DESIGN AND IMPLEMENTATION OF LIGHTWEIGHT ENCRYPTION ALGORITHM FOR WBAN

Dhivyadevi.R[1], Priyadharshini G[2], Preetha K[3], Poojha M[4]
Department of Electronics and Communication Engineering
KPR Institute of Engineering and technology, Coimbatore
[1]Asst.Prof, [2,3,4]Student scholars

Abstract

In wireless body area network (WBAN) the data gets corrupted during transmission and reception due to noises and inter-WBAN interference. WBAN must support the combination of low energy consumption and high reliability, but powerful encryption code increase the processing energy consumption of the receiver. So there is a trade-off between the transmitter and the processing energy consumption in the network. For e-health monitoring in WBAN systems transmission of body signals must be fast to ensure immediate diagnosis and health assistance. This requires a high power and energy efficient lightweight codes to reduce the power consumption to enhance the network lifeline

Keywords: *encryption, e-health, power consumption, Wireless body area network*

1. Introduction

WBAN is the realization result of the growing use of wireless networks. WBAN stands for wireless body area network which acts as a wireless communication networks for among the sensor nodes. The signal from the sensors which can be attached in and across the frame need to be accrued and dispatched at once. The statistics protection is an crucial thing to be assured in WBAN device. Data confidentiality prevents unauthorized get entry to the message or information via encryption algorithm and the best
tool which has safety key can decrypt the facts. The changes are prevented by way of message integrity which can be done by using an trespasser and this guarantees the message from transmitter ,not from the trespasser. At the receiver the message from the transmitter is demonstrated by data authentication. The recurrent message are avoided via replayed protection which can be universal by using the receiver. In order to gain this carrier, the consumer assign a series number to each packet and the packet with small sequence range are rejected on the receiver

2. Overview on wireless body area network

WSN (Wireless Sensor Network) has special applications and usages anywhere specifically in health care system and defence industries. In health care structures the WSN generation is carried out in the form of wireless body area network(WBAN). In order to measure diverse physiological activities of a affected person and document them continuously for scientific observation the WBAN includes a set of small independent sensor node of various types which are worn by the patients or implanted inside the patient's body. The clinicians display the sufferers remotely for the sensed records recorded by means of the sensors that's send to the health center network cloud for diagnosis purpose. This is depicted in Fig1. ECG (Electrocardiography), EMG (Electromyography), EEG (Electroencephalography) are the most usually used physiological sensors for monitoring heart
muscle and brain functioning respectively.

The foremost barriers for WBAN are bandwidth, dynamic topology, battery energy, overall performance and so on., which makes them exposed to protection assaults. Nevertheless WBAN has been efficiently stationed in fitness cares which incorporates monitoring of patient's fitness and e-health offerings. Overall throughput, robustness, flexibility and availability of WBAN is improved through its connectivity with the cloud.

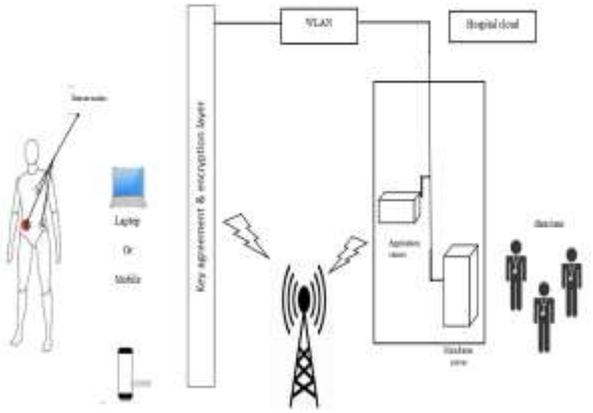

Fig1. WSN in health care systems

Therefore the memory garage and computational power is likewise extended.The proposed gadget makes use of mild weight encryption algorithm that is a cryptographic technique that has low computational complexities. The proposed set of rules is designed for WBAN to address security and reliability.

