Journal of Computer Science 10 (10): 2088-2094, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.2088.2094 Published Online 10 (10) 2014 (http://www.thescipub.com/jcs.toc)

A LIGHT-WEIGHT CRYPTOGRAPHY ANALYSIS FOR WIRELESS BASED HEALTHCARE APPLICATIONS

[1] S. Sangari and [2]Martin Leo Manickam

[1]Faculty of IT Department, Sathyabama University, Jeppiar Nagar, Chennai, India
[2]Faculty of ECE Department, St Joseph College of Engg., Chennai, Tamil Nadu, India

Received 2014-02-09; Revised 2014-02-17; Accepted 2014-06-28

ABSTRACT

Patient health monitoring devices are flexible. Powerful ECG acquisition system is used at anytime and anywhere in the patient monitoring system. The increasing feasibility and convenience of mobile healthcare has already introduced several significant challenges in hospitals, healthcare providers, policy makers and patients. This study provides adaptive humming bird algorithm of light weight cryptography. This method has higher level of security over health care application with adaptive Humming Bird Algorithm for ECG acquisition systems which enables Intensive Care Monitoring. This study provides a key agreement scheme that allows neighboring nodes in BAN to share the common keys generated by electrocardiogram signal. The proposed ECG-humming bird key agreement scheme enables the secure communication over the WBAN. The experimental results are presented, which show that the proposed scheme provide better security performance in terms of false acceptance rate and false rejection rate than other approaches.

Keywords: Wireless Body Area Network, Electrocardiogram Signal

1. INTRODUCTION

In Wireless body area networks are networks of wireless wearable sensors placed on the human body (Cherukuri *et al*., 2003). The WBAN offers great benefits to patients and healthcare providers and also improve the quality of life style. The WBAN is used for monitoring patients at homes and also work places without going to the hospital. Data security should be important concern in WBAN. The unauthorized users try to access and modify the healthcare information. The lack of security features not only affect the patient security and privacy and also the compromise the patient safety (Ethala *et al*., 2013; Kalyani and Chellappan, 2012). Because the eavesdroppers Authenticated encryption algorithm provides confidentiality and integrity protection of messages using a single processing step. The security mechanisms ensure the confidentiality, integrity and availability of WBAN. In this study, we present a new key agreement scheme ECG-Humming bird which uses ECG signals for generating the keys. The proposed schemes avoid the pre key distribution overhead. Humming bird is an authenticating encryption primitive. It has been designed particularly for resource-constrained devices such as wireless sensors, RFID tags, smart meters and industrial controllers. Humming bird can be implemented in very small hardware or software footprint and it is suitable for providing security in low-cost ubiquitous devices. A considerable body of research has been focused on providing cryptographic functionality to resource constrained devices, while scarce computational and storage capabilities of low-cost smart devices make the problem challenging (Wang *et al*., 2011; 2012). This emerging research area is usually referred to as lightweight cryptography which has to deal with the tradeoff among security, cost and performance. The rest of the paper is organized as follows. Section II introduces exiting security solution that applicable to WBAN. Section III describes the healthcare architecture and describes the proposed ECG-

Corresponding Author: Sangari, S., Faculty of IT Department, Sathyabama University, Jeppiar Nagar, Chennai, India

Humming bird scheme for secure communication over WBAN. In section IV performance analysis of proposed algorithm is evaluated based on false acceptance rate and false rejection rate parameters. Finally conclusions are given in section V.

