ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(34), DOI: 10.17485/ijst/2015/v8i34/85274, December 2015* ISSN (Online) : 0974-5645

Switch Pattern Encryption Based WBAN Security in an IoT Environment

R. Sujatha[1*] and M. Ramakrishnan[2]

[1]Department of Electronics and Communication Engineering, Velammal Engineering College, Chennai - 600066,
Tamil Nadu, India;
ece.sujatha@velammal.edu.in
[2]Department of Computer Applications, Madurai Kamaraj University, Madurai - 22, Tamil Nadu, India;
eceweekly@gmail.com, ramkrishod@gmail.com

Abstract

Data security is a major challenge in E health monitoring research. Nowadays Wireless body area networks faces various security threats. Authentication is very much required in health care domain, as an open IOT environment is accessed by all. In this article, we have proposed efficient Light weight embedded cryptographic architecture using switch pattern encryption for WBAN security. The security is ensured to the wearable sensors in such a way that any external unknown entity cannot access patient's physiological data and deceive the medical professionals. The main aim of this work is to improvise the security and privacy of E healthcare monitoring systems when compared with the existing findings. Proposed algorithm overcomes DoS attacks in the BAN environment and reduces the runtime for the switch pattern encryption algorithm. Signcryption can be included along with switch pattern encryption as a future work in order to achieve confidentiality and authentication in a single step.

Keywords: Continous Wavelet Transform, Discrete Meyer Wavelet Transform, Denial of Service Attacks, Internet of Things, Switch Pattern Encryption, Wireless Body Area Networks

1. Introduction

Nowadays people who are unknown to each other communicate in an open insecure environment. To ensure privacy we always encrypt the message with a key to produce a cipher text, and only the authenticated person can decrypt the cipher text. This ensures that the data transmitted in the insecure channel is not tampered. By receiving the enciphered text, receiver uses the decryption key to retrieve the original text. There is a need to secure patient medical data in the IoT environment. In wireless Body area networks, nodes are very closely placed on the cloth or sometimes implanted in the skin to improve ant to monitor the health of the patient. Use of WBAN's overcomes the condition that the patient has to stay in the hospital. In order to protect the sensitive medical information. We construct a switch pattern encryption scheme that provides a greater efficiency when compared to previous methodologies. By doing this, information transmitted from the BAN is totally secured from unauthorized parties. Proposed method is basically based on linear algebra and number theory. Switch pattern encryption h prevents denial of service attacks. A Chipcon CC1000 radio is used, which consumes 28.6 μJ and 59.2 μJ respectively to receive and transmit one byte. Attribute-based encryption paradigm has been proposed work for the secure WBAN domain which also reduces the cost of certificate verification.

[*] Author for correspondence

2. Related Work

The Fuzzy attribute based signcryption proposed in[1], provides both security and authentication for BAN's. Game theory is applied to address the power control problem. In a cooperate power control game, as long as each node in the WBANs follows the game rules, a equilibrium solution can be reached, which is optimal for all individuals. The inter-network interference mitigation for WBANs has been studied in this paper. Due to the fact that WBANs are carried by human bodies, the inter-network interference occurs when people are close to each other. Thus, the social interaction information will play an important role in inter-network interference mitigation. Zhang[2] considered both social interaction information and the movement of individuals when a power game is used to mitigate the inter-network interference.

The Gaussian Process (GP) framework is used as a principle performance inference parameter for the data obtained from wearable sensors in the noisy environment. The notion of GP as a distribution over functions, is well suited to the analysis of time series of patient physiological data, in which we perform inference over functions. The approach proposed in[3], contrasts with conventional probabilistic approaches which define distributions over individual data points.

Garth, et al.[4] proposed a security solution in biomedical sensor network to achieve link-layer encryption and data authentication. The data packet is encrypted with a group key common to the sensor nodes and computes a message authentication code (MAC) for the entire packet including the header. This group key is shared network-wide and manually programmed into the nodes prior to deployment. This network-wide key presents a single point of vulnerability. If a node is compromised and the keying material is revealed, the entire network can be compromised.

Raghav V, et al. presented a security suite for WBANs comprised of IAMKeys, and KEMESIS, a key management scheme for security[5].

Detailed description of intrusion detection system based on local reputation scheme is presented in[6]. The System also includes concept of fading, drawback is, it allows the nodes which are previously considered as malicious to become a part of the network again. The biomedical data, collected by wearable sensors will be transmitted using cell phones towards the corresponding health monitoring centers via various wireless networks. The Elliptic Curve Cryptography (ECC) Algorithm is used for encryption.

