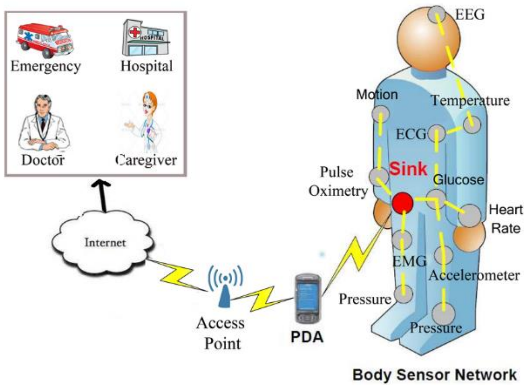

Fig 2. Example of a body sensor network.

Test environment

To test the security of the encrypted link, two LAN nodes are set up.

Fig 3 Structure of Test Environment

A common setup looks like the one shown in Figure 3, which consists of two nodes running on different computers. Both of these computers have Intel Core 2 Duo E8400 processors (at 3.00GHz) and 4GB of RAM, and they are running Windows 7 (32-bit). Most programs run on Eclipse's J2EE platform.

3. Performance

Our first secure communication testing included a wide variety of symmetric cipher modes and other communication encryption techniques. AES and RC4 are the two most often used symmetric ciphers in this environment. AES may be implemented in one of six different modes due to the fact that it is a block en--cryption cipher: There is a great deal of semantic overlap between "Cipher Block Chaining" (CBC), "Electronic

Codebook" (ECB), "Cipher Feed-Back" (CFB), "Output Feed-Back" (OFB), "Propagating Cipher Block Chaining" (PCBC), and "Counter" (CTR).

A number of symmetric encryption techniques are put to the test in Figure 4 by being asked to encrypt and subsequently decode a completely arbitrary message. The whole process just takes a few nanoseconds. Ten thousand iterations are performed, and the average time between failures is calculated.

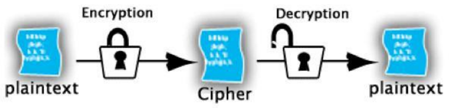

Fig 4 Performance test Scenario

Figure 4 depicts the final outcome of the test for the performance of a 128-bit key. Along the x-axis is the total number of bytes in the generated text. The y-axis displays the mean time of the tests in nanoseconds. The graph displays the almost constant standard deviation of text sizes between 10 and 10,000 bytes. RC4 is the superior choice almost often. Even with a larger word capacity of 100,000 characters, ECB mode remains the fastest. Below is a breakdown of CBC and RC4. The last group consists of a CFB, an OFB, a CTR, and a PCBC. The conclusion from the experiment may be explained by considering the fundamental concepts at play.

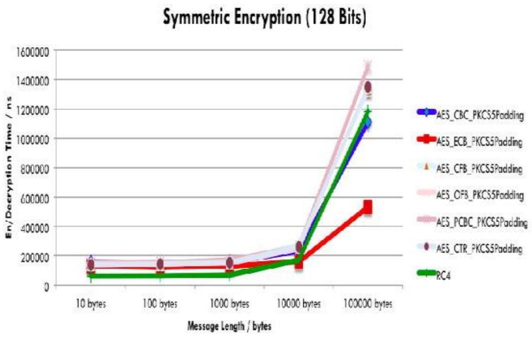

Fig 5 Symmetric Encryption (128 Bits)

Figure 5 displays the results of a performance test using a 192-bit key. Between 1 and 10,000, RC4 is still the best option. The rest look just like Figure 5 in every respect. Figure 5 shows that even when the data size is increased to 100,000 bytes, ECB is still the fastest. The results of a comparable performance test using a 256-bit key are shown in Figure 6. The difference between the three estimates is negligible, with the exception of longer texts, when CBC has a little advantage.

