Secure Wireless Body Area Network (WBAN) Communication Method Using New Random Key Management Scheme

Reza Khalilian[11], Abdalhossein Rezai [2] and Farhad Mesrinejad[3]

[1]Department of Electrical and Computer, Islamic Azad University, Majlesi Branch, Isfahan, Iran.
[2]Academic Center for Education, Culture and Research (ACECR), IUT branch, 8415681167, Isfahan, Iran.
[3]Advanced Research Center for Engineering Science, Islamic Azad University, Majlesi Branch, Isfahan, Iran.
[1]rezakhalilian@gmail.com, [2]rezaie@acecr.ac.ir, [3]mesri110@yahoo.com

Abstract

Wireless Body Area Networks (WBANs) have an important role in healthcare. So, the security of WBANs becomes a challenging issue. High performance encryption method and efficient key management scheme are required for securing WBAN communications. This study presents and evaluates an efficient key management scheme and efficient encryption method for improving WBAN security. We proposed a new random key management scheme. The proposed method utilized Advanced Encryption Standard (AES)-256 to encrypt the bio signals. Simulation results show that the proposed method has advantages compared to other secure WBAN communication methods.

***Keywords**: Security, Wireless Body Area Network (WBAN), Advanced Encryption Standard (AES), Bio Signals, Key Management Scheme.*

1. Introduction

Wireless Body Area Networks (WBANs) commonly consist of smart sensors and wireless transmission channels. Sensors are located on/under the skin, in the body and clothes. These sensors collect, receive, process, compress and transmit medical data and environment conditions to the medical server [1]. WBANs provide telemedicine and real-time healthcare monitoring by registering records and vital sings in every time [2, 3]. So, the security of WBAN becomes a challenge issue [4]. High performance key management scheme and efficient encryption method are required for securing WBAN communications. Symmetric encryption method such as AES are commonly used system for data encryption, but the AES have the same cipher output for the same input at the different times. On the other hands, the number of data in the WBAN is limited (about 20). This means that, we have the same cipher text outputs. Although, the utilized algorithm in this case may be very complex, but key will be easily revealed. Figure 1 shows the block diagram of symmetric encryption system for bio signals.

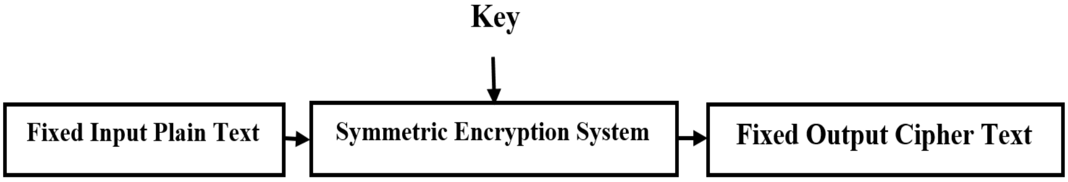


Figure 1. Symmetric Encryption System for Bio Signals

[1] Corresponding Author

ISSN: 1738-9976 IJSIA

The input and output of symmetric encryption system which is shown in figure 1, can be written as follows:

Fix **P**lain **T**ext (FPT) → **F**ix **C**ipher **T**ext (FCT) (1)

On the other hand, AES was recommended by National Institute of Standard (NIST) for block cipher-based symmetric key standard to secure data communication. It is because AES has high speed and low resource requirements [5]. Motivated by these facts, we attempt to use AES for securing WBANs.

This paper presents and evaluates a new method to improve the WBAN security. We proposed a new key management scheme for secure WBAN communication. Using this new key management scheme, the outputs for same input will be different in different times.

The proposed method has been simulated using MATLAB and C#. The simulation results show that the proposed method has advantages in comparison with other methods used for secure WBAN communications.

The rest of this paper is organized as follows: Section 2 presents the related works about WBAN secure communication. In section 3, the proposed method is presented. the simulation results of the proposed method are presented in section 4. Section 5 compares the simulation results. Finally, conclusion is presented in section 6.

2. Related Works

The WBAN was addressed for the first time in a primitive work by Van Dam [6] in 2001. Since the WBAN plays a vital role in the healthcare applications, the importance of security in the WBANs are considerably increased. There are several attempts to improve the security issue in WBANs [7, 8]. In [7], a real-time healthcare system has been provided in complex situations that can take data processing carried from sensors to out of the body. The WBAN communications are useful plan for discover body movements that occur during the walking [8]. Radio frequency communication interference is tested for power consumption in the conventional wireless devices that arise around the person with the WBAN. The authors of [9-12] have presented solutions such as security, confidentiality at the time of creation, transmission, storage and processing of data in the WBAN. Ahmed et al. [10, 11] assessed security issues such as reliability and accuracy of data. In addition, there are many research, which used various wireless technologies in their projects in the field of short-range WBAN, such as WPAN, WBAN, Bluetooth and Zigbee [12, 13]. Hur et al. [12] used the Zigbee to collect data. This architecture is suitable for low power consumption in the real-time medical care system. Huang et al. [14] evaluated the energy efficiency in WBAN. Rezai et al. [15-26] have presented methods for security improvement and energy efficient for wireless networks that are used in the proposed key management.

