Research Journal of Applied Sciences, Engineering and Technology 11(5): 516-522, 2015
DOI: 10.19026/rjaset.11.1856
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: May 11, 2015 Accepted: June 22, 2015 Published: October 15, 2015

Research Article

A Lightweight Symmetric Key based Cryptographic System for Wireless Body Sensor Network

[1]A. Sivasangari and [2]J. Martin Leo Manickam
[1]Department of Information Technology, Sathyabama University,
[2]Department of Electronics and Communication Engineering, St Joseph College of Engineering,
Chennai, India

Abstract: Of late, E-health monitoring is gaining its limelight because of its flexibility of service. This methodology makes it possible to monitor a patient in a remote area, by exploiting wireless biosensors attached in the patient's body. These biosensors collect different physiological signals from the human body and forward all the collected information to the server or to the doctors. This data transmission is vulnerable to several security attacks. It is necessary to provide security and hence a three layered lightweight symmetric key based cryptographic system is proposed. This system ensures several security measures such as access control, data confidentiality and integrity etc. Finally, the proposed system is analyzed with several performance metrics. The system proves its efficiency and is shown in graphical results.

Keywords: Biosensors, E-health monitoring, symmetric key based cryptography, wireless body sensor networks

INTRODUCTION

Of late, E-health monitoring is gaining its limelight because of its flexibility of service. This methodology makes it possible to monitor a patient in a remote area, by exploiting wireless biosensors attached in the patient's body. These biosensors collect different physiological signals from the human body and forward all the collected information to the server or to the doctors (Miao *et al*., 2012). In case of any dangerous situation, the patient is alarmed with messages through the monitoring system. These remote monitoring systems are fruitful in places where scarcity of physicians is observed.

All the detected information is passed into a powerful node attached in the human body. Thus, the transmission of collected information from the human body to the physician involves three levels of transmission. They are data transmission between biosensors and sensor head, data transmission between the sensor head and the base station and data transmission between the base station and the physician (Lin *et al*., 2011).

As this network deals with very confidential medical information, a strict security and privacy policy has to be enforced. If the security policy is not up to the mark, the patient's medical data can be gained access by the intruder and this may result in wrong diagnosis, Venkatasubramanian *et al*. (2008). This is a serious issue needed to be addressed (Fig. 1).

This study proposes an approach that securely transmits medical information, in all the three levels of data transfer. The biosensor detects the rate of heart beat and ECG is generated. This ECG is converted to data and the QRS positions of signals are analyzed, as they are the most important information for analysis, as done by Kohler *et al*. (2002), Lee and Buckley (1999) and Zhang and Lian (2007). This extracted important information is encrypted by using symmetric key based cryptography Fig. 2.

This study provides security in all the three stages of data transmission. Initially, in the first stage, every bio-sensor registers it with the sensor head to ensure the identity and to avoid miscommunication. Bio-sensors detect the QRS peaks of the ECG signal. The detected QRS peaks are transferred to the sensor head with the sensor ID and timestamp. In the second phase of the system, the sensor head registers itself to the base station and authentication is performed. Symmetric key encryption is performed and then the encrypted data is hidden within a cover image. Sensor head then forwards the encrypted and embedded data to the base station.

Finally in the last phase, the physician can access the medical data after clearing the access control step. If the physician needs to access the data, then Acc_R is sent to the base station. The base station then sends the decryption key which is encrypted by the phy_{id}. The physician has to decrypt the key, in order to gain access to the data. In this study, we focus on extracting QRS

Corresponding Author: A. Sivasangari, Department of Information Technology, Sathyabama University, Chennai, India

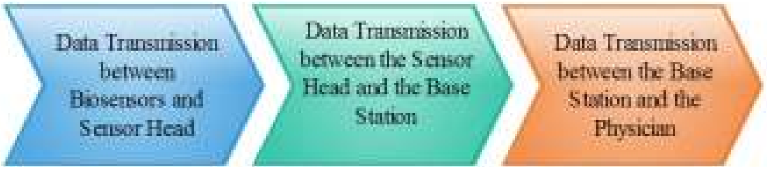
Data Transmission between Biosensors and Sensor Head
Data Transmission between the Sensor Head and the Base Station
Data Transmission between the Base Station and the Physician

