Secure Communication over BSN Using Modified Feather Light Weight Block (MFLB) Cipher Encryption

A. Siva Sangari[1]*, J. Martin Leo Manickam[2]

[1]Department of Information Technology, Sathyabama University, Chennai, India.
[2]Department of ECE, St. Joseph College of Engineering, Chennai, India.

* Corresponding author. Email: siva.kumaresh08@gmail.com

Manuscript submitted December 5, 2014; accepted June 8, 2015.
doi: 10.17706/jsw.10.8.961-970

Abstract: Wireless Body Sensor Network (WBSN) has tremendous applications in healthcare domain. The body sensors collects personal as well as medical information form patient's body and transmit it to healthcare people through internet. In this period of time, it is crucial to ensure security and privacy due to unauthorized access of personal health information by intruder or eavesdroppers. Therefore, encryption is needed before transmitting the data into wireless network. In this paper, a novel lightweight block cipher called (MFLB- Modified Feather Light weight Block) based on Fiestel Cipher structure has been proposed for encryption and Attribute Based Key-Exchange (ABKE) for key management. Thus, the proposed approach achieves high efficiency and security in low energy sensor device and also gives solution to secure key exchange. The security analysis of this scheme proves its strength and efficiency against other techniques.

Key words: Wireless body sensor network (WBSN), block cipher, feistel structure, attribute based key-exchange (ABKE).

1. Introduction

Human health monitoring has significantly benefited from the current developments in sensor technology and wireless communication, which enabled the utilization of sensor to aid in recording biometric information remotely. The inactive lifestyles have increased the threat of possibly fatal medical circumstances like diabetes, cardiac disease, and high blood pressure and the lack of healthcare have contributed to increase in their risk. Provided the unpredictable nature of deterioration of such conditions, continuous and systematic monitoring considers high priority.

Wireless body area networks also known as Body Sensor Networks (BSN) are a special kind of wireless sensor networks, where a collection of sensors are positioned on the human body [1, 2], to measure certain physiological factors of a person and forward it to the monitoring hospital or medical centre. This transmission happens through internet or some kind cellular networks utilizing personal digital assistance or any other devices. Fig. 1 shows the typical body sensor network architecture. Thus, BSN seem to be a favourable solution to the issue of continuous health monitoring. Here, the patients' health information travels through an open wireless channel in order to arrive at the intermediary devices and finally at the monitoring station. This, combined with the fact that the therapeutic decisions are carried out based on the information received, a substantial focus on the research of BSN has gained significant consideration.

The security in BSN is of vital importance because of coupling the medical information with the resource constrained individual body sensors that require lightweight solutions. Security must be offered between the patients and the physicians via key management solutions.

Basically, security solutions provided for body sensor network must satisfy the following security features. The medical information must be accessible only by the specific patient and their doctors thereby ensuring confidentiality. To avoid medical information from getting in to the hands of unauthorized persons, the information must be authenticated. Thus, the information must be encrypted before transmitting and storing at the server. Encryption is one of the powerful for securing medical information. In this paper, lightweight block cipher based on Fiestel Cipher structure has been proposed for encrypting the medical information and key management is achieved using Attribute Based Key-Exchange (ABKE).

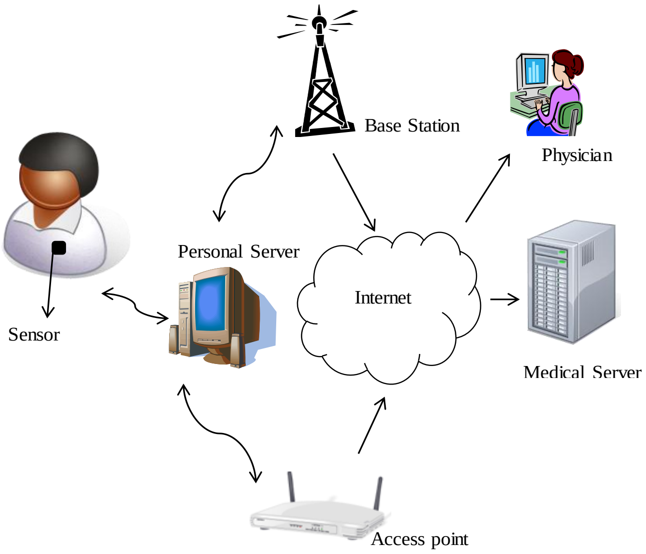


Fig. 1. Typical architecture of body sensor network.