2. RELATED WORKS

A typical topology of WBANs includes multiple types of medical sensors that can be wirelessly connected to other medical sensors or to the control nodes (e.g., Smart phones), which could interface with other types of networks such as WiMAX or WiFI to further deliver the collected medical information to the information center (Ab-Rahman *et al*., 2013; Aris *et al*., 2011). Much great effort has been devoted to develop secure communication schemes between the internet and control nodes (Barni *et al*., 2011). Thus, our studies focus on the securing inter sensor communication over the body area. In WBAN (Miao *et al*., 2009; Bao *et al*., 2005), key distribution is always vulnerable to man in the middle attack. The threats can be categorized: Active attack and passive attack. The active attackers can able to drop messages and replay old messages, modify messages. The passive attackers capable of listening the communication over WBAN. A comprehensive survey on wireless body area networks is given in (Chen *et al*., 2011). Besides the transitional key distribution schemes, there are several on-going research works that implement the key distribution using biometric features. The fuzzy vault scheme was proposed by Jules and Sudan (Liu and Kwak, 2010). This approach generates the polynomial that encodes the information. The security of vault depends on adding extra chaff points which brings the communication overhead. This method uses fuzzy vault scheme to lock the key and unlock the Vault to regenerate the key at receiver side. Liu and Kwak (2010; Babu and Singh, 2013) proposed hybrid security mechanism for secure communication over WBAN. The asymmetric cryptography only employed for node association process (Poon *et al*., 2006; Raghini *et al*., 2013). The symmetric cryptography is used for link level security. The traditional asymmetric cryptography has heavy exponential calculations and also size and computation capabilities. The authors (Kaur *et al*., 2010; Duraisamy and Ragavendran, 2013) proposed a watermarking-based ECG signal tempering identification approach. A low frequency 15-digit chirp code is embedded in wirelessly transmitted ECG signal. That scheme can also completely remove chirp code watermarks from reconstructed ECG signal to minimize ECG visualization distortion (Zhang *et al*., 2012).

3. PROBLEM FORMULATION

3.1. Overview of WBAN

The BSN architecture presented in this article includes several key components; the basic structure of BSN is shown in **Fig. 1**, where wireless physiological sensors are used to measure the status of the patient. However, relying only on the physiological data can often involve false detections due to motion artifacts and changes of physiological/emotional stress. For example, sudden heart rate changes increases due to exercise rather than arrhythmia.

To capture the context aware sensors are incorporated into the design of the BSN, relevant episodes and the mobile phone.

3.2. Proposed ECG-Humming Bird Scheme

We propose an ECG-Humming bird scheme for secure communication over WBAN. The sender and receiver have ability to get ECG signals from human body. The extracted feature can be used as key for encryption and decryption. In the proposed scheme, at the sender, the feature extracted from ECG signal to form a key for encryption.

In the receiver side, it decrypts the message using the key extracted from the ECG signal. The **Fig. 2** shows the proposed ECG-Humming bird scheme.

3.3. Humming Bird Algorithm

Humming Bird (HB) is a rotor based encryption algorithm designed for resource constrained devices. Humming bird is an ultra-lightweight cryptographic primitive for encryption and authentication in severely resource-constrained environments. We propose an ECG-Humming bird scheme for secure communication over WBAN.

Humming bird is a combination of a block cipher and stream cipher with:

- 16-bit block size
- 256-bit key size
- 80-bit internal state

Humming bird encrypts 16-bit blocks of data using a 256-bit key. The underlying architecture of Humming bird is original and hybrid (with elements of block and stream ciphers).The encryption and decryption procedure (**Fig. 3 and 4)** can be represented as a continuously working rotor-based machine. Four identical internal block ciphers play a role of virtual rotors.

