Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 842608, 11 pages
http://dx.doi.org/10.1155/2013/842608

Research Article

A Hybrid Security Mechanism for Intra-WBAN and Inter-WBAN Communications

Sarah Irum,[1] Aftab Ali,[1] Farrukh Aslam Khan,[1,2] and Haider Abbas[2,3]

[1] *National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan*
[2] *King Saud University, Riyadh 11653, Saudi Arabia*
[3] *National University of Sciences & Technology, Islamabad 44000, Pakistan*

Correspondence should be addressed to Farrukh Aslam Khan; fakhan@ksu.edu.sa

Received 27 January 2013; Revised 25 May 2013; Accepted 10 June 2013

Academic Editor: Muhammad Khurram Khan

The emerging wireless body area networks (WBANs) have a great potential for the growth and development of future ubiquitous healthcare systems. However, due to the use of unreliable wireless media, WBANs are exposed to a variety of attacks. The prevention of these attacks depends upon the cryptographic techniques. The strength of cryptography is based on the keys used for encryption and decryption in the communication process. Security is still an alarming challenge for WBANs and needs attention of the research community. The proposed work introduces a hybrid key management scheme for both intra-WBAN and inter-WBAN communications. The proposed technique is based on preloaded keys as well as keys automatically generated from biometrics of the human body. The biometric-based calculations are of linear time complexity to cater the strict resource constraints and security requirements of WBANs. The proposed security mechanism provides an efficient solution for the security of both intra-WBAN and inter-WBAN communications. The results of the proposed technique are compared with an existing key management technique known as BARI+. The results show significant improvement over the results produced by BARI+ in terms of storage, communication, energy overhead, and security.

1. Introduction

Wireless body area network (WBAN) is a special type of network in which sensors are deployed on the human body. The sensors collect physiological values from the body and transmit the collected records to the concerned medical server. The applications of WBANs include health monitoring of patients in a hospital and monitoring of soldiers in a battlefield. The WBAN monitoring system is used to monitor a person's vital signs remotely. The system also receives feedback for maintaining a good health status of the subject so that proper action can be taken to rectify the abnormalities [1, 2]. The introduction of WBANs to E-Health monitoring system has revolutionized the field of health monitoring and resulted in better quality of life [3]. Since we deal with the personal information of a person, the security and privacy becomes an essential part of this communication. In case of medical applications, the security threats may lead a patient to a dangerous condition, and sometimes to the death of the patient [4]. WBAN communication can be classified into intra-WBAN communication and inter-WBAN communication. Intra-WBAN communication refers to the on-body sensors communication while inter-WBAN communication refers to the communication between two different WBANs. WBAN communication faces security issues as biomedical sensors implanted on the human body for mobile healthcare monitoring communicate with external networks, which increases the security risk. Since biomedical sensor nodes are allowed to monitor and transmit potentially sensitive medical data, the security and privacy becomes a major concern in WBANs. WBANs consist of lightweight sensors, which are limited both in terms of computational and communication resources; therefore, the security models and protocols used for wireless sensor networks (WSNs) cannot be applied to WBANs in exactly the same manner for different resource-constrained applications and scenarios [5, 6].

The existing key management techniques for WBANs are either plug-and-play or based on preloading. The work proposed in this paper consists of a hybrid technique; that is, it supports both plug-and-play capability as well as some

predeployment of keys in order to strengthen the security in WBANs. In intra-WBAN communication of the proposed technique, the sensors measure physiological values (PVs) of the human body, and then by using those PVs, the keys are calculated among the sensor nodes. All this process is carried out in an automatic manner; that is, the sensors are put on the human body and the keys are calculated automatically for secure communication. In intra-WBAN communication, our technique has linear time complexity that is $O(n)$ for feature generation from electrocardiogram (EKG) signals. The proposed inter-WBAN communication is purely based on preloading of keys. We use minimum number of keys for preloading in the sensor's memory due to its small storage capability. So our hybrid technique is efficient in terms of memory utilization and also in terms of security because the combination of auto key generation and preloading of keys strengthens the security of the technique. Inter-WBAN communication includes the communication between personal servers (PSs). The communication among different PSs is needed when a PS is out of range of a medical server (MS). A PS communicates with another PS and transmits its data to the MS through the nearby PS. Our scheme supports the use of biometric measurements. Keys are generated with the help of biometrics of any PS. The PS generates key pool using its biometric values and then transmits to the whole network. Our scheme also makes use of key refreshment mechanism schedule. MS assigns any PS (key generator) the responsibility of refreshing the key. A list of the notations used in this paper is found in the abbreviations section.

The major contributions of the proposed work are summarized as follows. (1) For intra-WBAN communication, we propose a hybrid scheme by keeping in view the security requirements, storage, and power constraints of a WBAN. (2) For inter-WBAN communication, we propose a lightweight key management scheme based on preloading of keys. (3) The proposed scheme for inter-WBAN communication also uses PVs for the generation of keys in key refreshment phase. (4) The security analysis is done by keeping in view the attacks on both intra-WBAN and inter-WBAN communications. (5) The storage and communication overhead, as well as energy efficiency, are analyzed by comparing the proposed technique with a well-known key management technique known as BARI+ [7].

The rest of the paper is organized as follows. In Section 2, the related work is presented. Section 3 discusses the system model whereas Section 4 describes the proposed technique for intra-WBAN communication. Section 5 describes the proposed technique for inter-WBAN communication. The performance of our proposed technique is analyzed in Section 6, whereas Section 7 concludes the paper.

2. Related Work

The first work that addresses the issue of security for implantable and wearable medical sensors was presented in [8]. These devices are used for nursing human body over long periods of time [9]. Ensuring the security of communication among these devices is critically important [10, 11]. Some works describe the use of human body as a means of generating cryptographic keys for securing intersensor communication. Human body can produce many specific physiological values that are time-variant and are not easy to guess [12]. Using this property of human body for cryptographic purposes provides strong security and gives us great opportunity for automatic key distribution and plug-and-play capability. Both the sender and the receiver can now measure the physiological values from their environment and use them for security purposes whenever they want to communicate [8]. The services like confidentiality and integrity are also ensured in some previous works as discussed in the TLS (transport layer security) protocol [13]. TLS provides privacy and data integrity between two communicating applications. SHELL [14] is a scalable, hierarchical, efficient, and location-aware key management scheme for WSNs. SHELL also provides integrity and confidentiality services in WSNs. SHELL is based on exclusion basis systems (EBSs), which is a combinatorial formulation of the problem of group key management. The main drawback of these protocols for using in WBANs is that these protocols do not fulfill the storage and power limitations of WBANs. Hence, these protocols are not suitable to be used in WBANs. There are some symmetric key management schemes available in the literature for secure trust establishment such as predeployment of keys in nodes, intersensor-communication based key agreement, and public-key-based key agreement schemes. Each of these schemes has its own limitations like memory problem, authentication from a centralized authority, complex mathematics, and so forth, which make these schemes difficult to use in WBANs [8].