3. The Proposed Method

The proposed method utilizes new key management scheme and AES-256. So, this section outlines the proposed key management and the utilized AES-256.

3.1 The Proposed Key Management Scheme

The proposed method using a new key management scheme. Using this new method, the cipher text for two same plaintexts can be different with each other. This means that for the same plain text, the cipher text will be different in two times. In other words, the key is variable with the time. Figure 2 shows the block diagram of the proposed method.

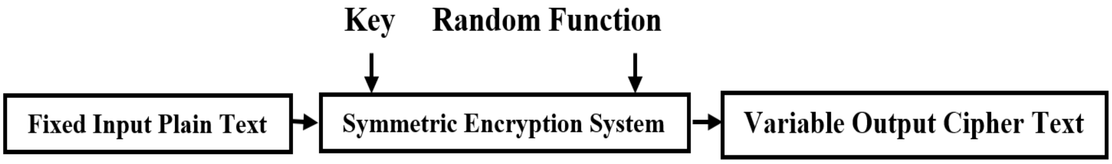


Figure 2. Block Diagram of the Proposed Method

The input and output of symmetric encryption system which is shown in figure 2, can be written as follows:

Fixed **P**lain **T**ext (FPT) → **V**ariable **E**ncrypted **T**ext (VET) (2)

For example, in the time of t_1, the output for the input $K=K_0\ldots K_N$ is as follows:
Out= $a_1\ldots a_n$
While in the time of t_2, the output for the same input is as follows:
Out= $b_1\ldots b_n$.
Protocol 1 shows the proposed key management scheme in the proposed method.

Protocol 1. The Proposed Key Management Scheme in the Proposed Method

(1) Private key (key 2) is generated based on the time.
(2) Private key (key 2) is encrypted using public key (key 1).
(3) Server send encrypted key to clients
(4) Bio signals are encrypted using private key
(5) Sensors send the encrypted bio signals.
(6) Receiver extracts the time information and random function, when cipher bio signals are received to the destination.

Figure 3 shows the encryption method of bio signals in the proposed method.

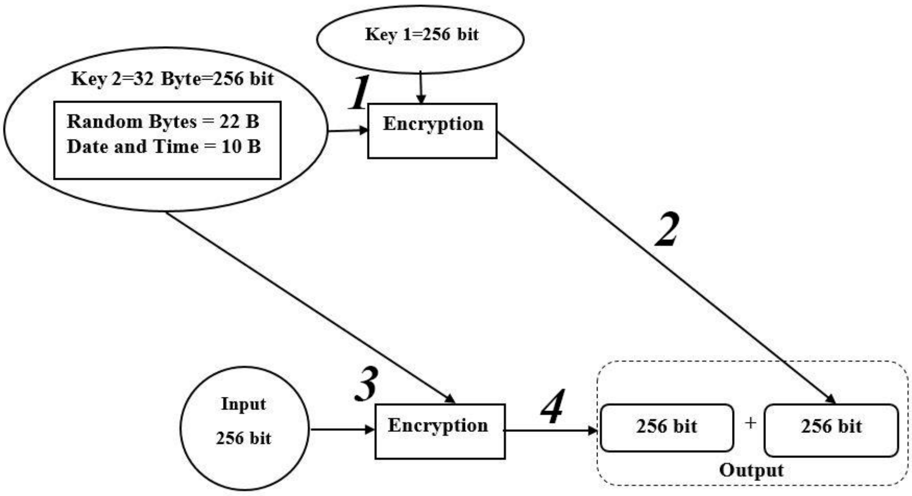


Figure 3. The Block Diagram of Encryption Method of Bio-signals in the Proposed Method

As it is shown in figure 3, the proposed method gets inputs in 128 or 256 bits. This means that, every time a 128 or 256-bit block of stream data are scanned by input. Then, these scanned data are encrypted using pre-specified key. This protocol can be interacted 128, 192 and 256 bits. We have used 256-bit key in our scheme. In the proposed method, two keys are utilized to encrypt the data: (a) Public key (256 bits) that exchange between transmitter and receiver. (b) Private key (256 bits) that is made from random bytes and time function. The key 1 is encrypted using key 2. Then encrypted key is sent to the output. Finally, input data is encrypted by key 2 and send to the output.

