Pak. J. Biotechnol. Vol. 14 (2) 257–264 (2017)
www.pjbt.org

ISSN Print: 1812- 1837
ISSN Online: 2312- 7791

A 128-BIT SECRET KEY GENERATION USING UNIQUE ECG BIO-SIGNAL FOR MEDICAL DATA CRYPTOGRAPHY IN LIGHTWEIGHT WIRELESS BODY AREA NETWORKS

M.V. Karthikeyan[1], J. Martin Leo Manickam[2]

Department of Electronics and Communication Engineering, St.Joseph's College of Engineering, OMR, Chennai-119, India. E.mail: Karthik.me09@gmail.com; [2]Departnment of Electronics and Communication Engineering, St. Joseph's College Of Engineering, Tamilnadu, Chennai - 600119, India. E.mail: josephmartin74@yahoo.co.in

ABSTRACT

In wireless Body Area Sensor Networks, the communication with the In-body Medical sensor node placed inside the patient must be crypto graphed to protect it. Existing wireless sensor network modes are not suitable for Wireless Body Area sensor Networks (WBAN) as these are resource constrained devices. Securing the implanted device in WBAN is essential for preserving not only the privacy of patient data, but also for ensuring safety of healthcare delivery. This paper presents a secret key generation scheme from the ECG signal parameters and allows device authentication. The proposed model allows the doctor to generate secret key from the ECG signal parameter of the patient without using the battery power of IBS node and providing authentication for both nodes without any initialization or pre-deployment of secret key. Simply we can deploy the sensor in a WBAN and make them to communicate securely (a plug and play model). In our analysis, result and compared with other key generation protocols. Showing that proposed method is a viable key generation and key agreement model for WBAN.

Keywords – ECG, In-body medical sensor, Secure Force Algorithm, Daubechies wavelet 4.

1. INTRODUCTION

The Wireless Body Area sensor Network (WBAN) was first invented by T.G.Zimmers in 1996. At that time, it was simply an extension of the existing technology known as wireless personal area networks. In the History of WBAN (IEEE 802.15.6 & IEEE802.15.4J) Initially Wireless Next Generation (WNG) was established in January 2006 (Kwak *et al.*,2010) within Working Group(WG15). Then in the year May 2006, Interesting Group of WBAN, (IGWBAN) was established (Astrin *et al.*, 2009). Then IGWBAN converted into study group SGWBAN by IEEE 802.15 and certified as Task Group TG6. In May 2008, the TG6 submitted all the analysis into a single document after its call. In April 2010, IEEE802.15.6 established the first standard of WBAN, and an optimized low power on body/in body nodes for various applications in medical and Non-medical fields. In the later year, at February 2012 a full and approved version of IEEE802.15.6 was published and its aim is: "To develop a communication standard for low power devices and operation on, in or around the human body (not limited to humans) to serve a variety of applications including medical, personal entertainment, consumer electronics and others". The IEEE802.15.6 has provided its latest international standard for providing low power, short range and reliable wireless communication around human body with 75.9 Kbps for a narrow band and extended it upto 15.6Mbps for ultra wide band. Table 1. Shows the various WBAN frequencies (Kwak *et al.*, 2010; Tachtatzis *et al.*, 2010) allocated by IEEE 802.15.6. The WBAN devices must be properly explored because the expected health care expenditure at 2022 is to reach 20% of the gross domestic product (GDP). The various WBAN Frequency Band:

Table 1: WBAN Frequency Range

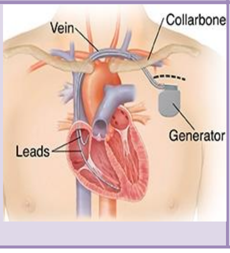
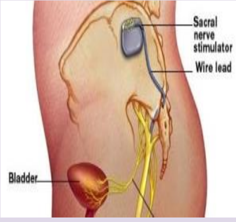
HBC		**MICS BAND**	**WIRELESS MEDICAL TELEMETRY SERVICE(WMTS)**			**WIFI ZIGBEE BLUETOOTH**	**UWB**
HF	**VHF**	**402-405 MHZ**	**608-614 MHZ**	**1395-1400 MHZ**	**1427-1432 MHZ**	**2.4GHZ**	**3GHZ 10GHZ**
14 -18 MHZ	**25-29 MHZ**						

II. IMPLANTABLE MEDICAL DEVICES

The Implanted Medical devices are a miniature structures placed inside the patient's body to perform some lifesaving functions. The processor, memory and battery are of small in size and battery can be changed rarely maximum of 5-10 years. Where these batteries are not-reachable and fixed inside the patient's body have a lot of limitations and make IMDs (Denning *et al.*,2010) security design a more challenging one when compared with other medical devices (as security consume battery power twice the power of a normal operation). WBAN is being applied in medical, nonmedical areas and also in astronaut space suits. Of all these inventions and standards still WBAN has not seen its complete form. Recent studies have also proved the various kinds of attacks on IMDs. The Implantable Cardiac Defibrillators (ICDs), neuro stimulators and implantable drug delivery systems use miniaturized embedded boards for health monitoring and post-operative purpose to perform automatic functions. Table .2 shows the history of Implanted medical devices. Now the latest development technology era, is an external device called Radiowave frequency programmer is designed to perform various tasks such as communication, data extraction and controls with the internally adopted IMDs.

