International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
***Article Received:** 20 May 2023 **Revised:** 28 May 2023 **Accepted:** 16 August 2023*

"Dynamic Shield: An Algorithm for Secured Data Transmission in Dynamic WBAN Scenarios"

Mr. Dhiraj Sanjay Kalyankar[1]

Research Scholar, Department Of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore (M. P.) –452010

Dr. Ajay R. Raundale[2]
Research Guide, Department Of Computer Science & Engineering, Assistant Professor,
Dr. A. P. J. Abdul Kalam University, Indore (M. P.) –452010

ABSTRACT: Healthcare monitoring, sports performance monitoring, industrial wearable sensors, smart retail clothes, and emergency response wearable are all used to evaluate the suggested algorithms. The results show how crucial it is to tailor your choice of cryptographic algorithms to your specific use case and available resources. Data privacy and integrity can be maintained in ever-changing network topologies with the help of the study's suggested strategies for achieving this goal. Building trust and confidence in the dependability of WBAN systems, the suggested algorithms provide powerful security against data breaches, unlawful access, and data loss. With the growing popularity of WBANs in crucial settings, this research provides a solid groundwork for safe and reliable data transmission, opening the door to the easy incorporation of wearable technology in a wide range of uses.

KEYWORDS: WBAN, sensors, topologies, dynamic network, cryptographic

INTRODUCTION

The goal of signal compression for physiological data is to keep the signal quality at a clinically acceptable level while reducing the number of bits required for transmission. When it comes to acquiring data to prolong a WBAN node's lifespan, the Compression Sensing (CS) method has shown to be the most promising and an emerging paradigm. Therefore, it is important to create rapid and accurate CS based reconstruction methods of signals at the receiver of WBAN and develop a CS-based power efficient independent CS compression technique based on the changing ECG and PPG signal at WBAN node. Compression sensing techniques are used in the real world for a wide variety of purposes, including but not limited to signal sparse illustration and reconstruction, energy efficient signal detection, secure communication, and data compression. However, the CS technique is limited in its ability to manage with optimum regeneration and multi-model information compression for long-term communication over wireless LANs because to fluctuations in independent features like frequency or time domain components, non-linearity, and sparsity.

The use of CS techniques reduces the amount of data sent across the channel. As a result, it allows for more productive use of time and materials. However, improving compression while maintaining high standards of reconstruction quality is a difficult issue. Compressed signal (CS) techniques, such as wavelet compression, have been used to the sparse signal in both the frequency and temporal domains. Existing CS methods assume sparsity to be constant throughout time, however this is not the case for PPG and ECG data. The nonlinearity of sparsity across the functional time limits the effectiveness of key current approaches.

Variable sparsity also introduces an inaccuracy during reconstruction. An effective CS strategy makes use of techniques including feature correlation estimation and learning, as well as temporal and spatial feature generation. This method improves compactness, analysis, and dissemination. Multi-model bio-physiological constraints extraction and communication relies heavily on the wavelet illustration, coefficient knowledge, and its reliance. The use of machine learning techniques to overcome data scarcity is well documented in reviews of the relevant literature. This lessens the burden on the transmission of data. Machine learning is helpful for signal regeneration because it reduces the size of the sparse matrix that must be retrieved and the number of calculations required to do so.

LITERATURE REVIEW

Rani, Chintala et.al (2018). Wireless body area networks (WBANs) are becoming more popular in the modern world. WBAN consists of many sensing devices used in industries such as medical, defense, and others. These sensors may either be surgically implanted or worn externally. Protecting the privacy of their patients is a top priority for WBANs. Therefore, we explore a wide variety of data-encryption methods in this study. The WBAN depends on body sensors, and because each sensor has its own power source, the network needs efficient lightweight algorithms to provide security without draining too much juice.