Figure 4 shows the decryption method of bio signals in the proposed method.

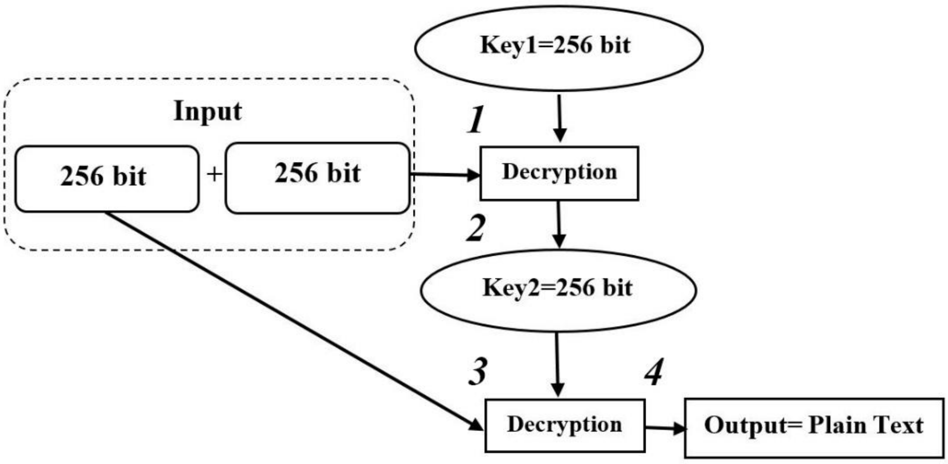


Figure 4. The block Diagram of Decryption Method of Bio-signals in the Proposed Method

Similarly, we have two keys: (a) Public key (key 1) like before. (b) Private key (key 2) which is made from time function and random bytes. First of all, system gets 256 bits of cipher text, which is decrypted using Key 1. Then, it compares date and time information in transmitter with date, time and random bytes (22 byte) to key 2. Finally, second 256 bit cipher text is received and it is decrypted for second time. In fact, this algorithm gets 48 bytes and delivers 32 bytes. 16 bytes are key and 32 bytes are information.

3.2. The Utilized AES-256

In the original algorithm of Rijndael [5] the length of input data stream can be 128, 192 or 256 bits. In the AES 256-bit, key is extended an array named word that shown by W and any word is extended from 32 bits to 44 bits. The key in each round, gets the four elements of this array. The key schedule algorithm has the role of providing key for each round which is based on the original key. It should be noted that operations are performed on Bytes. So, AES is a stream encryption. A 256 bit plaintext comes in to the form of a 4 × 4 state matrix. Each element shows a Byte of bio signal. Input bio signals are stored in the state matrix columnar. Finally this matrix is generating cipher bio signals. In each round of AES, 4 operations are performed on the state matrix: S-BOX and P-BOX, rows shift, mix columns and add round key. Figure 5 shows these operations [27].