3. Literature review

3.1 "AN ENERGY EFFICIENT DECODING SCHEME FOR LDPC CODES IN WIRELESS BODY AREA SENSOR NETWORKS"

Javaid N, Rehman O, Alrajeh N, et al. Proposed a traditional studies work that specializes in minimizing power[1]. The power required for decoding is significantly large than the transmitting for accomplishing the preferred BER, we require iterative message passing set of rules for low Density Parity Check Code (LDPC). To offer faulty transmission in WBAN automated repeat requests (ARQ) method is applied by using the usage of ARQ protocol. Error correcting codes are used to reduce the variety of re-transmission. ECC require procedure electricity on the sensor node. In LDPC Code a clause of linear block code and their parity take a look at matrix contains just a few number of 1s in evaluation of 0s. They may be represented as tanner graph, that comprise sets of nodes i.E the test node and the variable node. Belief propagation set of rules are used to decode LDPC codes and this gives /allows in a hit interpreting. In order to lessen the number of iterations this paper proposes an efficient early stopping technique AID. AID predicts the threshold for the iterations of a block. This approach is efficient giving low SNR and thereby decreasing the processing delay. By this technique we will reduce 20 to 25% of the total energy consumption.

3.2 "LEA: 128-BIT BLOCK CIPHER FOR FAST ENCRYPTION ON COMMON PROCESSORS"

D. Hong, J.-K. Lee, D.C. Kim et al., presented a new block cipher LEA, of 128 BIT block size and 128,192 or 256 bit key size[2]. This processor provides a high speed software. LEA is faster than AES on Intel, AMD, ARN. LEA provides security against all the existing attacks on block ciphers. The important information must be protected from various threats in the network, it implies the use of cryptographic system in software platform. The encryption in software is easy when compared to the hardware system. For message authentication, data encryption random bit generation block ciphers are widely used in cryptographic primitives. In order to simplify the structure light weight block ciphers are used. The plain text is converted in to a cipher text in the process of encryption whereas in decryption the reverse process is applied. The LEA encryption procedure consists of 24 rounds for 128-bit keys. For a round structure with 32-bit ARX operation we need two keys XORs, one addition and one bitwise rotation. These are the characteristics of the Canteaut-Chabaud method. This simplification provides small-sized hardware and software. The security analysis of cryptographic technique is done by searching, constructing various characteristics such as differential and linear traits. Different possible attacks occur while maintaining security, viz., linear attack, differential attack, integral attack, linear correlation attack, boomerang attack. The security against these attacks is provided by implementing a tiny code size. Thus proper optimization in power and area is obtained along with secured data transmission.

3.3 “DATA SECURITY AND PRIVACY IN WIRELESS BODY AREA NETWORK”

The WBAN is an emerging technology in E-health care. That allows data of the patients and body movements that are collected by the body sensors. Ming Li and Wenjing Lou proposed a method that is highly used in emergency medical response systems[3]. There is a big challenge while considering the security and usability of the patient’s private data. This data of the patient is shared among doctors, health care staff, insurance companies, researchers, etc., This technique eliminates the need of the people to visit hospitals frequently and can also monitor their health periodically. The vital signals from the body such as ECG, EEG, pulse rate, blood pressure etc., are sensed and collected by the body sensors, the collected data is transmitted to one or more local servers to perform data processing where the axis control should be context-aware and flexible. Through data privacy only the authorized person can access the data. To provide secured data storage the information from the patient should be stored without any leakage and must be highly confidential. By introducing new and enhanced cryptographic techniques we can provide a better solution for data security. SKC-based scheme, PKC-based scheme and several other schemes are used to access data. In emergency health care it is important to allow on-demand access policy adaptations. This facility offered by the WBAN system will change people’s health care experiences by providing a more secure, private and reliable design.

