ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Biometric Authentication System for Body Area Network

P.Abina[1], K.Dhivyakala[2],L.Suganya[3],S.Mary Praveena[4]

UG student, Dept. of ECE , Sri Ramakrishna Institute Of Technology, Coimbatore, India.[1]

UG student, Dept. of ECE , Sri Ramakrishna Institute Of Technology, Coimbatore, India.[2]

UG student, Dept. of ECE , Sri Ramakrishna Institute Of Technology, Coimbatore, India.[3]

Associate professor, Dept. of ECE , Sri Ramakrishna Institute Of Technology, Coimbatore, India.[4]

Abstract: The rapid growth in physiological sensors, low-power integrated circuits, and wireless communication has enabled a new invention of wireless sensor networks, now used for purposes such as monitoring traffic and health etc. Wireless body area network (BAN) is a promising technology for real-time monitoring of physiological signals to support medical applications. In order to ensure the trustworthy and reliable gathering of patient's critical health information, it is essential to provide node authentication servicing a BAN, which prevents an attacker from impersonation and false data/command injection. Cryptographic techniques are observed to provide significant results in protecting data from hackers and attackers. Some of the existing cryptographic algorithms such as selective encryption provide first-rate results. The present research work mainly deals with securing the ECG data in Wireless Body Area Sensor Network before transmission. Neighboring nodes in BANs to share a common key generated by electrocardiogram (ECG) signals. The improved IJS scheme is proposed to set up the key agreement for the message authentication. The proposed ECG-IJS key agreement can secure data communications over BANs in a plug-n-play manner without any key distribution overheads. Both the simulation and experimental results are presented, which demonstrate that the proposed ECG-IJS scheme can achieve better security performance in terms of several performance metrics such as false acceptance rate (FAR) and false rejection rate (FRR) than other existing approaches. In addition, the power consumption analysis also shows that the proposed ECG-IJS scheme can achieve energy efficiency for BANs.

Keywords: Electrocardiogram (ECG), energy consumption, fuzzy vault, monic polynomial, wireless body area networks (BANs), Improved Jules Suden (ECG-IJS).

I. INTRODUCTION

The body area network (BAN) is a smart biomedical sensor platform, which provides the ability to measure a wide range of signals, such as heart rate (ECG), activity, temperature or muscle activity (EMG). This can all be integrated into a small, lightweight device that can analyze the measured signals and transmit them to a user interface wirelessly the BAN technology is specifically designed for healthcare and research applications. The system can be used to measure relevant body parameters. These can be translated by algorithms into meaningful information for use in an app on a smart phone or tablet. The nonintrusive and ambulatory health monitoring of patients vital signs over BANs provides an economical solution to the current healthcare system, in which the healthcare information can be distributed to users anytime through handheld devices and internet. A BANs consists of a set of mobile and small size intercommunicating sensors, which are either wearable or can be implanted into the human body for monitoring vital signs (e.g., heart rate, brain activity, blood pressure, and oxygen saturation) and/or environmental parameters (e.g., location, temperature, humidity, and light) and movements. However, there are several research challenges. Before

BANs can be widely deployed. First, the sensors have limited resources in terms of energy, bandwidth, memory, and computational capability; a lightweight communication solution should be pursued in BANs. Second, since the performance of BANs is closely related to people's health, it is important to have safe sensor networks in which the requirements of medical data privacy, confidentiality, authentication, and integrity should be satisfied. The lack of security in the operation and communication of resource-constrained medical sensor nodes in BANs has been an obstacle to move the technology forward.

A. Cryptography and Authentication for Secure Multimedia Healthcare Services

In BANs, sensors usually rely on the cryptographic keys to secure multimedia data communications. Numerous key management and distribution schemes have been developed to offer the security in general wireless sensor networks. However, they cannot be directly applied for the BANs due to the scale of biomedical sensors. However, designing an efficient key management and agreement scheme in BANs is still challenging. The key distribution methods, such as probabilistic key distribution, SPINS, LEAP, and asymmetric cryptosystems, have been developed to distribute security keys in BANs. But these methods are not easily implemented in body sensors due to limited sensor resources, or requiring predeployment of the
secret keys that are hard to be replaced and are vulnerable to offline crack. In addition, the overheads of the key management and distributions in these methods are huge when large number of sensor nodes is deployed. Security and privacy are important components in WBANs.