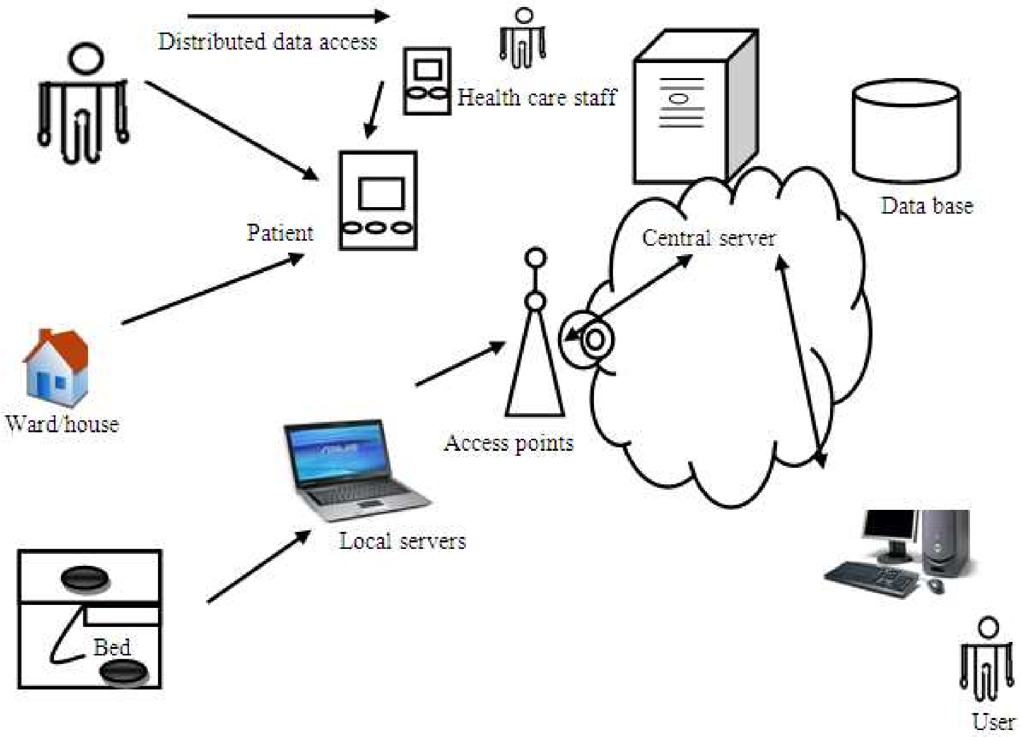


Fig. 1. Architecture of healthcare monitoring system

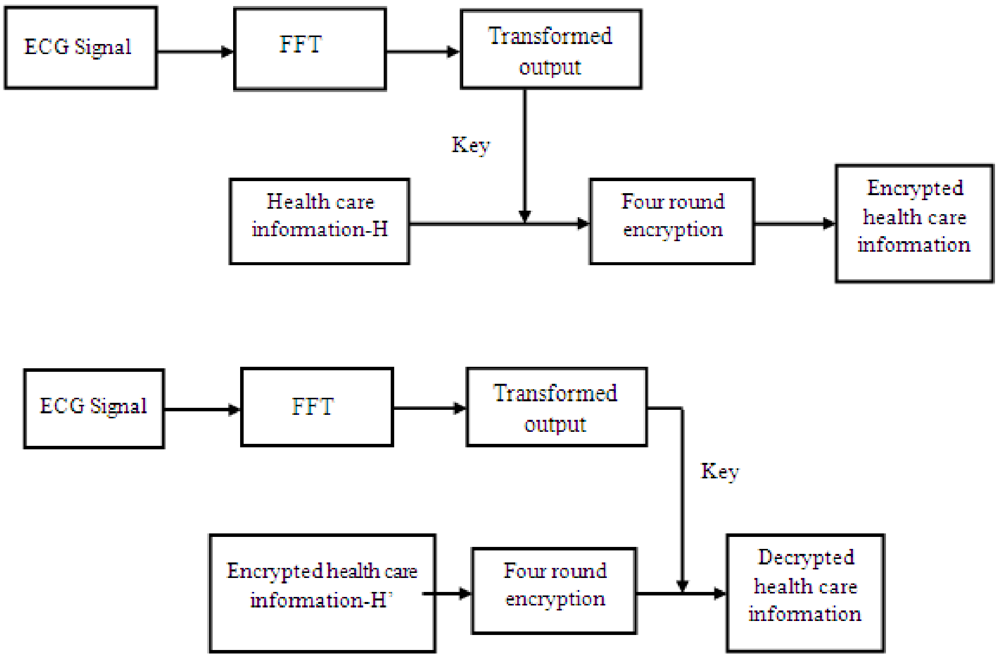

ECG Signal
FFT
Transformed output
Key
Health care information-H
Four round encryption
Encrypted health care information
ECG Signal
FFT
Transformed output
Key
Encrypted health care information-H'
Four round encryption
Decrypted health care information