Fig. 1: Processes involved in the system

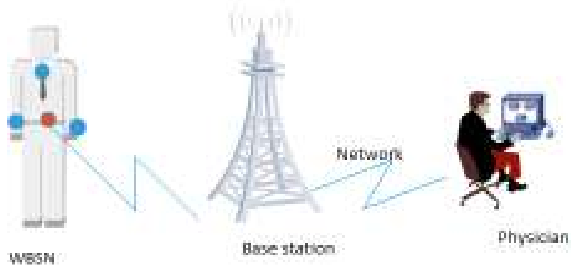

Fig. 2: Wireless body sensor networks

signals and to provide security through all the three different phases.

LITERATURE REVIEW

Several works have been proposed to enforce security policies for wireless body sensor networks and are studied below. Already proposed security schemes for Mobile Ad hoc Networks and Wireless Sensor Networks do not suit Body Sensor Networks, owing to its communication abilities and battery backup.

Several systems concentrating over encryption, key management and access control mechanisms can be studied in the works proposed by Hu *et al*. (2013), Keoh *et al*. (2009), Law *et al*. (2011), Li *et al*. (2013), (2010), Malan *et al*. (2004), Tan *et al*. (2008), (2009) and Xu *et al*. (2011). The physiological signals were introduced by Venkatasubramanian and Gupta (2006), in order to carry out a secure inter-sensor communication. In the work proposed by Poon *et al*. (2006), the Inter-Pulse Interval is used to produce cryptographic keys.

A Sensor Network for Assessment of patients is presented by Poon *et al*. (2006), which provides privacy, authenticity and integrity of medical data. Malasri and Wang (2009) use symmetric keys are generated by ECC ad RC5 block cipher is employed to assure data confidentiality and integrity, but this system is inefficient because of its computational overhead. A lightweight trust based model is proposed by He *et al*. (2012), in order to deal with the security breaches.

In the work proposed by Upmanyu *et al*. (2010), a secure and a blind biometric authentication protocol is presented. This protocol assures user's privacy, template protection and trust issues. A secure and a novel lightweight network admission and transmission protocol is presented by Daojing *et al*. (2013). ECG is manipulated by morphological schemes in the works proposed by Chen and Duan (2005), Chu *et al*. (1989), Hu and Bao (2010), Trahanias (1993), Zhang and Lian (2009) and Zhang *et al*. (2007).

Motivated by the aforementioned works, we propose a system that extracts QRS signals and are encrypted by a lightweight symmetric key based protocol. This system provides user access control, privacy and authentication, which are the important attributes of security.

PROPOSED METHODOLOGY

This study aims to arrive at a secure system that provides privacy, authenticity, access control, confidentiality and integrity. Privacy is guaranteed by keeping the data private such that the unintended users cannot use or tamper the data by any means. Every communication can turn its leaf out, only when the authentication procedure gets over. Access control mechanisms sieve through the users such that it determines who can access what. Confidentiality ensures that only the intended users can gain access to the data (usage of decryption key). Integrity is achieved such that illegitimate alteration over the data should not be possible.

This study concentrates on three stages of data transmission and they are data transmission between biosensors and sensor head, data transmission between the sensor head and the base station and data transmission between the base station and the physician. A short summary of every stage is presented below.

Data transmission between biosensors and sensor head:

- Each bio-sensor registers it with the sensor head to ensure the identity and to avoid miscommunication.
- Bio-sensors detect the QRS peaks of the ECG signal.
- The detected QRS peaks are transferred to the sensor head with the sensor ID and timestamp.

Data transmission between the sensor head and the base station:

- The sensor head registers itself to the base station and authentication is performed.
- Symmetric key encryption is performed and then the encrypted data is hidden within a cover image.

- Sensor head then forwards the encrypted and embedded data to the base station.

Data transmission between the base station and the physician:

- The physician can access the medical data after passing the access control step.
- If the physician needs to access the data, then Acc_R is sent to the base station. The base station then sends the decryption key which is encrypted by the phy_{id}. The physician has to decrypt the key, in order to gain access to the data.