Since recently, researchers have been focusing on applications of WBANs and have designed key management techniques for WBANs by using physiological values of the human body such as EKG. The use of EKG signal for generating pairwise keys brings plug-and-play capability in WBANs. Both communicating sensors first sense the EKG values and then, by applying certain hashing and watermarking technique, exchange these values for generating common keys for communication [15, 16]. In [17, 18], the idea of cluster-based secure key agreement protocol for WBANs is presented. The authors use physiological value-based keys for secure cluster topology formation. In [19, 20], the interpulse interval derived from ECG/PPG signals is used to generate common cryptographic keys. In [21], the authors proposed the use of fuzzy vault for physiological signal-based key agreement (PSKA) to secure intersensor communication. In [11], the authors proposed a lightweight security scheme for WBAN communication. The authors also proposed a microcontroller design to reduce energy consumption in WBAN communication. Restrained energy model is considered in this approach where star topology is used for WBAN communication using time division multiple access medium access control (TDMA MAC). The energy overhead is evaluated for the security mechanism introduced in the WBAN. The authors in [22] proposed a security mechanism for WBANs. They reviewed IBE-Lite [23] technique and addressed its limitations such as exposure of master key, partial heath records decryption problem

after rekeying, and lack of adequate privacy provisioning. To overcome these limitations, the authors proposed a scheme that introduced anonymity and unlinkability and offered authorized access of patients' health information. However, they use third party for key generation that itself introduces overhead to the WBAN communication. In [24], the authors proposed a security suite for WBANs. To improve the security of a WBAN, the authors presented techniques such as independent and adaptive management of keys (IAMKeys) for security in WBANs and key management and encryption for securing intersensor communication (KEMESIS). In the proposed schemes, the keys are generated randomly and the security is ensured by eliminating the key exchange between sensor nodes.

In BARI+ [7], the authors proposed a key management scheme purely based on preloading of keys. They use the concept of preloading in intra-WBAN communication. However, in intra-WBAN communication, the advantages of preloading are not so useful due to the fact that preloading-based schemes have no variations and same keys are used for communication between different sensor nodes, whereas in PV-based solution every node that wants to communicate with another node will calculate its own keys. Similarly, in preloading-based schemes, if a key is captured during a communication process, the next key calculations and communications are totally based on that captured key. So, the newly calculated key will also be compromised. While in PV-based key generation, the next set of values cannot be guessed. Preloading of keys for WSNs has also been used in several other papers such as [25–27]. All the PV-based techniques discussed so far are developed purely for intra-WBAN communication without considering inter-WBAN communication. Also, there is a need for a hybrid kind of key agreement scheme that combines the advantages of both PV and preloading-based key agreement. The work presented in this paper uses a hybrid approach for key agreement in WBANs, which tackles the problems of both intra-WBAN and inter-WBAN communications. We present a technique that uses preloading of keys and also generates biometric keys automatically. Keeping in view the strict resource constraints and security requirements of WBANs, minimal preloading of keys is used in the proposed approach.

3. System Model

We assume a WBAN to consist of sensor devices that are capable of measuring biometrics related to human body and also a high power and high storage device known as personal server (PS), which can be a laptop or a hand-held device. Medical server (MS) receives all the information collected by PS through the sensor nodes. All sensor nodes are directly connected to their relevant PSs. Sensor nodes measure biometrics and forward them to the PS. PS in turn transmits collected information to the MS through the internet. Each WBAN is associated with one body. Multiple WBANs are associated with the central MS. PS can communicate with other PSs as well as the MS. The MS stores and processes the information of all the WBANs that are associated with it.

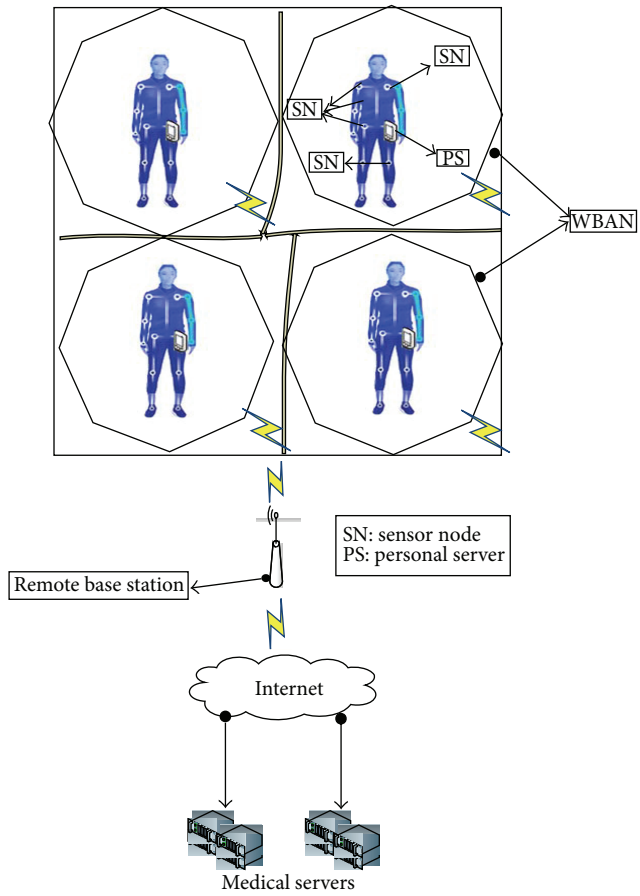

Figure 1: System architecture of wireless body area networks.

All sensor nodes are constrained in energy because they use rechargeable batteries. Sensor nodes are ordinary devices with limited computation, communication, energy supply, and storage capabilities. PS is a powerful node and has more computation, communication, energy supply, and storage capabilities. We assume that the PS is preloaded with node identities and relevant keys before deployment. Keeping in view the storage constraints, in intra-WBAN communication, only one key is preloaded in sensor nodes before deployment. The system architecture of the WBAN, as per our assumptions, is shown in Figure 1. The application scenario of inter-WBAN communication includes multiple bodies under surveillance and all bodies communicate to a remote base station, like in the battlefield, the soldiers are deployed in the enemy territory and they communicate to the remote base station in their own territory. As in Figure 1, the PSs of all the bodies communicate to the base station and then through Internet to the remote MS.