Fig. 2. Proposed system based on HB

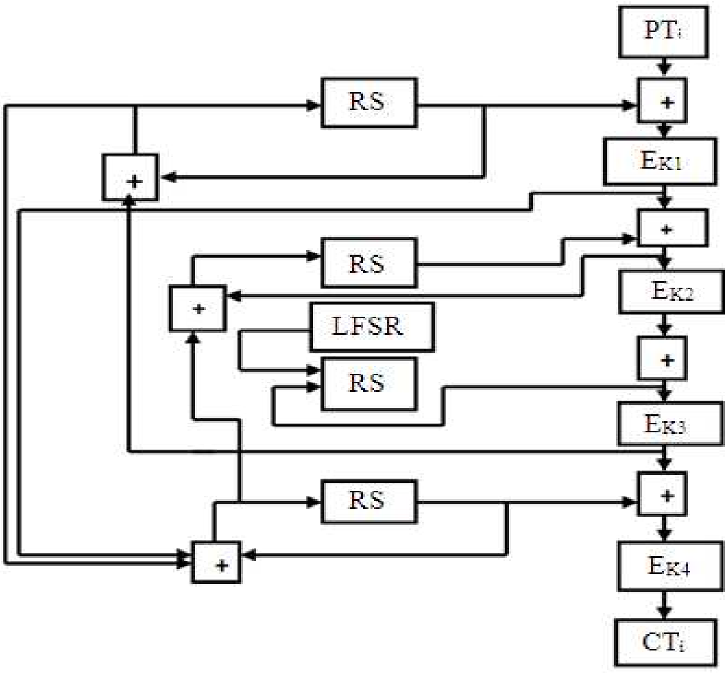


Fig. 3. Encryption process

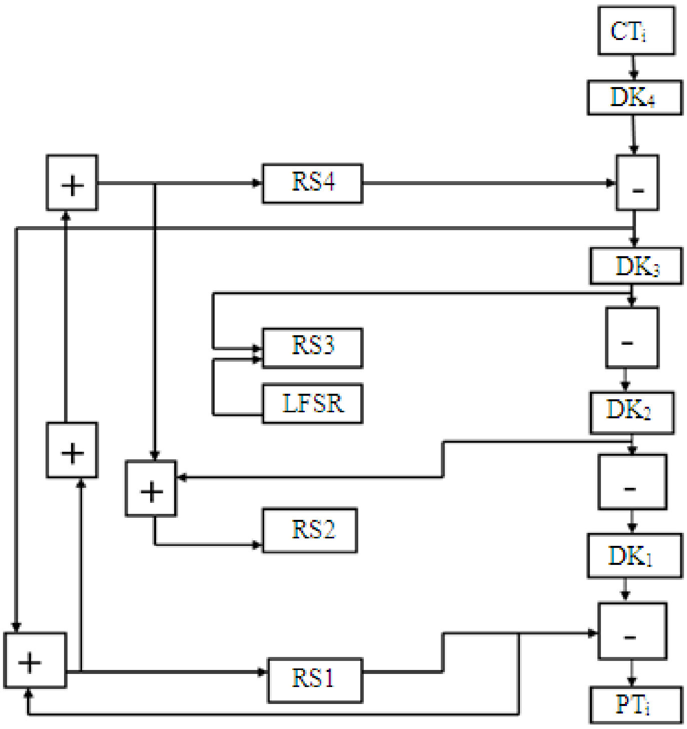


Fig. 4. Decryption process

They perform a set of operations on short 16-bit data blocks. The step operation can be used to fetch the peak signals from the ECG data in one instance that can also be generated in another instance possessing the same key. It can also be used to obscure the current state within an instance of HB while still keeping two instances in synchronization. This can be useful when the plaintext and the cipher text are being sent as part of authentication. The STEP operation can be used to advance the state of a HB instance so that the state directly after the encrypt is obscured in the event that the instance is compromised.

The encryption process for the Humming bird cryptographic algorithm, included simply for the sake of completeness. Humming bird is a block cipher not a stream cipher but the rotor machine equipped with novel rotor-stepping rules. It has a Hybrid structure of block cipher and stream cipher with 80-bit internal state, 16-bit block size and 256-bit key size. A top-level description of the Humming bird encryption consists of four 16-bit block ciphers Ek1, Ek2, Ek3 and Ek4 and the four 16-bit internal states registers RS1, RS2, RS3 and RS4 and 16-stage Linear Feedback Shift Register (LFSR). PTi represents the i-th plaintext block and CTi represents the corresponding i-the cipher text block. The 256-bit key K is divided into four 64-bit sub keys k1, k2, k3 and k4 are used in the four corresponding block ciphers. The encryption process for the Humming bird cipher is a four stage process. It is very similar to the initialization process in structure and the actual encryption includes updating of the state registers as well as the LFSR.