Data transmission between biosensors and sensor head: Initially, the ECG of a patient is converted to binary data. The binary data is encrypted based on lightweight symmetric key based cryptography. The extraction of QRS signals are done by the following steps. It is necessary to consider the limited power and computational support of bio-sensors, QRS detection algorithm based on morphological operators is used by Zhang and Tae-Wuk (2012). The main merit of morphological operators is that it works over spatial domain and not over frequency. These operations work on the basis of mathematical formulation and are simple to implement.

Sensor registration with the sensor head: In this phase, all the bio-sensors present in the human body are needed to get registered with the sensor head, in order to perform data transmission. Initially, the bio-sensors present in the human body sends a J_{Rq} along with the bio-sensor ID to the sensor head. This is to avoid misconception of bio-sensors. The sensor head verifies the bio-sensor ID and accepts the J_{Rq}, if it belongs to the concerned human body.

This process is then followed by transmitting the encrypted QRS peaks to the sensor head. The encryption is carried out by the symmetric keys and is explained below.

Detection of QRS peaks in ECG signal: Several morphological operators such as dilate, erode, open and close, in order to extract the QRS peaks of the signal. The dilation operation enlarges the input object, whereas the erode operator reduces or shrinks the input object. The open operator makes the edges or outline of the input object in even fashion. The close operator fills the gap between the edges and also the tiny holes are excluded. This study exploits dilate and erode operators.

Steps to detect QRS peaks:

Step 1: Dilate and erode the input signal S_d and S_r respectively.
Step 2: Calculate the average av of $S_d\ and\ S_r$.
Step 3: Calculate the difference between the average and the input signal.
Step 4: Apply modulus operation to improve the quality of filtered ECG signal.
Step 5: Choose an adaptive threshold as the deciding function.

The adaptive threshold depends on the signal, so that it can adapts to the changing behavior of the signal. The threshold can be selected by the following:

$$th = \begin{cases} 0.1M, M < 3 \\ 0.3M, 3 \leq M \leq 7 \\ 0.13M, M > 7 \end{cases} \tag{1}$$

In (1), M is derived from the signal that is within the range of millivolts. Thus, the QRS peaks are detected.

Data transfer from bio-sensor to sensor head: The detected QRS peaks are then transferred by the bio-sensors to the sensor head. This transmission consists of the detected QRS peaks, bio-sensors' ID and the timestamp. The sensor head verifies and accepts the data that has been sent:

$$bi\_sen_i \rightarrow SH: \{d \big| bi_{sen_{id}} \big| ts\} \tag{2}$$

where,
bi_sen_i = The bio-sensor
SH = The sensor head
d = The data
$bi_{sen_{id}}$ = The unique identifier of the bio-sensor
ts = The timestamp

Data transmission between the sensor head and the base station: This phase focuses on several aspects of security issues. Keys are generated and the encryption is carried out. The encrypted QRS peaks are hidden within a cover image, by exploiting watermarking concept. The QRS peaks embedded cover image is sent to the base station.

Sensor head registration: The unique identifier of the sensor head is shared with the base station. Upon verification, the master key is issued for the sensor head by the base station. When a sensor head node needs to transfer data to the base station, the sensor head sends a D_R along with the sh_{id} and timestamp to the base station. The D_R is verified by the base station and the randomly generated key for data transmission k_{ms} along with the k_{mk} is provided. k_{mk} is recycled for every period of time:

$$\begin{cases} SH_i \rightarrow BS: \{sh_{id}\}\ Identifier\ sharing; \\ BS \rightarrow SH_i: \{mk\}\ Master\ key\ transmission \\ SH_i \rightarrow BS: \{D_r|sh_{id}|ts\}\ Data\ request\ transmission \end{cases} \tag{3}$$

$$BS \rightarrow SH_i: \{k_{ms}|k_{mk}|ts\} \quad (4)$$

where,

SH = The sensor head
BS = The base station
sh_{id} = The unique identifier of sensor head
mk = The master key
ts = The timestamp
k_{mk} = Recycled for every minute

Symmetric key encryption: Symmetric key systems rely on a single key for both encryption and decryption process. Symmetric key systems are faster and simple to implement. Due to the resource restriction of bio-sensors, symmetric keys are exploited by this system. After the detection of QRS peaks, encryption is performed by the symmetric key.