The rest of the paper is organized as follows: Section 2 presents the previous research work carried out for securing information stored in BSN, Section 3 presents the system model and in Section 4 the proposed modified feather light weight block cipher for encrypting the information is presented, in Section 5 the proposed ABKE for key exchange and authentication is presented, Section 6 presents the results and Section 7 concludes the paper.

2. Related Works

Several research works has been carried out for securing the medical inf network [3]-[6]. In [7] cryptographic keys are generated from the electrocardiogram (ECG) signals and are used for encrypting the communication between pair of sensor nodes in BSN. In this work, the ECG values are obtained for a specific interval of the signal and the fast Fourier transform is employed to extract the coefficients. Then feature vectors are generated based on these coefficients that are used for generation of keys. The derived key is then used to encrypt the communication. The aim of this work is to secure the inter sensor communication. The key generated using this approach is different for various people since the ECG value is different for each people.

In [8] a two-tier authentication scheme is used for securing healthcare information's of the BSN. Here, security is achieved in two phases: In the first phase a unique key is generated in a decentralized manner and is used to encrypt the information. In the second phase, the key is utilized as a session key for authenticating data aggregation node from the sensor node. This approach provides security, authorization and confidentiality of the healthcare information.

A hybrid authenticated key agreement through rekeying has been proposed for body sensor networks [9]. The approach is based on symmetric cryptography and elliptic curve for the purpose of key agreement. [10] uses a Elliptic Curve Cryptography (ECC) for generating keys that is used to encrypt the communication between the sensor node and the base station. In this approach, RC5 block cipher is used for encryption and decryption process. This process ensures data integrity and confidentiality.

In [11] security in body sensor network is achieved by employing cryptographic techniques. Here, the ECG signals are utilized to generate keys. In this work, encryption is performed using Advanced Encryption Standard (AES). The Public Key Cryptography (PKC) with re-keying approach has been utilized for key establishment [12]. Here, RSA and DHECC parameters are utilized for key-agreement protocol that provides rekeying features. A particular routing algorithm has been used in the agreement phase for achieving resilience, scalability and memory efficiency. But the RSA and DHECC as well as PKC increases the computational cost of the BSN.

A novel chaos based encryption technique has been developed [13] for avoiding unauthorized access of ECG signal in inter- body sensor network communication. Here true random numbers are used for deriving the chaos key. This approach uses Diffie Hellman key exchange algorithm for exchanging the key between the node and the base station.

In [14] EKG is used as physiological measures to generate cryptographic keys for securing inter sensor communication. First the communicating sensor nodes sense EKG values and then hashing and watermarking approaches are applied to exchange values to generate public key for communication. [15] also utilizes biometric measures as symmetric keys as they as random. In this framework, key refreshment concept is utilized where the server provides key refreshment schedule to all the nodes of the BSN. This schedule exchanges the key allocated to it for communication. Here three keys namely, communication key, administrative key and basic key are utilized.

3. System Model

The proposed model considers a heterogeneous wireless body sensor network. The BSN (Body Sensor Network) is composed of sensor nodes, an individual coordinator node (ICN), a sink node, Base Station and a healthcare service and alert (HSA) system. The base station is responsible for obtaining physiological signs from the patients and these sensors are implanted on the body of the patients. The individual coordinator node (ICN) is responsible for collecting the data sensed by the sensor implanted on the patient's body. The ICN transmits the collected data to the sink nodes which is the forwarded to the healthcare service and alert system via the bases station. The healthcare service and alert system stores the information received from the base station. If a patient requires immediate attention, the doctors who have authorization can access the information from HSA.