Roy, Sathi et.al. (2022). In this research, we provide a stochastic model for the coordination units of many WBANs. In a Smart Home situation, many patients may be in close proximity to one another while their vitals are monitored by a WBAN system. Coordinators of WBANs must thus use adaptive transmission algorithms that balance improving the likelihood of data transmission while minimizing the risks of packet loss due to inter-BAN interference when more than one WBAN is present. Therefore, the proposed action is divided into two parts. Coordinators in a WBAN are characterized stochastically, and the offline transmission strategy problem they face is expressed as a Markov Decision Process (MDP). Transmission options are affected by channel conditions and buffer states, both of which are expected to be represented by state parameters in MDP. The formulation is solved offline in advance to find the appropriate transmission mechanisms for a broad variety of input conditions. In the post-deployment phase, the coordinator nodes will apply such transmission rules for inter-WBAN communication. Castalia simulations are used to demonstrate the robustness of the suggested approach under both typical and severe conditions.

Iyobhebhe, Matthew et.al (2022). Wireless body area networks (WBANs) construct several transceiver nodes in, on, or around a patient's body to transfer physiological signals to the sink node, which are subsequently communicated to the medical staff through a medical server. WBANs are focused on energy-driven sensor networks. Because of their limited availability, strategic management is required. Quality of service (QoS) demands thorough monitoring of not just throughput and accuracy, but also at the receiving nodes. An abnormal data status that requires rapid intervention by medical professionals to avert irreversible harm or death is the definition of critical data transmission. This review article focuses on the conveyance of crucial data in wireless BAS. Many previous publications in this vein have tackled issues like energy efficiency, security, privacy, connection quality, throughput, network optimization, etc., but none of them consider the possibility of sending life-saving information directly to the sink node, without any intermediary nodes that would require the physiological signals to be sent multiple times. We are motivated to close the knowledge gap by the physical separation of these scholars. This article gave a comprehensive review of the current research and development in the design and implementation of WBANs for the transmission of critical data. Additionally, a practical approach of determining the threshold using the primary data index seen during transmission was investigated.

Dharshini, P. et.al (2015). Data corruption or loss during transmission is a serious concern in Wireless Body Area Networks (WBAN). One proposed approach for reliable data transmission in WBAN is called Adaptive Reliable Cooperative Data Transmission (ARCDT). Data loss is avoided by utilizing a "multi-relay" approach in which all relays are actively involved in collecting data from the sensor network and delivering it on to the "sink." The findings show that the WBAN data transmission overhead was reduced by 13%, and that other QoS indicators also saw significant improvements.

Pathak, Vinay et.al (2021). As sensor and embedded technology for tracking the human body and its environment, wireless body area networks (WBANs) are gaining ground. As well as being helpful in times of epidemic, it enables a broad range of clinical uses. It's on the leading edge of medicine, and many researchers are interested in it because they see a bright future for it. Information collected by different wireless sensors or nodes is very sensitive, critical, and significant due to the nature of the data being collected: human lives. WBANs have the potential to lessen social contact, hence slowing the transmission of infectious diseases. Data privacy and accuracy continue to be widely studied because of the dynamic and expanding nature of attacks, as well as for the enhancement of performance. A system for assuring data security is a viable solution to the issues stated above. The patient's file has to be kept current at all times. Beneficial aspects of WBANs include the personalized and consistent supply of accurate health information to the patient.

PROPOSED SECURITY SUITE

WBANs provide a promising solution to the problem of continuous health monitoring. However, proper security measures are required since sensitive patient health information will be sent through a wireless link. Because of the importance of the data for making medical decisions, there has been a lot of money poured into studying WBANs. The two primary components of a WBAN are the human sensor network, which is made up of all the individual sensors and connects to the WBAN central controller (WCC), and the network that links the WCC to the monitoring station. However, it is impossible to implement similarly advanced security algorithms across all of these sub-networks due to the restricted resources of the sensors. We propose a security suite that uses a secure approach for communication between WBAN-monitoring stations and a variant of the same technology for the human body's network of sensors to circumvent this issue. Our method is an effort to reduce the burden on both of the networks while still ensuring secure connection.