When a sensor head needs to transfer data to the base station, a D_R along with the sh_{id} and timestamp is sent to the base station. The D_R is verified by the base station and the randomly generated key for data transmission k_{ms} along with the k_{mk} is provided back to the sensor head. Data transfer format is provided below:

$$sh_i \rightarrow BS: \{d|ts\}_{k_{sym}} \quad (5)$$

In the above equation:

sh_i = The sensor head
BS = The base station
d = The data
ts = The timestamp
k_{sym} = The key that is used for encryption

The symmetric key is generated by:

$$k_{sym} = \mu. k_{mk}(k_{ms}(sh_{id})) \quad (6)$$

μ is the pseudo-random number generator that randomly generates prime numbers, k_{mk} is the key supplied by the base station after handshaking procedure, k_{ms} is the randomly generated key for data transmission by the base station and sh_{id} is the sensor head id. The encrypted data is embedded within the cover image and is explained below.

Hiding the encrypted data into a cover image: In order to improve the security, this system exploits watermarking concept also. Any image can be chosen as the cover medium for the encrypted signal. This study applies Lifting Wavelet Transform (LWT) over the cover image and approximation band alone is considered. This is followed by the determination of the size of encrypted data and the space required to accommodate the encrypted data is figured out. All the encrypted data bits are embedded within the approximation band, based on an embedding sequence. The pixels of the approximation band are added with the data bits. This process is continued until all the data bits are embedded.

Data transfer from sensor head to base station: On successful registration of sensor head with the base station, the base station issues the master key. When a sensor head wants to transfer data, it raises the D_R and is sent along with the sh_{id} and timestamp to the base station. The D_R is verified by the base station and the randomly generated key for data transmission k_{ms} along with the k_{mk} is provided. Encryption is carried out by this way and the encrypted data is embedded into the cover image and sent to the base station as mentioned in Eq. (3) and (4).

Data transmission between the base station and the physician: Every physician in a healthcare centre is provided with the user name and password. The base station verifies the identity of the physician by certain security questions, which were initially answered by the physician. The physician can gain access to the data that has been sent only after successful decryption.

Every physician will be provided with a unique id, phy_{id}. If the physician needs to access the data, then the physician sends Acc_R to the base station. The base station then sends the decryption key which is encrypted by the phy_{id}. The physician has to decrypt the key, in order to gain access to the data. Initially, the encrypted data bits which are embedded in the cover image are needed to be extracted and is discussed in below section:

$$phy_i \rightarrow BS: \{phy_{id}|Acc_R|ts\} \quad (7)$$

$$BS \rightarrow phy_i: \{Dcn_{key}\}_{phy_{id}} \quad (8)$$

Data extraction: Embedded data can be extracted by the application of LWT and consider the approximation band alone. Every pixel pair is processed so as to extract the data bits. The pixels of the approximation band are subtracted from the data bits. Thus, the data bits are obtained from the cover image.

Decryption: After the successful extraction of the encrypted data, it is necessary to decrypt the data for gaining access to the data. The decryption key can be obtained from the base station, on request. When the base station receives Acc_R from the physician, it sends the decryption key that is encrypted by the phy_{id}. The physician decrypts the key and obtains the decryption key for gaining access to the QRS peaks.

RESULT ANALYSIS

This study is analyzed by performance metrics such as false acceptance and rejection rate, half total error, message passing ability and key generation time. The proposed work is compared with the existing works such as LDAE proposed by Daojing *et al.* (2013), SPOC proposed by Zhang and Lian (2009) and BSGE