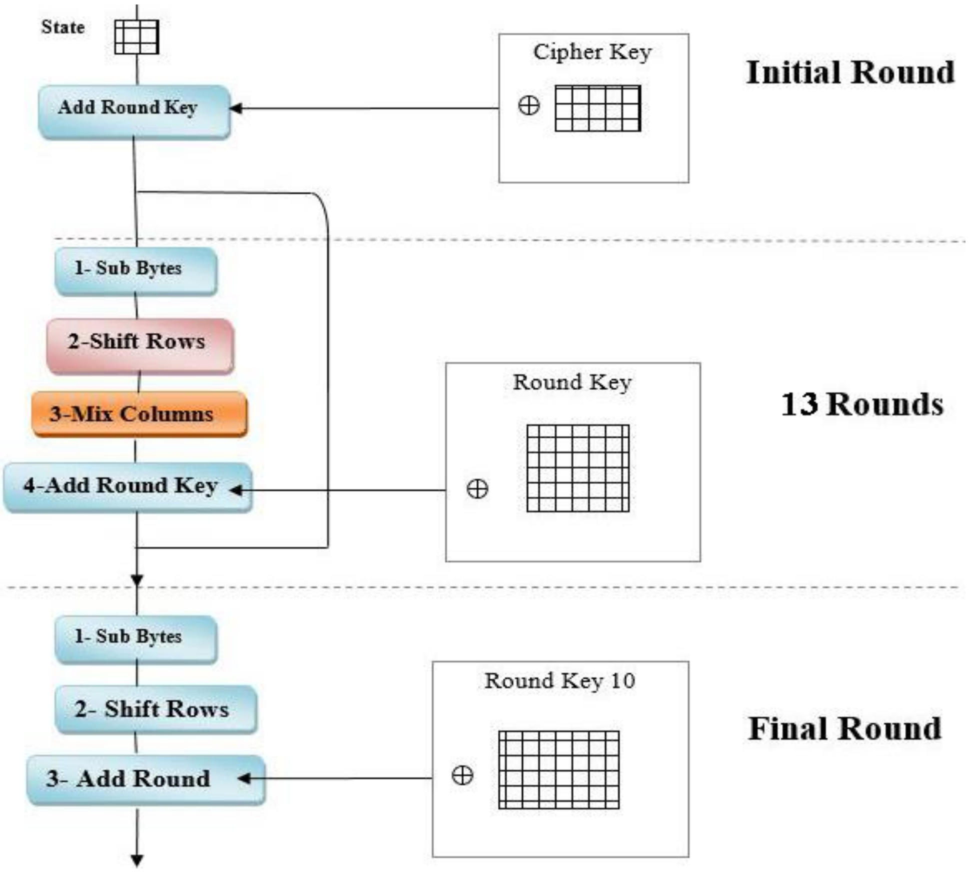


Figure 5. AES Encryption Steps [27]

3.2.1 Substitution Bytes (S-Box) and Permutation Bytes (P-Box)

In this step, the matrix elements use the table that named S-Box. S-Box is a nonlinear function. It is implemented using a 16*16 sate table. This conversion table is built based on values in Galois field that shown by GF (2^8) and it is resistant against the known attacks. The table's row and column determines input and output values that are stored in these values table. Having an element of the state matrix, we can obtained the other elements. This means that "four left bits" of elements denote the row and four right bits of elements denote the column of sate table, which is used to reverse S-Box table to decrypt. The P-Box replaces each Byte of state matrix values based on a substitution of fixed table with the new values. AES has 32 Bytes in the substitution of elements that have been organized in a 16 × 16 matrix. To replace Bytes with the equivalent, four least significant bits in Bytes as the number of rows and four most significant bits as the number of columns are applied in this state table. It is corresponding element, which is used instead of original value [27].

3.2.2. Rows Shift to the Left

First row don't have any shift, second row has 1 Byte circular shift to the left, third row has double Byte circular shift to the left and fourth row has three Bytes circular shift to the left. Circular shift is performed to the right in decryption. Since data is stored in a column in the state matrix, this step will do a permutation between columns [27].

3.2.3. Mix Columns

The linear mix of columns using matrix multiplication. Each column is processed separately. It means that each Byte replaced with a value for each of four elements in column. Mix columns in AES is the same as XOR summation, but multiplication in the AES is operated in GF (2^8). Mix columns function independently hashes each columns of the sate array and scrambling the other columns. Each column of state is multiplied in a fixed matrix to obtain new column. Matrix multiplication takes place on the GF. The GF is the Galois fields and that is not an ordinary matrix multiplication. The AES is distinguished from other existing methods. It is because this method is mathematical base, scrambling operations and hash functions [27].