- Development of IMD

Table 2. History of IMDs

FIRST PACE MAKER	FIRST IN-BODY PACEMAKER	FIRST SPINAL CORD SIMULATIONS	FIRST COCHLEAR IN-BODY SURGERY	ICD	BLOOD GLUCOSE MONITOR (WIRELESS)
1926	1960	1967	1978	1985	2006
					

This exposure of the (Radio-wave) wireless module in IMDs to the surrounding have created many security issues and attacks. One such feared of situation arise, to the top most person of the U.S.Government (U.S.Vice – President). In Dick Cheney's case, doctors advised to put off the wireless module in Cheney's pacemaker and he underwent a surgery in the year 2010 to switch off the wireless module. Of all these issues, we had taken the secure communication of medical data between the sensor nodes as a mandatory one. The data that is communicated must assure confidentiality, integrity, authentication, data freshness and non-repudiation with failure of any one the above parameters, the medical data received can't be used for diagnosis. To protect the medical data the existing cryptographic security methods like Asymmetric, Symmetric and cryptographic signatures (Karthikeyan *et al*.,2010) are analysed. Asymmetric key cryptographic uses public key and private key for encryption and decryption. There is no need to pre-deploy the key in sender and receiver end nodes. But the process overhead is high consuming more resources, making it a unsuitable security model for WBAN. But where RSA, ELgammal and ECC are still implemented. In symmetric key crypto systems like AES, DES, IDEA, RC4, RC5 a common secret key is shared between the sender and receiver node. Pre-deployment of secret key is not recommended in WBAN because of its small memory and repeated key usage can reveal the key, but used in majority of the WBAN systems. Many other security systems are being proposed in combination or separately with the cryptosystems additional integrity and authentication. They are Hash function, Digital signature and polynomials.

III. RELATED WORKS

In (Zhang *et al*.,2006) (Shu-di Bao *et al*.,2008) the authors have implemented a Biometric based key generation scheme, using the inter-pulse interval of the ECG. They have generated a 128-bit secret key. But the analysis is made in time domain which increases the computation time and not suitable for WBAN scheme. The Fuzzy vault scheme (Venkatasubramanian *et al*., 2008) deals with a random set data receiver of different patient and is an error tolerant scheme. It uses a 128-bit Bio-secret key and this system uses polynomial reconstruction and fuzzy to secure the data.

In physiological signal, based key agreement (Venkatasubramanian *et al*., 2010), Fuzzy vault is used for inter-sensor communication which is a suitable design for Biomedical based secure data sharing system. It uses a 128-bit secret key for data encryption and decryption. But the extra overhead in additional chaff point's generation makes it an imperfect solution.

In (Zhaoyang Zhang *et al*., 2010), improved Juel's algorithms (IJS) the author used an advanced fuzzy vault scheme. This scheme is used in real time systems to improve the authentication. This scheme proves to be a more suitable model for WBAN as there is no chaff point generation implementation. He generated a 128-bit secret key using the Bio-medical signal from the patient. This scheme has provided a better error tolerance than to previous scheme and has an optimal value of the entropy loss. Still the scheme has a higher order vault size and a disadvantage of no chaff point.

The Authors (Halpetin *et al*, 2008) had demonstrated about the active and passive attacks, on the wireless communication channel. In this if the advisory is equipped with a commercial programmable device, he can easily launch an passive attack on the ICDs. Thus, breaching the privacy of the patients' medical information's like medical ID number, medical parameters and history of the patients, etc. When an active attack is launched, it's possible to change the fibrillation modes or change in the treatment to the patients. All these are possible as the data through the wireless communication channel between the programmer and ICD is in plain text form.

Another similar work is demonstrated by Li et al (Li *et al*., 2011) in a commercial glucose monitoring system and in insulin delivering pump. When an active attack is made on these devices, it is possible to change the data obtained from the glucose monitor and when a compromise is made on the insulin pump, the discharge of insulin to the patient will be stopped/ injected to a higher value than prescribed. The active attacks on ICDs are life threatening to the patients and therefore, the security of communication underlying in ICD must be addressed before its wide spread of deployment in patients is established.