3.4 “A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design”

Azza Zayed Alshamsi, Ezedin Salem Barka, and Mohamed Adel Serhani have put forward that to maintain the medical ethical principles, the wireless body area networks must explore and adopt amongst the widespread security suggestions[4]. The additional power intake added by means of the security schemes is estimated primarily based on the hardware additives (microprocessor and radio), network topology and the MAC frame. Low power WBAN devices support data rates ranging from 10Kb/s to 10Mb/s and guarantee sensitive personal data protection. Here the standard CCM mode is used for the security services. The confidentiality and authenticity of the encrypted data is assured by the Counter with Cipher Block Chaining - Message Authentication Code (CCM). The proposed secure scheme consists of the phases namely master key, pre-loading, neighbor discovery, link key computation and key update. There is no need for key re-initialization for communication with fixed participants. The energy dissipation produced by the security services is estimated by using the off-shelf components, microprocessors and radio. Thus a specific microprocessor design is proposed that reduces the energy dissipation in the overall system design and ensures accelerated security functionality. This microprocessor design enables the system to achieve more energy efficiency with further reduction in the frequency or voltage. Also, the commercial processor is replaced by a new custom and optimized processor that uses less memory and less clock cycles to deliver the output.

4. Lightweight encryption algorithm

LEA is a lightweight block cipher introduced in 2014 by the Electronics and Communication Research Institute in Korea. LEA uses ARX design for its algorithm which is very efficient small devices with limited resource due to its small code size and low power consumption. LEA uses a block size of 128-bits and variable key sizes of 128, 192 and 256-bits. Based on the key size being utilized the LEA algorithms are represented as LEA-126, LEA-192 and LEA-256. The algorithm operates in two stages namely the round key generation and the encryption/decryption process.

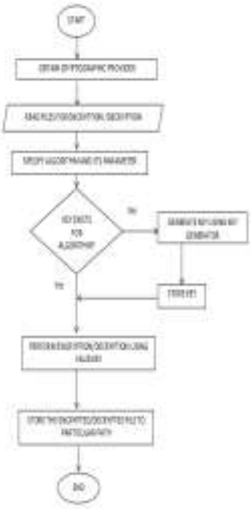

Fig2. Flow of LEA process

Existing AES algorithm

Advanced encryption standard has four stages in a single round of operation (Fig.5). The number of transformation rounds depends on the size of the key, here we use a 128-bit key and a set of 10 rounds is performed for both encryption and decryption process. In case of 192-bits or 256-bits key size the number of transformation rounds will be 12 or 14 respectively.

Initial step is called SubBytes, this is a non-linear substitution step where each byte is replaced with another according to a lookup table. The Subbytes step is followed by ShiftRows which is a transposition step where each row of the state is shifted cyclically a certain number of steps.

The output of the sub byte step passed to the next stage called the Mix Columns which is a mixing operation that operates on the columns of the state, combining the four bytes in every column.

Finally, Add Round Key wherein each byte of the dominion is blended with the round key. The sub key delivered through using combining it with each byte of the state using bitwise XOR operation.

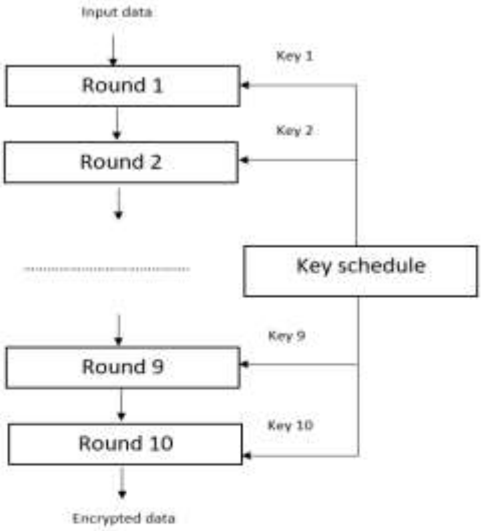

Fig3. Data path for data block and key size of 128 bits

Description of proposed algorithm

The proposed design is to provide data transmission with optimized area and power consumption using an efficient Lightweight Encryption Algorithm(LEA) in WBAN. In this process the patient's vital signals such as pulse rate, heart rate etc., will be sensed by the sensors and the sensed data is securely encrypted using modified algorithm. Later the encrypted data will be sent to the mobile stations where the data will be decrypted. The WBAN sensor imposes certain constraints like memory space limitation during its implementation. Therefore, memory efficient design algorithm must be considered.