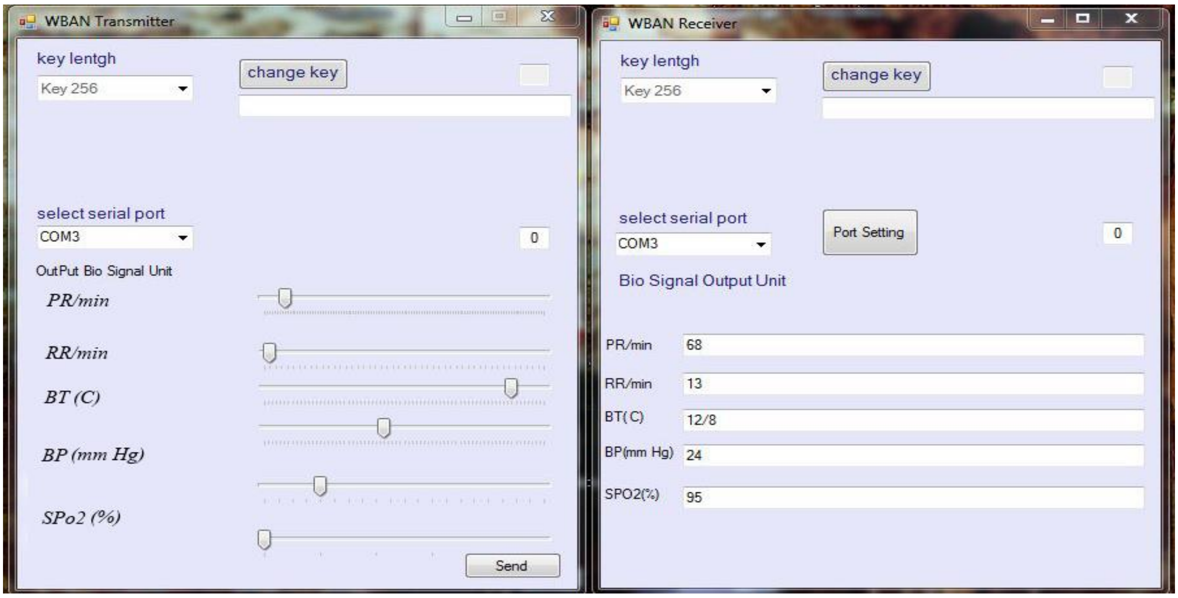
3.2.4. Add Round Key

Binary summation is down for state matrix and add round key. State Matrix is XOR with round key. This operation is performed columnar. For decryption, this operation is performed too [27].

4. Simulation Results

To show the applicability of the proposed method in the WBAN, the behavior of WBAN using the proposed method has been simulated in C#. In our simulation, the patient's bio signals have been sent to a database or medical station.

Figure 6 shows the designed WBAN emulator for encryption and decryption in the developed simulator.



WBAN Transmitter
key lentgh: Key 256
select serial port: COM3
0
OutPut Bio Signal Unit
PR/min
RR/min
BT (C)
BP (mm Hg)
SPo2 (%)

WBAN Receiver
key lentgh: Key 256
select serial port: COM3
0
Bio Signal Output Unit
PR/min: 68
RR/min: 13
BT(C): 12/8
BP(mm Hg): 24
SPO2(%): 95

Figure 6. WBAN Emulator Encryption and Decryption

In this method, after adjusting the COM port and key length, the evaluate simulator encrypt the data. Then, we send the encrypted data. On the review side, the receiver adjust COM port to receive the encrypted medical data. After receiving the encrypted medical data, the receiver decrypts the encrypted medical data.

5. Evaluation and Comparison of results

We simulated DES, 3-DES, standard AES, AES with proposed key management scheme and bio-signal encryption in MATLAB 2014 and C#. The advantages of the proposed method are confidentiality, integrity, availability, and energy efficient that are as follows.

5.1 Confidentiality

In the hole attacks, attacker deletes or sends optional packets. This subject undermines the reliability. Figure 7 shows the confidentiality in the proposed method. Reliability according to (3) is improved up to 50%.

$$Improvement = |(1 - \frac{packets\ error\ rate\ in\ the\ proposed\ method}{packets\ error\ rate\ in\ the\ old\ method})| \times 100$$
(3)

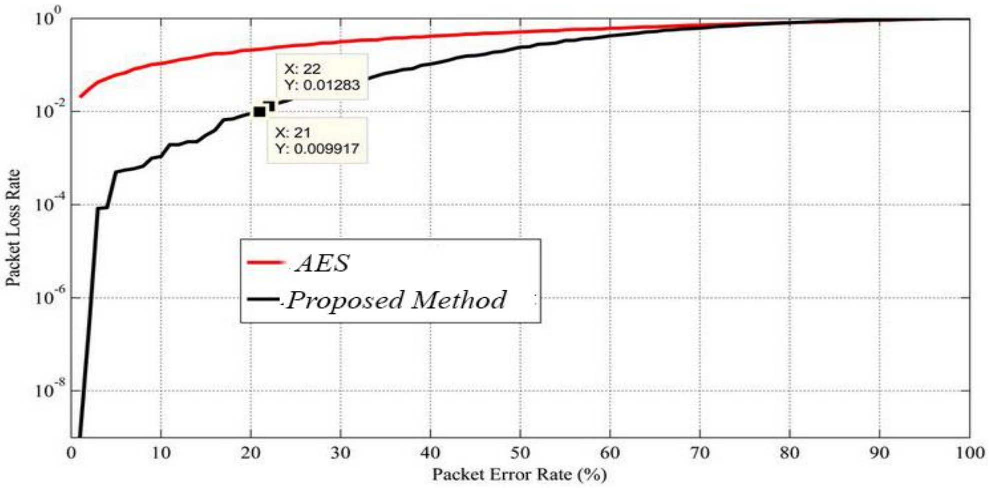


Figure 7. Confidentiality for packet loss rate

5.2. Integrity (source and data)

Data integrity is calculated based on the rate of alive nodes that see in figure 8. Alive nodes rate has improved up to 50% according to (4).