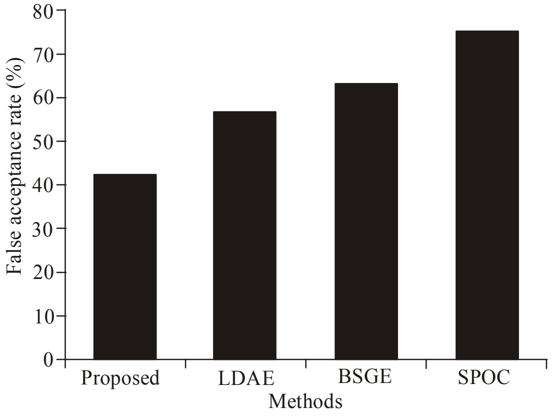

Fig. 3: False acceptance rate analysis

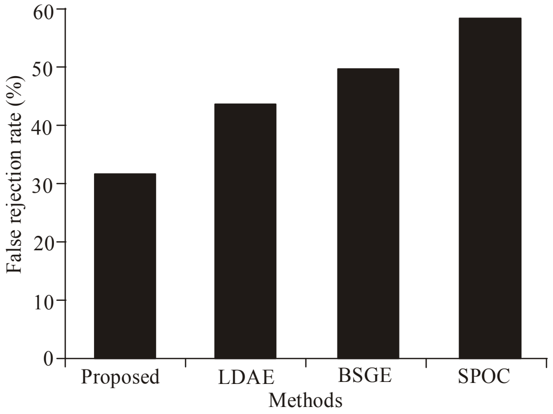

Fig. 4: False rejection rate analysis

proposed by Hu and Bao (2010). MATLAB is utilized to carry out this research work. This study is evaluated with MIT/BIH standard ECG database provided by Goldberger *et al.* (2013) and the least false acceptance and rejection rate is achieved.

False acceptance and rejection rate: All the sensors transmit the messages to the sensor head, which is the most powerful node. Suppose, many patients are in and around with implanted sensors, then the messages passed by the bio-sensor must reach the corresponding sensor head. In case, if a sensor from patient P1 reaches the sensor head of patient P2, the sensor head must reject the request. False acceptance rate is the rate at which the sensor head accepts messages wrongly from the attached bio-sensors. False rejection rate is the rate at which the sensor head rejects the message of the bio-sensors of the same patient Fig. 3 and 4.

Half total error rate: Half total error rate is calculated by subtracting Balanced Classification Rate (BCR) from 1. The experimental result is shown in Fig. 5:

$$Half\ total\ error\ rate = 1 - BCR \qquad (9)$$

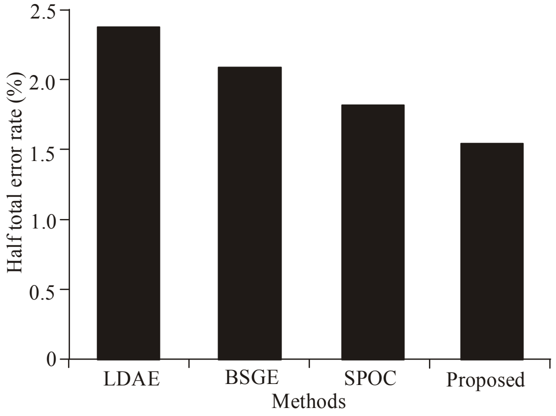

Fig. 5: Half total error rate analysis

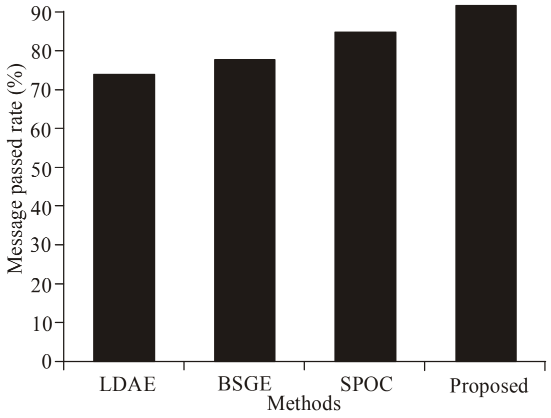

Fig. 6: Message passing ability analysis

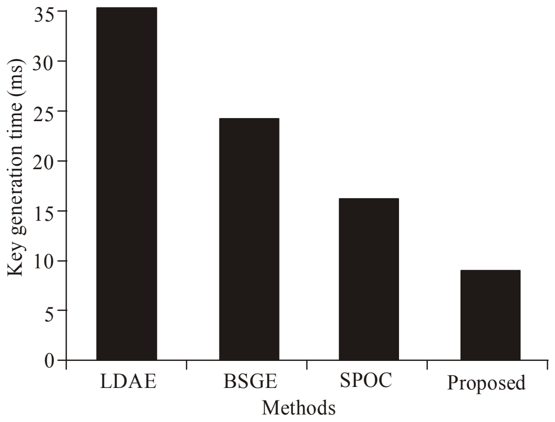

Fig. 7: Key generation time analysis

where,

$$BCR = \frac{1}{2}\left(\frac{TP}{TP+FN} + \frac{TN}{TN+FP}\right)$$

TP	= True positive
TN	= True negative
FP	= False positive
FN	= False negative

Message passing ability analysis: The message passing ability of different systems are compared and the proposed system outperforms all the other systems. The message passing ability is measured by total number of messages sent successfully, without any complexity and the results are shown in Fig. 6.

Key generation time analysis: The time it takes to generate the key can be given by the Fig. 7 and is compared with several existing systems. Our proposed work takes lesser time to generate the key.

On analyzing the experimental results, it is evident that the system works well for several performance measures. The proposed work is very fast in key generation. The false acceptance and rejection rates along with half total error rate are considerably low.

CONCLUSION

This study considers three different stages of data transmission. They are data transmission between biosensors and sensor head, data transmission between the sensor head and the base station and data transmission between the base station and the physician. In every stage, we enforce a security constraint and thereby the data is transmitted securely to the physician. Initially, the QRS signals are detected by the morphological operations such as erosion and dilation. A lightweight symmetric key based encryption along with watermarking is exploited to arrive at a reasonable security of the system. This study ensures privacy, access control, data confidentiality and integrity to the system.

REFERENCES

Chen, Y.L. and H.L. Duan, 2005. A QRS complex detection algorithm based on mathematical morphology and envelope. Proceeding of the 27th IEEE Annual International Conference of the Engineering in Medicine and Biology Society (EMBS, 2005). Shanghai, China, January 17-18, pp: 4654-4657.

Chu, C.H., N. Chu and E.J. Delp, 1989. Impulsive noise suppression and background normalization of electrocardiogram signals using morphological operators. IEEE T. Bio-Med. Eng., 36(2): 262-273.

Daojing, H., C. Chun, S. Chan, B. Jiajun and Z. Pingxin, 2013. Secure and lightweight network admission and transmission protocol for body sensor networks. IEEE J. Biomed. Health Inform., 17: 664-674.

Goldberger, A.L., L.A.N. Amaral, L. Glass, J.M. Hausdorff, P.Ch. Ivanov, R.G. Mark, J.E. Mietus, G.B. Moody, C.K. Peng and H.E. Stanley, 2013. Physiobank, PhysioToolkit, and PhysioNet: Components of a New Research Resource for Complex Physiologic Signals. Circulation, 101(23): e215-e220.

He, D., C. Chen, S. Chan, J. Bu and A. Vasilakos, 2012. ReTrust: Attack resistant and lightweight trust management for medical sensor networks. IEEE T. Inf. Technol. B., 16(4): 623-632.

Hu, C., N. Zhang, H. Li, X. Cheng and X. Liao, 2013. Body area network: A fuzzy attribute-based signcryption scheme. IEEE J. Sel. Area. Comm., 31: 37-46.

Hu, J.L. and S.D. Bao, 2010. An approach to QRS complex detection based on multiscale mathematical morphology. Proceeding of the 3rd International Conference on Biomedical Engineering and Informatics (BMEI). Yantai, pp: 725-729.

Keoh, S., E. Lupu and M. Sloman, 2009. Securing body sensor networks: Sensor association and key management. Proceeding of the IEEE International Conference on Pervasive Computing and Communications. Galveston, TX, March 9-13, pp: 1-6.

Kohler, B.U., C. Hennig and R. Orglmeister, 2002. The principles of software QRS detection. IEEE Eng. Med. Biol., 21(1): 42-57.