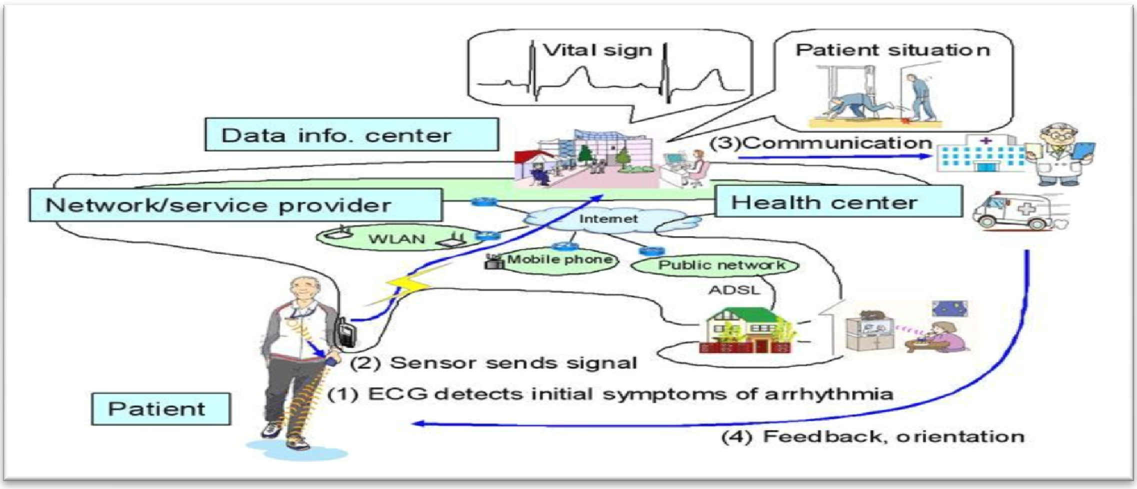


Fig .1 Body area network

In this paper, a new key agreement scheme called ECG-Improved Jules Sudan (IJS), which utilizes physiological signal such as ECG signals for generating cryptographic keys. Using ECG-IJS scheme, the secure intersensor communication could be implemented in a "plug and play" manner, which means that no previous key distribution is needed. The secret keys used in the communication are generated based on the ECG signals, which meets the requirements of long, random, time variant keys..The proposed key is generated from universally measurable physiological stimuli (ECG) that is unique and distinctive for each person. Additionally, the ECG-IJS scheme only needs a small time period to generate keys with low computational requirements. The ECG-IJS scheme can also achieve better performance in term of false acceptance rate (FAR) and false reject ratio (FRR) than the existing research work. In addition, it is an energy efficient scheme because it does not require the chaff points (communication overheads). A power consumption analysis is given to demonstrate the energy efficiency of the proposed ECG-IJS scheme.

II. LITERATURE SURVEY

Lin Yao, Bing Liu, GuoweiWu, Kai Yao, and JiaWang, 'A Biometric Key Establishment Protocol for Body Area Networks' ,IJDSN,vol.2011, According to this paper, a biometric key establishment scheme to protect the confidentiality and integrity of the sensitive health information. Our protocol attempts to solve the problem of security and privacy in BANs. It also aims to securely and efficiently generating and distributing the session key between a biosensor and CU. Our protocol is based on Biometric Encryption. In our protocol, ECG as the dynamic biometrics is utilized to authenticate between a biosensor and CU. The idea of using ECG comes from the observation that the human body is dynamic and complex and the physiological state of a subject is quite randomness and time variance.ECG is typically collected and utilized in many recognition applications, which is in accordance with the data minimization principle.