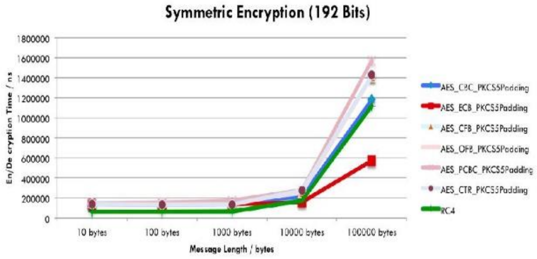

Fig 6 Symmetric Encryption (192 Bits**)**

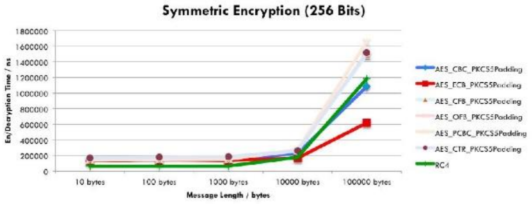

Fig 7 Symmetric Encryption (256 Bits)

4. Conclusion

Wireless body area networks (WBAN) have recently emerged as a promising technology that may one day aid physicians in making more precise diagnoses of a broad variety of potentially deadly disorders. One intriguing possibility is to use smartphones as a foundation for a network of sensors placed throughout the body. Their popularity and ease of use make them a good option for inclusion in monitoring and control systems. Due to the sensitive nature of health information, medical services, and data, WBAN has higher reliability standards. Improving reliability is a dynamic area of study with several applications down the road. This thesis presents the results of investigation into novel approaches to bolster the dependability of Wireless Body Area Networks. We deploy technologies that emphasize fault management and fault avoidance to increase the efficiency of WSNs and WBANs by accounting for the requirements, limitations, and quirks of WBAN.

Reference

[1] Subramanian, kanaga suba raja & jebarajan, t. Reliable and secured data transmission in wireless body area networks (wban). European journal of scientific research. Vol. 82. Issue 2, Page No. 173-184. 2012

[2] Elias, Jocelyne & jarray, Abdallah & Salazar, Javier & karmouch, Ahmed & mehaoua, Ahmed. A reliable design of wireless body area networks. Globecom - IEEE global telecommunications conference. Vol. 32, Issue 11, Page No. 2742-2748. 2013 10.1109/glocom.2013.6831489.

[3] Liu, lifei & haipeng, peng & yang, yixian & cheng, shizhuo. (2018). Flexible and secure data transmission system based on semi-tensor

compressive sensing in wireless body area networks. Ieee internet of things journal. Vol. 87, Issue 2, Page No. 1-1. 2018, 10.1109/jiot.2018.2881129.

[4] Subramanian, Kananga Suba raja & kiruthika, Usha. An energy efficient method for secure and reliable data transmission in wireless body area networks using relaodv. Wireless personal communications. Vol. 83. Issue 2, Page No. 1123-1127, 2015, 10.1007/s11277-015-2577-x.

[5] Kathuria, madhumita & gambhir, sapna. Reliable packet transmission in wban with dynamic and optimized qos using multi-objective lion cooperative hunt optimizer. Multimedia tools and applications. Vol. 80. Issue 32, Page No. 1-44. 2021, 10.1007/s11042-020-10144-9.

[6] Saha, ramesh & biswas, suparna & sarmah, satyajit & karmakar, sushanta & das, pranesh. Design and implementation of routing algorithm to enhance network lifetime in WBAN. Wireless personal communications. Vol. 118. Issue 21, Page No. 1-38. 2020, 10.1007/s11277-020-08054-y.

[7] Mkongwa, kefa & zhang, chaozhu & liu, qingling. A reliable data transmission mechanism in coexisting IEEE 802.15.4-beacon enabled wireless body area networks. Wireless personal communications. Vol. 128. Issue 43, Page no. 1-22. 2022, 10.1007/s11277-022-09987-2.

[8] Movassaghi, samaneh & majidi, akbar & jamalipour, abbas & smith, david & abolhasan, mehran. Enabling interference-aware and energy-efficient coexistence of multiple wireless body area networks with unknown dynamics. Ieee access. Vol. 4. Issue 2, Page No. 1-1. 2016, 10.1109/access.2016.2577681.