4. Proposed Scheme for Intra-WBAN Communication

Intra-WBAN communication includes the communication of sensor nodes with the PS. We propose a hybrid approach for key management in intra-WBAN communication. Due to the memory limitations, only a single key named as secret

key $K_{SN,MS}$ is preloaded in the sensor nodes and is used in case of PS compromise. Other keys are generated by sensors themselves using their biometrics. The process is done in two steps: feature generation and key agreement.

4.1. Feature Generation. In the feature generation phase, features are extracted and then quantized for secure intersensor communication with the help of EKG using discrete wavelet transform (DWT). DWT allows good localization both in time and spatial frequency domains and is computationally inexpensive. In the process of communication between SNs and PS, sensors sample the EKG signal at the sampling rate of 125 Hz in time duration of 5 seconds. To remove unnecessary frequency components, the signal is then filtered. 625 samples are produced by five-second sample of EKG and then divided into 5 parts of 125 samples each. DWT is applied on each part after applying filtration. The 320 coefficients feature vector is formed by concatenating the 64 coefficients horizontally. In the quantization phase, the generated feature vector is divided into 20 blocks, each containing 16 coefficients, and then they are quantized into a binary stream.

4.2. Key Agreement. After the process of quantization, creation of feature vectors, and formation of blocks, the key agreement process is done. In the key agreement phase, PS broadcasts data request message as shown in message m_1 of Figure 2, consisting of ID_{PS}, DataReq, and nonce. All sensor nodes which have the required data first compute the shared pairwise key with the PS by applying keyed hash function on feature blocks, ID_{PS} and ID_{SN} as follows:

$$\begin{aligned} K_{PS,SN} &= \mathrm{HMAC}\left((b_{11}, N) \cdots (b_{211}, N), \mathrm{ID}_{PS} \parallel \mathrm{ID}_{SN}\right) \\ m_1 &: \mathrm{PS} \longrightarrow * : \mathrm{ID}_{PS}, \mathrm{DataReq}, \mathrm{nonce} \\ m_2 &: \mathrm{SN} \longrightarrow \mathrm{PS} : \mathrm{ID}_{SN}, \mathrm{EK}_{PS,SN}\left(\mathrm{ID}_{SN}, \mathrm{Data}\right), \\ &\quad \mathrm{MAC}_{K_{PS,SN}}\left(\mathrm{ID}_{SN}, \mathrm{nonce}, \mathrm{Data}\right). \end{aligned} \tag{1}$$

SN encrypts the data with key $K_{PS,SN}$ and also computes MAC on ID_{SN}, nonce, and data using the same key $K_{PS,SN}$. SN sends its ID, encrypted data, and MAC to the PS as shown in message m_2. When PS receives this message, first it calculates the $K_{PS,SN}$ by applying the keyed hash function on the feature blocks, ID_{PS} and ID_{SN}. As feature blocks are the same on both sides, $K_{PS,SN}$ generated by PS will be same as that of SN. Incorporation of ID_{SN} in key generation process ensures the establishment of unique pairwise key of PS with all communicating SNs. PS decrypts the message with $K_{PS,SN}$ and compares ID_{SN} and received feature blocks (data) with decrypted message ID_{SN} and feature block on PS to ensure that both parties have generated the same key. The message authenticity is checked by PS through MAC verification with $K_{PS,SN}$.

In Figure 2, the key agreement phase is shown. EKG signal is used for feature generation. Feature vector of 320 coefficients is generated by concatenating 64 coefficients horizontally. These generated features are then divided into 20 blocks of 16 coefficients and then quantized into the binary stream. PS sends data request with its ID to SNs. SNs generate the shared pairwise key with PS by applying keyed hashing on the feature blocks and IDs of both PS and SN. The resulting key is used to encrypt data requested by the PS [9]. Data is verified through MAC verification of the PS. Hamming distance is calculated to verify that the data blocks of both the sender and the receiver are the same.

4.3. Rekeying. In intra-WBAN communication, there is a need to have a common key in order to securely communicate messages to PS. Key is computed after network initialization and generation of the shared pairwise keys between PS and SNs. PS broadcasts a signaling message of GenKey to direct the SNs to generate a common key as follows:

$$m_1 : \mathrm{PS} \longrightarrow * : \mathrm{GenKey}\left(\mathrm{ID}_{PS}\right). \tag{2}$$

Each SN when receives this message generates the key (K) by applying keyed hash function on feature blocks and ID_{PS} as follows:

$$K = \mathrm{HMAC}\left((b_{11}, N) \cdots (b_{211}, N), \mathrm{ID}_{PS}\right). \tag{3}$$

WBAN key K is refreshed after fixed intervals. When PS wants to refresh K, it sends GenKey message and SNs upon receiving this message and regenerates K by applying keyed-hash function on the current feature blocks and ID_{PS}.

5. Proposed Scheme for Inter-WBAN Communication

Inter-WBAN communication includes the communication of a PS with other PSs. Each body in the WBAN contains one PS. The communication of different PSs is needed when a PS is out of range of the MS. PS communicates with other PSs and transmits data to the MS through the nearby PS. Our proposed scheme supports the use of biometric measurements. Keys are generated with the help of biometrics of any PS. The PS generates key pool using its biometrics and then transmits to the whole network. Our scheme for inter-WBAN communication also makes use of key refreshment mechanism schedule. MS assigns any PS (key generator) the responsibility of refreshing the key. Figure 3 shows the manner in which our scheme manages the keys of a WBAN.

Our scheme consists of four types of keys: administrative key (K_{admin}), network key (K_{net}), basic keys of all personal servers, and $K_{MS,PS}$ key shared between MS and PS. Administrative key and basic keys are preloaded in all PSs. Network key K_{net} is a network wide key and is used to transfer data through the network in a secure manner. In our scheme, K_{net} is managed by the MS. Since K_{net} is used very frequently, it may come under cryptanalytic attacks and must be refreshed regularly. Administrative key K_{admin} is used to refresh K_{net}. K_{admin} is also a group key but it is not used as frequently as K_{net}. Naturally, K_{admin} is less exposed as compared to K_{net}. Also, K_{admin} needs to be refreshed through some other key at some point in time. Therefore, we employ basic keys K_{PSbsc} in our key management framework. Every PS has its own K_{PSbsc}, which it shares only with the MS. $K_{MS,PS}$ is used by PS to send data to the MS and it is only shared between PS and MS.