4. EXPERIMENTAL RESULTS

We validated the proposed ECG-Humming bird scheme for secure communication over WBAN. We begin by discussing the collection procedure and evaluate performance of proposed algorithm based on false acceptance rate and false rejection rate parameters. The ECG signals are downloaded from MIT-BIH database and apply FFT transform to the ECG signal. The peak values can be identified. The extracted features can be used as key. The peak values can be used to differentiate the measurement of one patient from other one. The **Fig. 5** shows the feature extraction process of ECG signal. False acceptance rate and false rejection rate were used to characterize the proposed scheme.

The false rejection rate can be defined as the two features from the different persons were matched and false acceptance rate can be defined as the two features from the same person at same time were unmatched. The half total error rate can be calculated by HTER = FAR + FRR/2. When t value increases, the false acceptance rate also increased and when the t value increases, the false rejection rate also decreased.

The False Acceptance Rate (FAR), False Rejection Rate (FRR) and Half Error Total Rate (HETR) performance evaluated by ECG data and tolerance values are discussed in **Table 1** and plotted in **Fig. 6.**

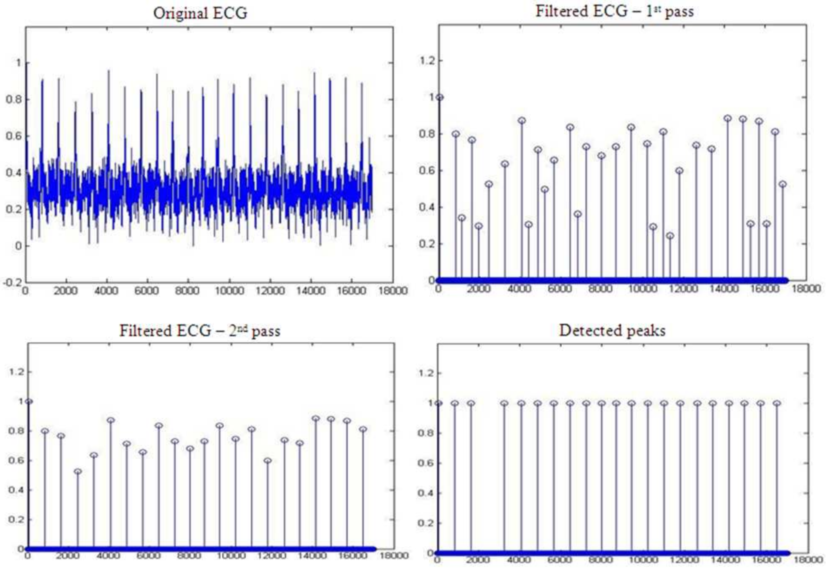
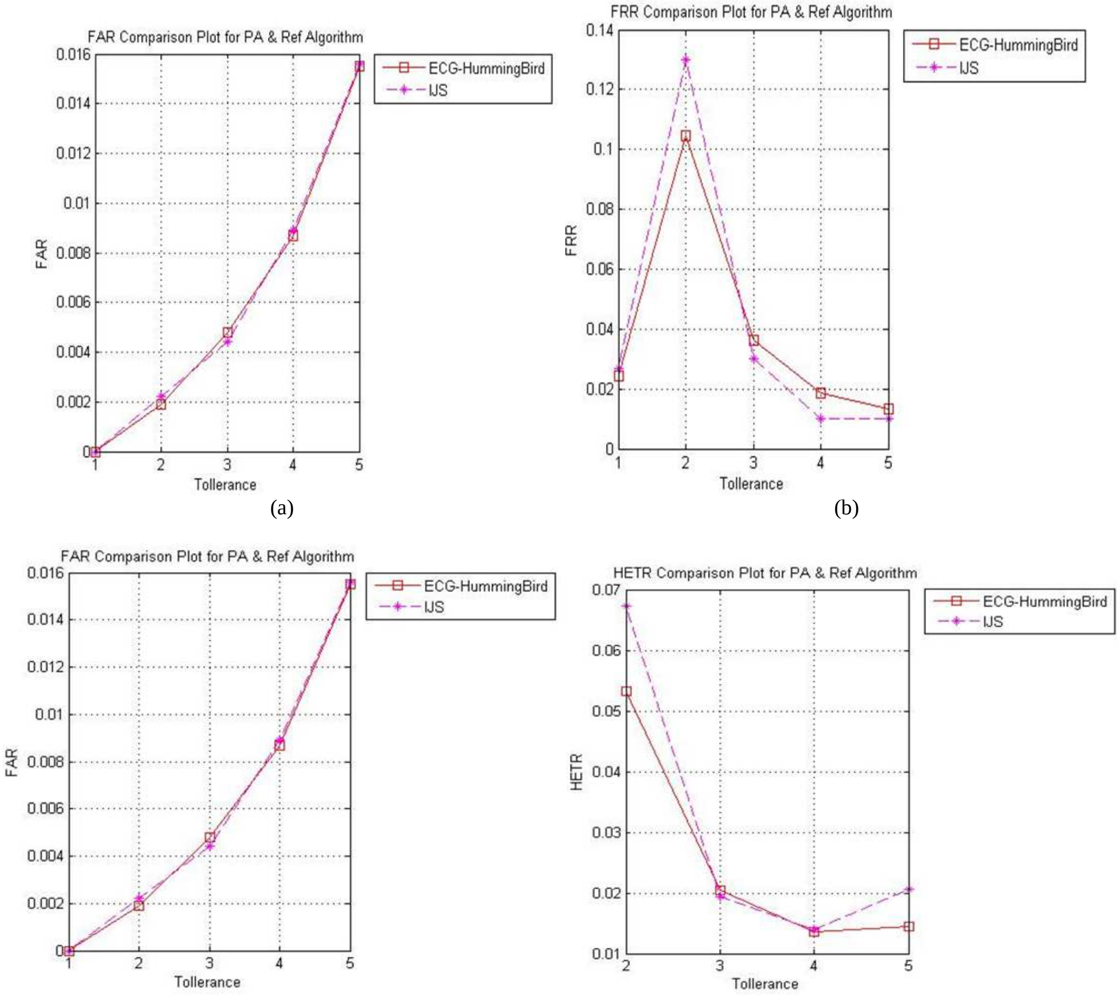