In the work proposed by Shu di *et al.,* (2008) for key agreement, the time interval between the RR intervals is taken to generate the secret key and device authentication, but due to more time consumption in sensing the ECG signal, the model was not fully successful.

Then author (Venkatasubramanian *et al.*, 2010), applied the frequency parameters of the ECG signal are extracted and a 128-bit secret is generated for data security and device authentication, but using Fuzzy vault (V^{th} order polynomial) made the process complex and the additional chaff points added the extra overhead made it a less suitable model for WBAN.

In this paper, we have presented a new scheme, Biomedical based secret key generation [BSKG]. The 128- bit secret key is generated from the real time ECG signal parameters of the patient, in this key generation process various parameters of the ECG signal are calculated and 128 bits are formed, these bits are random and highly unique, that do not occur. Thus, by sensing the ECG signal for one minute a key is generated that archives the objective of secret key generation and device authentication without any key predeployment. We had used the light weight secure force (SF) algorithm for generating the 128-bit secret key from the ECG signal parameters and for device authentication. Where the secret key k1, k2, k3, k4 and k5 are formed by the programmer end and not by the IBS. Thus, SF algorithm archives the goal of WBAN and protects the IBS from attacks and also increases the battery life. In the below given table. 3 the various existing key generation and key agreement techniques are given. It shows from where the input for key generation is taken, the security code used to encrypt the data and the other major parameters that provide weightage for the proposed method.

Table 3: Comparison with existing models

PARAMETERS	**WBAN KEY AGREEMENT MODELs**			
	(Venkatasubramanian *et al.*,2008)	(Venkatasubramanian *et al.*,2010)	(Shu-Di Bao *et al.,2008)*	**Proposed method**
128 Bit Key Generated With	Blood pressure, Glucose	ECG signal frequency	ECG signal RR-Interval	ECG signal parameters
Cryptographic Code	Nil	Fuzzy vault	Fuzzy commitment	Secure Force algorithm
Process Overhead	Less	High	High	**Less**
Key Complexity	Less	High	High	High
Security Level	Less	Unbreakable	Unbreakable	Unbreakable
Memory Occupied	Less	High	High	**Less**

In the above table 3. its easily understood that ECG signal parameters are used to generate the secret key, the process over head is less as SF is designed for WSN and the memory occupied is less as the key generation is not performed by the IBS. Thus, it is clearly visible that the proposed method is a better key generation (Key$_{128}$) and device authentication model.

IV. KEY GENERATION SYSTEM DESCRIPTION

(a) **ECG signal features extraction using daubechies4 (DB4) wavelet:** The ECG signal is the electrical activity of the heart beat which is a unique pattern for every individual which can be used to form a Biomedical pattern to identify and authenticate the individual. The ECG signal shown in Figure. 1. has four entities–P wave, QRS complex, T wave and U wave (Balaji et al., 2015). The P wave is an overlap pattern and very strong that represent the artial depolarization. Next QRS complex arises due to the ventricular depolarization, and T wave represents the ventrical depolarization shows the end of cardio cycle. In many systems, the U wave is neglected as they don't show any significant value in heart- beat. We identify the distinct feature of the ECG signal with the DB4 wavelet the DB4 wavelet (Mahmoodabadi *et al.*, 2005) and recommend DB4 is the suitable model to extract the features and noise elimination (Maheswari *et al.,* 2017) in ECG signal. Thus, we have implemented DB4 for a feature extraction using Matlab. In this we have 2^1 to 2^5 level of decomposition. But a 2^8 level of decomposition of ECG signal gives a better output (it's not performed due to its complex nature). The DB4 also eliminates the Baseline drift elimination and removal of 50Hz supply frequency noise.

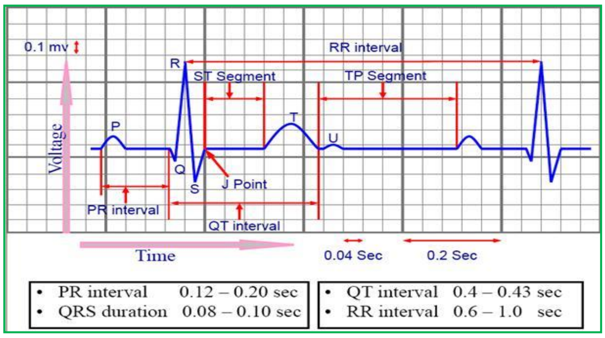

0.1 mv
RR interval
R
ST Segment
TP Segment
T
P
U
Voltage
Q
S
J Point
PR interval
QT interval
Time
0.04 Sec
0.2 Sec
• PR interval 0.12 – 0.20 sec
• QRS duration 0.08 – 0.10 sec
• QT interval 0.4 – 0.43 sec
• RR interval 0.6 – 1.0 sec