$$Improvement = |(1 - \frac{alive\ nodes\ rate\ in\ the\ proposed\ method}{alive\ nodes\ rate\ in\ the\ old\ method})| \times 100 \quad (4)$$

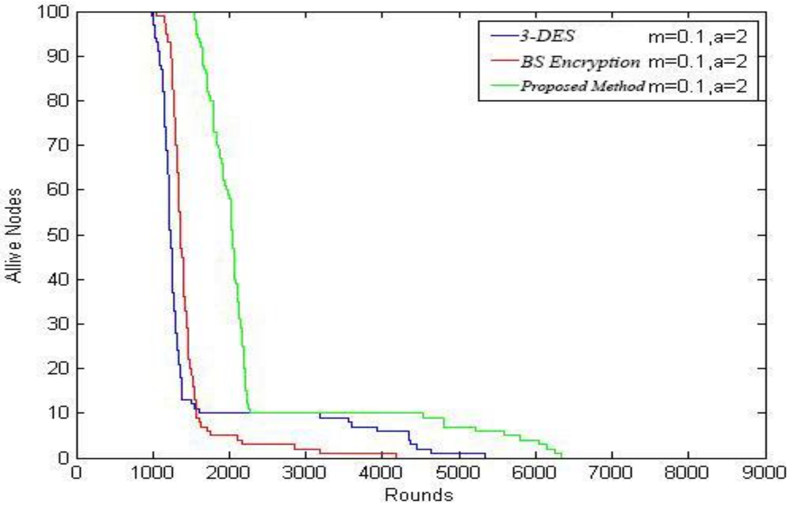


Figure 8. Integrity for Alive Nodes Rate

5.3. Availability

Ubiquity is the most important features of real-time telemedicine healthcare system. In the proposed method healthcare services have the most quality than the other encryptions as it is shown in figure 9. According to (5) Quality of Service (QoS) for received packets rate to the medical base station has improved up to 75%.

$$Improvement = |(1 - \frac{Packets\ rate\ recieve\ to\ destination\ in\ the\ proposed\ mehtod}{Packets\ rate\ recieve\ to\ destination\ in\ the\ old\ method}) \times 100| \quad (5)$$

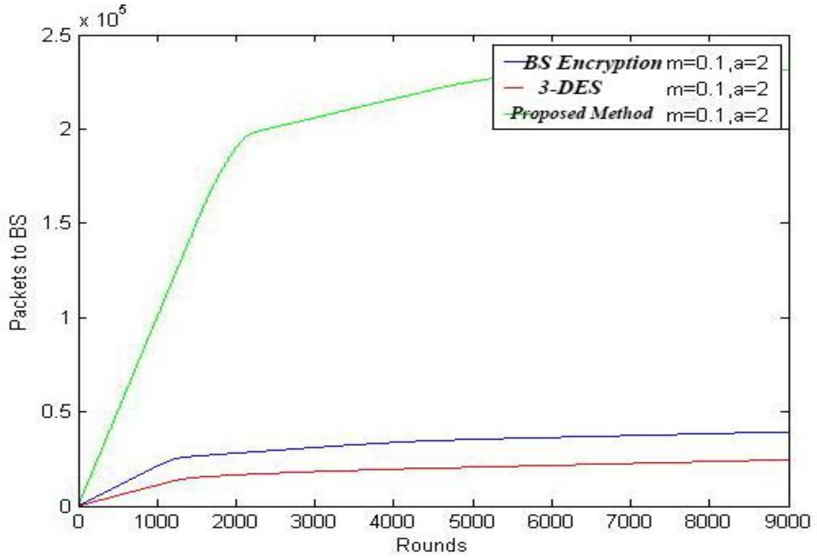


Figure 9. Quality of Service for Received Packets Rate to the Medical base Station

5.4. Energy Efficient

Figure 10 shows the bio-signal encryption using DES, 3-DES, standard AES, and AES using the proposed key management scheme power saving after 10 seconds execution.

