J Med Syst (2014) 38:33
DOI 10.1007/s10916-014-0033-1

PATIENT FACING SYSTEMS

A Broadcast-Based Key Agreement Scheme Using Set Reconciliation for Wireless Body Area Networks

Aftab Ali · Farrukh Aslam Khan

Received: 16 December 2013 / Accepted: 10 March 2014 / Published online: 18 April 2014

Abstract Information and communication technologies have thrived over the last few years. Healthcare systems have also benefited from this progression. A wireless body area network (WBAN) consists of small, low-power sensors used to monitor human physiological values remotely, which enables physicians to remotely monitor the health of patients. Communication security in WBANs is essential because it involves human physiological data. Key agreement and authentication are the primary issues in the security of WBANs. To agree upon a common key, the nodes exchange information with each other using wireless communication. This information exchange process must be secure enough or the information exchange should be minimized to a certain level so that if information leak occurs, it does not affect the overall system. Most of the existing solutions for this problem exchange too much information for the sake of key agreement; getting this information is sufficient for an attacker to reproduce the key. Set reconciliation is a technique used to reconcile two similar sets held by two different hosts with minimal communication complexity. This paper presents a broadcast-based key agreement scheme using set reconciliation for secure communication in WBANs. The proposed scheme allows the neighboring nodes to agree upon a common key with the personal server (PS), generated from the electrocardiogram (EKG) feature set of the host body. Minimal information is exchanged in a broadcast manner, and even if every node is missing a different subset, by reconciling these feature sets, the whole network will still agree upon a single common key. Because of the limited information exchange, if an attacker gets the information in any way, he/she will not be able to reproduce the key. The proposed scheme mitigates replay, selective forwarding, and denial of service attacks using a challenge-response authentication mechanism. The simulation results show that the proposed scheme has a great deal of adoptability in terms of security, communication overhead, and running time complexity, as compared to the existing EKG-based key agreement scheme.

Keywords Healthcare · Wireless body area networks · Key management · Set reconciliation

This article is part of the Topical Collection on *Patient Facing Systems*

A. Ali · F. A. Khan (✉)
National University of Computer and Emerging Science,
A. K. Brohi Road, H-11/4, Islamabad, Pakistan
e-mail: fakhan@ksu.edu.sa

A. Ali
e-mail: aftab.ali@nu.edu.pk

A. Ali · F. A. Khan
King Saud University, Riyadh, Saudi Arabia

Introduction

The use of information and communication technology has brought a revolution to the medical field. A wireless body area network (WBAN) is formed by wearing sensor-equipped clothes or implanting sensors into the human body. WBANs are specifically designed to be used in healthcare and emergency response scenarios. In such a scenario, the nodes in WBAN measure the vital signs from the body and send this information to a medical server located in the hospital. A physician in the hospital then examines the vital signs for diagnosis and other medical purposes. Securing WBAN communication is very important, because in order to provide quality healthcare facilities to its wearer, a WBAN uses human personal data i.e., physiological values (PVs). Inappropriate security measures may lead to a wrong diagnosis and could eventually result in the loss of human life [1].

One way to provide secure inter-sensor communication in WBANs is to use cryptographic keys. The main issue with cryptographic keys is the use of a specialized key distribution scheme. These key distribution schemes are of different types or classes and have some sort of dependency on pre-deployed keys, like probabilistic key distribution [2], master-key based distribution [3], etc. To avoid the pre-deployment of keys, asymmetric cryptosystems such as Diffie-Hellman are used for security purposes, but these kinds of schemes are prone to Man-in-the-Middle attacks. In addition, WBAN is comprised of small sensors with limited memory and power sources. In such a special network, the security, energy, and other requirements differ from ordinary Wireless Sensor Networks (WSNs). The security protocols designed for WSNs cannot be directly applied to WBAN communications because of their energy and storage constraints. Moreover, the key management protocols for WSNs will not work as efficiently as protocols specifically designed for WBANs [4, 5], e.g., public key-based protocols will be computationally expensive to use in WBANs [6]. There are some usable security (i.e., plug-n-play) schemes for WBANs [7–9, 17]. The advantages of these usable security schemes are their friendly nature for network topology changes, without compromising the security of the network. The issue with such techniques is that these schemes exchange too much information when the key agreement takes place. For example, the schemes in [9] and [17] exchange the whole feature set between the communicating sensors. After each node gets the feature set of the other communicating sensor, the sender will then agree upon a common key with the receiver, if the sender and receiver have the same feature sets. Now consider, if an attacker gets these feature sets, then he/she might easily generate the key. Moreover, the attacker can replay these feature sets in order to launch a replay attack, which will eventually open the door for selective-forwarding and denial-of-service attacks.