Figure 1: ECG signal

(b) **Secure Force Algorithm:** It is a symmetric algorithm developed using Feistel Structure. The SF algorithm (Mansoor *et al.*,2013) is a lightweight WSN security model. This algorithm generates a multiple secret key k1, k2, k3, k4 and k5 with manual input to sensors. Each key is of 16-bit size extending the key length to 128-bit. It uses a simple arithmetic, logical and swapping operations. The multiple Secret Key are transmitted over a channel to the patient in Body sensor node (BSN) where SF encryption part is stored inside it. This also has simple arithmetic logical operations for encryption. Then encrypted message is transmitted to the BNC. The encrypted data is transmitted back to the source end. Thus, with the MSK, the message is decrypted and original information is extracted. This model is suitable for our real-time message and device authentication systems.

(c) **ECG signal 128-bit multiple key generations:** As the ECG signal is unique by nature and measured in real time from the subject, it is used to generate the secret key. The various features obtained from the ECG signal to generate the secret key are.

i) Average time interval: The average measure of time interval between consecutive peaks and taking the rounded off to nearest integer and is converted into a 16-bit binary value.

ii) Square Number: The value is obtained from the average time.

iii) Beat Rate: The heart rate of the patient is obtained by measuring the peak R in one minute.

iv) Maximum value of R Peak: On obtaining the ECG signal the highest R value is detected as it is a unique pattern.

v) The mean variance and standard deviation and waveform length are converted into 16bit separately to form the secret key.

All these are basic parameters of any signal feature extraction and the length of the waveform is usually a fixed value. From all these 8-parameters we generate individually 16 bit values and are concatenated to form (Key$_{128}$) as given in eqa 1.

Key$_{128}$ = Avg time││Sq-No││Beat Rate││ Max R peak││Mean││Variance││Stand deviation││Waveform length. (1)

This key is given as an input to the SF algorithm secret key generation system to obtain a multiple secure key of 128-bit length.

V. WBAN ARCHITECTURE: In WBAN Architecture we have actuators and sensor for communication which range from few to tens in a mobile handset, it reaches to tens to hundred when connected to an internet gateway. In IEEE Wireless Personal Area Networks, it is given as a typical WBAN network having a scalable architecture and that can support 6 to 256 nodes. In IEEE draft standard, mentioned it can support 256 nodes with 10 piconets per person in each network with a 6m^3. The IEEE 802.15.6 has defined a standard of 64 nodes due to limitations in Transmission strategies (Patel *et al*., 2010). It states only one hub can exist in a WBAN and nodes ranges upto 0 to *n*maxBANsize. Lewis (2010) stated that 2-4 WBAN is allowed in (per m^2), a maximum of 256 nodes can exist per network. Zasowski *et al.*, (2003) reported that the one-octel WBAN address allocation is used to represent WBAN identifier (WBAN ID) in a node, hub or in a WBAN in its frame exchange communication. The Octet address ranges from *x*00 to *x*ff to a max count range of (0 – 255). In wireless body Area sensor networks, various type of Bio-medical sensor like Blood pressure, Glucometer, Plethsmogram, EEG, ECG, EMG, Pulse Oximetry, CO$_2$ Gas sensor, DNA sensor and Pacemakers are interconnected to a Body Area Network coordinator (BNC). The BNC is a non-resource constraint device and carry vital information to a caretaker, Hospital or to an emergency (Latr`e *et al*., 2011, Hanson *et al.*, 2009) unit through a Home Access point (HPA). A secured communication scheme is required in order to safely communicate the Bio-medical signals obtained from the patient through a communication channel. The three-tier architecture of the WBAN is the most common method of data transmission through the channel in a patient to doctor's end communication. In the below shown figure 2, the Tier 3 is the connection between the Internet Cloud to the doctor at the remote end.