Fig. 2 illustrates the proposed security model. The security architecture comprises of the following modules: encryption and decryption module and key exchange module. In the encryption module the health information obtained from the senor nodes are encrypted before transmitting the information over the wireless medium. The encryption is done using 128-bit key. The keys are generated using the ECG (Electro Cardiogram) signals. The key generation module provides secured key exchange for ensuring authentication. This is done by a trusted third party. The trusted third party is responsible for monitoring health care information and distributing keys to the authorized person. In the decryption module, the encrypted health information is decrypted using the 128-bit key by the authorized person.

4. Modified Feather Light Weight Block (MFLB) Cipher Encryption

The Modified Feather Light Weight Block (MFLB) Cipher encryption is used for encrypting the medical data. This algorithm is based on the feistel structure. The proposed scheme performs encryption based on the following steps: generating keys and performing encryption.

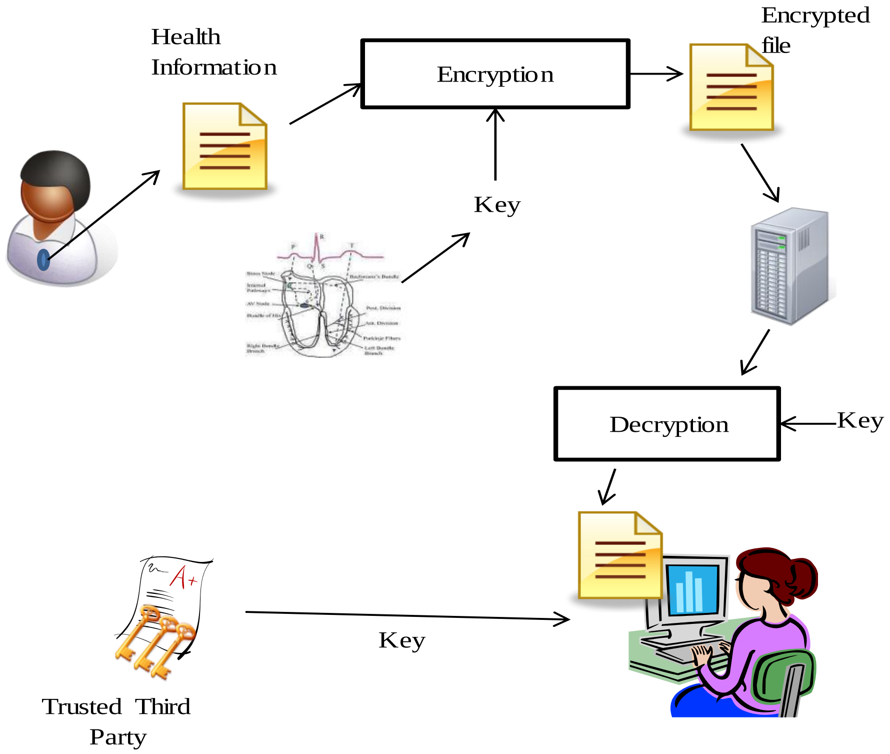


Fig. 2. Proposed security model.

4.1. Key Generation

Keys for symmetric cryptographic algorithms are generated by using standard key generating functions. Here, biometric features are used for generating keys, since cryptographic keys require high degree of uncertainty, the keys generated from the time varying signals provides high security. The ECG signal is utilized as a biometric feature to secure the BSN communication. Here, ECG signal IPI (Interpulsed Interval) is used as biometric feature. The Interpulsed Interval is the time interval between the RR signals of the ECG signal. The main process is to generate key from the ECG signal.

The generation of the key is as follows: The ECG signal of a particular node is measured and is sampled employing a frequency of 1000 Hz. The maximum amplitude of the signal is then estimated. The difference between the R peaks is estimated, which is called as IPI. The IPI is then converted into binary string to form 128 bit key.

