(IJRST) 2016, Vol. No. 6, Issue No. IV, Oct-Dec **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

ECG BASED DATA ENCRYPTION SCHEME FOR IMPLANTABLE MEDICAL DEVICES

Keerthi Raj[1], Baby John[2]

M TECH Student, Department of Electronics and Communication Engineering, GISAT Engineering College,Kottayam, Kerala, India[1]

HOD and professor, Department of Electronics and Communication Engineering, GISAT Engineering College, Kottayam, Kerala, India[2]

ABSTRACT

New Technologies are appearing to provide a more efficient treatment of diseases or human deficiencies. Implantable medical devices constitute one example, these being devices with more computing, decision making and communication capabilities. Several research works in the computer security field have identified serious security and privacy risks in IMDs that could compromise the implant and even the health of patient who carries it. Implantable Medical Devices (IMDs), such as pacemakers, implantable cardiac defibrillators, neuro-stimulators, drug delivery systems perform a variety of health monitoring and therapeutic functions. Currently wireless communication capabilities have been embedded as an intrinsic part of many modern IMDs. The ECG based data encryption is designed with the ability to provide information-theoretically unbreakable encryption .Here ECG features are used to facilitate a key distribution. The random binary strings generated from ECG signals are directly used as key for encryption. The IMD encrypts its secret data with one key before transmission and after receiving the ciphertext, a programmer decrypts the secret data using another synchronously generated key.

Keywords:*Encryption,Decryption,Ciphertext, Implantable medical devices (IMDs), Electrocardiogram (ECG).*

1. INTRODUCTION

Implantable Medical Devices are electronic devices implanted within the body to treat a medical condition, monitor the state or improve the functioning of some body part or just to provide the patient with a capability that he did not possess before. No scheme currently exists that can provide a perfect encryption method to protect sensitive and critical IMD data for patients. So the security solution is called an ECG-based data encryption scheme. This is an extension of previous work on the IMD security which focused on the ECG-based key distribution between the IMD and the programmer. The IMD encrypts its secret data with one key before transmission and after receiving the ciphertext the programmer decrypts the secret data using another synchronously generated key. This scheme addresses a pair of conflicting requirements underlying high security and high accessibility. That is any device without any knowledge of a password must not be allowed to have access to or decode information from IMDs.

The EDE implements a simple security policy for IMDs, the touch–decipher: a programmer has an ability to decrypt the ciphertext if and only if it has a significant physical contact with the

patient's body. This property is decided by properties of generated ECG keys. The properties are randomness, temporal variance and distinctiveness among individuals. The decryption capability disabled once the Programmer loses physical contact with the patient. This touch deciphers policy balances requirements of security and accessibility. Emergency medical responders can gain access to the IMD by making a physical contact with the patient's body. But adversary's access is to be prevented without access to real-time ECG data.

The EDE scheme is based on physiological signal-based OTPs which use binary strings generated from ECG as keys for direct encryption. Security keys in this scheme are generated from ECG signals and are used to encrypt secret data directly. Compared to traditional symmetric key-based encryption systems, the EDE has the advantages that the EDE scheme combines two well-known techniques of classic One-Time Pads and Error Correcting Codes to achieve a cryptographic primitive for IMDs. It inherits the property of perfect secrecy from OTPs, and even has an ability to resist brute-force attacks. Figure 1.1 shows ECG decoding and data encryption.