Set reconciliation [10] is used to reconcile two similar sets held by two different hosts in a communication efficient manner, for example, two hosts A and B have two similar sets m and n, respectively. If $m = \{1, 2, 3, 4, 5, 6, 8, 10\}$ and $n = \{1, 2, 4, 5, 6, 8, 9\}$, by reconciling these two sets held by these two hosts, we can come up with a solution set or reconciled set. The reconciled set includes the elements of both the sets, as well as the missing elements of both sets. In addition, the differences in the sets are eliminated with a minimal exchange of information. This reduces the communication and computational complexity of the set reconciliation process. Now, if we map the reconciliation process on electrocardiogram (EKG) feature sets exchanged between communicating sensors, where both the sensors are located on the same body and measure the same EKG values, this results in the calculation of two similar sets by two different hosts. By reconciling the sets held by these hosts, the differences are eradicated with a minimal exchange of information, and both hosts get the common sets.

In this paper, we propose a broadcast-based EKG key agreement scheme using set reconciliation for WBANs. The scheme provides usable (i.e., plug-n-play) security for inter-sensor communication in WBANs, which eliminates the use of an explicit key distribution scheme. The keys are generated from peak values of EKG signals of the human body. The advantage of using the EKG as a means for generating common keys is that it fulfills all the requirements, like the long, random, time variant keys proposed in [5]. To the best of our knowledge, the proposed scheme is the first broadcast-based set reconciliation scheme for EKG key agreement that is specifically designed for WBANs. In the proposed scheme, for the nodes to agree with the personal server (PS) upon a single common key, the PS broadcasts minimal information about its calculated feature set for the generation of a key. Every node in the network receives the information and starts the reconciliation process with the PS. After reconciliation, each node comes up with a common key with the PS. Because of its broadcast nature, the whole WBAN is populated with a single common communication key, which reduces the storage and communication overheads. The minimal exchange of information makes the scheme less prone to brute-force attacks. Similarly, attacks like replay, selective forwarding, and denial of service are mitigated by using a challenge-response-based authentication mechanism. The PS broadcasts a challenge in the network and every node has to come up with the legitimate response to the PS. The PS then checks the legitimacy and authenticity of the responses from the sensor nodes, and eliminates the nodes with illegitimate and unauthentic responses. In this way, the proposed scheme separates legitimate and attacker nodes in the network. The proposed scheme is analyzed and tested in terms of security, energy efficiency, and communication overhead. The results and analysis of our experiments show that the proposed scheme is a better choice for WBANs in terms of energy efficiency, communication overhead, as well as security.

The remainder of this paper is organized as follows. In "Related Work" section, the background and related literature is discussed. "System Model" section elaborates on the proposed system model. "Experiments and Results" section presents the experimental analysis and results of our scheme, while "Conclusion" section concludes our work.