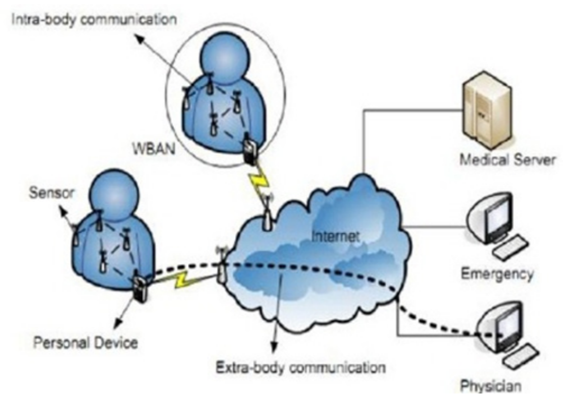


Figure 1. WBAN Architecture.

Zhang, et al. examined possible attacks in BANs and presented key management schemes that are useful for BANs security. Biochannels are utilized to assist secure information transmission within a BAN[7].

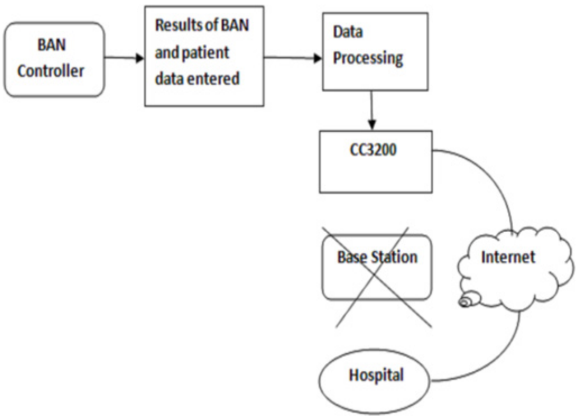


Figure 2. E Health monitoring architecture using TICC3200.

Li, et al. analyzed dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data in BAN[8].

Subsequently, Ren[9] enables the opportunity for innovative use of clinical monitoring devices to exchange wirelessly patient health information. Healthcare policies have various blockers that state how data should be protected.

Al Ameen, et al. discussed the security and privacy issues of wireless sensor networks within healthcare perspective and the possible measures are suggested[10].

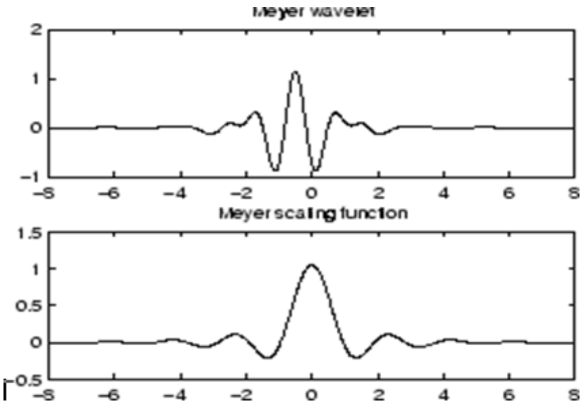


Figure 3. Patient ECG Signal.

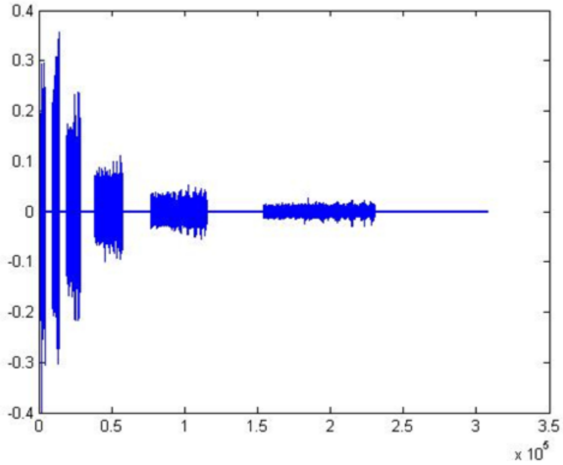


Figure 4. DWT Processed ECG signal.

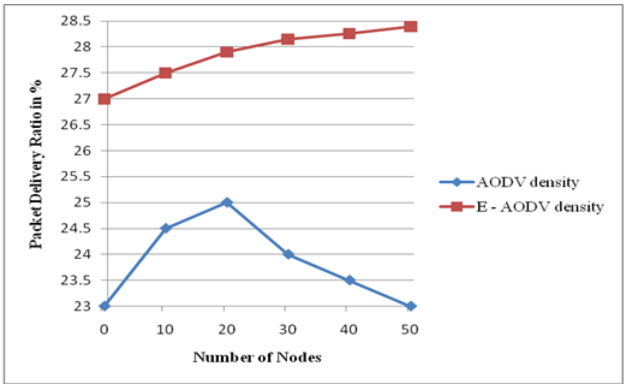


Figure 5. Switch Pattern Encrypted ECG signal.

The issues of privacy and security continues to be a major concern. With data transmission, the data leave the area of control by a specific user, which may have implications on privacy and security. The light weight identity based cryptography is employed by Wang[11] in which a person's identity is used to perform cryptography.