4.2. Encryption/Decryption

The information that has to be transmitted over the BSN is encrypted for ensuring secured transmission. Here a light weight block cipher based on feistel structure is employed for encryption. The use of feistel structure provides the advantage of using the same algorithm for both encryption and decryption process. The proposed scheme encrypts a 64 bit block of data using 128-bit key. The 64 bit plain text Mi is divided into two blocks of 32-bit each, ML and M/R and produces a 64 bit cipher text. The encryption process uses a 64 round feistel structure. Fig. 3 shows a typical feistel structure. The input to the first round is the plain text Mi (ML || MR) . The input to the *i*+1 round is computed as follows

$$L_{i+1} = R_i \qquad\qquad R_{i+1} = L_i \oplus F(k_i, L_i) \tag{1}$$

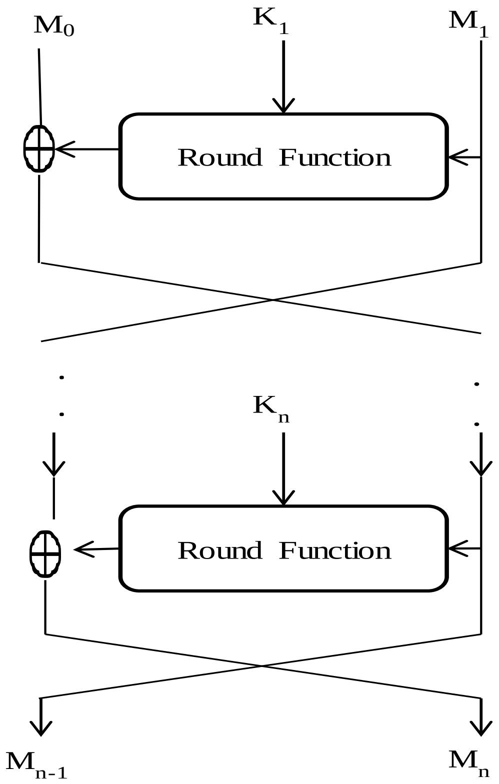


Fig. 3. Feistel structure.

The cipher text C_i is obtained by concatenating the two strings obtained in the last round. The process of round is described below.

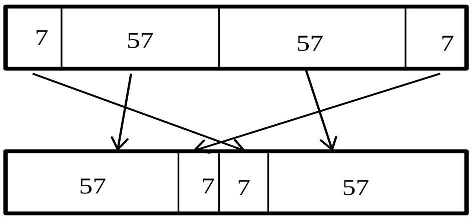


Fig. 4. Round function generation.

4.2.1. Round function (F)

The round function takes 32 bit input M_i and generates a 32 bit output Y_i. In this process two weight functions W_1 and W_2 are used. The round function is applied on the 32 bit input M_i as follows: The input M_i is Ex-OR with the random key K_i. This function produces two 16 bit outputs Xi and Yi. These two outputs are then processed through the wright functions W_1 and W_2 to produce the 32 bit output Y. The process of generating random keys is described below.

4.2.2. Key scheduling

The key schedule produces a round key Rk (32 × 64) from the secret key, kn where n is 128. It uses a double swap function for generating the 128 bit key. Fig. 4 illustrates the process of round function generation. The double swap function is described as follows:

$$Y_{128} \leftarrow X_{128} \tag{2}$$

$$Y = X[64 - 120]||X[0 - 6]||X[121 - 127]||X[7 - 63] \quad (3)$$

4.2.3. Weight function (W1)

In this function the 16 bit input is divided into four blocks consisting of 4 bits each and an S- box is applied in parallel to produce a 16 bit output. The working of the weight function is described below.

$$Y_1 = W_1(X = X_1 + X_2 + X_3 + X_4) \quad (4)$$

First, S-box is applied on X to produces S_1, and then circular shift is applied on S_1 to produce S_2. Then S_1 is Ex-OR with S_2 to produce Y_1.