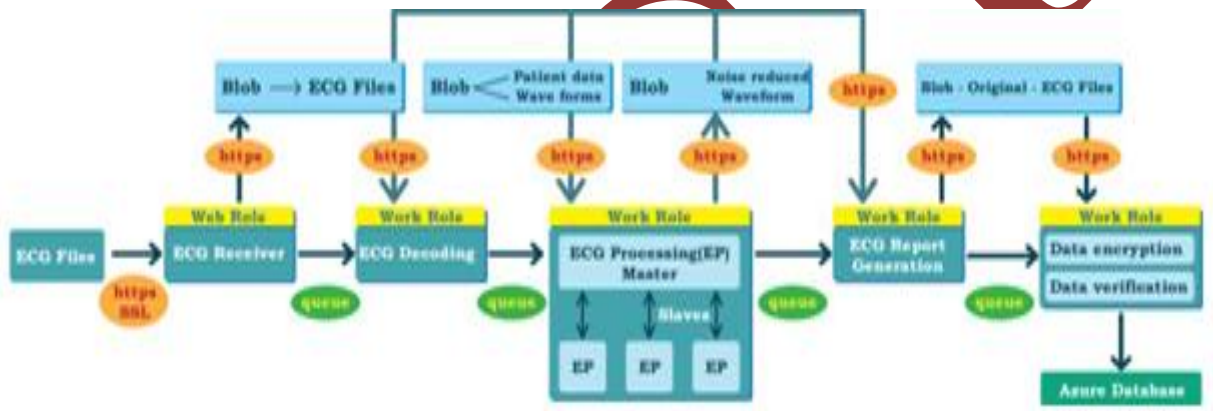

Figure 1.1: Simplified model of ECG decoding and data encryption

The EDE scheme does not require a cryptographic infrastructure to support key pre-distribution, storage, revocation and refreshment. This is because OTP keys are generated from ECG signals by each sensor dynamically before each round of encryption. The EDE scheme does not need to protect random seeds either since ECG is used as a natural random source to generate keys. Symmetric key algorithm uses them same key to encrypt and decrypt the message, whilethe asymmetric key algorithm uses two different keys for encryption and decryption. Here a public key is used toencrypt the message while the private key is used to decrypt the cipher text. In context to the public key cryptography,public key is known to the public while private key is private to the receiver of the message.

The remaining part of this paper is organized as follows: section II covers the literature review, section III describes about the cryptanalysis, section IV covers the proposed system, section V shows the simulation results and finally section VI concludes this paper.

2. LITERATURE REVIEW

Implantable medical devices can save lives and greatly improve a patient's quality of life. As the use of wireless IMDs increases and there will be a heightened need to address IMD security and patient privacy under adversarial conditions [1].A non-key based security scheme employs an external authentication proxy embedded in a gateway to authenticate the identity of a programmer. The gateway here employs a transmitting antenna to send data and jamming signals. When an adversary launches attacks, the gateway jams the request signal to the IMD and authenticates its identity [2].

The lightweight security protocol providing authentication and confidentiality to wireless energy-limited IMDs that operate on small energy sources such as battery for many years [3]. We need a solution to secure IMDs against unauthorized access, battery depletion and denial of service attacks.A radio frequency energy harvesting solution is used to design a powerless mutual authentication protocol.Implantable medical devices are surgically implanted into a human body to collect physiological data and perform medical therapeutic functions. They are increasingly being used to improve the quality of life of patients by treating chronic ailments such as cardiac arrhymia, diabetes and parkinson's disease. A radio frequency harvesting solution is used to design a powerless mutual authentication protocol. Radio frequency uses electromagnetic fields to automatically identify and track tags attached to objects [4].

Secure and energy-efficient communication between implantable medical devices and authorized external users is attracting increasing attention these days. A new implant system architecture is proposed, where security and main-implant functionality are made decoupled by running the tasks onto two separate cores [5]. Most IMDs lack a security mechanism. The unique challenge is that IMDs should be able to be accessed by doctors at any legitimate hospital for emergency purposes, but conventional security mechanism using keys or credentials cannot guarantee that doctors could obtain keys timely in emergency situations. To address this unique challenge,an ECG-based Secret Data Sharing scheme is presented, which does not require predeployed keys.This scheme makes use of electrocardiograph features to hide a secret within the IMD before transmission and then reveal the secret with simultaneously measured ECG features by an external programmer[6].

The problems of cryptography and secrecy systems furnish an interesting application of communication theory. A detailed study is made of the ways of breaking them [7].Quantum secure direct communication is the direct communication of secret messages without first producing a shared secret key. It may be used in some urgent circumstances [8].But physical key protected one-time pad describes an encrypted communication principle that forms a secure link between two parties without electronically saving either of their keys. Instead, random cryptographic bits are kept safe within the unique mesoscopic randomness of two volumetric scattering materials [9].