Comparison with SSL

The Sensible Things platform originally supported SSL (secure socket layer) communication capability. The cipher type "SSL_DH_anon_WITH_RC4_128_MD5" should be adopted as the standard. Key exchanges in this SSL encryption are performed using the Diffie-Hellman (DH) method, and both the RC4 and MD5 digest algorithms utilize 128-bit keys. "anon" denotes anonymous encryption, in which nodes may choose whether or not to share their

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
Article Received: *20 May 2023* ***Revised:*** *28 May 2023* ***Accepted:*** *16 August 2023*

certificates with one another. Scholarly research on DH in this setting requires the assumption that no man-in-the-middle assault has been launched against it. For encrypted messaging, similar block cipher techniques are used.

Using one of these protocols, a random test of a certain length will be created at one node and sent to another. After receiving the message, Node 2 will react as soon as it is able to. Due to their misalignment, only one of these nodes can capture the whole of the broadcast.

Figure 1 is a comparison between SSL and the security protocol. Each result is based on an average of 1,000 transmissions at consistently measurable intervals. The x-axis shows the total amount of bytes in each output message, while the y-axis displays the actual transmission time. Compared to SSL, the recommended method of secure communication (green line) is clearly superior. The suggested protocol is often five times faster than SSL.

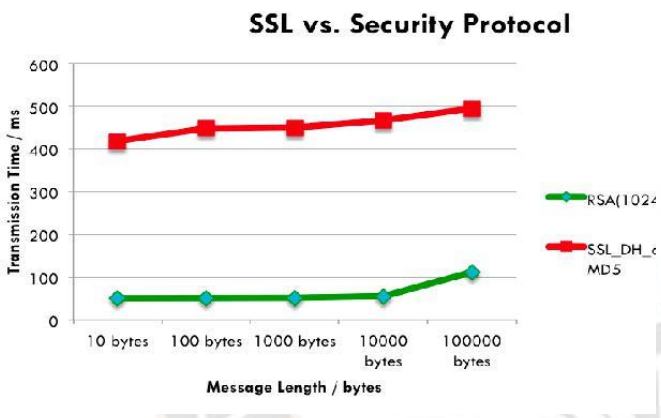

Figure 1 SSL vs. security protocol

Security Protocol Analysis

This section introduces the protocol in its abbreviated form. Public keys and corresponding secret keys are represented by and, respectively, for principals A and the authentication server S. In response to a request from user A, server S returns the "!" that serves as the session key between the two parties. S sends back to A an encrypted response using its private key. Parties A and S will exchange public keys and a new nonce encrypted using Party S's public key and Party A's secret key once the nonce has been verified. In turn, S uses A's public key to encrypt a session key, which is then sent along with the encrypted communication. Last but not least, the use is typical in the final message. As long as S can distinguish his messages from A's, any function will do. The first message is disregarded since it does not contribute to the logical aspects of the protocol. Message 2 is also straightforward, as is Message 3. The following two messages, however, have no discernible context. Message 4 uses! ′ As a secret, which is why the >! notation is used. Message 5's session key was left out of the first draft. This message might be interpreted as confirmation that A intends for S to believe it already has the session key. We may now convince ourselves that the ideal--ized protocol is a faithful representation of the actual protocol.

Secure Communication Analysis

This assessment is made from the vantage point of the project's encrypted messaging infrastructure. Due to its focus on the technical features of encrypted communication, this research may be more difficult to grasp than a protocol analysis, which examines the protocol's underlying logic. Possible applications of this study's findings in future research include elucidating possible pitfalls and limitations of the implementation.

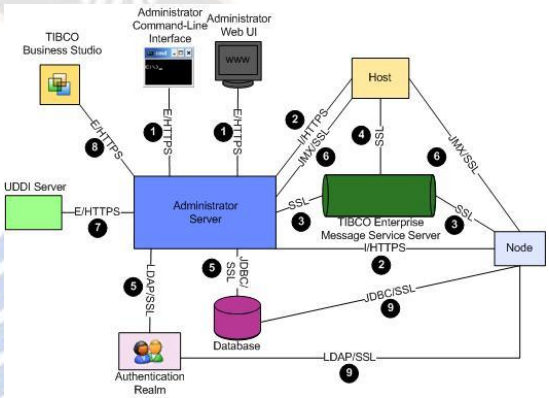

Figure 2 Secure Communication

Cryptography is still the first and most important step in developing any kind of security mechanism. Most cryptographic concepts are both well-known and straightforward to put into practice. Existing libraries that have previously been built, tested, and updated by security organizations may be preferable to use to save time and effort. The dangers (such as Heartbleed) of adopting already-released libraries are outweighed by their advantages due to time and knowledge restrictions.