3. Proposed Work

The proposed approach offers data confidentiality and integrity in WBANs. WBAN acts as an interface network between IoT environment and the wearable sensors placed on the human body that measures temperature, heart rate etc. It forwards the patient data to the hospital which has to avoid any misinterpretation of information. The processing and analysis of patient signals is performed using discrete meyer wavelet transform. Security parameters such as confidentiality, authenticity and collusion resistance ensures authenticated transmission of health information.

4. Switch Pattern Encryption

Symmetric key primitives is used to perform pattern matching on encrypted data, without making the data vulnerable to the adversaries. The key for pattern based encryption is any matrix. For eg:

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \rightarrow \boxed{\text{Pattern Matrix}}$$

In the above case, we have taken the matrix size to be 3 × 3, however it can be any size (as long as it is square for pattern matrix). To encipher, we need to break the message into chunks of 3. We now take the first 3 characters from our plaintext, ATT and create a vector that corresponds to the letters. (Replace A with 0, B with 1 ... Z with 25 etc.) to get: [0 19 19] (this is ['A' 'T' 'T']).

A matrix multiplication process is performed: This is implemented for all 3 letter blocks in the plaintext. The plaintext may have to be padded with some extra letters to make sure that there is a whole number of blocks.

By doing this, information transmitted from the BAN is secured from unauthorized parties. It thus achieves authenticity and the data is unaltered. This prevents denial of service attacks and the patient's information is not disclosed to anyone.

The inbuilt internet access within the CC3200 chip avoids delay in transferring the signals. The data encrypted using discrete meyer wavelet is transmitted to the hospital. This preserves the privacy of the information. CC3200 especially designed for IoT is used which has a simple link Wi-Fi internet-on chip that has a reduced computation cost with an inbuilt Wifi.

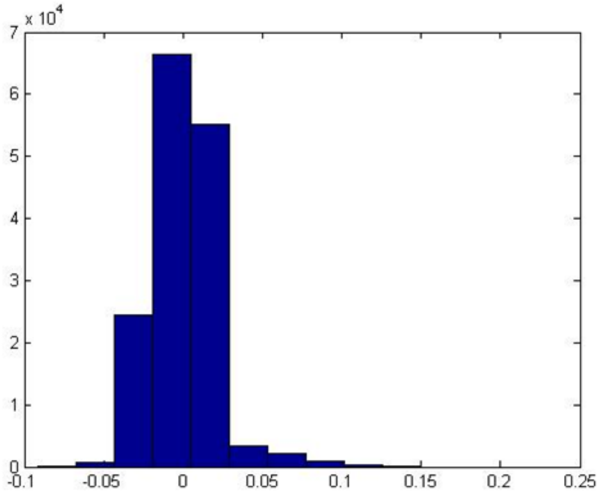
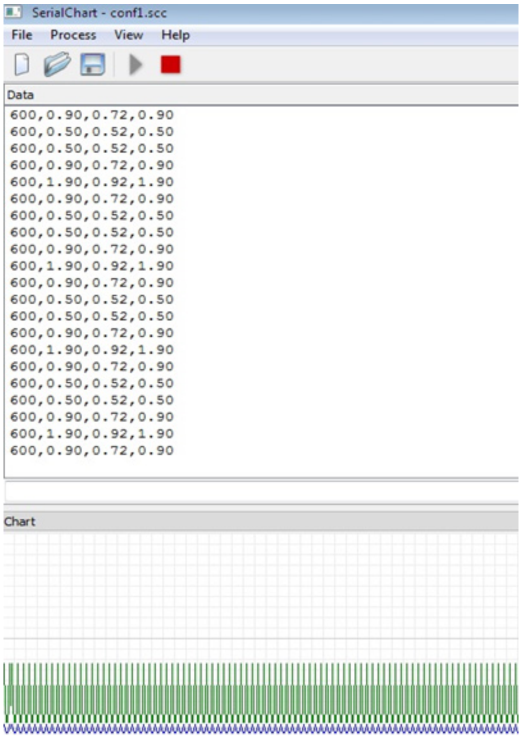


Figure 6. Decrypted ECG signal.



```
600,0.90,0.72,0.90
600,0.50,0.52,0.50
600,0.50,0.52,0.50
600,0.90,0.72,0.90
600,1.90,0.92,1.90
600,0.90,0.72,0.90
600,0.50,0.52,0.50
600,0.50,0.52,0.50
600,0.90,0.72,0.90
600,1.90,0.92,1.90
600,0.90,0.72,0.90
600,0.50,0.52,0.50
600,0.50,0.52,0.50
600,0.90,0.72,0.90
600,1.90,0.92,1.90
600,0.90,0.72,0.90
600,0.50,0.52,0.50
600,0.50,0.52,0.50
600,0.90,0.72,0.90
600,1.90,0.92,1.90
600,0.90,0.72,0.90
```

Figure 7. Data rate of the transmitted data.