Wireless body area networks have drawn much attention from research community and industry in recent years.Neighbouring nodes in body area networks share a common key generated by electrocardiogram signals[10].Implantable medical devices are increasingly being used to improve patients' medical outcomes.Designers of IMDs already balance safety,reliability,complexity,power consumption and cost.However recent research has demonstrated that designers should also consider security and data privacy to protect patients from acts of theft or malice,especially as

medical technology becomes increasingly connected to other systems via wireless communications or the internet[11].We have to quantify the energy cost of authentication and key exchange based on public-key cryptography [12].

3. SYSTEM MODELLING

In this section adversarial and operational models, as well as ECG signal models are presented before detailing the EDE scheme.

3.1: THREAT MODELLING AND ASSUMPTIONS

Proper threat modelling is a vital aspect of security design. IMDs communicate with an external device called a programmer. A wireless session with the IMD is initiated by the programmer during which the private data in the IMD are shared with or the parameters.

1. PASSIVE EAVESDROPPERS

A passive eavesdropper listens to an IMD's wireless transmissions and tries to capture and decode transmitted data with off-the-shelf or custom –built radio equipment.

2. ACTIVE EAVESDROPPERS

An active adversary extends the eavesdropper's capabilities and has the ability to reply recorded control commands, or generate new radio commands, to an IMD, aiming at triggering data transmission from the IMD or modifying the IMD's settings. Assume that adversaries cannot measure real-time ECG signals from a patient. As measuring ECG signals requires a physical contact with the patient's body, the attack would be detected by the patient immediately.

3.2: ECG MODELLING

The random keys extract from ECG signals for encryption .An example of consecutive ECG signal is shown in figure 3.1.One ECG trace includes three major waves: P wave, QRS complex and T wave. The P wave represents the ventricular depolarization while the T wave represents the ventricles repolarization. As the R-peak is the most prominent feature of the ECG waveform, it can be used to represent a heartbeat: two consecutive R peaks is the heartbeat duration and referred to as the Inter-Pulse-Interval (IPI).

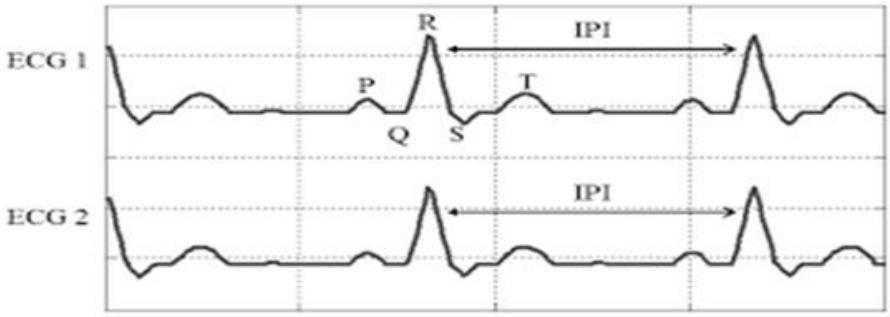

Fig 3.1: Two simultaneously sampled ECG signals from two parts of the same patient's body

OTP keys are generated from synchronously sampled ECG signals in the IMD and the programmer. Figure shows an example of two synchronously measured ECG signals. These two signals are from the same signal source that is heartbeats. So they have major part in common. A minor difference between them is caused by measurement errors from instruments and other factors.

4. PROPOSED SYSTEM

The proposed scheme addresses a pair of conflicting requirements underlying IMD security: high security and high accessibility .That is any device without any knowledge of a password must not be allowed to have access to or decode information from IMDs.

4.1: EDE SCHEME ARCHITECTURE

The EDE scheme includes two components: The IMD and the programmer. The IMD is an electronic device which is implanted in the body to assist or monitor a patient's health, while the programmer is an outside device which has the ability to access data in the IMD and program it wirelessly. Both of them are currently standard medical devices and most IMDs have the capability of measuring ECG signals.

In this scheme ,an ECG sensor is connected to the programmer and measures ECG signals from, for example ,the wrist of the patient. It is convenient to add an ECG measuring function into the programmer since it is an outside device and is normally kept in hospital.

One key feature of the EDE is that the keys are independently generated by each device. The EDE does not require key distribution or transmission from one sensor to another. Key refreshment can be easily achieved by generating keys at two sensors directly. Also there is no need of key storage and revocation, since a fresh pair of keys will be generated before each new encryption cycle and will not be re-used according to OTP rules.