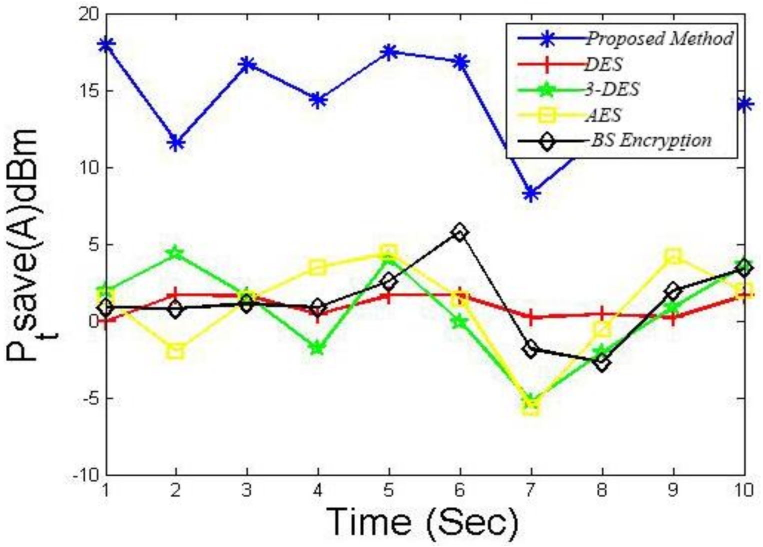


Figure 10. Energy Efficient for Packets Delay Rate

Power saving is calculated from (6). Energy efficient at least is 16.66% and it is increased up to 17%.

$$Improvement = |(1 - \frac{power\ saving\ in\ the\ proposed\ method}{power\ saving\ in\ the\ old\ method})| \times 100 \qquad (6)$$

6. Conclusion

Real-time healthcare monitoring is an important challenging issue in the telemedicine. Design of real-time and secure WBAN is the most important point in these systems. This paper presented and evaluated novel method for securing the WBAN communications. The proposed method utilized novel key management scheme to improve the security of WBANs. Using the proposed key management scheme, the outputs for the same inputs are different in the different times. In addition, we used AES-256 for encryption and decryption. The proposed method has been simulated using C# and MATLAB 2014. The simulation results showed that the proposed method has advantages compared to other methods that are used for secure WBAN communications.

References

[1] E. Abedini, A. Rezai, “A Modified Digital to Digital Encoding Method to Improve the Wireless Body Area Network (WBAN) Transmission”, 2nd IEEE Int. Conf. knowledge based eng. Innov. (KBEI), **(2015)**, pp. 219-222.

[2] A. Rahman, R. Ahmad and M. Zulfa Mohamad, “Developing Forensic Readiness Secure Network Architecture for Wireless Body Area Network (WBAN)”, Int. J. Secur. Its Appl., vol.8, no.5, **(2014)**, pp. 403-420.

[3] B. Burrows, L. R. Brown, Ch. Lavin, H. Kane, R. M. Routledge, M. Renner, B. Halweil, “Vital Signs, The Environmental Trends that are Shaping our Future: 2000–2001”, Earth scan Publication Ltd, The Worldwatch Institute of Island Press, vol. 22, no. 131, **(2015)**, pp. 9-95.

[4] M. Ameen, J. Liu, and K. Kwak, “Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications”, J. Medical Syst., vol. 36, no. 1, **(2012)**, pp.93-101.

[5] J. Daemon, and V. Rijmen, “AES Proposal: Rijndael”, Banksys Katholieke Universities LeuvzXen, Belgium, AES submission June **(2001)**.

[6] K. Van Dam, S. Pitchers, and M. Barnard, “Wireless Body Area Networks: Towards a Wearable Future”, In Proc. WWRF Kick off Meeting, Munich, Germany, **(2001)**, pp.6-7.

[7] J. L. Brooks and J. A. Goss, “Security Issues and Resulting Security Policies for Mobile Devices”, Thesis, naval postgraduate School, Monterey, California **(2013)**.

[8] P. J. Chuang and T.Y. Chu, “An Efficient Multicast Routing Protocol in Manets”, Adv. Sci. Tech. Lett., vol.41, **(2013)**, pp.21-25.

[9] S. Lim, T. Oh, Y. Choi, and T. Lakshman, “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring”, in proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, and Trustworthy Comput. (SUTC), **(2010),** pp. 327 - 332.

[10] P. Kumar, and H. J. Lee, “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey”, Sensors, vol. 12, no.1, **(2012)**, pp. 55-91.

[11] Hague, M and Ahmed, Sh. I, “Security in Pervasive Computing: Current Status and Open Issues”, Int. J. Netw. Secur., vol.3, no.3, (2006), pp.203-214.

[12] Bhaskar, P, Ahamed, Sh. I, “Privacy in pervasive computing and open issues”, Int. J. Netw.ork Security, (2007), vol.3, no.3, pp.203-214.

[13] K. Hur, W.S. Sohn, J. K. Kim and Y. S. Lee, “IEEE 802.15.6 WBAN Beaconing for Wireless USB Protocol Adaptation”, Int. J. Software Eng. its Appl., vol. 7, no. 4, (2013), pp. 1-14.

[14] J. Huang, “On the Internal Structure of the Advanced Encryption Standard and Two AES-based Cryptographic Constructions”, School of Computer Science and Software Engineering, University of Wollongong, no. 3517, **(2012)**.