$$S_1 = \{S\ (X_1)||S\ (X_2)||S\ (X_3)||S\ (X_4)\} \quad (5)$$

$$Y_1 = S_1 \oplus S_2 \quad (6)$$

4.2.4. Weight function (W2)

In this function the 16 bit input is divided into four blocks consisting of 4 bits each and an S- box is applied in parallel to produce a 16 bit output. The working of the weight function is described below.

$$Y_5 = W_1(Y = Y_1 + Y_2 + Y_3 + Y_4) \quad (7)$$

First, S-box is applied on X to produces S_1, and then circular shift is applied on S$_1$ to produce S$_2$. Then S_1 is Ex-OR with S_2 to produce Y_1.

$$S_1 = \{S\ (Y_1)||S\ (Y_2)||S\ (Y)||S\ (Y_4)\} \quad (8)$$

$$Y_5 = S_3 \oplus S_4 \quad (9)$$

Finally, the output of the round function F is given as $F = Y_1||Y_5$.

Table 1. S Box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	2	E	F	5	C	1	9	A	B	4	6	8	0	7	3	D

The decryption is same as the encryption process; the difference is that round keys are employed in reverse order. The decryption is achieved by computing

$$L_i = R_{i+1} \oplus F(k_i, L_{i+1}) \qquad R_i = L_{i+1} \quad (10)$$

5. Attribute Based Key-Exchange (ABKE)

The key exchange protocols are the approach by which two users that communicate over a network generates a shared secret key. These protocols are necessary for allowing users to utilize shared key cryptography for protecting data transmitted over the insecure network. Thus, they are the vital part for providing a secured communication and are the most widely utilized cryptographic protocols. In this security frame work, an Attribute Based Key Exchange (ABKE) is employed.

The ABKE (Attribute Based Key Exchange) comprises the following algorithms: Setup, Key Gen and Key Exchange. Each user in this protocol executes the key exchange algorithm takes as input the master public key MPK, attributes private key PK and an access structure A. If the attribute satisfies the access structure A, it produces the session key SK as output.

Access Structure: Let S be access structure in the form tree. The interior nodes of S indicate a threshold gate and the leaf node represents the attributes. The number of children of node i is represented as n_i and its threshold level is represented as τ_i ($0 \leq \tau_i \leq n_i$). The threshold gate associated with an interior node having the value τ_i, output the value true (i.e., 1) only if at least τ_i of its children is true. If the threshold gate is an and gate then $\tau_i = n_i$ or if it is OR gate the output is $\tau_i = 1$. The parent of the node i is represented as paren(i) while the attribute is represented as att(i).

Satisfying an Access Structure: Let r be the root of the access structure S and the sub tree of the node *i* is represented as S_i. Let $S_i(\alpha) = 1$, represents the set of attributes α that satisfies the access structure. The function $S_i(\alpha)$ is calculated as follows: if i is the interior node, for every chidren of i , $S_i(\alpha)$ is calculated. $S_i(\alpha)$ returns true if only τ_i children of i returns true. If i is the leaf node, $S_i(\alpha)$ returns 1 if att(i) $\in \alpha$.

Setup: In this phase, the security parameter's' and the universe attribute description are taken as input and produces master key mk and the public key *pk* as output.

Key Gen: Here, the master key mk, the public key *pk* and a set of user attributes s are given as input and produces private key as output.

Key Exchange: This takes public key *pk*, private key for an attribute set's' and an access structure A as input. If the attribute set's' satisfies A, the key exchange generates outgoing messages and accepts incoming messages from the user. The output of the key exchange is the session key.

Communication Structure: Let c = $\{c_1, c_2, \ldots c_m\}$ be the set of m users. Each user is assumed to have a set of attributes. Let PK_i be the private key of the attribute S_i of the user c_i. The users are provided with the access structure. If a user needs to establish a session key, the attribute set S_i is first checked against the access structure A. If S_i satisfies A ($(S_i) \in A$) the executes the protocol. Thus, the user whose attribute set satisfies the access structure computes the session key.