Another key feature is that the EDE scheme inherits the property of perfect secrecy from OTPs, and can provide information-theoretically secure encryption for IMDs. As IMDs normally perform therapeutic or life-saving functions,this feature is critical to IMD security. Inherent characteristics of ECG bit strings of randomness, temporal variance and distinctiveness ensure that OTP keys cannot be probed, duplicated or speculated without a physical contact with the patient's body.

(IJRST) 2016, Vol. No. 6, Issue No. IV, Oct-Dec e-ISSN: 2249-0604, p-ISSN: 2454-180X

In figure4.1 it can be seen that the IMD and the programmer measure ECG synchronously and random binary key sets,(Ka) and (Kb) ,are then generated by each device. (Ka) is used to encrypt secret data with modified OTPs in the IMD while (Kb) is used to decrypt the ciphertext.

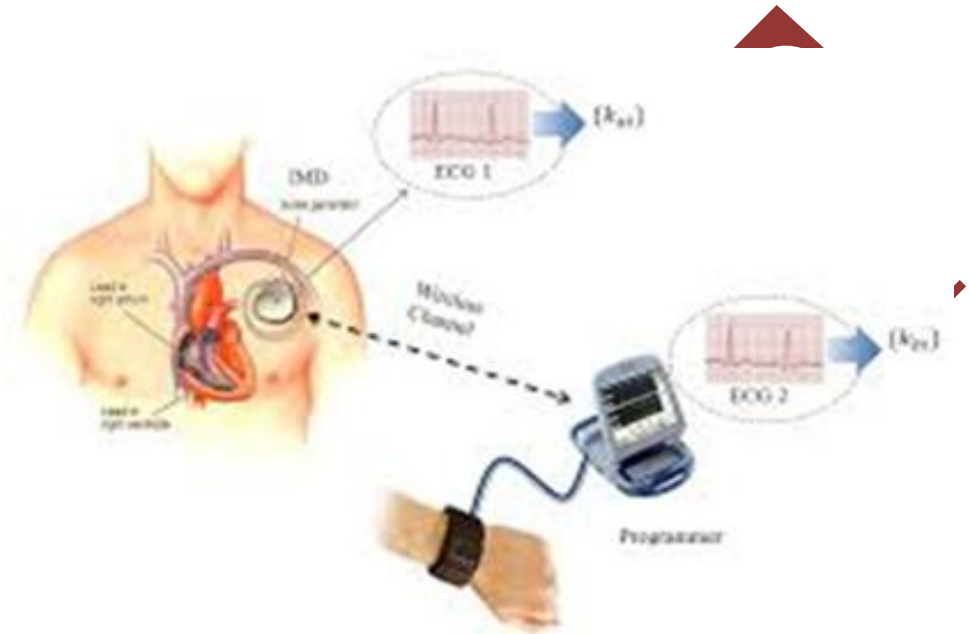

Fig 4.1: Secure communications with the EDE scheme

One key feature of EDE is that the keys are independently generated by each device. The EDE does not require key distribution or transmission from one sensor to another. Key refreshment can be easily achieved by generating keys at two sensors directly. Also there is no need of keys, (Ka) and (Kb), will be generated before each new encryption cycle and will not be re-used according to OTP rules.

4.2: ECG BASED DATA ENCRYPTION SCHEME

One-Time Pads have limited applications in the modern computing era. This is because OTPs require the storage of a large number of random keys and guarantee that no keys are re-used. The EDE scheme applies a practical and secure approximation of OTPs for the IMD system where the OTP keys are generated by the sender and the receiver respectively and synchronously. Sofirst design a modified OTP algorithm for IMD encryption and then propose a protocol which executes the EDE scheme with this algorithm.

4.2.1: LINEAR ERROR CORRECTING CODES

Here design a system with a secret‘s ‘in the secret space ‘S’.The encryption algorithm is Fenc and the decryption algorithm is Fdec .Considering the mismatch between Ka and Kb .The designed EDE algorithm has to satisfy that an encryption/decryption pair (Fenc,Fdec) with parameters (S,Ka,Kb) is complete with error tolerance ε when the following condition holds. For each si € S and each key pair (Ka,Kb) where |Ka-Kb| ≤ ε ,the decryption process Fdec (Kb(Fenc(si , Ka))=si is with an overwhelming probability.