L. Eschenauer and V. D. Gligor, 'A Key-Management Scheme forDistributed Sensor Networks', Version: pp. 41–47, November 18–22, 2002,According to this paper, a key-management scheme designed to satisfy both operational and security requirements of DSNs. The scheme includes selective distribution and revocation of keys to sensor nodes as well as node re-keying without substantial computation and communication capabilities. It relies on probabilistic key sharing among the nodes of a random graph and uses simple protocols for shared-key discovery and path-key establishment, and for key revocation, re-keying, and incremental addition of nodes. The security and network connectivity characteristics supported by the key-management scheme are discussed and simulation experiments presented.

C. Poon, Y.-T. Zhang and S.-D. Bao, 'A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health',vol. 44, no. 4, pp. 73–81, Apr. 2006, According to this paper, a novel biometrics approach to secure wireless BASNs for tele medicine and m-health, and illustrate the concept by using IPI as an example. Evaluating the method on 838 datasets collected from 99 subjects, it is found that the minimum HTER is 2.58 percent (FAR = 1.18 percent and FRR =3.99 percent) when the signals are sampled at 1000 Hz and the trait is coded into a 128-bit binary sequence. The study has opened up a few key issues for future investigation, including compensation schemes for the asynchrony of different channels (due to diseases, physiological phenomena, motion artifacts, diction errors, etc.), coding schemes, and other suitable biometric traits.

III. PROPOSED METHOD

In proposed system, an ECG-IJS key agreement is used to secure data communication in BANs. Especially, this approach focuses on the intercommunication and authentication between the sensor nodes in the BANs. Compared with the original fuzzy vault scheme, the IJS algorithm does not use the chaff points to shelter the information. Thus, it reduces the transmission overheads, saves the transmission energy and prolongs the lifetime of the battery.

In the scheme, both the sender and the receiver have the capability to sample the ECG signals from the human body. Thus, the same feature extraction algorithm can be utilized to generate features form the collected ECG signals.

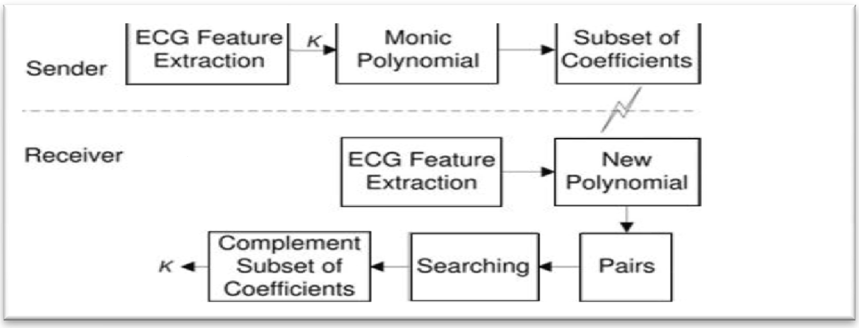


Fig .2 Process of ECG-IJS algorithm

IV. SYSTEM DESIGN

In this system, the integrity and confidentiality of sensitive medical data among sensor nodes must be protected against modification or other malicious attacks, because malicious or fraudulent (i.e., alteration of drug dosages or treatment procedures) can be extremely hazardous.

A. Feature Extraction

In image processing, feature extraction is a special form of dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant then the input data will be transformed into a reduced representation set of features. Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input.

1)Process: When two sensors in a BANs want to securely communicate each other by using ECG signal measured separately from the same body, the ECG features first need to be extracted from the sampled ECG signals. In our proposed scheme, we perform a frequency-domain analysis of ECG signals for generating the features. This is because that the frequency components of physiological signals, at any given time, have statistically similar values as long as they are measured on the body. A time-domain analysis shows that the values of the ECG signals measured at different parts of the body (from different leads) have similar trend but diverse values. In this validation process of the proposed ECG-IJS scheme, the ECG signals are downloaded from MIT-BIH Arrhythmia database. The MIT-BIH Arrhythmia Database contains 48 half-hour excerpts of two-channel ambulatory ECG recordings. The recordings were digitized at 360 samples per second per channel with 11-bit resolution over a 10-mV range.