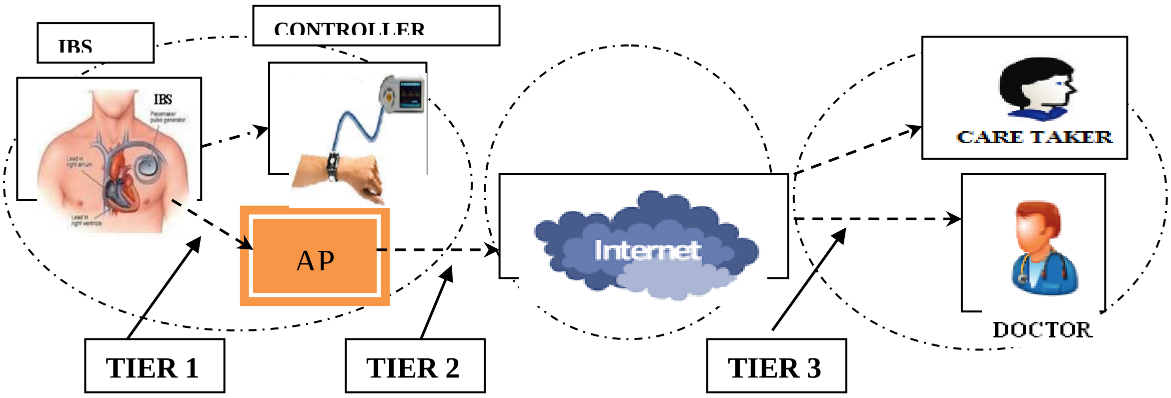


Figure. 2: Architecture of wireless body area sensor network

The Tire 2 is the link between Access point (AP) and to the internet cloud. In this communication channel (Tier 2 and Tier 3) the devices used are not resource constrained, so a high complex level of cryptography method can be deployed. Working with the protection of the Tier1, communication between the IBS and the Access point or a controller, a secure communication design is not yet fully designed and proven to satisfy all the security needs. Thus, we had taken only Tier 1 communication channel and modelled a Bio-secure cryptographic code to provide Authentication, data confidentially and data integrity. Thus, protecting the patient data being eavesdropped or by having middle men attacks.

(a) **Tier 1 comm unication Security algorithm:** In our proposed work, a real-time model is taken as shown in figure.3 and is experimentally analyzed to verify the strength of the Bio-secure cryptography model.

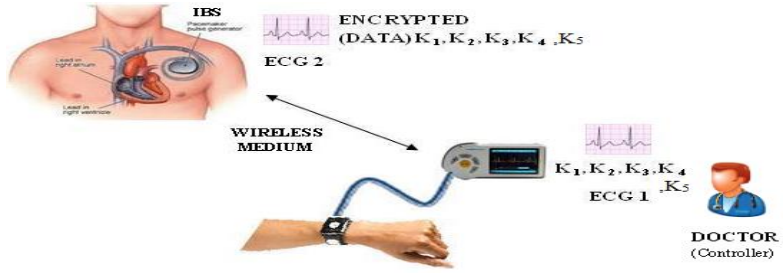

IBS
Pacemaker pulse generator
Lead in right atrium
Lead in right ventricle
ENCRYPTED (DATA) K_1, K_2, K_3, K_4, K_5
ECG 2
WIRELESS MEDIUM
K_1, K_2, K_3, K_4, K_5
ECG 1
DOCTOR (Controller)

Figure 3: WBAN programming Model

The two devices that must be authenticated are the IBS and the controller, and both the devices must be synchronized in time and it is performed by IEEE 1588 standard [30]. Once synchronization is over, the following three stages of operation provide data security:

(a) Key Generation (Key_{128}), Transmission to IBS node by controller node.

(b) Encryption by using secret key (Key_{128}) at IBS node and Transmission to controller node.

(c) Verification of Encrypted data received at controller end for data Authentication and Confidentiality.

(a) **Key Generation, Transmission to IBS node by controller node:** The key generation is quite complex process and more energy consuming one. Thus, the controller (programmer) which is not a resource constrained device performs this process. The first step in this, is the secret key generation with the patient ECG signal (Bio-medical patterns are unique). The ECG sig-nal from the patient is recorded for one minute and all the eight parameters are calculated as stated in section –III to create the secret key with multiple 128 bit (Key_{128}). The entire transmission model is shown figure 4