Related Work

Recently, many clinical prototypes have been designed for implantable and wearable health monitoring sensors. In order to form a WBAN, these sensor devices are connected to a personal server (PS) to forward the human personal data collected by the sensor devices to remote medical servers

[11]. The involvement of human personal data gives these networks high importance. Similarly, the security of such networks is equally important [12, 13], because security will increase the confidence of the user, which will eventually increase the usability and productivity of the system. As described earlier in "Introduction" section, the sensors used in healthcare systems have limited capabilities. Because of these constraints, security schemes that are complex and computationally intensive, such as Public Key Infrastructure (PKI) [14, 15], are not suitable for securing healthcare applications.

Some of the schemes [16, 17] are pre-deployment based, which store some keys in the sensor memory before deployment. These schemes suffer from forward secrecy problems, and also consume more memory, which makes these schemes unsuitable for WBANs. Fuzzy Attribute-Based Signcryption (FABSC) is presented in [17] and the key generation process ensures the secure distribution of private keys by selecting random polynomials. There are some schemes which are based on other properties i.e., received signal strength (RSS) of the WBAN. In [18] the communicating sensors first sense the RSS values, and then apply the DWT for feature extraction. To agree upon a common key and remove the unmatched bits, a fuzzy commitment scheme [19] is used. The scheme in [20] involves human interaction channel for secure key agreement process in WBAN.

There are some techniques that use biometrics as a tool for generating cryptographic keys for secure inter-sensor communications in WBANs [21]. The advantage of using biometrics as a means for generating keys is that biometric data like an EKG are time variant in nature. So, the keys produced by such time variant values are extremely random [22–25], and provide usable security to WBANs, i.e., no initialization. In [9, 22–24], the authors used EKG as a physiological measure for generating cryptographic keys for secure inter-sensor communication. Similarly, in [27], the authors used an EKG to generate keys for secure intra-WBAN communication. The authors in [28] secured the cluster formation process, as well as the intra-WBAN communications, by using keys generated from the EKG values of the human body. The communicating sensors first calculate the EKG values, and then these values are exchanged between the communicating sensors for the generation of common keys for communication.

All of the above biometric-based security schemes exchange the whole feature set to agree upon a common key. This exchange makes these schemes risky to use for the communication of human personal data, i.e., PVs, because the data is communicated over an unreliable wireless medium. Because of this communication, the schemes are prone to different types of attacks like modification attack and forgery. Moreover, transferring the whole feature set increases the communication overhead, which reduces the performance and usability of the schemes. The scheme in [29] uses set reconciliation on ordered set representation of EKG data to obtain common key for communication. Similarly, the scheme in [30] also uses set reconciliation for unordered set of biometric values, and divides the set into time slots to avoid the synchronization problem. The set reconciliation based schemes in [29, 30] do not use peak values in the EKG signal, instead these schemes use the whole EKG signal, which reduces the randomness of the generated key.

The scheme proposed in this paper uses only the peak values in the EKG signal for set reconciliation and communicates the evaluation points, as well as the values at these points in the characteristic polynomial. The communicated values form a small subset of the characteristic polynomial of the feature set formed by peak values in the EKG signal of the subject body. This reduces the communication overhead by communicating minimal number of bits. The advantage of communicating the evaluation points is that, if they are captured by an adversary, he/she cannot obtain the original feature set. The broadcast nature of key agreement in the proposed scheme has the advantage of agreeing the whole network upon a single key in one go, which reduces the time duration of key agreement and allows the whole network to use a single common key. Similarly, different bits missing by different hosts can still reconcile to a single common key. These properties of the proposed scheme make it secure and efficient as compared to the schemes discussed above. Moreover, only one key is stored in the whole network and is used by all the sensors to perform inter-sensor communication.

System Model

We assume that the WBAN is a network of sensor nodes implanted on the human body, with the ability of measuring PVs of the body. Sensor nodes are ordinary devices with limited computation, communication, and storage capabilities. A PS is a powerful sensor node having high computation, communication, energy supply, and storage capabilities. The system architecture of a WBAN is shown in Fig. 1.