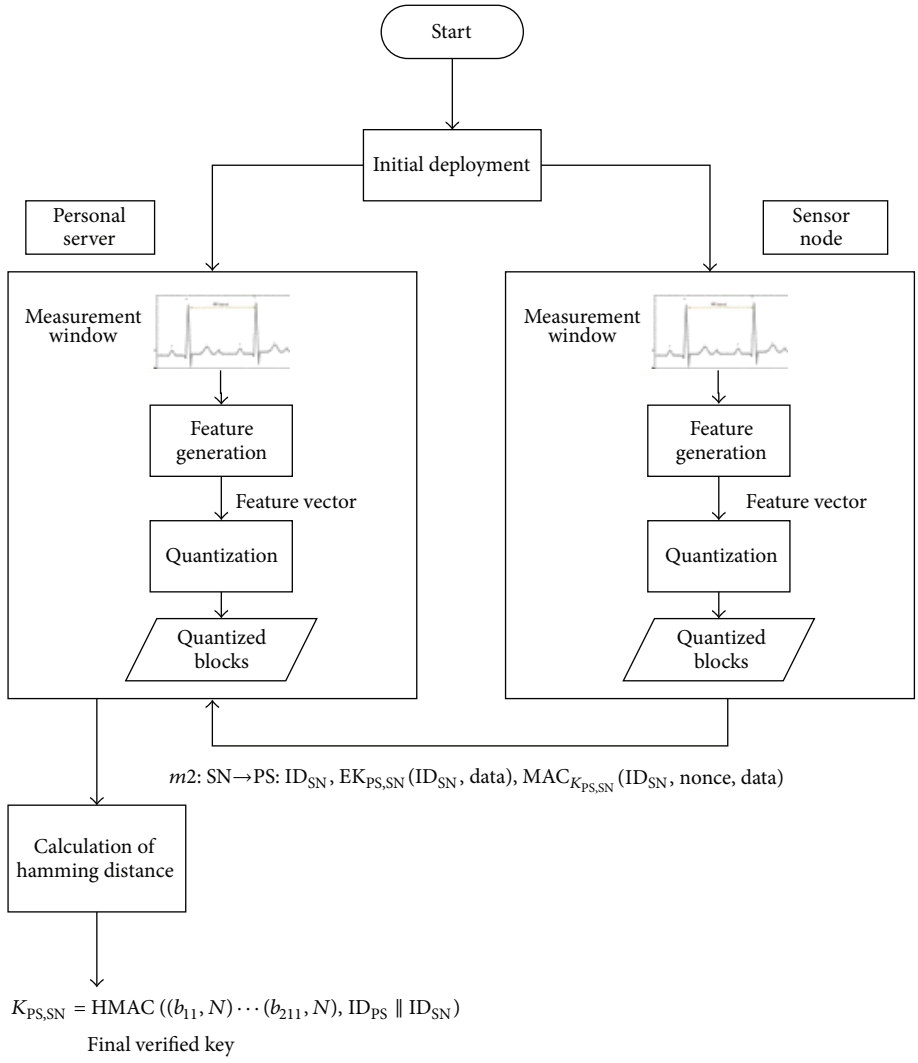

Figure 2: Flowchart of the proposed scheme for intra-WBAN communication.

5.1. Initial Deployment. All PSs are deployed in the beginning. Throughout the network lifetime, PS is connected with the medical server through an external secure communication channel, which may be the Internet. Personal servers come preloaded with K_{admin} and their relevant basic keys and authentication codes. These codes are used to authenticate PSs. After the PS is deployed, sensor devices are deployed on various parts of the body. Soon after deployment, each PS sends discovery message to the MS as follows:

$$m_1 : \forall \text{PS}^i \in \{\text{PS}\} : \text{PS}^i \longrightarrow \text{MS} : \text{EK}^i_{\text{PSbsc}} \left\{\text{ID}^i \mid \text{Auth\_code}^i\right\}. \tag{4}$$

MS authenticates PS and sends the key $K_{\text{MS,PS}}$ and IDs of sensor nodes that are to be deployed in PS:

$$m_2 : \forall \text{PS}^i \in \{\text{PS}\} : \text{MS} \longrightarrow \text{PS}^i : \text{EK}^i_{\text{PSbsc}} \left\{K^i_{\text{MS,PS}} \mid \forall \text{SN}^j \in \{\text{SN}\} : \left\{\text{ID}\left(\text{SN}^i\right)\right\}\right\}. \tag{5}$$

MS assigns any PS the responsibility to generate K_{net} and sends the key refreshment schedule to all PSs in the network as shown in Table 1:

$$m_3 : \text{MS} \longrightarrow \text{KG}^i : \text{EK}_{\text{admin}} \times \left\{\text{Key}_{\text{Gen}_{\text{msg}}} \mid \text{EK}^i_{\text{new}}\text{PSbsc} \mid \text{Timestamp} \mid \text{Key\_Ref\_Schedule}\right\}. \tag{6}$$

The assigned PS generates K_{net} using its biometrics. PS generates key pool with the help of its biometric and assigns K_{net} randomly from its generated key pool:

$$m_4 : \text{KG} \longrightarrow * : \text{EK}_{\text{admin}} \{K_{\text{net}}\}. \tag{7}$$

5.2. Rekeying. In order to refresh K_{net}, MS sends message to KeyGen to refresh K_{net}:

$$m_1 : \text{MS} \longrightarrow \text{KG}^i : \text{EK}_{\text{admin}}$$

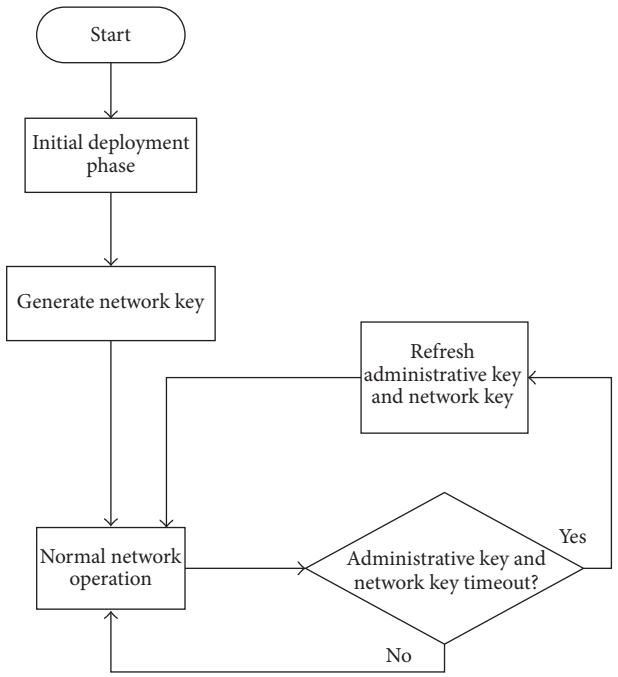

Figure 3: Flowchart of our proposed scheme for inter-WBAN communication.

$$\times \left\{\text{Key\_Ref\_msg} \mid \text{EK}^{i}_{\text{new}}\text{PSbsc} \mid \text{Key\_Ref\_Schedule} \mid \text{Timestamp}\right\}. \tag{8}$$