STEP 1: Get the ECG data for fixed time duration of 4 s. The reason for choosing 4 s duration is to include at least one heart beat.
STEP 2: Resample the ECG data at 120 Hz.
STEP 3: Conduct 512 points FFT of the ECG data,extract the first 256 coefficients because the coefficients are symmetric.
STEP 4: Detect the local peaks on the extracted FFT coefficients. Each of the peak location index is used as a feature.
The ECG signals measured on the different areas of the body have statistically similar values within a time period. There are two reasons for selecting the FFT peak location index as a feature. First, the feature changes dynamically but can easily be detected with low computational complexity. Second, the body's physiological behaviors will be characterized by the peak location index features in the Fourier transform domain. Therefore, the peak location index is a good candidate that can be used to differentiate measurements (collected by a sensor) of one patient from those of different patients. The feature provides an efficient representation of ECG signals for the data authentication and secret key agreement. However, our proposed authentication framework does not limit to using the peak location index. Potential features such as the P-R interval could also be applied as long as they can meet the required authentication performance (i.e., FAR and FRR).

B. Data Hiding

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can read it. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the ciphertext should not be able to determine anything about the original message. An authorized party,

however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.
*1)Reed-Solomon Codes:*RS codes, which are BCH codes, are used in applications such as spacecraft communications, compact disc players, disk drives, and two-dimensional bar codes. According to Bossert (1999) the relationship between BCH and RS codes is such that RS codes comprise a subset of BCH codes and occasionally BCH codes comprise a subset of RS codes. Van Lint (1999) defines an RS code as a primitive BCH code of length $n=q-1$ over *GF* (q).
*2)Process of Key Hiding:*The sender measures the ECG signals and glucose data, and the glucose data will be sent to the receiver. The receivers have statistically similar ECG signals when two sensors measure the ECG from the same body. Both the sender and the receiver use the same future extraction algorithm to generate feature set called IJS coefficients. Once the features are generated, the sender uses it as a key to encrypt the glucose data, and then send the following packet to the receiver: {IDs , IDr, E, S,N1 ,MAC(k, S|M|N1 |IDs)}, where the IDs and IDr are the IDs of the sender and receiver, respectively. *M* is the original message. *E* is the encrypted message. *N*1 is a nonce used for the signature. *S* is the subset of *t* monic polynomial coefficients. MAC is a message authentication code using the Hash functions (e.g., SHA-1 or SHA-2), and the *k* is generated from the ECG features at the receiver site.

In IJS algorithm, the sender can construct a unique monic polynomial using the *F* as the roots and send parts of the coefficients to the receiver. Without knowing most of the roots, it is impossible for receiver to reconstruct the monic polynomial to discover *K*. When the receiver receives the coefficients sent by the sender, it can reconstruct the polynomial by *F’* it has. The receiver could successfully reconstruct the monic polynomial only when *F’* and *F* share most common elements. Compared with the original fuzzy vault algorithm, the IJS algorithm does not using chaff points to hide the secret (Key). Thus, the communication overhead between the sender and the receiver is significantly reduced.

C. Data Recovering

A key-recovery attack is an adversary's attempt to recover the cryptographic key of an encryption scheme. Historically, cryptanalysis of block ciphers has focused on key-recovery, but security against these sorts of attacks is a very weak guarantee since it may not be necessary to recover the key to obtain partial information about the message or decrypt message entirely. Modern cryptography uses more robust notions of security. Recently, indistinguishability underadaptive chosen-ciphertext attack (IND-CCA2 security) has become the "golden standard" of security. The most obvious key-recovery attack is the exhaustive key-search attack. But modern ciphers often have a key space of size 2^{128} or greater, making such attacks infeasible with current technology.