4.2.2: MODIFIED ONE-TIME PAD ALGORITHM

For classical OTPs working over a secret ‘Si’ in the secret space S, a corresponding key‘ki’ in the key space K , the resulted cryptogram space C is denoted by Ci=f(Si,ki) =Si+ki where f is a function with a unique inverse and + is the XOR operation which mixes each bit of ‘Si’ with each bit of ‘ki’.Thereafter ‘Ci’is to be sent through a public channel. At the receiving end,the same OTP key‘ki’is applied to decrypt the secret ‘Si’. For a series of secret messages the S={s1,s2..},the corresponding cryptogram is denoted by Mc = F(s) ={f(s1,k1),f(s2,k2)…}.OTPs become unbreakable only when the used keys are kept secret, never re-used in whole or part and the same length as the message. Figure 4.2 shows the one-time pad protocol.

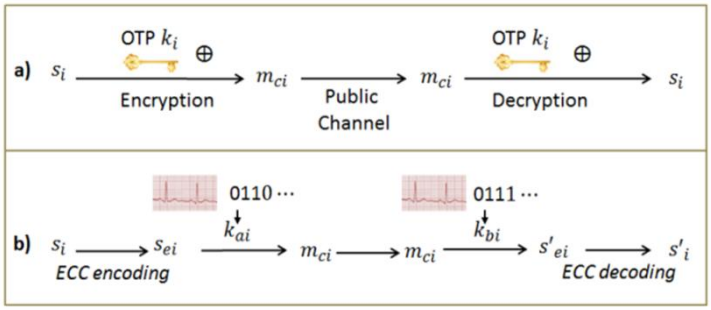

Fig 4.2: The One-Time Pad protocol

4.2.3: OTP KEY GENERATION

The fundamental and critical part of the EDE scheme is to generate pairs of ECG Binary Strings synchronously satisfying two basic requirements: randomness and low mismatch rate. ECG IPIs computed from the same ECG signal measured at different parts of the body by two sensors are not completely identical. Here propose an improved ECG BS generation algorithm is described in four steps.

Step 1 [Simple Moving Average (SMA)]: The SMA is an un-weighted mean of a series of a different subsets in the whole data sequence.

Step 2 (Gray Coding): The Gray Code is not common binary code, to quantize IPIs. The most important feature of Gray Code is that there is only bit difference between two successive values.

Step3 (LSB removal): The Least Significant Bit (LSB) of SMA processed IPIs was normally different. In order to reduce the mismatch rate, the LSB is not used in this scheme.

Step 4 (Parity Check): Bits from two consecutive SMA-processed IPIs at both sides are extracted to form an 8-bit block. Then both sides calculate the parity information. If the parity is the same, each side extracts 7 bits of the block and discards the last bit as the parity check leaks one bit of information. This process moves ahead until there are 127 bits on each side.

4.2.4: COMMUNICATION PROTOCOL DESIGN

1. ECG BINARY STRING GENERATION

The programmer sends a synchronization request to the IMD for sampling ECG which indicates the sampling start-time T with a timestamp in the frame. Since there would be a timing difference two clocks residing in the IMD and the programmer. In the EDE scheme the programmer is selected as a master while the IMD is a slave .In the synchronization frame, the programmer its current time and sends to the IMD. Since the IMD is very close to the programmer, the transmission time of this frame is negligible. Therefore, the IMD uses current time to correct its clock.

After the clock synchronization, the IMD and the programmer sample ECG signals synchronously at the time two highly matched and random ECG binary strings are then generated by the IMD and programmer. There is no requirement of key pre-distribution or transmission here as keys will be generated by each device independently.

2. PROCESS IN THE IMD

After generating the key, the process is executed in the IMD. Firstly the secret is encoded by an ECC encoding process to create redundant information is added for error correction purposes. Then the cryptogram is created by XOR operation. A hash value is computed by a one way hash function in order to check message integrity and correctness of decoded secret at the programmer. A fresh random number generated by a counter, nonce, is used as a session identifier to prevent potential replay attacks. A message includes the identity numbers of the IMD and the programmer. The message along with the hash value is then sent to the programmer through a public channel.