[9] Ahamed, rafi & rao, bhoopal. Design of cryptographically secure aes like s-box using second order reversible cellular automata for wireless body area network applications. Healthcare technology letters. Vol. 3. Issue 10. Page No. 1123-1127, 2016, 1049/htl.2016.0033.

[10] Zang, weilin & li, ye. Gait cycle driven transmission power control scheme for wireless body area network. Ieee journal of biomedical and health informatics. Vol. 32, Issue 1, Pp. 10-18, 2017, 1109/jbhi.2017.2688401.

[11] Guo, Y., Wu, D., Liu, G., Zhao, G., Huang, B., & Wang, L. A low-cost body inertial-sensing network for practical gait discrimination of hemiplegia patients. Telemedicine and e-Health, Vol. 18, Issue 10, Page No. 748-754. 2012

[12] GK, R., & Baskaran, K. A survey on futuristic health care system: WBANs. Procedia Engineering, Vol. 30, Issue 4, Page No. 889-896. 2012

[13] Marinkovic, S., & Popovici, E. Ultra-low power signal-oriented approach for wireless health monitoring. Sensors, Vol. 12, Issue 6, Page No. 7917-7937. 2012

[14] Custodio, V., Herrera, F. J., López, G., & Moreno, J. I. A review on architectures and communications technologies for wearable health-monitoring systems. Sensors, Vol. 12, Issue 10, Page No. 13907-13946. 2012

[15] Nie, Z., Ma, J., Li, Z., Chen, H., & Wang, L. Dynamic propagation channel characterization and modeling for human body communication. Sensors, Vol. 12, Issue 12, Page No. 17569-17587. 2012

[16] Felisberto, F., Costa, N., Fdez-Riverola, F., & Pereira, A. Unobstructive Body Area Networks (BAN) for efficient movement monitoring. Sensors, Vol. 12, Issue 9, 12473-12488. 2012

[17] Arefin, M. T., Ali, M. H., & Haque, A. F. Wireless body area network: An overview and various applications. Journal of Computer and Communications, Vol. 5, Issue 7, Page No. 53-64. 2017

[18] Rodenas-Herraiz, D., Garcia-Sanchez, A. J., Garcia-Sanchez, F., & Garcia-Haro, J. Current trends in wireless mesh sensor networks: A review of competing approaches. Sensors, Vol. 13, Issue 5, Page No. 5958- 5995. 2013

[19] Blumrosen, G., & Luttwak, A. Human body parts tracking and kinematic features assessment based on RSSI and inertial sensor measurements. Sensors, Vol. 13, Issue 9, Page No. 11289-11313. 2013

[20] Saleem, S., Ullah, S., & Kwak, K. S. A study of IEEE 802.15. 4 security frameworks for wireless body area networks. Sensors, Vol. 11, Issue 2, 1383-1395. 2011

[21] Guo, Y., Wu, D., Liu, G., Zhao, G., Huang, B., & Wang, L. A low-cost body inertial-sensing network for practical gait discrimination of hemiplegia patients. Telemedicine and e-Health, Vol. 18, Issue 10, Page No. 748-754. 2012

[22] GK, R., & Baskaran, K. A survey on futuristic health care system: WBANs. Procedia Engineering, Vol. 30, Issue 31, Page no. 889-896. 2012

[23] Marinkovic, S., & Popovici, E. Ultra-low power signal-oriented approach for wireless health monitoring. Sensors, Vol. 12, Issue 6, Page no. 7917-7937. 2012

[24] K Shankar et al., “Improving the security and authentication of the cloud with IOT using hybrid optimization-based quantum hash function,” Journal of Intelligent Systems and Internet of Things, vol. 1, Issue no. 2, pp. 61–1, 2021.

[25] S. Farrag and W. Alexan, “Secure 3d data hiding technique based on a mesh traversal algorithm,” Multimedia Tools and Applications, vol. 79, Issue no. 39, Page No. 289–29 303, 2020.

[26] P. Yang, Y. Lao, and P. Li, “Robust watermarking for deep neural networks via bi-level optimization,” in Proceedings of the IEEE/CVF International Conference on Computer Vision, Vol. 2021, Issue 43, Page No.14841–14850. 2021