Set Reconciliation

Minsky et al. [10] proposed a set reconciliation scheme with nearly optimal communication complexity. The reconciliation of data sets among hosts is the process of agreeing upon the intersection of the two sets. Consider two hosts **A** and **B**, each with a set of length $\boldsymbol{b}$ bit strings. The process of agreeing these two hosts upon the intersection of their respective sets, with minimal amount of communication and exchanges is called set reconciliation. The communication complexity of the reconciliation protocol is dependent upon the symmetric difference between the two sets, i.e., the difference increases the complexity. Under certain circumstances, no interactions between hosts are needed by these protocols, but the

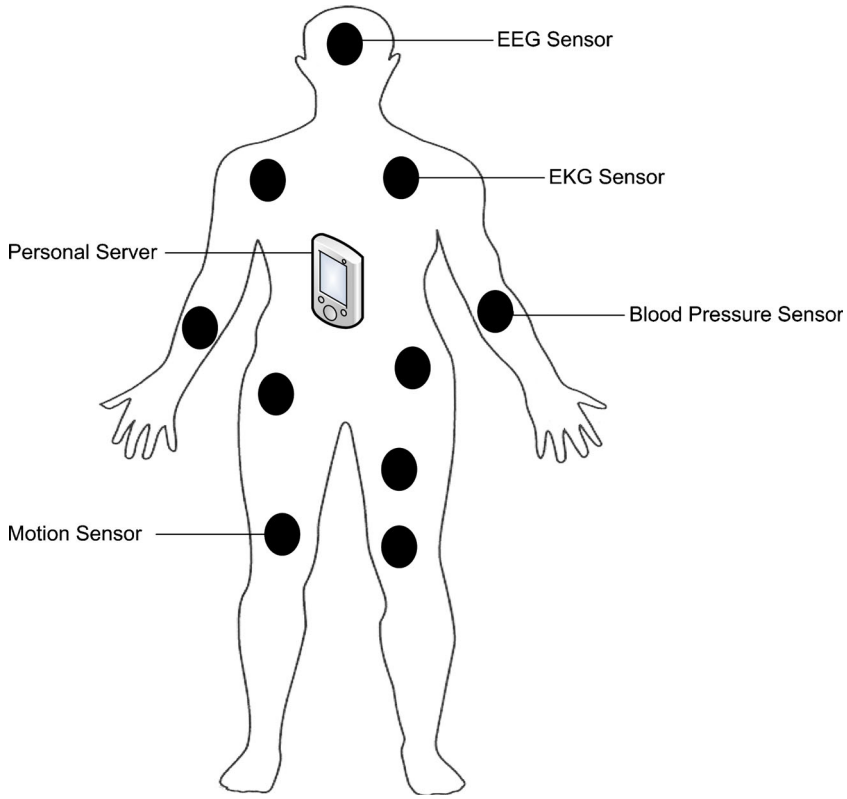

Fig. 1 Architecture of a Wireless Body Area Network (WBAN)

communication is one way [25]. Thus, host "**A**" broadcasts an "***m***" bit message, and every host $\mathbf{B_i}$ whose set differs from **A**'s set by at most ***m*** bit strings (each of length ***b***) can recover the bit strings it is missing. This works even if each host $\mathbf{B}_i$ is missing a different set of bit strings, so that the total number of distinct bit strings that can be recovered is much larger than ***m***. This set reconciliation process is shown in Fig. 2, and the involved steps are as follows:

Step 1. Both hosts **A** and **B** evaluate $\chi_{SA}(Z)$ and $\chi_{SB}(Z)$ respectively at the same evaluation points.

Step 2. The evaluations of $\chi_{SA}(Z)$ and $\chi_{SB}(Z)$ are combined to compute the value of $\chi_{SA}(Z)/\chi_{SB}(Z)$ at each of the evaluation points. These values are then used to recover the coefficients of the reduced rational function $\chi_{SA}(Z)/\chi_{SB}(Z)$

Step 3. Now, the factorization of $(\chi_{\Delta A}(Z))$ and $\chi_{\Delta B}(Z)$ reveals the elements of ΔPS and $\Delta \boldsymbol{B}_i$.