The proposed architecture will provide high-speed and low area constraints for suitable implementation of Advanced Encryption Standard (AES). The vital body signals like ECG signal is collected from the patient's body as input data and then encoded by using the modified algorithm.

The modification in the algorithm is done by merging the steps SubBytes and ShiftRow into a single step (Fig.6). Since the final position of each byte of the ShiftRow step is already known the generated bytes after the SubBytes step is directly stored in their respective shifted positions. This process helps to eliminate the necessity to perform a separate step for shifting rows. This reduces the additional pipelined resources.By using this modified encryption algorithm the overall power consumption and area can be reduced.

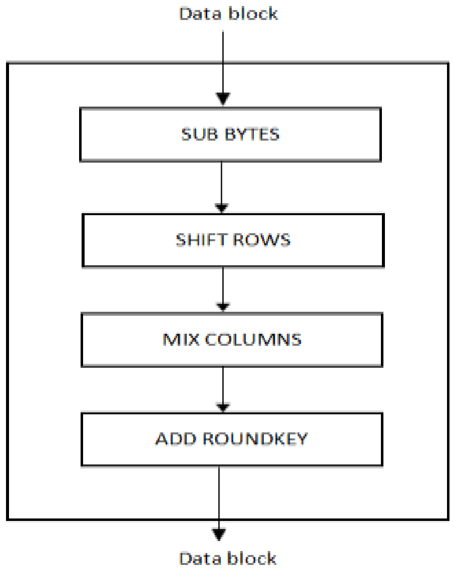

fig5.Structure of one internal round in existing algorithm

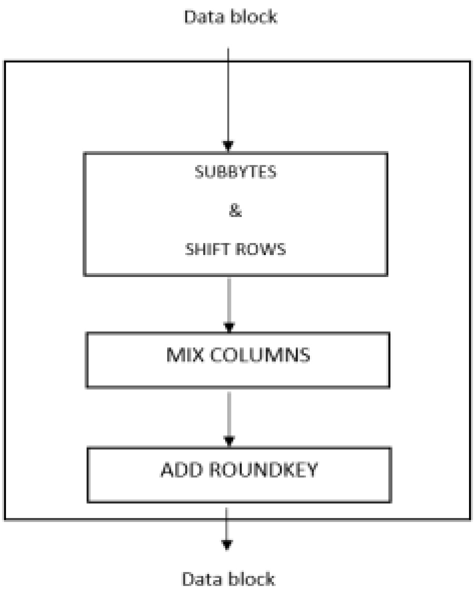

Fig6. Structure of one internal round in modified algorithm

5. Results

The synthesis and analysis of the proposed system is done using the Xilinx ISE tool. With the implementation of the proposed work the results have been tabulated. Table 1. shows the comparative results of the overall delay (in nanoseconds) and power (in watts) between the existing and proposed work. Table 2. includes the device utilization between the existing and proposed work. Table 3. represents the comparative Power Analysis report. Thus, on implementation of the modified algorithm and with the results it is noticeable that the proposed work surpasses the existing algorithm.