Fig. 5. Feature extraction (a) Original ECG (b) Filtered ECG 1 St pass (c) Filtered ECG 2 and pass (d) Detected peaks finally



(a) (b)

(a) (b)

Fig. 6. (a) FAR Vs FRR (b) FRR comparison (c) FAR comparison (d) HETR comparison

Table 1. FAR and FRR performance

	IJS			ECG-Humming bird		
Tollerance	FAR	FRR	HETR	FAR	FRR	HETR
1	0.0000	0.027	0.2350	0.0000	0.0242	0.0121
2	0.0022	0.130	0.0672	0.0019	0.1047	0.0533
3	0.0044	0.030	0.0194	0.0048	0.0362	0.0205
4	0.0089	0.010	0.0139	0.0087	0.0186	0.0136
5	0.0156	0.010	0.0206	0.0155	0.0133	0.0144

5. CONCLUSION

This study proposes a sufficiently matured humming bird encryption algorithm for secured bio-health science applications based on the Electro Cardio Gram (ECG) signals. As the ECG signals will be varying from person to person it is highly motivated to extract the peak valued features and to apply intelligent encryption algorithm for a secured transmission. High quality randomness of the ECG signals results in a widely expanded key space which would be an ideal key generator for data encryption. Here, authorized personnel follow a decryption algorithm in such a way to maintain the zero data loss. The analysis of the ECG signal is intended to be more important in bio-health science applications. As an extendable future enhancement there is a possibility of using PPG signal to generate the key and also use energy efficient light weight security mechanism.

6. REFERENCES

Ab-Rahman, M.S., Hadiguna and L.S. Supian, 2013. Power analysis on same filter different sources for selection of spectral filters in optical demultiplexer. J. Comput. Sci., 9: 866-874. DOI: 10.3844/jcssp.2013.866.874

Aris, S., A. Messai, M. Benslama, M. Nadjim and M.M. Elharti *et al*., 2011. Integration of quantum cryptography through satellite networks transmission. Am. J. Applied Sci., 8: 71-76. DOI: 10.3844/ajassp.2011.71.76

Babu, A.M. and K.J. Singh, 2013. Performance evaluation of chaotic encryption technique. Am. J. Applied Sci., 10: 35-41. DOI: 10.3844/ajassp.2013.35.41