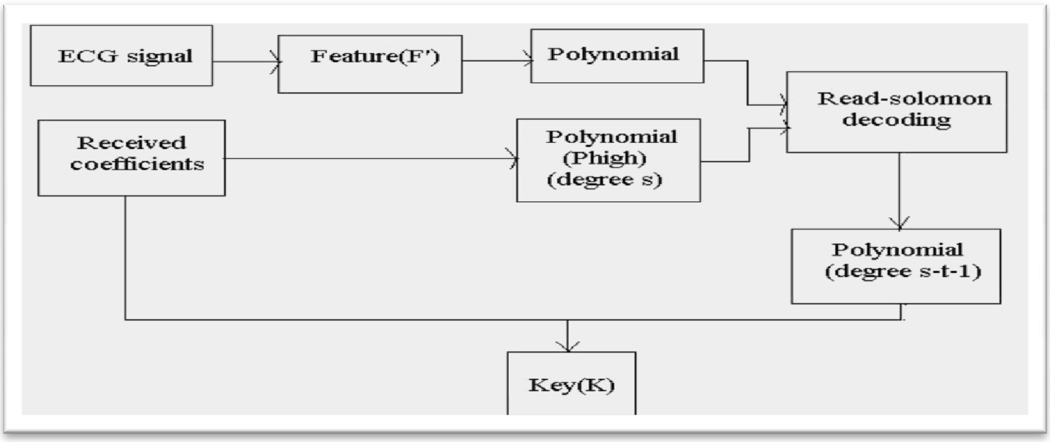


Fig .3 Block diagram of key recovery algorithm

1)ECG-IJS Key Recovery Algorithm:
STEP 1: extracting the feature $F\_$ from the ECG signal.
STEP 2: constructing a new ECG feature polynomial $p$high with degree s using the coefficients it receives.
STEP 3: evaluating the above polynomial on all points in $F\_$ to get a set of pairs.
STEP 4: using Reed–Solomon decoding to search for a polynomial with degree $s - t-$ 1 to meet most of the pairs.
STEP 5: reconstruct the ECG vault secret K by searching results and coefficients received from the sender.

After receiving the package from the sender, the receiver uses the feature extracting from the ECG and the receiver data set S to recover the secret k by the proposed ECG-IJS algorithm. The secret k is further used to decrypt the encrypted message E to obtain the original glucose data M.

V. AUTHENTICATION FOR BIOMETRIC SYSTEM

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be. Authentication often involves verifying the validity of at least one form of identification.

The receiver uses the same authentication algorithm with the sender to recalculate the MAC. If the MAC value calculated by the receiver is equal to the MAC value received from the sender, the authentication succeeds. Otherwise, the authentication fails and the received packet will be discarded.

A. Data Authentication

Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. This style of authentication cannot be applied to a broadcast setting, without placing much stronger trust assumptions on the network nodes. To send authentic data to mutually untrusted receivers, using a symmetric MAC is insecure: Any one of the receivers knows the MAC key, and hence could impersonate the sender and forge messages to other receivers. Hence, an asymmetric mechanism is needed to achieve authenticated broadcast. One of our contributions is to construct authenticated broadcast from symmetric primitives only, and introduce asymmetry with delayed key disclosure and one-way function key chains.

VI. EXPERIMENTAL RESULTS

In this paper, we validate the proposed ECG-IJS scheme. The validation begins with the feature extraction from the ECG signals, followed by the FAR and FRR analysis. After that, the security analysis of the proposed ECG-IJS scheme is discussed.

A. Feature Extraction

When two sensors in a BANs want to securely communicate each other by using ECG signal measured separately from the same body, the ECG features first need to be extracted from the sampled ECG signals. In our proposed scheme, we perform a frequency-domain analysis of ECG signals for generating the features. This is because that the frequency components of physiological signals, at any given time, have statistically similar values as long as they are measured on the body. A time domain analysis shows that the values of the ECG signals measured at different parts of the body (from different leads) have similar trend but diverse values. In this validation process of the proposed ECG-IJS scheme, the ECG signals are downloaded from MIT-BIH Arrhythmia database . The MIT-BIH Arrhythmia Database contains 48 half-hour excerpts of two-channel ambulatory ECG recordings. The recordings were digitized at 360 samples per second per channel with 11-bit resolution over a 10-mV range . The Feature extraction process is shown as follows.

1) Get the ECG data for a fixed time duration of 4 s. The reason for choosing a 4 s duration is that we want it to include at least one heart beat.

2) Resample the ECG data at 120 Hz.

3) Conduct 512 points FFT of the ECG data, extract the first 256 coefficients because the coefficients are symmetric.

4) Detect the local peaks on the extracted FFT coefficients, each of the peak location index is used as a feature.