Table 1.Overall Delay and Power comparison table

S.No.	***WORK***	***OVERALL DELAY (ns)***	***POWER (W)***
1	EXISTING	1.570	7.100
2	PROPOSED	0.656	3.908

Table 2.Comparative Device Utilization Summary table

S. No.	***WORK***	***NO. OF SLICE REGISTERS***	***NO. OF SLICE LUTs***
1	EXISTING	512	1,091
2	PROPOSED	256	64

Table 3.Comparative Power analysis table

S.No.	***EXISTING WORK***		***PROPOSED WORK***	
	On-Chip	**Power (W)**	**On-Chip**	**Power (W)**
1	Clocks	0.151	Clocks	0.075
2	Logic	0.184	Logic	0.004
3	IOs	4.194	IOs	1.410
4	Leakage	2.444	Leakage	2.380
5	Total	7.100	Total	3.908

6. Conclusion

The WBAN system is an emerging technique for e-health monitoring in health care. The WBAN sensors are designed to collect the patient’s vital signals and transmit them to the servers in health care units for further diagnosis. The possible data corruption is overcome by cryptographic applications. Thus the proposed design follows a lightweight algorithm to ensure fast and energy-efficient transfer of data along with security and reliability.

References

1. Javaid N, Rehman O, Alrajeh N, et al ,“AID: An energy efficient decoding scheme for LDPC codes in wireless body area sensor networks”, in Procedia computer Science,21, 2013, 449-454.
2. D. Hong, J.-K. Lee, D.C. Kim, D. Kwon, K. H. Ryu, and D.G. Lee, “LEA: A block cipher for fast encryption on common processors”, in Information Security Applications, ed: Springer,2013, pp. 3-27.
3. Bhoopal Rao Gangadari, Shaik Rafi Ahamed, “Programmable Cellular Automata based low power Architecture to S-Box : An Application to WBAN”, Springer, Circuits, Systems, and Signal Processing, vol. 37, 2017, pp.1116-1133.
4. Ming Li, Wenjing Lou, Kui Ren, “Data Security and Privacy in Wireless Body Area Networks”, in IEEE Wireless Communications, 2010, 17(1) 51-58.
5. Azza Zayed Alshamsi, Ezedin Salem Barka,Mohamed Adel Serhani, “Lightweight encryption algorithm in WBAN for e-Health monitoring”, 12th International Conference on Innovations in Information Technology (IIT),IEEE,vol.144, 2016, pp.978-1-5090-5343-8.
6. Bogdanov and M. Wang, “Zero correlation linear cryptanalysis with reduced data complexity”, in Fast Software Encryption, 2012, pp.29-48.
7. E. Biham, A. Biryukov , and A. Shamir , “Cryptanalysis of skipjack reduced to 31 rounds using Impossible differentials, “Journal of Cryptology”, vol.18, pp.291-311,2005.
8. L. Knudsen and D. Wagner, “Integral cryptanalysis” in Fast Software Encryption ,2002, pp.1112-127.
9. S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, “A biometric-based security for data authentication in wireless body area network (wban)”, in Advanced Communication Technology (ICACT), 15th International Conference, pp. 998-1001, 2013.
10. D. Lee, D.-C. Kim, D. Kwon, and H. Kim, “Efficient hardware implementation of the lightweight block encryption algorithm”, Sensors, vol. 14, pp. 975-994, 2014.

11. M.Chen, S.Gonzalez, A.Vasilakos, H.Cao, and V.C.M.Leung, “Body area networks: a survey”, MONET., vol. 16, no. 2, 2011, pp. 171–193.
12. R. L. Rivest, M. Robshaw, R. Sidney, and Y. L. Yin, “The RC6TM block cipher,” in First Advanced Encryption Standard (AES) Conference, 1998.
13. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, et al., “HIGHT: A new block cipher suitable for low-resource device,” in Cryptographic Hardware and Embedded Systems-CHES 2006, ed: Springer, 2006, pp. 46-59.
14. S.Rajagopalan and S.Rethinam and S.Janakiraman and H.N.Upadhyay and R.Amirtharajan, “Cellular automata synthetic image: A trio approach to image encryption”, ICCCI, 2017, pp. 1–6.