Over ninety percent of it was built using the excellent Java cryptography framework. Although its APIs are well-documented, its lack of transparency prevents many of them from being extended. Since these libraries are closed-source, any potential issues may take longer to resolve. This might be disregarded if the project moves forward. During construction, a security hole in the key store library was uncovered. The code has been annotated to show where this function shouldn't be used. The remaining 10% is completed making advantage of the excellent support for certificate operations provided by the Bouncy Castle libraries. However, developers have reported confusion about Bouncy Castle's encryption APIs due to a lack of documentation. There are various certificate APIs in the Java cryptography architecture that have been deprecated because they are so old.

The session key's time limit should also be mentioned as a possible issue. This setting may be accessed via the system's security menu, as was previously mentioned. This choice's worth is established by the requirements of the application. There is a trade-off between security and performance, so developers should give this some care. Therefore, keeping the session key active for longer than required increases the likelihood that it may be compromised. Because the system will have to produce and exchange fresh session keys more often if it's too short, performance will suffer. The IoT has boosted people's happiness by streamlining a variety of processes, such as communication, access to information, and safety precautions. Its infinite scalability makes for a dynamic social model. However, as the complexity of systems and applications grows, it becomes increasingly challenging to provide a security mechanism that reliably protects communication flow. We proposed a P2P-based, decentralized security protocol to address this concern. Secure methods of communication have been implemented in a similar fashion on the Sensible Things platform.

The required properties of this protocol are achieved by a collection of ways. It's scalable since it doesn't need a central server or a middleman when communicating with other devices. Instead than relying on a resource-intensive database to hold keys and certificates, a lightweight key store is used. The system's previous encryption, SSL, is obsoleted by the usage of this faster alternative. This is because fewer meetings call for handshakes. Its flexibility and suitability to a broad variety of uses are enhanced by a dynamic mechanism for modifying the security level. Information may only be trusted if it is encrypted and signed properly. A certificate produced by a reliable node is used to verify the identity of the subject. The information is reliably and rapidly sent to you so that it may be used whenever you need it. By accurately reflecting the core values of the Sen--sible Things platform, this protocol is a major boon to the system.

Using an abstract factory design, secure communication is developed to strengthen component cohesiveness and reduce reliance. Using a method design template for the most essential processes allows for simple expansion of the secure communication. The use of test--driven development helps to prolong the life of this safe link by ensuring that all necessary features are met.

Security issues in the proposed protocol may be found and eliminated with the use of BAN logic, which is used as an analytical tool to examine and analyze the protocol. The analysis shows that, under reasonable assumptions, it is possible to meet the security requirements. In addition, we do an SSL performance comparison test using Sensible Things. Tests demonstrate that the proposed security is far more effective than SSL, while also saving time and resources by avoiding unnecessary handshakes.

To safeguard the infrastructure supporting the Internet of Things, this study provides a workable solution. With the new secure connectivity in place, all data sent between Sensible Things is substantially safer. It is feasible to build mutually secure channels of communication between several systems. Individuals' privacy when utilizing the Internet of Things will be protected thanks to this measure. Also, it contributes to the growth of the Internet of Things. This study sets the path for future applications of Internet of Things technology, which might improve people's quality of life by reducing stress and increasing security.