The ECG signals measured on the different areas of the body have statistically similar values within a time period. There are two reasons for selecting the FFT peak location index as a feature. First, the feature changes dynamically but can easily be detected with low computational complexity. Second, the body's physiological behaviors will be characterized by the peak location index features in the Fourier transform domain. Therefore, the peak location index is a good candidate that can be used to differentiate measurements (collected by a sensor) of one patient from those of different patients. The feature provides an efficient representation of ECG signals for the data authentication and secret key agreement. However, our proposed authentication framework does not limit to using the peak location index. Potential features such as the P-R interval could also be applied as long as they can meet the required authentication performance (i.e., FAR and FRR).

B. Performance Analysis

In this paper, we consider securing the communication between any two nodes within the same WBAN. We assume that the sensor nodes have the capability of measuring the ECG signals with an attached ECG sensor. In this part, FAR and FRR are used to evaluate the performance of the proposed ECG-IJS scheme. The half total error rate (HTER), computed by HTER = (FAR + FRR)/2, is also obtained. This is because if the system could tolerate more different features between the sender and the receiver, the possibility of matching two feature sets that do not belong to the same person increase and thus the FAR increase. In contrast to the FAR, the FRR decreases when *t* increases, this is because when *t* increases, these two feature sets coming person are more likely to be matched.

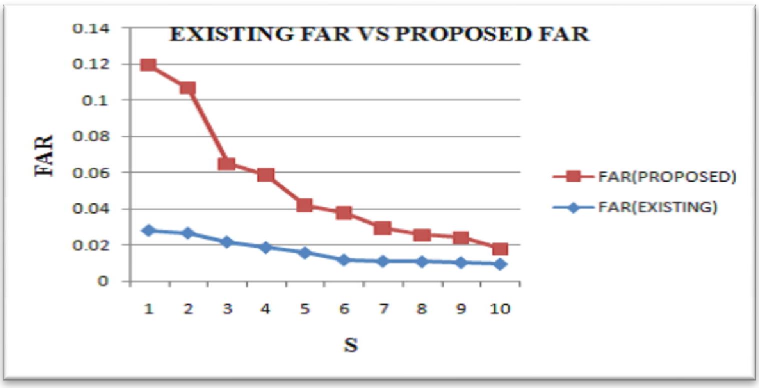


Fig .4 Chart for existing FAR Vs proposed FAR

Thus, the probability of recovering one set using the other sets also increases.

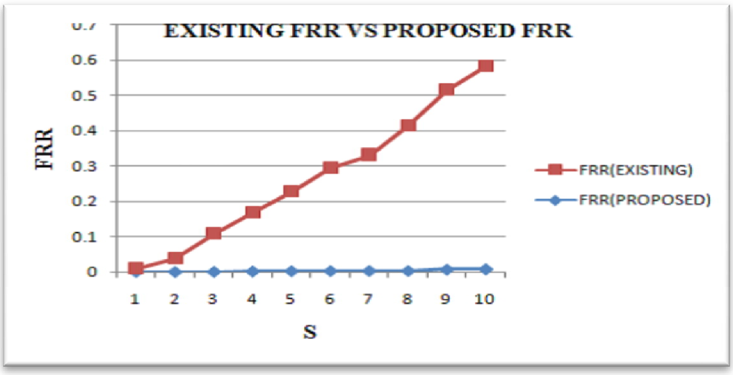
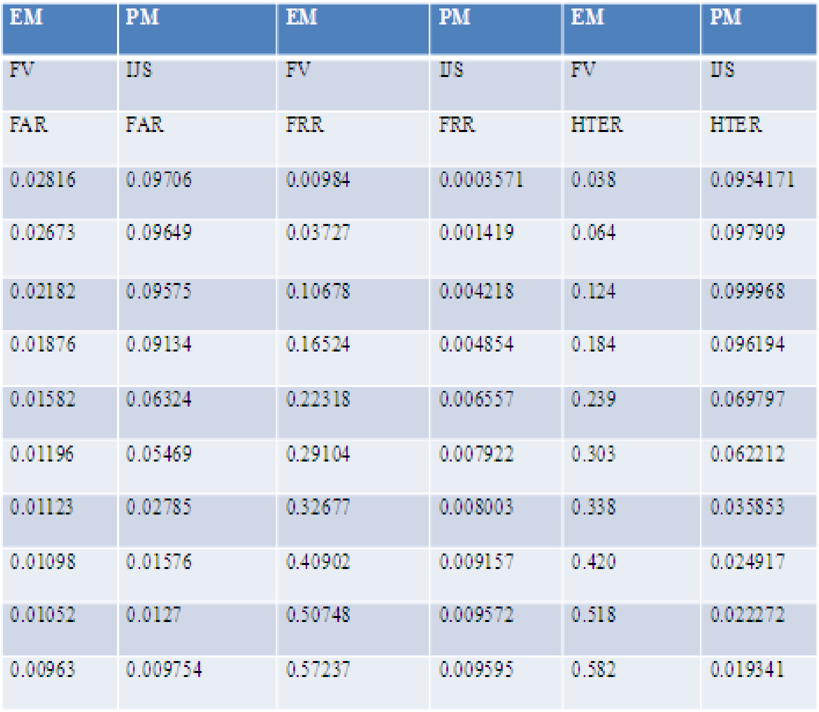