KeyGen computes new value of K_{net} from its biometrics. It then broadcasts to the whole network encrypting with K_{admin} as follows:

$$m_2 : \text{KG} \longrightarrow * : \text{EK}_{\text{admin}} \left\{K_{\text{new}}\text{net}\right\}. \tag{9}$$

MS sends new refreshment schedule to all PSs encrypting with the current value of K_{admin} when the refreshment schedule expires:

$$m_1 : \text{MS} \longrightarrow * : \text{EK}_{\text{admin}} \left\{\text{Key}_{\text{Ref}_{\text{Schedule}}} \mid \text{Timestamp}\right\}. \tag{10}$$

Administrative key K_{admin} is refreshed periodically. The assigned PS, when its turn arrives computes value from its biometrics. It generates key pool and assigns K_{admin} randomly from the generated values. PS broadcasts newly generated value of K_{admin} to the network:

$$m_2 : \text{KG} \longrightarrow * : E^{K}_{\text{old}}\text{admin} \left\{K_{\text{new}}\text{admin}\right\}. \tag{11}$$

Basic keys K_{bsc} of all PSs are refreshed when they are used.

5.3. Personal Server Addition. We assume that MS contains all the information of the deployed PSs and the newly deployed PSs as all PSs transmit data to the MS. The addition of PS is possible; that is, in case of PS compromise new PS is added to the network. When a PS is added to the network, it sends discovery message to MS as follows:

Table 1: Example of Key Refreshment Schedule with n slots.

New schedule	Turn 1	Turn 2	Turn 3		Turn N
MS	PS_{10}	PS_{5}	PS_{3}	$\cdots$	PS_{6}

$$m_1 : \forall \text{PS}^{i} \in \{\text{newPS}\} : \text{PS}^{i} \longrightarrow \text{MS} : \text{EK}^{i}_{\text{PSbsc}} \left\{\text{ID}^{i} \mid \text{Auth\_code}^{i}\right\}. \tag{12}$$

MS authenticates its ID and authentication code and sends $K_{\text{MS,PS}}$ to the newly deployed PS. MS also sends the information of sensor nodes that are to be deployed in the PS and the relevant keys:

$$m_2 : \forall \text{PS}^{i} \in \{\text{newPS}\} : \text{MS} \longrightarrow \text{PS}^{i} : \text{EK}^{i}_{\text{PSbsc}} \times \left\{K^{i}_{\text{MS,PS}} \mid K_{\text{admin}} \mid K_{\text{net}} \mid \forall \text{SN}^{j} \in \{\text{SN}\} : \left\{\text{ID}\left(\text{SN}^{i}\right)\right\}\right\}. \tag{13}$$

Administrative key and network key are refreshed always when a new PS is added into the network following the same rekeying method.

6. Analysis and Comparison

In this section, we analyze our proposed technique with respect to storage, communication, and energy overhead as well as perform the security and performance analysis. We also compare our proposed technique with a well-known key management technique known as BARI+ [7]. Our proposed scheme involves values that are time variant, that is, EKG values that possess the randomness property. We use HMAC-MD5 for hashing. HMAC-MD5 is more efficient than other hashing techniques as it takes less computation cycles for key generation [28]. Randomness of keys can be determined by calculating the probabilities of keys.

6.1. Storage Overhead. Storage overhead is computed by analyzing all the keys and authentication codes for nodes of different types. Storage requirements of authentication nodes are not included in the analysis. In intra-WBAN communication, we use only one key for communication in the network. Sensor nodes store one key $\text{KS}_{\text{SN,MS}}$ which is computed through biometrics. Two short integers are reserved for the computation of key whereas one short integer is equivalent to 2 bytes. In (14), z is the length of the key:

$$S_{\text{SN}} = z + 4. \tag{14}$$

PS stores all IDs of sensor nodes, $K_{\text{PS,SN}}$ and 4 bytes for the computation of biometric based key. Storing a sensor node's identity requires 2 bytes. Another 2 bytes are required to specify timeout after which the sensor node refreshes $K_{\text{PS,SN}}$. The storage overhead of PS for intra-WBAN communication can be computed using (15). Figure 4 shows the storage

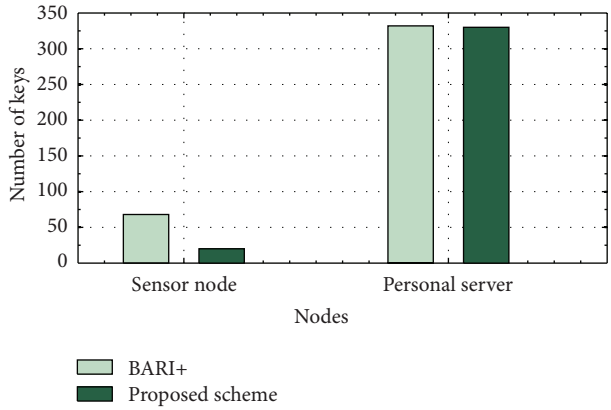

Figure 4: Storage overhead comparison of BARI+ and the proposed scheme for intra-WBAN communication.

Table 2: Storage requirement (in bytes) of each type of nodes for intra-WBAN communication.

Technique	Sensor node	Personal server
BARI+	$(4 \times z) + 4$	$[(r + 2) \times z] + (4 \times r)$
Proposed scheme	$z + 4$	$(r \times z) + (4 \times r) + 4$

overhead of BARI+ and the proposed scheme for intra-WBAN communication. For comparison, the number of sensor nodes (r) is assumed to be 15 and the key size is assumed to be 16 bytes in our simulations. It is evident from Figure 4 that the proposed scheme outperforms BARI+ in case of sensor memory utilization, while in case of PS memory consumption, the proposed scheme is equivalent to BARI+:

$$S_{\text{PS}} = (r \times z) + (4 \times r) + 4. \tag{15}$$

In inter-WBAN communication, only PS takes part in the network communication. So, the PS stores the key refreshment schedule which takes 4 integer bytes. Three keys K_{net}, K_{admin}, and K_{bsc} are stored in PS. PS also stores a key pool of s size and each key of z bytes. Overall storage requirement of PS is calculated as follows:

$$S_{\text{PS}} = (3 \times z) + (s \times z) + 4. \tag{16}$$

Storage requirements of BARI+ and the proposed scheme are shown in Table 2.

6.2. Communication Overhead. Communication overhead is computed for both intra-WBAN and inter-WBAN communication. Intra-WBAN communication overhead is very simple as all nodes are in the range of each other and the average messages transmitted by sensor nodes are very less. For both types of communication, each node sends one message in the initial deployment phase. Table 3 shows the average number of messages transmitted by each type of node in initial deployment phase in both of the schemes.