6. Results and Discussion

Simulations are performed to evaluate the performance of the proposed encryption algorithm. The simulations are carried out using NS2 considering an area of 50 X 50 m. It uses an exponential traffic mode for transmission and TCP is utilized as a transport protocol between the sender and the sink node. Table 2 summarizes the simulation parameters used.

Table 2. Simulation Parameters

Simulator	NS2
Area	50 × 50 meters
No of nodes	500
Traffic Mode	Exponential
Simulation Time	40 secs
Transport Protocol	TCP

6.1. Discussion

6.1.1. MFLB

The performance of the proposed encryption scheme (MFLB) is measured and analysed in terms of execution time. Execution time is defined as the time taken by the algorithm to encrypt and decrypt a particular data length. Fig. 5 shows the execution time of the proposed algorithm for encryption, decryption and key generation for various file size. The results show that the execution time varies for various file sizes.

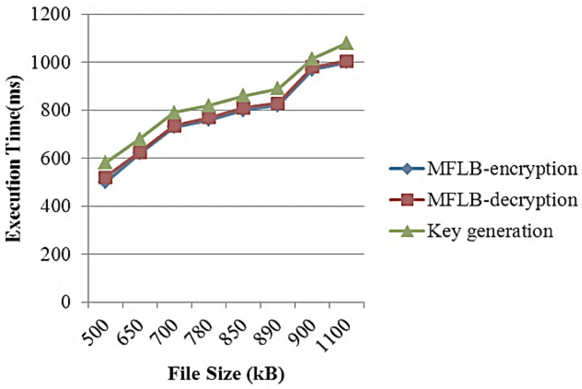
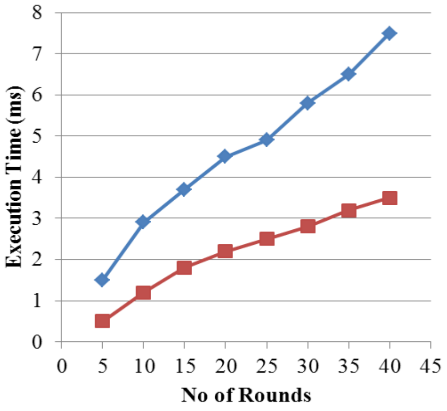


Fig. 5. Execution time.



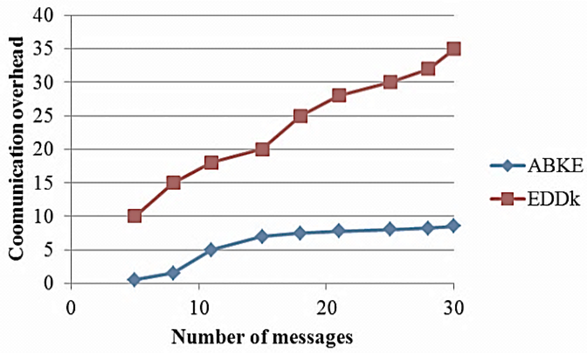


Fig. 6 Execution time of key exchange protocols. Fig. 7. Key exchange communication overhead.

6.1.2. ABKE

The performance of the proposed ABKE is measured and analysed in terms of execution time and overhead. Fig. 6 shows the execution time for Energy-Efficient Distributed Deterministic Key Management (EDDK) and the proposed attribute based key exchange (ABKE). The results indicate the execution time of EDDK increases with increase in the number of rounds when compared to the ABKE. Therefore for application involving frequent key exchange, the use of ABKE would be a preferable choice.

Fig. 7 shows the communication overhead involved in key exchange. The results show that the communication overhead for existing EDDK is more when compared to the proposed approach.