Proposed Scheme

On the basis of the set reconciliation scheme described in "Set Reconciliation" Section, we propose a broadcast-based key agreement scheme that uses set reconciliation to secure inter-sensor communications in WBANs. The proposed scheme has two main steps i.e., Feature Selection and EKG-Based Key Agreement Scheme Using Set Reconciliation:

Feature Selection

In the feature selection phase, every node in the network generates physiological value-based features from the EKG signal of the body. For the generation of these features, sensors sample the EKG signal at a specific sampling rate for a fixed duration. A Discrete Wavelet Transform (DWT) is applied to each sample. For the peak selection process, these coefficients are then passed through a peak detection function. After peak detection, each of the peak values and index pairs is quantized to form a feature vector FV = $\{FV^1, FV^2, \ldots. FV^N\}$, where FV^N represents the concatenated peak value and peak index pair, and ***N*** is the size of the feature vector.

EKG-Based Key Agreement Scheme Using Set Reconciliation

Based on the Set Reconciliation scheme, a broadcast-based EKG set reconciliation key agreement scheme is proposed. In the proposed scheme, PS broadcasts an "***m***" bit message containing some parts of the FV coefficients (characteristic polynomial of FV) into the network (WBAN). All the intended receivers ($\mathbf{B_i}$) receive the message containing the evaluation points and the values at these points in the characteristic polynomial of FV sent by the PS. These characteristic

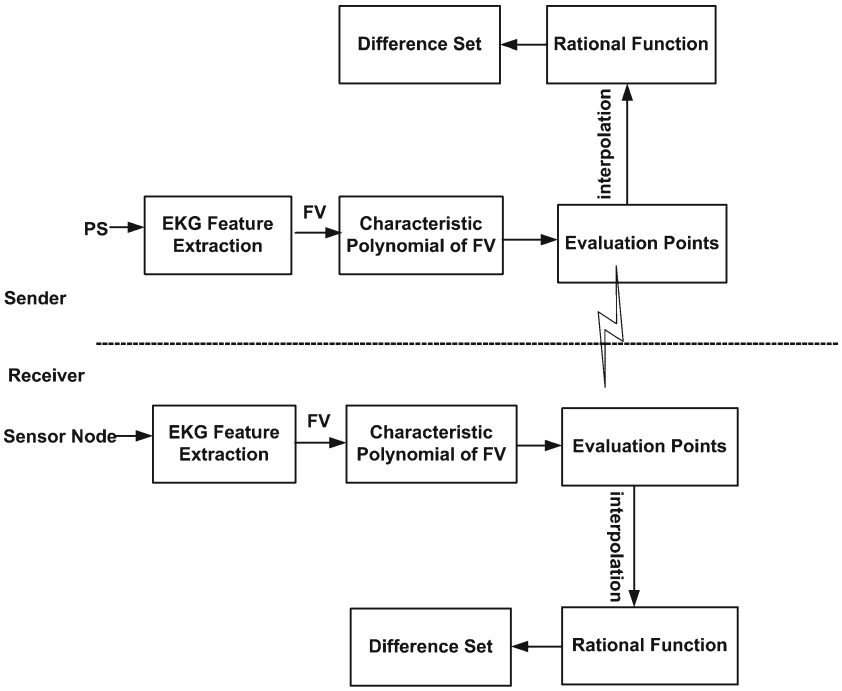

Fig. 2 EKG-based key agreement scheme using set reconciliation

polynomials are then combined to calculate the ratio between the characteristic polynomial of both the sets formed by receiving the set of PS and the set calculated at each node. These values are interpolated to recover the coefficients of the reduced rational function by factoring the elements of ΔPS and $\Delta\mathbf{B_i}$, which are the difference sets of the PS and the sensor nodes ($\mathbf{B_i}$). In step 3, every node $\mathbf{B_i}$ calculates the difference between the FV values of PS and the values calculated by the node itself. The broadcast-based set reconciliation process can be shown by the following steps:

Step 1: Both PS and the sensor nodes ($\mathbf{B_i}$) evaluate $\chi_{SPS}(Z)$ and $\chi_{SBi}(Z)$ respectively at the same evaluation points.