To refresh K_{net}, MS directs PS to refresh the network key. PS generates new network key by using its biometrics and sends to the whole network. Table 4 shows the average number of messages transmitted by each type of nodes in refreshment of network key in both of the schemes.

Table 3: Average number of messages transmitted by each type of nodes in initial deployment.

Technique	Sensor node	Personal server
BARI+	1	1
Proposed scheme	1	1

Table 4: Average number of messages transmitted by each type of nodes in key refreshment phase.

Technique	Sensor node	Personal server
BARI+	—	1
Proposed scheme	—	2

Table 5: Average number of messages transmitted by each type of nodes when administrative key is refreshed.

Technique	Sensor node	Personal server
BARI+	$1/r$	$((2 \times y) + 1)$
Proposed scheme	—	$1/r$

To refresh K_{admin}, each PS sends one message in every schedule in order to refresh the administrative key. The average messages transmitted by all PSs are $1/r$, if all PSs participate in refreshment of K_{admin}. Table 5 shows the average number of messages transmitted by each type of node in refreshment of the administrative key in both of the schemes.

6.3. Energy Consumption. Energy consumption is computed by calculating the total number of messages transmitted by all types of nodes. Energy is dependent on the distance between the PS and the sensor nodes. As the distance between PS and sensor node increases, its energy consumption also increases. Energy is calculated using the ratio model given in [11, 29, 30]. The following formula is used for the calculation of energy:

$$\text{Energy} = \text{data\_packet} * \left(2 * e\_\text{elect} + e\_\text{emp} * \text{distance}\right). \tag{17}$$

In (17), data_packet represents the number of packets transmitted by all types of nodes, e_elect is the energy consumption in the electronics for sending or receiving one bit, and e_emp is the transmit amplifier. Figure 5 shows the energy consumption in WBAN communication for transmission of 200 data packets. The number of keys used to refresh the administrative key is less than BARI+ that is why energy consumed by BARI+ is very high in the process of administrative key refreshment. In the proposed technique, the messages transmitted to refresh keys are higher as compared to BARI+, that is why more energy is consumed in the key refreshment phase.

6.4. Node Eviction. Node eviction means that any node in the network leaves the network for some reason, for example, power consumption, node emigration, node capture, and so

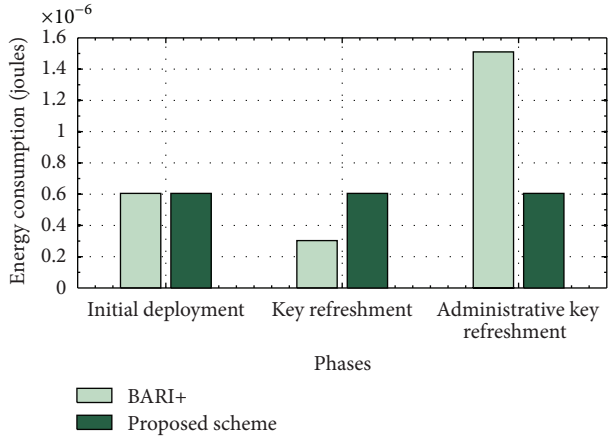

Figure 5: Energy comparison of all phases in BARI+ and the proposed scheme.

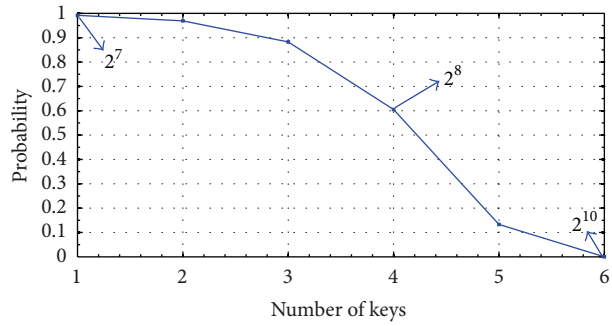

Figure 6: Probability of uniquely generated keys.

forth. We assume that the compromised nodes, the energy-exhausted nodes, and the migrated nodes can eventually be detected by most of its neighbors within a certain time period by sending the keep-alive messages. If a certain node does not respond to a keep-alive message, then the neighboring nodes remove that node from its neighbor list.

6.5. Security Analysis. Our proposed technique is analyzed by considering both insider and outsider attacks. WBAN faces both types of attacks. In passive eavesdropping, the attacker records encrypted keys. In replay attacks, the attacker captures legitimate messages and replays these messages in the network. Insider attacks include physical access of the nodes and attacker can launch multiple attacks such as unauthorized access to data, false injection of data, and alteration of health data.

6.5.1. Outsider Attack. Only the authorized sensors can communicate in the network; that is, without proper authorization, sensor nodes cannot communicate in the network. The communication among the sensor nodes is secured by using the keys like K_{admin}, $K_{\text{MS,PS}}$, K_{bsc}, and K_{net}. Sensors lying outside of the network are categorized as outsiders and cannot participate in the communication without properly assigned key materials. So if an outsider tries to attack, our authentication mechanism provides strong protection against the outsider attacks by ignoring all communications from the stranger nodes.

6.5.2. Replay Attacks. In replay attacks, an attacker stores previous messages and then resends those messages to launch the attack. The proposed scheme uses a nonce and timestamps to prevent the replay attacks. The nonce is checked to see if it duplicates a previously presented value. The timestamp allows receivers to limit how long nonces are retained. If an attacker gains some information and then replays it, the attacker will be caught because of the difference in nonce and timestamp.

6.5.3. PS Compromise. The proposed scheme shows a strong resilience against the capture of the PS. Network key K_{net} is generated using the biometrics of KeyGen. In rekeying technique, the probability of a key repeat in the network depends upon the length of the key and the total number of keys generated by KeyGen. For this purpose, we use the formula of "Birthday Paradox." For 64-bit length key, 264 combinations of keys are used. In "Birthday Paradox" the probability of repeating the key is 0.5 in 232 attempts, which is also a big number. Since a WBAN has much lesser number of nodes than 232 (e.g., 215), the probability of repeating a key in entire network decreases. Due to the randomness property of biometrics, the probability of repeating a key approaches to zero. Figure 6 shows that at initial stage, the probability of keys to be unique remains closer to one. After the initial phase, the curve starts declining and then approaches to zero. The main focus of the analysis is to find a threshold at which the probabilities that all keys generated are unique and no key gets repeated falls within 1 to 0.999999. If a PS is compromised by an adversary, MS revokes the existing keys of the PS. PS is recovered by using the secret key $K_{\text{MS,SN}}$ and the authentication codes of PS are refreshed. In intra-WBAN communication, new PS is verified by the secret key $K_{\text{MS,SN}}$. In inter-WBAN communication, MS directs KeyGen node to generate new Network key K_{net} and Admin key K_{admin} using the rekeying method.