7. Conclusion

In this paper, secured communication in body sensor network is provided by using a novel light weight based block cipher based encryption called modified feather light weight block (MFLB). The encryption process is based on feistel structure. The ECG signals are used to generate keys. Moreover, an attribute based key exchange (ABKE) approach has been utilized for providing authentication. Thus, the proposed algorithm provides simple and secured encryption and provides authentication to each user for the purpose of decryption in BSN. The results show that the proposed MFLB provides high level of security to the information stored in BSN.

References

[1] Chiu, C. T., Wang, H. D., Sheng, Z., & Li, Q. (2008). Body sensor network security: An identity-based cryptography approach. *Proceedings of the ACM Conference on Wireless Network Security*.

[2] Hao, Y., & Foster, R. (2008). Wireless body sensor networks for health-monitoring applications. *Physiological Measurement*.

[3] Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2008). Body sensor network security: An identity-based cryptography approach. *Proceedings of the First ACM Conference on Wireless Network Security*.

[4] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. *Advances in Cryptology Eurocrypt*.

[5] Sahanaa, I. S. M. (2011). Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis. *Proceedings of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology*.

[6] Lee, P. Y. D, & H. J. Lee. (2010). Secure health monitoring using medical wireless sensor networks. *Proceedings of the 6th International Conference on Networked Computing and Advanced Information Management*.

[7] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. S. (2008). EKG-based key agreement in body sensor networks. *Proceedings of the IEEE INFOCOM Workshops*.

[8] Kanjee, M. R., Divi, K., & Liu, H. (2010). A two-tiered authentication and encryption scheme in secure healthcare sensor networks. *Proceedings of the International Conference on Information Assurance and Security*.

[9] Amin, N., Asad, M. N., & Chaudhry, S. A. (2012). An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. *Proceedings of the IEEE International Conference on Networking, Sensing and Control*.

[10] Malasri, K., & Wang, L. (2009). Design and implementation of a secure wireless mote-based medical sensor network. *Sensors*.

[11] Liu, J. W., Zhang, Z. H., Rong, S., & Kwak, K. S. (2012). Certificateless remote anonymous authentication schemes for wireless body area networks. *Proceedings of the IEEE International Conference on Communications (ICC)*.

[12] Eldefrawy, M. H, Khan, M. K., & Alghathbar, K. (2010). A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. *Proceedings of the IEEE International Conference on Anti-Counterfeiting Security and Identification in Communication*.

[13] Sufi, F., Han, F., Khalil, I., & Hu, J. (2010). A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. *Security and Communication Networks*.

[14] Aftab, A., & Farrukh, A. K. (2010). An improved EKG-based key agreement scheme for body area networks. *Proceedings of the International Conference on Information Security and Assurance*.

[15] Raazi, S. M. K., & Lee, H. (2009). BARI: A distributed key management approach for wireless body area networks. *Proceedings of the International Conference on Computational Intelligence and Security*.

A. Siva Sangari is working as an assistant professor in the Department Information Technology at Sathyabama University, Chennai. She received her B.E. degree in computer science and engineering from Kalasalingam College of Engineering, Srivilliputtur in 2003. She received her M.E. degree in computer science from Govt College of Engineering, Tirunelveli in 2007. She has over 8 years of experience in teaching and guiding projects for Undergraduate and post graduate students. She has to her credit 11 publications in national/international conferences and journals. Her areas of interests include wireless sensor networks, mobile computing and network security.

J. Martin Leo Manickam is working as a professor in the Department Electronics and Communication Engineering at St. Joseph's College of Engineering, Chennai. He received his B.E. degree in electronics and communication engineering from Alagappa Chettiar College of Engineering and Technology, Karaikkudi in 1995. He received his M.E. degree in optical communication and the Ph.D degree in information and communication engineering from the College of Engineering, Anna University, Chennai. He has over 17 years of experience in teaching and guiding projects for undergraduate and post graduate students. He has to his credit 20 publications in national/international conferences and journals. His areas of interests include mobile ad hoc networks, wireless sensor networks, digital communication and network security.