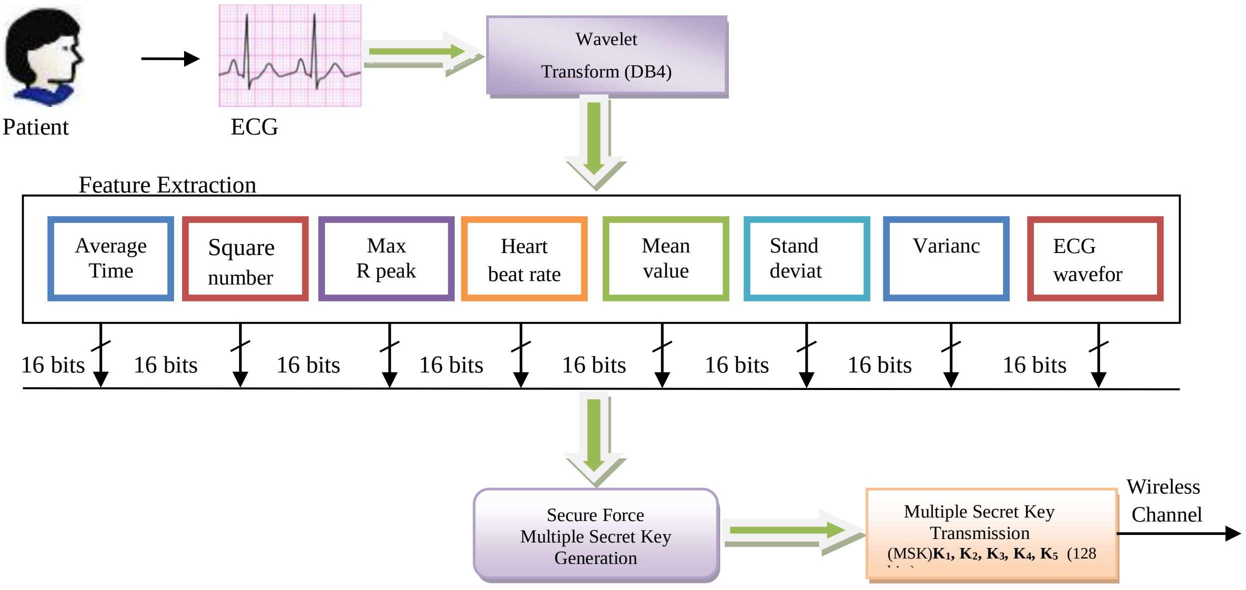


Figure 4: Multiple Secret Key Generation and Transmission

(b) **Encryption using secure key (Key_{128}) at IBS node and Transmission to controller node:** The IBS node (pacemaker) simultaneously records the ECG signal of the patient for one minute duration and stores it, on receiving the secret key (Key_{128}). The IBS having the lightweight secure force encryption algorithm in it, encrypts the ECG signal (Data) that is recorded with the secret key (Key_{128}) received from the controller.

Once the process is over, the encrypted message is transmitted to the controller node without change in data size. Here the main advantage over all other security model is that, the secret key generation is formed by the external node and only the encryption is performed in the IBS, so objective of low battery power consumption is achieved. Our main contribution in the work is the generation of the secret key (Key_{128}) from the Fuzzy Bio-Medical (ECG) signal which can't be generated by any other systems (unique pattern), making the security model a more robust configuration. Thus, any type of key pre-deployment and key generation at the IBS node is completely eliminated.

The encryption and decryption module is shown in figure 5.

(c) **Verification of Encrypted data received at controller end for data Authentication and Confidentiality:** The encrypted message is received by the controller node (Doctor's end) who performs all control actions in the IBS (pacemaker). The controller attempts to decrypt the encrypted message with the secret key (Key_{128}), upon decryption, it compares the ECG signal captured from the IBS device and the ECG signal in it.

$$\textbf{[Data]}_{\textbf{IBS}}\textbf{=Decrypt [(Encrypted message)}_{\textbf{(Key128)}}\textbf{]}_{\textbf{(Key128)}} \quad \textbf{(2)}$$

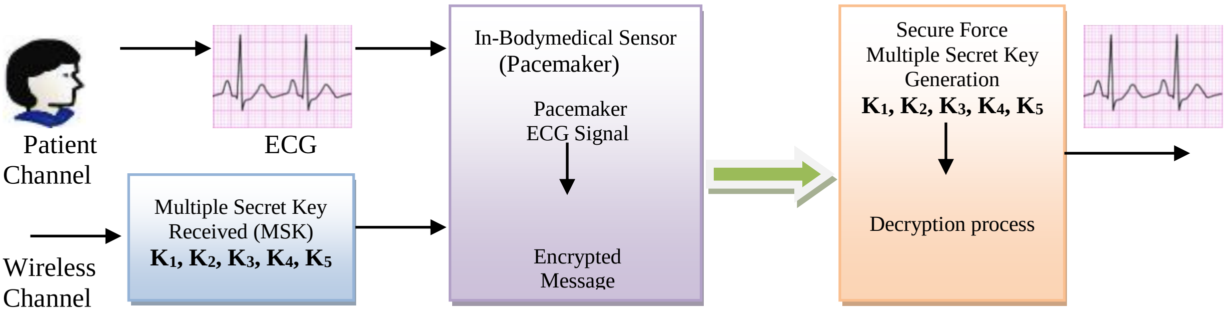


Figure 5: Sender node Encryption process and Receiver Node Decryption process

When both the data are similar the IBS is authenticated by the controller and vice versa and further communication is executed.

$$\textbf{[Data]}_{\textbf{CONTROLLER}} = \textbf{[Data]}_{\textbf{IBS}} \qquad \textbf{(3)}$$

$\textbf{[Data]}_{\textbf{IBS}}$ **= IBS Authenticated**

At the same time when the encrypted data mismatches with the decrypted message, device authentication fails.

$$\textbf{[Data]}_{\textbf{CONTROLLER}} \neq \textbf{[Data]}_{\textbf{IBS}} \qquad \textbf{(4)}$$

$\textbf{[Data]}_{\textbf{IBS}}$ **= Mismatched Authentication Failed**

Then the controller will once again initiate the entire process for secure communication and for other control actions. It is assumed that there will be (1sec) time delay between these two measured ECG signal by the devices and during transmission encrypted data, no transmission error has occurred.