6.5.4. Sensor Node Compromise. The probability of sensor node compromise is less in WBANs as compared to WSNs. However, in case of sensor node compromise, new keys are generated by rekeying method in intra-WBAN communication in the proposed technique.

6.5.5. KeyGen Compromise. In inter-WBAN communication, PS serves as KeyGen node for communication in the network and for rekeying. If a KeyGen node is compromised, the responsibility of generating keys is shifted to another PS by the MS.

6.5.6. Confidentiality. In the proposed technique, the network traffic is secured by encrypting all messages using secret keys. Confidentiality is maintained by protecting data against the unintended parties. An attacker cannot overhear the network unless it obtains the secret key. In the proposed technique, we encrypt the data by using keys. Encrypted data ensures the secure communication of intra-WBAN and inter-WBAN communication.

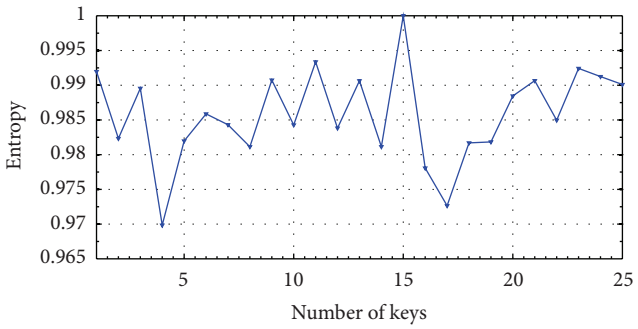

Figure 7: Average entropy of keys for 31 subjects.

6.5.7. Authentication. To protect network from false injection of data, data authentication is required. An attacker can easily inject false message, so the receiver has to make sure that the data received originates from the relevant sender. MAC is applied on each message between PS and sensor node to achieve authentication in the proposed technique for intra-WBAN and inter-WBAN communications.

6.5.8. Integrity. To ensure the integrity of data, we use MAC authentication in intra-WBAN communication in the proposed technique. Alteration and modification of data can be easily determined by using the MAC. Data integrity ensures the accuracy of data being transmitted.

6.5.9. Freshness. The attacker can capture the data and replay it. Data freshness ensures that the frames transmitted are not reused. Data freshness is guaranteed by using rekeying method in both intra-WBAN and inter-WBAN communications.

6.6. Performance Analysis. For the performance analysis of our proposed scheme, we compare different hashing schemes. According to our comparisons by running HMAC-MD5, SHA1 and MD5 for 2.9 seconds, the data is processed by these algorithms against each block size mentioned in Table 6. The results in Table 6 show that HMAC-MD5 processes more bytes of data as compared to other techniques. The implementation is done on a system with 4GB RAM, 2.20 GHZ processor and Red Hat Enterprise Level 5 operating system.

6.6.1. Randomness. For intra-WBAN communication, the randomness of keys is determined by calculating the entropy of the keys using NIST randomness testing suite. Entropy is calculated for 31 subjects over 100 random start times. Entropy of keys almost reaches to 1 in our case, which means that no data is repeated as shown in Figure 7. The purpose of this test is to compare the frequency of overlapping blocks of two consecutive lengths for a random sequence. In the proposed inter-WBAN technique, the randomness of data is ensured by calculating the average entropy of 31 subjects as shown in Figure 7.

Several tests are performed such as frequency, block frequency, cumulative sums, runs, nonoverlapping template, and linear complexity in NIST randomness testing suite as shown in Figure 8. These algorithms are used to test the randomness of the data. By using these algorithms, deviations of a binary sequence from randomness are detected. These tests detect whether the pattern is repeated in the sequence. By these tests, critical value is determined. If the test exceeds the critical value, it means that the data is not random. Results of these tests can be determined by checking the P value of these algorithms. If P value is greater than 0.01, it means that the test is successful and the sequence is random. Simulation is performed on all the above tests for EKG-based data. Figure 8 shows the NIST randomness testing suite results for randomness of the generated keys.

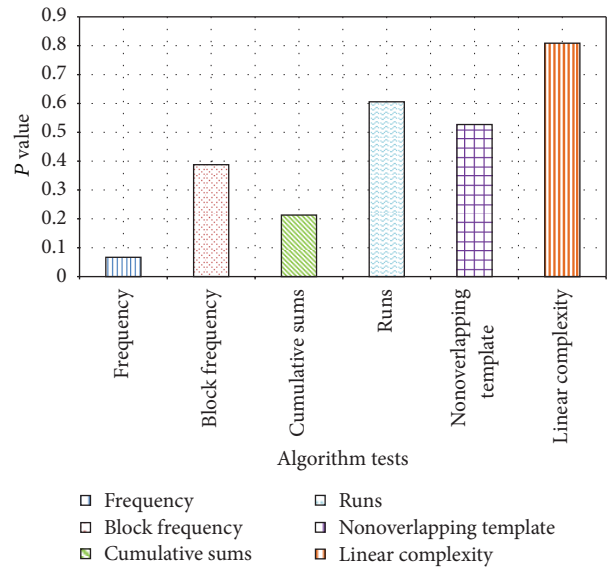

Figure 8: NIST randomness testing suite results for the generated keys.

6.6.2. Distinctiveness. In intra-WBAN communication, distinctiveness or uniqueness of keys is determined by calculating the hamming distance of 31 subject keys. Hamming distance is a measure of calculating the difference between two vectors. Distinctiveness of 31 subject keys means that the keys are identical for the same subject and different for other subjects. The results are shown in Figure 9 at random start time. The figure shows that the values at the diagonal are zero, which means that same subject keys are similar and others are different.

6.6.3. Computational Cost. In the proposed technique, we use only one key for the security of intra-WBAN communication and minimum keys are used for inter-WBAN communication. In intra-WBAN communication, discrete wavelet transform- (DWT-) based solution is used as its computational cost is $O(n)$ [10], which is faster than the techniques such as fast Fourier transform (FFT) used by many other researchers.

7. Conclusion

Wireless body area networks (WBANs) have numerous applications, including patients monitoring and assisted living.

Table 6: Memory usage of different schemes.