[15] S. Soltani, A. Rezai, “A Novel Low Power and Low Voltage Bulk-Input Four-Quadrant Analog Multiplier in Voltage Mode”, International Journal of Multimedia and Ubiquitous Engineering, vol. 11, no. 1, **(2016)**, pp. 159-168.

[16] A. Rezai, P. Keshavarzi, and Z. Moraveji, “Advance Hybrid Key Management Architecture for SCADA Network Security”, Sec. Comm. Netw. Doi: 10.1002/Sec. 1612 **(2016)**.

[17] A. Rezai, P. Keshavarzi, and Z. Moraveji, “Key Management Issue in SCADA Network: a Review”, Eng. Sci. Tech., int. j. Doi: 10. 1016/ j. jestch. 2016.08.011. **(2016)**.

[18] A. Rezai, P. Keshavarzi, and Z. Moraveji, "Secure SCADA Communication by Using a Modified Key Management Scheme", ISA Trans. Vol. 52, no. 4, **(2013)**, pp. 517-524.

[19] A. Rezai, and P. Keshavarzi, "A New Left-to-Right Scalar Multiplication Algorithm Using a New Reading Technique", Int. J. Sec. APP., Vol. 8, no. 3, **(2014)**, pp. 31-38.

[20] A. Rezai, and P. Keshavarzi,"CCS Representation: A new non-adjacent form and its application in ECC, J. Basic Appl. Sci. Res., Vol.2, no.5, **(2012)**, pp.4577- 4586.

[21] A. Rezai, and P. Keshavarzi, "High-performance scalable architecture for modular multiplication using a new digit-serial computation", Microelec. J., Vol. 55, **(2016)**, pp. 169–178.

[22] A. Rezai, and P. Keshavarzi, "A New Finite Field Multiplication Algorithm to Improve Elliptic Curve Cryptosystem Implementations", J. Inf. Syst. Telecomm., Vol.1, no. 2, **(2013)**, pp.119-129

[23] A. Rezai, and P. Keshavarzi, "High-Throughput Modular Multiplication and Exponentiation Algorithm Using Multibit-Scan-Multibit-Shift technique", IEEE Trans. VLSI syst., Vol. 23, no. 9, **(2015)**, pp.1710-1719.

[24] A. Rezai, and P. Keshavarzi, "Compact SD: A New Encoding Algorithm and Its Application in Multiplication", Int. j. comput. Math. Doi: 10.1080/00207160.2015.1119269, **(2016)**.

[25] A. Rezai, and P. Keshavarzi, "Algorithm Design and Theoretical Analysis of a Novel CMM Modular Exponentiation Algorithm Large Integer", RAIRO- Theor. Inf. Appl., Vol. 49, no. 3, **(2015)**, pp. 255-268.

[26] R. Khalilian, A. Rezai, and E. Abedini, "An efficient method to improve WBAN security", Adv. Sci. Tech. Lett., vol. 64, **(2014)**, pp.43-46

[27] W. Stallings, "Cryptography and Network Security, Principle and practice", 5th Edition, chapter 5, Vice president and editorial dire, **(2012)**.

Authors

Reza Khalilian received the B.S. degree from department of ICT engineering of ACECR (IUT) in 2011. M.S. degree from Majlesi City University in 2014. Associate in the Electronics at Shahid Rajaie University of technology in 2008. He is currently an engineer at department of computer and digital media institute in KHIUSF, producing digital library. His research interests: Bio-electric; WBAN (security, energy efficient, bio-signals, bio-Sensors, design and architecture, hardware, telemedicine, information theory and codding, prevention cancer).

Abdalhossein Rezai is an assistant professor in Academic Center for Education, Culture and Research (ACECR), Isfahan University of Technology (IUT) branch, Isfahan, Iran. He received Ph.D. degree from Semnan University, Semnan, Iran in 2013, M.S. and B.S. degree from Isfahan University of Technology (IUT), Isfahan, Iran in 1999, and 2003, respectively. His research interests include network security, cryptography algorithm and its application, and neural network implementation in Nano electronics.

Farhad Mesrinejad received his B.Eng. (1993) in electronic engineering and M.Sc. (1997) in communication system engineering from Islamic Azad University of NajafAbad. He also received his Ph.D. (2012) in communication and network engineering from University Putra Malaysia (UPM). He is assistant professor at the department of electrical and computer engineering, and works in advanced engineering research center Islamic Azad University of Majlesi. His research area is IP-based wireless sensor networks, 6LoWPAN, wireless communications, image and signal processing.