V. RESULT

As we lack the ability in obtaining the ECG signal from the pacemaker or from a lab, we follow the similar procedure (Venkatasubramanian *et al*., 2010, Zhaoyang Zhang *et al*., 2010, Hu *et al*., 2013) by using MIT – BIM physio bank data base. We explicitly consider only the MIT- BIH Atrial fibrillation (AFOB) (Goldberger *et al.*, 2000) from 24 subjects (250 Hz, 607 Mbit) of data as these signals are generated from In-body medical sensor (pacemaker). These signals are used for our experimental work.

A 128- bit secret key Randomness test with Normal distribution curve: In the proposed algorithm, we generate a 128-bit secret key (Key_{128}) from the unique ECG signal of the patient, so that the secret key generated from it, cannot be recreated by anyone else. To check the randomness of the generated key, it is analyzed with a Normal Distribution curve. A continuous ECG signal for 1 hour is taken from a single patient and a histogram plot is generated for its RR interval. Over this plot, the normal distribution curve is imposed as shown in figure 6. We can see the histogram plot completely fits inside the curve and implies that the secret key generated from the ECG signal is highly random, that even the same patient can't regenerate the key next time.

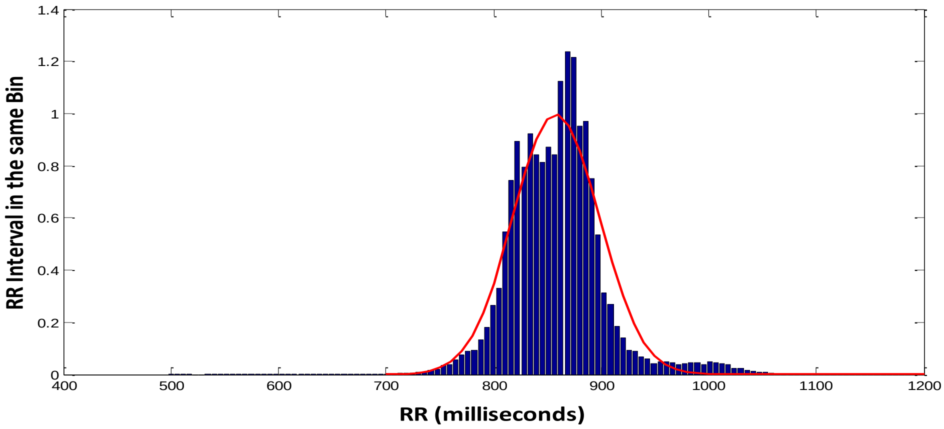


Figure 6: Histogram of ECG signals.

CONCLUSION

In this paper, we had presented a Bio-signal based 128-bit secret key generating method combined with a lightweight SF algorithm, which is already a proven model in wireless Sensor Networks. The secret key is key is generated by the programmer and shared with the IBS module, achieving the design goal of device authenticated without any form of setup or initialization. Simple calculation is done with ECG signal parameters in a transparent way and generate a 128-bit secret random key (Key_{128}). Thus, we proposed and analyzed a secret key generation model for scavenging energy device in human body.

In near future, we had planned to embed error correction coding algorithm in the receiver end. The encrypted data from the IBS is transmitted in wireless medium to the receiver, due to external noise source, a single bit error may occur. In order to detect and correct these errors at the receiver end, we introduce a CRC -16 codes in the existing model.

REFERENCES

Astrin W.A., H.B. Li, and R. Kohno, Standardization for body area networks. IEICE Trans. Communication. **2:** 366–372(2009).

Ary Goldberger L., Luis A. N. Amaral, Leon Glass, Jeffrey M. Hausdorff, Plamen Ch. Ivanov, Roger G. Mark, Joseph E. Mietus, George B. Moody, Chung-Kang Peng and H. Eugene Stanley, Physio Bank, physioToolkit, and physioNet:Components of a new research resource for complex physiologic signals. Circulation 101: e215-e220 (2000).

Balaji G.N., T.S. Subashini, N. Chidambaram, Detection of Heart Muscle Damage from Automated Analysis of Echocardiogram Video. IETE Journal of Research 61: 236-243 (2015).