Fig .5 Chart for existing FRR Vs proposed FRR

Fig. 4 and 5 show the FAR and FRR performance when the degree of the monic polynomial *s* changes (the difference tolerance *t* is set to 2). It is shown in Fig. 4 that the FAR decrease when *s* increase. When *t* is fixed, the bigger *s* means that more shared features in the feature set is needed to successfully recover the secret *k*. Thus, the probability of mismatching the feature sets decreases. In Fig. 5, the FRR increases when *s* increases.

TABLE I

EXISTING METHOD(FUZZY VAULT) VS PROPOSED METHOD(IJS)



EM	PM	EM	PM	EM	PM
FV	IJS	FV	IJS	FV	IJS
FAR	FAR	FRR	FRR	HTER	HTER
0.02816	0.09706	0.00984	0.0003571	0.038	0.0954171
0.02673	0.09649	0.03727	0.001419	0.064	0.097909
0.02182	0.09575	0.10678	0.004218	0.124	0.099968
0.01876	0.09134	0.16524	0.004854	0.184	0.096194
0.01582	0.06324	0.22318	0.006557	0.239	0.069797
0.01196	0.05469	0.29104	0.007922	0.303	0.062212
0.01123	0.02785	0.32677	0.008003	0.338	0.035853
0.01098	0.01576	0.40902	0.009157	0.420	0.024917
0.01052	0.0127	0.50748	0.009572	0.518	0.022272
0.00963	0.009754	0.57237	0.009595	0.582	0.019341

.