5. Simulation Parameters

To simulate and analyze the patients signals the Discrete Meyer Wavelet transform (DWT), is used which is implemented in Matlab. This provides sufficient information both for analysis and synthesis of the original signal, with a significant reduction in the computation time. The DWT is considerably easier to implement when compared with Continous Wavelet Transform (CWT). It is a tool that separates data into different frequencies, components, and then studies each component with resolution matched to its scale. The frequency components are analyzed which consists of the important information hidden inside it. The patient data can be diagnosed more easily when the frequency content is analyzed clearly.

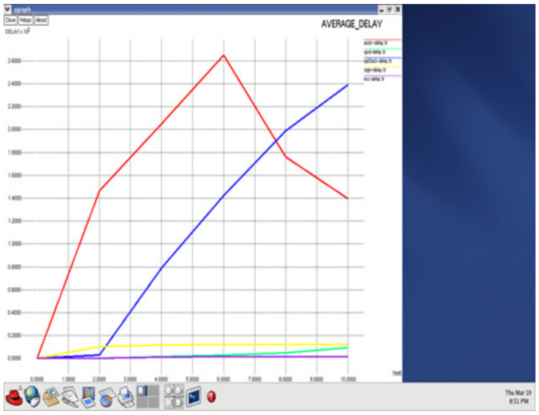


Figure 8. Comparison of DWT and CWT based on Data rate.

6. Results and Discussion

The patient information is analyzed and encrypted using switch pattern encryption. The data rate of the encrypted information has been received at a faster rate and thereby reduces the delay considerably. The data along with the signals is transmitted and received at a data rate of 9600 bps. The encrypted signal using switch pattern encryption has been reproduced at the receiver which is free from password guessing attacks.

As a result, some of the problems like eaves dropping, data modifications are also reduced considerably.

7. Graphical Interpretation

Comparison has been done for the delay parameter for DWT and CWT. The graph compares the performances of the applied algorithm in terms of run time (in seconds). The structure is analysed in the presence of DoS attacks (namely Gray hole attack). Due to the behavior of the malicious nodes in the body area network, high degree of packet drop is observed in this system. Thus, the delay is significantly decreased by using switch pattern encryption in the DWT mode .

To counteract these DoS attacks in an IoT environment, Signcryption can also be used , thereby it introduces the data confidentiality and authenticity of the data packet. By counteracting the malicious nodes, the delay in the network is significantly reduced.

8. Conclusion

The proposed switch pattern encryption based architecture enhances the security of body area network in an IoT environment .This scheme is realized in the presence of DoS attacks. In the future, this proposal may be extended to experiment by using signcryption along with switch pattern encryption to provide even stronger encryption techniques to completely avoid the adversaries who attack the network. The proposed work addresses the WBAN security of using switch Pattern Encryption in terms of Computational time, and Data delivery rate. There are many challenges that still need to be addressed, especially based on signcryption and interoperability between BANs.

9. References

1. Hu C, Zhang N, Li H, Cheng X. Body area network security fuzzy attribute based signcryption scheme. IEEE Journal on Selected Areas in Communications/Supplement. 2013 Sep; 31(9).
2. Zhang Z, Wang H, Wang C, Fang H. Interference mitigation for cyber physical wireless body area network system using social networks. IEEE Transactions on Emerging Topics in Computing. 2013.
3. Clifton DA, Pimentel MAF, Watkinson PJ, Tarassenko L. Gaussian processes for personalized E-health monitoring with wearable sensors. IEEE Transactions on Biomedical Engineering. 2013 Jan; 60(1).
4. Crosby GV, Ghosh T, Murimi R, Chin CA. Wireless body area networks for healthcare. International Journal of Ad hoc, Sensor and Ubiquitous Computing. 2012 Jun; 3.
5. Sampangi RV, Dey S, Sampalli S. A Security suite for wireless body area networks. International Journal of Network Security and its Applications. 2012 Jan; 4(1).
6. Lakhina S, Mahmood Z, Site S. Secure Pervasive Computing Environment for Health Monitoring. International Journal of Computer Technology and Electronics Engineering. 2011; 1(2).
7. Zhang P. A review on body area networks security for healthcare. ISRN Communication Networks. 2011; 21.
8. Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. IEEE Wireless Comm. 2010; 17(1).
9. Ren Y, Boukerche A. Monitoring patients via a secure and mobile healthcare system. IEEE Wireless Communications. 2010; 17(1):59–65.
10. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst. 2012 Feb; 36(1):93–101
11. Tan C, Wang H, Zhong S, Li Q. A lightweight identity-base cryptography for body sensor networks. 2009; 13(6):926–32.