Denning T., A. Borning, B. Friedman, B. T. Gill, T. Kohno and W. H.Maisel, Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Pp.917–926 (2010)

Edison J. and K.Lee, IEEE 1588 standard for a precision clock synchronization protocol for a networked measurement and control system. Proceedings 2nd ISA/IEEE Sensor International Conference Pp. 98-105 (2002).

FDA U.S., Vulnerabilities of hospiralifecare PCA3 and PCA5 infusion pump systems: FDA safety communication. [Online]. Available: http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm446809.html. Feistel Cipher: https://simple.wikipedia.org/wiki/Feistel_cipher

Halperin D., T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, Pacemakers and implantable cardiac defibrillators: Software radio attacks and zeropower defences. In Proceedings of the 2008 IEEE Symposium on Security and Privacy. IEEE Computer Society Pp. 129–142(2008).

Hanson M., H. Powell, A. Barth, K. Ringgenberg, B. Calhoun, J. Aylor, and J. Lach, Body area sensor networks: Challenges and opportunities.Computer **42**: 58 –65 (2009).

Hu C., X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. Proc. IEEE INFO-COM Pp. 2274-2282(2013).

IEEE p802. 15-10 wireless personal area networks (2011).

IEEE p802.15.6/d0 draft standard for body area network. IEEE Draft (2010).

IEEE standard for local and metropolitan area networks: Part 15.6: Wireless body area networks. IEEE submission (2012).

Karthikeyan M.V., J.Martin Leo Manickam, Security Issues in Wireless Body Area Networks: In Biosignal Input Fuzzy Security Model: A Survey. Research Journal of Pharmaceutical, Biological and Chemical Sciences **7**: 1755-1773 (2016).

Kwak A.K., S. Ullah, and N. Ullah, An overview of IEEE 802.15.6 standard. 3rd Int. Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL) Pp. 1 –6 (2010).

Latr´e B., B. Braem, I. Moerman, C. Blondia, and P. Demeester, A survey on wireless body area networks.Wireless Network **17**: 1–18 (2011).

Lewis D., 802.15.6 call for applications-response summary. In 15-08-0407-00-0006-tg6-applications -summary.doc.

Lewis D., IEEE p802.15.6/d0 draft standard for body area network. In 15-10-0245-06-0006. (2010).

Li C., A. Raghunathan, and N. K. Jha, Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In e-Health Networking Applications and Services (Healthcom), 13th IEEE International Conference Pp. 150–156 (2011).

Maheswari M., R. Gayathri and S. Vimal, Design and Performance Analysis of Low Noise Amplifier with Filters for WBAN Based Health Monitoring System. Pak. J. Biotechnol. **14**(1): 49-54 (2017).

Mahmoodabadi S., A. Ahmadin and M. Abolhasani, ECG feature extraction using Daubechies Wavelet. proceedings of the fifth IASTED International conference on Visualization, Imaging and Image Processing Pp. 343 – 348 (2005).

Mansoor Ebrahim,Chai and Wai Chong, Secure Force: A low-complexity cryptographic algorithm for Wireless Sensor Network (WSN), IEEE International Conference Control System, Computing and Engineering (2013).

Patel M. and J. Wang, Applications, challenges, and prospective in emerging body area networking technologies. Wireless Communnication. **17**: 80–88 (2010).

Shu-Di Bao, C. Poon,Yuan-Ting and Zhang,Lian, FengShen, Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network. IEEE Transactions on Information Technology In Biomedicine **12**: 772-779 (2008).

Tachtatzis C., F. Franco, D. Tracey, N. Timmons, and J. Morrison, An energy analysis of IEEE 802.15.6 scheduled access modes. In IEEE GLOBECOM Workshops (GC Wkshps) Pp.1270 –1275 (2010).

Venkatasubramanian K.K., A.Banerjee and S.K.S.Gupta, Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks. In- Procedings of IEEE Military Communications Conference Pp. 1–

7 (2008).

Venkatasubramanian K.K, A. Banerjee and S. K. S. Gupta. PSKA: Usable and secure key agreement scheme for body area networks. Trans. Info. Tech. Biomed.**14**: 60-68 (2010).

Zasowski T., F. Althaus, M. Stager, A. Wittneben, and G. Troster, UWB for noninvasive wireless body area networks: channel measurements and results. In IEEE Conf. on Ultra Wideband Systems and Technologies PP. 285 – 289 (2003).

Zhang Y.T., and S. D. Bao, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communication. Magazine **44**: 73-81 (2006).

Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos and Hua Fang, ECG-Cryptography and Authentication in Body Area Networks. IEEE Transactions on Information Technology in Bio-medicine **16(**6): 1070-1078 **(**2012).