3. PROCESS IN THE PROGRAMMER

After receiving the message, the process in the programmer is reverse to the process in the IMD. Consider the potential channel interference. The programmer decrypts the message by XOR operation. An ECC decoding process is then performed to correct error bits. The hash function is compared with the received hash so as to check the integrity of the received message and

(IJRST) 2016, Vol. No. 6, Issue No. IV, Oct-Dec e-ISSN: 2249-0604, p-ISSN: 2454-180X

correctness of the decoded secret. If the hash functions are equal, the received message is not modified in transmission and the obtained secret is also same. Then a 'success' code is then assigned to the acknowledgement. Otherwise acknowledgement is assigned a failure code. The programmer finally sends acknowledgement to the IMD to confirm the decryption results.

5. EXPERIMENTAL RESULTS AND DISCUSSION

This section provides an evaluation of the EDE scheme by performing a series of experiments. Lacking the ability to obtain IPI measurements from IMDs, generate OTP keys by using the ECG data from the MIT PhysioBank database. Experiments were carried out on the ECG data from 167 subjects: 18 subjects from the MIT-BIH Normal Sinus Rhythm (NSRDB), 79 subjects from European ST-T, 47 subjects from MIT-BIH Arrhythmia and 23 subjects from MIT-BIH Atrial Fibrillation. Considering potential applications to pacemakers or ICDs,the last two databases contain arrhythmia ECG signals.

5.1: OTP KEY RANDOMNESS ANALYSIS

Randomness is a vital requirement of using generated ECG binary strings, that is, OTP keys, for security purposes. The EDE scheme relies upon generated ECG BSs following what Shannon defines a purely random process. The first experiment was to analyse the randomness of captured ECG IPI values. There collected 15000 consecutive IPI values fit into a normal distribution. Thus the distribution of consecutive IPIs is almost normal, which indicates the randomness of ECG IPI values. This normal distribution is fundamental to generate random BSs from IPI values.
The entropy is to measure the uncertainty of generated ECG BSs. For a random variable X=0, 1 we can calculate the entropy of each bit sequence using the formula :(x) = -P0 log2 P0-P1 log2 P1 where P0 and P1 are the probability mass functions of 0s and 1s.

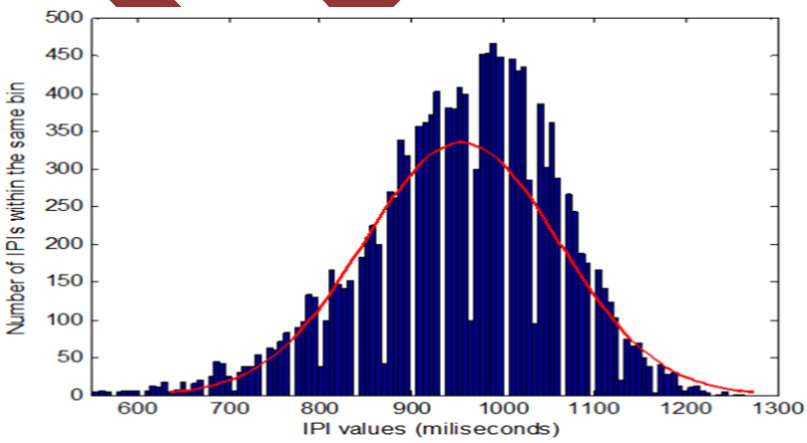

Fig 4.1: The histogram of consecutive IPI values sampled at 125 Hz with normal distribution fit.

The largest entropy result of bit strings generated from about 100 ECG samples. It can be seen that the entropy values of most ECG bit strings were close to 1, with the mean entropy of 0.992.Furthermore, a two-tail runs test with a significance level of 5%. Therefore the generated ECG bit strings have a good performance of randomness.