CONCLUSION

The IoT has boosted people's happiness by streamlining a variety of processes, such as communication, access to information, and safety precautions. Its infinite scalability makes for a dynamic social model. Systems and applications have increasing challenges in providing a security mechanism that adequately protects communication traffic in the face of growing complexity and threats. We proposed a peer-to-peer communication security protocol that is decentralized to address this problem. Secure methods of communication have been implemented in a similar fashion on the Sensible Things platform. The required properties of this protocol are achieved by a collection of ways. It's scalable since it doesn't need a central server or a middleman when communicating with other devices. Instead, then relying on a resource-intensive database to hold keys and certificates, a lightweight key store is used.

REFERENCE

1. ani, chintala & Jagan, lakku & harika, ch & amara, v.v.. Light weight encryption algorithms for wireless body area networks. International journal of engineering and technology(uae). Vol. 7. Issue 11, Page no. 64-66. 2018 10.14419/ijet.v7i2.20.11754.
2. Roy, sathi & roy, moumita & chowdhury, chandreyee. Novel data transmission schemes for inter-wban networks using markov decision process. Vol. 21, Issue 4, Page No. 178-185, 2022, 10.21203/rs.3.rs-1237442/v1.
3. Iyobhebhe, Matthew & tekanyi, abdoulie & usman, aliyu & kwembe, benjamin & eleshin, ridwan. A review on critical data transmission in wireless body area networks. Pakistan journal of engineering and technology. Vol. 8. Issue 4, Page No. 75-81. 2022, 10.51846/vol5iss4pp75-81.
4. Dharshini, p. & Muthu, tamilarasi. Adaptive reliable cooperative data transmission technique for wireless body area network. 2014 international conference on information communication and embedded systems, ICICES 2014. 10.1109/icices.2014.7034084.
5. Pathak, Vinay & Singh, Karan. Secure and efficient wbans algorithm with authentication mechanism.

Journal of intelligent & fuzzy systems. Vol. 41. Issue 3, Page No. 1-10. 2021, 10.3233/jifs-189873.

6. Peng, haipeng & tian, ye & kurths, juergen & yang, yixian & wang, daoshun. (2017). Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks. IEEE transactions on biomedical circuits and systems. Vol. 32, Issue 1, Page no. 10-18, 2017, 1109/tbcas.2017.2665659.
7. Shayokh, al & diro, abebe & satrya, gandeva & arief, muhammad. Efficient and secure data delivery in software defined wban for virtual hospital. Vol. 44, Issue 5, Page no. 12-16. 2016, 10.1109/iccerec.2016.7814973.
8. Thippun, pitchakron & sasiwat, yoschanin & buranapanichkit, dujdow & booranawong, apidet & jindapetch, nattha & saito, hiroshi. (2023). Implementation and experimental evaluation of dynamic capabilities in wireless body area networks: different setting parameters and environments. Journal of engineering and applied science. Vol. 70. Issue 1. Page no. 987-1012, 10.1186/s44147-022-00171-8.
9. Salayma, Marwa & al-dubai, Ahmed & romdhani, imed & Youssef, Nasser. New dynamic, reliable and energy efficient scheduling for wireless body area networks (wban). Vol. 43, Issue 2, Page No. 1134-1139, 2017, 10.1109/icc.2017.7996898.
10. Elias, Jocelyne. Optimal design of energy-efficient and cost-effective wireless body area networks. Ad hoc networks. Vol. 13. Issue 4, Page No. 560–574. 2014, 10.1016/j.adhoc.2013.10.010.
11. Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "Image encryption using 2d logistic-sine chaotic map," in 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE, 2014, pp. 3229–3234.
12. X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," IEEE Access, vol. 9, pp. 61 334–61 345, 2021.
13. M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Logistic sine map-based image encryption," in 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), 2019, pp. 290–295. doi: 10.23919/ SPA.2019.8936718.
14. M. ElBeltagy, W. Alexan, A. Elkhamry, M. Moustafa, and H. H. Hussein, "Image encryption through r¨ossler system, prng s-box and recam´an's sequence," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022, pp. 0716–0722. doi: 10.1109/CCWC54503. 2022.9720905.
15. C. E. Shannon, "Communication theory of secrecy systems," The Bell system technical journal, vol. 28, no. 4, pp. 656–715, 1949.