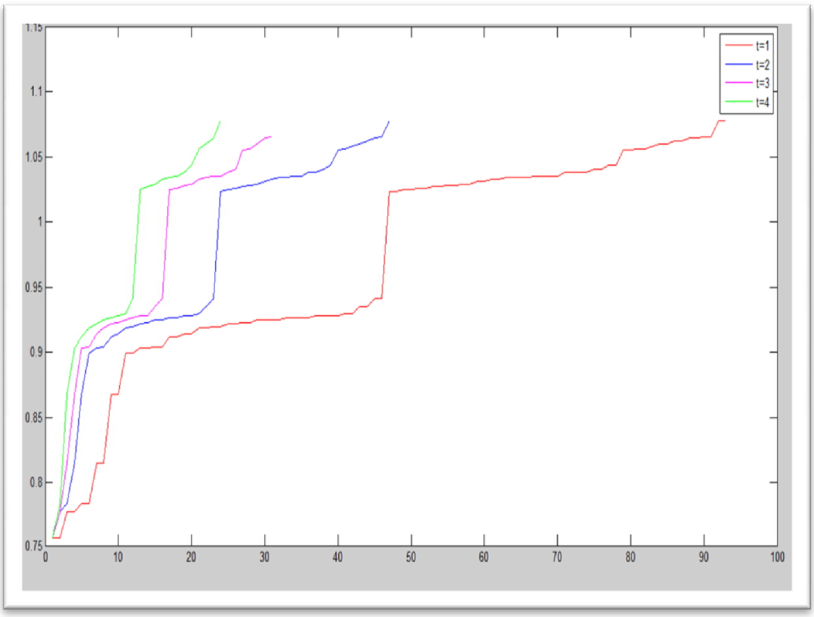


Fig .6 Polynomial s Vs Different t

In the figure 6, *t* denotes the number of coefficients and s denotes the degree of the monic polynomial. The ECG feature *F* is used as the root to build a unique ECG monic polynomial with degree *s*. The coefficients of the ECG monic polynomial are then calculated. For different t values sample coefficients are generated and the gulucose data is hidden into the samples.However, the complexity of the computation is increased when higher *s* is chosen.

VII. CONCLUSION

Secure communications in BANs are strongly required to preserve a person's health privacy and safety. Especially, in some applications, security attacks could even threaten the lives of people. In our project, an IJS scheme for key agreement, in which both privacy and authenticity are preserved in an energy-efficient manner. Our major contributions in this paper incudes several aspects: 1) the proposed ECG-IJS scheme can share a key in energy-efficient manner for BANs 2) a novel hash-based authentication approach using measured ECG signals at both sender's and receiver's sites and 3) a framework for the security analysis of BANs. In our proposed approach, ECG signals are used as biometric to generate keys which are used in data encryption and hash-based message authentication. The performance of the ECG-IJS scheme can be further improved by extracting more unique features for individuals and by adopting the optimal vault size and optimal difference tolerances.

ACKNOWLEDGMENT

We would like to express our sincere gratitude and heartful thanks to our principal **Dr. R.JOSEPH XAVIER**, for providing all kind of technological resources to bring out excellence for us.

We express our profound thanks to **PROF.K.VENKATASUBRAMANIAN**, Head of the department of Electronics and Communication Engineering, for extending his kind help in using all facilities in labs.

We take immense pleasure to thank our beloved guide **Dr.S.MARYPRAVEENA,** Associate Professor, Department of Electronics and Communication Engineering, for sparing his valuable time in guiding us and for his constant encouragement through the success of this project.

Last but not least, we are grateful to our **Parents** whose gracious encouragement allowed us to work with a clean mind and heart.

REFERENCES

[1] Zhaoyang Zhang, Honggang Wang, Athanasios,Vasilakos, and Hua Fang, "ECG-Cryptography and Authentication in BodyArea Networks" , IEEEtransactions on information technology in biomedicine, vol .16,no .6, Nov 2012.

[2] S. Choi, S.-J. Song, K. Sohn, H. Kim, J. Kim, J. Yoo, and H.-J. Yoo, "A low-power star-topology body area network controller for periodic data monitoring around and inside the human body," in *Proc. 10th IEEE Int. Symp. Wearable Comput.*, Oct. 2006, pp. 139–140.

[3] C. Poon,Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[4] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proc. IEEE-EMBS 2005. 27th Ann. Int. Conf. Eng. Med. Biol. Soc.*, 2005, pp. 2455– 2458.

[5] H.Wang, D. Peng,W.Wang, H. Sharif, H. hwa Chen, and A. Khoynezhad, "Resource-aware secure ECG healthcare monitoring through body sensor networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 12–19, Feb. 2010.

[6] Lin Yao, Bing Liu, GuoweiWu, Kai Yao, and JiaWang, 'A Biometric Key Establishment Protocol for Body Area Networks' ,IJDSN,vol.2011.

[7] J.-S. Lee, "Performance evaluation of IEEE 802.15.4 for low-rate wireless personal area networks," *IEEE Trans. Consumer Electron.*, vol. 52, no. 3, pp. 742–749, Aug. 2006.

[8] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proc. 2003 Int. Conf. Parallel Processing Workshops*, Oct. 2003, pp. 432–439.

[9] L. Yao, B. Liu, G. Wu, K. Yao, and J. Wang, "(2011) A biometric key establishment protocol for body area networks." *IJDSN*, vol. 2011.

[10] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: A new approach in human identification," *IEEE Trans. Instrum. Meas.*, vol. 50, no. 3, pp. 808–812, Jun. 2001.