Law, Y., G. Moniava, Z. Gong, P. Hartel and M. Palaniswami, 2011. Kalwen: A new practical and interoperable key management scheme for body sensor networks. Secur. Commun. Net., 4(11): 1309-1329.

Lee, H. and K.M. Buckley, 1999. ECG data compression using cut and align beats approach and 2D transforms. IEEE T. Bio-Med. Eng., 46(5): 556-564.

Li, M., Y. Shucheng, L. Wenjing and R. Kui, 2010. Group device pairing based secure sensor association and key management for body area networks. Proceeding of the IEEE INFOCOM, 2010. March 14-19, San Diego, pp: 1-9.

Li, M., S. Yu, J. Guttman, W. Lou and K. Ren, 2013. Secure ad-hoc trust initialization and key management in wireless body area networks. ACM T. Sensor Network., 9(2), DOI: 10.1145/2422966. 2422975.

Lin, Y., L. Bing, W. Guowei, Y. Kai and W. Jia, 2011. A biometric key establishment protocol for body area networks. Int. J. Distrib. Sens. N., 2011: 1-10, Article ID 282986.

Malan, D.J., M. Welsh and M.D. Smith, 2004. A public-key infrastructure for key distribution in tinyOS based on elliptic curve cryptography. Proceeding of the IEEE SECON, pp: 71-80.

Malasri, K. and L. Wang, 2009. Design and implementation of a secure wireless mote-based medical sensor network. Sensors, 9(8): 6273-6297.

Miao, F., S.D. Bao and Y. Li, 2012. Physiological Signal Based Biometrics for Securing Body Sensor Network. In: Yang J. and S.J. Xie (Eds.), New Trends and Developments in Biometrics, InTech, pp: 251-274. DOI: 10.5772/51856.

Poon, C.C.Y., 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(4): 73-81.

Tan, C., H. Wang, S. Zhong and Q. Li, 2008. Body sensor network security: An identity-based cryptography approach. Proceeding of the 1st ACM Conference on Wireless Network Security, pp: 148-153.

Tan, C., H. Wang, S. Zhong and Q. Li, 2009. IBE-Lite: A lightweight identity based cryptography for body sensor networks. IEEE T. Inf. Technol. B., 13(6): 926-932.

Trahanias, P.E., 1993. An approach to QRS complex detection using mathematical morphology. IEEE T. Bio-Med. Eng., 40(2): 201-205.

Upmanyu, M., A.M. Namboodiri, K. Srinathan and C.V. Jawahar, 2010. Blind authentication: A secure crypto-biometric verification protocol. IEEE T. Inf. Foren. Sec., 5: 255-268.

Venkatasubramanian, K. and S. Gupta, 2006. Security for pervasive health monitoring sensor applications. Proceeding of the 4th International Conference on Intelligent Sensing and Information Processing, pp: 197-202.

Venkatasubramanian, K., A. Banerjee and S. Gupta, 2008. Plethysmogram based secure inter-sensor communication in body area networks. Proceeding of the Military Communications Conference. San Diego, CA, pp: 1-7.

Xu, F., Z. Qin, C. Tan, B. Wang and Q. Li, 2011. IMDGuard: Securing implantable medical devices with the external wearable guardian. Proceeding of the IEEE INFOCOM. Shanghai, pp: 1862-1870.

Zhang, C.F. and B. Tae-Wuk, 2012. VLSI friendly ECG QRS complex detector for body sensor networks. IEEE J. Emerg. Sel. Top. Circ. Syst., 2(1): 52-59.

Zhang, F. and Y. Lian, 2007. Novel QRS detection by CWT for ECG sensor. Proceeding of the IEEE International Conference on Biomedical Circuits and Systems Conference. Montreal, Que, November 27-30, pp: 211-214.

Zhang, F. and Y. Lian, 2009. Effective ECG QRS detection based on multiscale mathematical morphology filtering. IEEE T. Biomed. Circ. Syst., 3(4): 220-228.

Zhang, F., J. Tan and Y. Lian, 2007. An effective QRS detection algorithm for wearable ECG in body area network. Proceeding of the IEEE International Conference on Biomedical Circuits and Systems Conference. Montreal, Que, November 27-30, pp: 195-198.