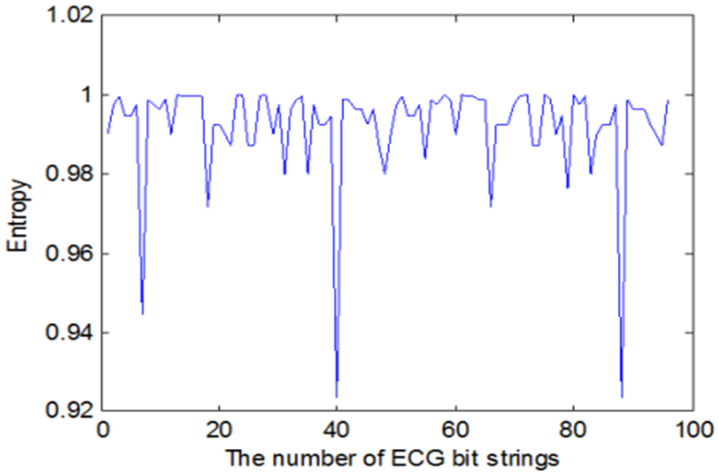

Fig 4.2: The calculated entropy of generated ECG binary strings

5.2: OTP KEY TEMPORAL VARIANCE

Here evaluates generated ECG binary strings for temporal variance to ensure that the encrypted secret cannot be decrypted by the same subject's historical or future ECG signals. In the experiment, sampled the ECG signals on each subject from the MIT-BIH NSRDB over 300 random start-times and computed the average Hamming distance between the keys. Figure 5.3 shows an experiment result from one subject. The x-axis represents ECG sample number in the IMD and the y-axis represents ECG sample number in the programmer.

5.3:OTP KEY DISTINCTIVENESS

The property of distinctiveness is to ensure that the secret encrypted by an IMD implanted in one subject cannot be decrypted by another programmer using ECG signals from another subject. This can distinguish IMD systems on different subjects. In the experiment, ECG signals are sampled on each subject from the MIT-BIH NSRDB over 300 random start-times and computed the average hamming distance between two ECG binary strings from different subjects. The average distance was 49.99 % (about 63 bits) which is similar to that for temporal variance above. This result shows that the secret encrypted by an IMD using ECG signals from one subject cannot be decrypted by another programmer using another subject's ECG signals. This can prevent attackers from decrypting secrets using a different subject's ECG data.

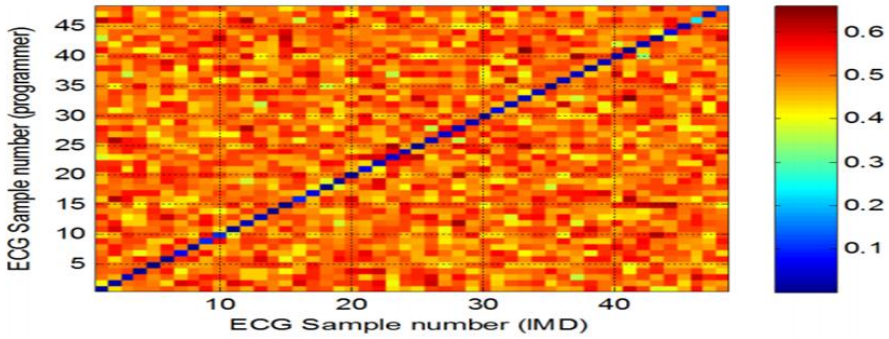

Fig 5.3: Hamming distance between two ECG binary strings generated from two different body parts of the same subject.

5.4: FAR/FRR ANALYSIS

False Rejection Rate and False Acceptance Rate (FAR) are two critical parameters to be taken into consideration when evaluating any biometric-based security schemes. In this experiment, FRR is the measure of likelihood that a programmer fails to decrypt a secret from an IMD by using simultaneously measured ECG signals from the same subject, while FAR is the measure of the likelihood that a programmer could decrypt a secret from an IMD by using the same subject's historical or future ECG data or data from another subject. Figure shows experiment results of FRR and FAR on each ECG database with BCH code length n=127.