Bao, S.D., Y.T. Zhang and L.F. Shen, 2005. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. Proceedings of the IEEE-EMBS 27th Annual International Conference Engineering in Medicine and Biology Society, (MBA’ 05), IEEE Xplore Press, Shanghai, pp: 2455-2458. DOI: 10.1109/IEMBS.2005.1616965

Barni, M., P. Failla, R. Lazzeretti, A.R. Sadeghi and T. Schneider *et al*., 2011. Privacy-preserving ECG classification with branching programs and neural networks. IEEE Trans. Inform. Forensics Sec., 6: 452-468. DOI: 10.1109/TIFS.2011.2108650

Chen, M., S. Gonzalez, A. Vasilakos, H. Cao and V.C. Leung *et al*., 2011. Body area networks: A survey. Mob. Netw. Appl., 16: 171-193. DOI: 10.1007/s11036-010-0260-8

Cherukuri, S., K. Venkatasubramanian and S. Gupta, 2003. Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. Proceedings of the International Conference Parallel Processing Workshops, Oct. 6-9, IEEE Xplore Press, pp: 432-439. DOI: 10.1109/ICPPW.2003.1240399

Duraisamy, K. and U. Ragavendran, 2013. Low power analog multiplier using MIFGMOS. J. Comput. Sci., 9: 514-520. DOI : 10.3844/jcssp.2013.514.520

Ethala, K., R. Seshadri, N.G. Renganathan and M.S. Saravanan, 2013. Secret handshake issue and validate authority based authentication system for wireless sensor network. J. Comput. Sci., 9: 1174-1180. DOI : 10.3844/jcssp.2013.1174.1180

Kalyani, P. and C. Chellappan, 2012. Enhanced RSACRT for energy efficient authentication to wireless sensor networks security. Am. J. Applied Sci., 9: 1660-1667. DOI: 10.3844/ajassp.2012.1660.1667

Kaur, S., O. Farooq, R. Singhal and B.S. Ahuja, 2010. Digital watermarking of ECG data for secure wireless Communication. Proceedings of the International Conference on Telecommunication and Computing Recent Trends in Information, Mar. 12-13, IEEE Xplore Press, Kochi, Kerala, pp: 140-144. DOI: 10.1109/ITC.2010.96

Liu, J. and K.S. Kwak, 2010. Hybrid security mechanisms for wireless body area networks. Proceedings of the 2nd International Conference on Ubiquitous and Future Networks, Jun. 16-18, IEEE Xplore Press, Jeju Island, Korea (South), pp: 98-103. DOI: 10.1109/ICUFN.2010.5547221

Miao, F., L. Jiang, Y. Li and Y.T Zhang, 2009. Biometrics based novel key distribution solution for body sensor networks. Proceedings of the IEEE Annual International Conference of Engineering in Medicine and Biology Society, Sept. 3-6, IEEE Xplore Press, Minneapolis MN, pp: 2458-2461. DOI: 10.1109/IEMBS.2009.5334698

Poon, C., Y.T. Zhang and S.D. Bao, 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Commun. Mag., 44: 73-81. DOI: 10.1109/MCOM.2006.1632652

Raghini, M., N.U. Maheswari and R. Venkatesh, 2013. Overview on key distribution primitives in wireless sensor network. J. Comput. Sci., 9: 543-550. DOI : 10.3844/jcssp.2013.543.550

Wang, W., H. Wang and M. Hempel, 2011. Secure stochastic ecg signals based on gaussian mixture model for e-healthcare systems, IEEE J. Syst., 5: 564-573. DOI: 10.1109/JSYST.2011.2165597

Wang, J., G. Jian, W. Xiaoke, L. Brian and D.L. Nathan *et al*., 2012. Accurate group-delay measurement for radial-velocity instruments using the dispersed fixed-delay interferometer method. Publicat. Astron. Soc. Pacific, 124: 598-605. DOI: 10.1086/666379

Zhang, Z., H. Wang, A.V. Vasilakos and H. Fang, 2012. ECG-cryptography and authentication in body area networks. IEEE Trans. Inform. Technol. Biomed., 16: 1070-1078. DOI: 10.1109/TITB.2012.2206115