Type	Block size				
	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
MD5	15364.25 k	54577.52 k	150091.94 k	272166.53 k	351300.27 k
HMAC (MD5)	22092.06 k	69330.07 k	178271.96 k	292575.70 k	360981.30 k
SHA1	16007.63 k	52851.41 k	135947.13 k	221869.91 k	272486.74 k

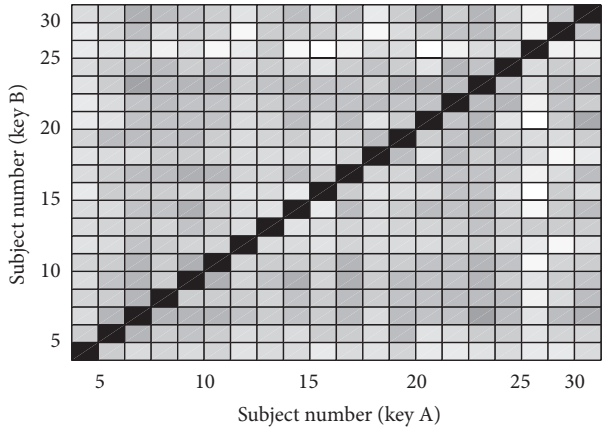

Figure 9: Hamming distance between keys generated from different subjects.

In case of patients monitoring, the human personal data is communicated over an unreliable wireless media, exposing the WBANs to a variety of attacks. Providing a security solution for WBANs will increase the user confidence, which will eventually cause increase in its usability and applicability. The technique presented in this paper is a hybrid security technique for intra-WBAN and inter-WBAN communications. The hybrid technique uses both autogeneration of keys as well as the preloading which makes it efficient in terms of both storage and security. The work presented is twofold; in the first phase, the communication is made secure in intra-WBAN communication by automatically generating keys in sensor nodes and preloading of only one key. In the second phase, the technique is extended to the security of inter-WBAN communication. Security in intra-WBAN is ensured by eliminating key exchange between sensor nodes and the PS. A preloading-based technique is presented for the security of inter-WBAN communication. We analyzed the security, storage requirements, and also its running time by comparing it with an existing technique known as BARI+. The comparison shows that the proposed technique is efficient in terms of all these parameters. Due to its hybrid security mechanism, the technique has a good tradeoff between security and resource constraints.

Abbreviations

WBAN: Wireless body area network
WSN: Wireless sensor network
MS: Medical server
PS: Personal server
SN: Sensor node
$K^i_{SN,MS}$: Key shared between sensor node i and the MS. It is preloaded in every node and refreshed whenever it is used.
K^i_{bsc}: Basic key of PS i shared with the PS. It is preloaded in every node and is refreshed whenever it is used
K_{net}: Network wide key
K_{admin}: Administrative key
m_i: Message number in a particular communication sequence
EK{$A \mid B$}: Values A and B are put together in a block/chunk and then the chunk is encrypted using key K.

Acknowledgment

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding of this research through the Research Group Project no. RGP-VPP-214.

References

[1] D. Raskovic, T. Martin, and E. Jovanov, "Medical monitoring applications for wearable computing," *Computer Journal*, vol. 47, no. 4, pp. 495–504, 2004.

[2] T. Martin, E. Jovanov, and D. Raskovic, "Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device," in *Proceedings of the 4th Intenational Symposium on Wearable Computers*, pp. 43–49, October 2000.

[3] S. Ullah, H. Higgins, B. Braem et al., "A comprehensive survey of wireless body area networks," *Journal of Medical Systems*, vol. 36, pp. 1065–1094, 2012.

[4] S. Saleem, S. Ullah, and H. S. Yoo, "On the security issues in wireless body area networks," *International Journal of Digital Content Technology and Its Applications*, vol. 3, no. 3, 2009.

[5] D. Djenouri, L. Khelladi, and N. Badache, "A survey on security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[6] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[7] K.-U. R. S. Muhammad, H. Lee, S. Lee, and Y.-K. Lee, "BARI+: a biometric based distributed key management approach for wireless body area networks," *Sensors*, vol. 10, no. 4, pp. 3911–3933, 2010.

[8] S. Cherukuri, K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the International Conference on Parallel Processing Workshops (WiSPr '03)*, Taiwan, 2003.

[9] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, no. 6, pp. 5561–5595, 2011.

[10] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[11] G. Selimis, L. Huang, F. Massé et al., "A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design," *Journal of Medical Systems*, vol. 35, no. 5, pp. 1289–1298, 2011.

[12] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," *International Journal of Network Security*, vol. 12, no. 2, pp. 75–83, 2011.

[13] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," The Internet Society: Reston, Va, USA, 1999.

[14] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865–882, 2006.

[15] A. Ali and F. A. Khan, "An improved EKG-based key agreement scheme for body area networks," *Communications in Computer and Information Science*, vol. 76, pp. 298–308, 2010.

[16] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proceedings of the IEEE INFOCOM Workshops*, New York, NY, USA, April 2008.

[17] K. K. Venkatasubramanian and S. K. S. Gupta, "Security for pervasive health monitoring sensor applications," in *Proceedings of the 4th International Conference on Intelligent Sensing and Information Processing (ICISIP '06)*, pp. 197–202, December 2006.

[18] A. Ali, S. Irum, F. Kausar, and F. A. Khan, "A cluster-based key agreement scheme using keyed hashing for Body Area Networks," *Multimedia Tools and Applications*, vol. 66, no. 2, pp. 201–214, 2013.

[19] C. C. Y. 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 Communications Magazine*, vol. 44, no. 4, pp. 73–81, 2006.

[20] 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 *Proceedings of the 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS '05)*, pp. 2455–2458, September 2005.

[21] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60–68, 2010.

[22] C. Huang, H. Lee, and D. H. Lee, "A privacy-strengthened scheme for E-Healthcare monitoring system," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2959–2971, 2012.

[23] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: a lightweight identity-based cryptography for body sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 6, pp. 926–932, 2009.

[24] R. V. Sampangi, S. Dey, S. R. Urs, and S. Sampalli, "A security suite for wireless body area networks," *International Journal of Network Security & Its Applications*, vol. 4, no. 1, 2012.

[25] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[26] G. Jolly, M. C. Kuscu, P. Kokate, and M. Younis, "A low-energy key management protocol for wireless sensor networks," in *Proceedings of the 8th IEEE International Symposium on Computers and Communication*, 2003.

[27] M. Boujelben, O. Cheikhrouhou, M. Abid, and H. Youssef, "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks," in *Proceedings of the 3rd International Conference on Sensor Technologies and Applications (SENSORCOMM '09)*, pp. 442–448, June 2009.

[28] F. Kausar, S. Hussain, L. T. Yang, and A. Masood, *Scalable and Efficient Key Management For Heterogeneous Sensor Networks*, Springer Science Business Media, LLC, 2008.

[29] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.

[30] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication algorithm for wireless microsensor networks," in *Proceeding of the 33rd International Conference on System Sciences*, pp. 1–10.