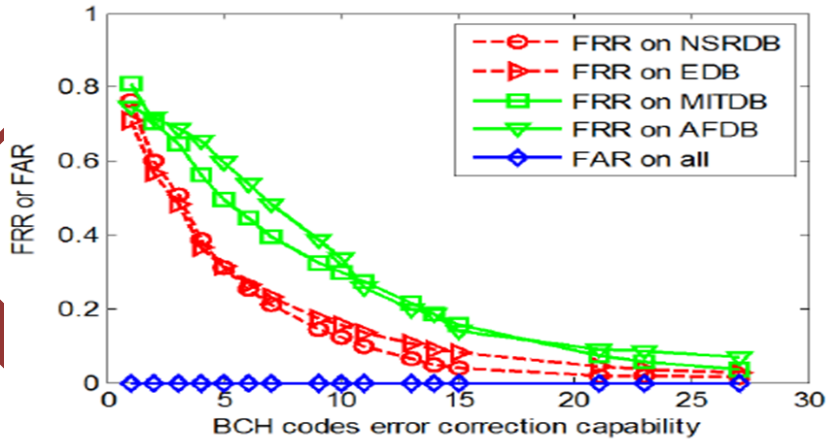

Fig 5.4: FRR and FAR vary versus BCH codes error correction capability

5.5: OVERHEAD ANALYSIS

Communication overhead is negligible in the EDE as the ciphertext sent into the channel is of the same length as the code word of BCH codes. Adding a large number of chaff points to hide data is not needed here as the secret data is already encrypted. The concern of computation overhead is about the processes within the IMD since it is battery powered and implanted in the body. The programmer, as an external device in the hospital or clinics, could be easily designed

with hardware capable of supporting intensive computational overheads. So we focus on overhead analysis on the IMD.

6. CONCLUSION

Here we presented an information-theoretically secure encryption method for IMDs, namely the ECG-based Data Encryption. The EDE combines two well-known techniques of one-time pads and error correcting codes to achieve a cryptographic primitive for IMDs. In emergencies, medical personnel can gain access to patients' IMDs by measuring the patients' real-time ECG data; thus the designed EDE scheme achieves a balance of high security and high accessibility. The EDE scheme uses physiological signal-based OTPs to encrypt secret data from IMDs before transmission. OTP keys are to be generated by each device from synchronously measured ECG signals. As ECG signals are used as natural random input into the encryption algorithm, there is no cryptographic infrastructure to support key distribution, storage, revocation and refreshment. The security analysis showed that the EDE scheme fulfills the requirements of OTP key management, and thus inherits the property of perfect secrecy from OTPs. Future work includes a game-based security proof and an in-field study of the EDE scheme to better understand the properties of the generated ECG BSs and evaluate the performance of the scheme.

REFERENCES

[1] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, ''Security and privacy for implantable medical devices,'' IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[2] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, ''A non-key based security scheme supporting emergency treatment of wireless implants,'' in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2014, pp. 647–652.

[3] S. Hosseini-Khayat, ''A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices,'' in Proc. 5th Int. Symp. Med. Inf. Commun. Technol. (ISMICT), Mar. 2011, pp. 6–9.

[4] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga, ''Securing implantable cardiac medical devices: Use of radio frequency energy harvesting,'' in Proc. 3rd Int. Workshop Trustworthy Embedded Devices, 2013, pp. 35–42.

[5] C. Strydis, R. M. Seepers, P. Peris-Lopez, D. Siskos, and I. Sourdis, ''A system architecture, processor, and communication protocol for secure implants,'' ACM Trans. Archit. Code Optim. (TACO), vol. 10, no. 4, 2013, Art. ID 57.

[6] G. Zheng, G. Fang, M. A. Orgun, R. Shankaran, and E. Dutkiewicz, ‘‘Securing wireless medical implants using an ECG-based secret data sharing scheme,’’ in Proc. 14th Int. Symp. Commun. Inf. Technol. (ISCIT), Sep. 2014, pp. 373–377.

[7] C. E. Shannon, ‘‘Communication theory of secrecy systems,’’ Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

[8] F.-G. Deng and G. L. Long, ‘‘Secure direct communication with a quantum one-time pad,’’ Phys. Rev. A, vol. 69, no. 5, p. 052319, 2004.

[9] R. Horstmeyer, B. Judkewitz, C. Yang, and I. M. Vellekoop, ‘‘Physical key- protected one time pad,’’ U.S. Patent 20130243187, Feb. 21, 2013.

[10] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, ‘‘ECG-cryptography and authentication in body area networks,’’ IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[11] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, ‘‘Design challenges for secure implantable medical devices,’’ in Proc. 49th Annu. Design Autom. Conf., Jun. 2012, pp. 12–17.

[12] A. S. Wander, N. Gura, H. Eberle,V. Gupta, and S.C. Shantz,``Energy analysis of public-key cryptography for wireless sensor networks," in Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. (PerCom), Mar. 2005.