Step 2: The evaluations of $\chi_{SPS}(Z)$ and $\chi_{SBi}(Z)$ are combined to compute the value of $(\chi_{SPS}(Z)/\chi_{SBi}(Z))$ at each of the evaluation points. These values are then used to recover the coefficients of the reduced rational function $(\chi_{SPS}(Z)/\chi_{SBi}(Z))$

Step 3: Now, the factorization of $(\chi_{\Delta PS}(Z))$ and $\chi_{\Delta Bi}(Z)$ reveals the elements of ΔPS and $\Delta\mathbf{B_i}$.

In the above steps, S_{PS} is the set calculated from the EKG values of the PS. S_{PS} contains the characteristic polynomial (χ_{SPS}) of FV, while FV itself contains the peak values and indexes calculated from the EKG values of the body. Similarly, SB_i is the set calculated by the sensor nodes to whom the PS broadcasted.

a) **Characteristic Polynomials**

The characteristic polynomial is the determinant of a square matrix, in which an arbitrary variable x is subtracted from each of the elements along the principal diagonal. The set reconciliation scheme is based on the characteristic polynomial (χ_S) and can be represented in a generalized form as follows:

$$\chi_S S(Z) = (Z-x_1)(Z-x_2)(Z-x_3)\ldots(Z-x_n) \quad (1)$$

The characteristic polynomial provides a generalized solution to the problem when there are multiple differences in the sets held by different hosts. The characteristic polynomial encodes several important properties of the set being reconciled, most notably its eigenvalues, its determinant, and its trace. By using these properties, the missing elements of the sets can be easily restored or recovered. The characteristic polynomial of the EKG feature set is calculated in order to reconcile and eliminate multiple differences in the feature sets held by two different hosts.

b) **Evaluation Points**

The set reconciliation process depends on the evaluation of the characteristic polynomial. The evaluation points must be chosen in advance in order to reduce the cost of searching the whole set of characteristic polynomials. The evaluation points are chosen randomly by the PS and are broadcast to the sensor nodes, along with the values of the characteristic polynomial at these evaluation points. Once the node receives the evaluation points and the values of the characteristic polynomial at these evaluation points, all the nodes evaluate the whole characteristic polynomial at the same evaluation points. On the basis of these evaluation points, each node calculates its differences with that of the PS.

c) **Rational Function**

Once the evaluation points are randomly selected, the rational function is calculated by using interpolation. Interpolation is a method of constructing new data points within the range of a discrete set of known data points. Consider, if ***P*** and ***Q*** are polynomials, then their quotient is called a rational function and is given by the formula below:

$$R(z) = \frac{P(z)}{Q(z)} \quad (2)$$

The interpolated rational function is computed on the basis of the received evaluation points and the values of the characteristic polynomial at these evaluation points.

d) **Difference Set**

After the rational function calculation, the difference set between the values of PS and sensor nodes (B_i) is also calculated. The difference set shows the total number of differences between the PS and the corresponding sensor node. Once the difference set is calculated, both the parties know the differences in the other sets. Hence, agreeing upon a common set (key) is done by eliminating these differences.

e) **Challenge-Response based Authentication**

In order to perform secure and efficient communications in WBANs, the nodes must be authenticated and verified before the actual data transfer. The purpose of this authentication is to detect and prevent attacks such as replay, selective-forwarding, and denial-of-service. Even encrypted messages can be replicated by an attacker to attract traffic, simply by using a message with the right node identity. In such a scenario, the message content itself could not be of much interest to the attacker, because the message is encrypted. Instead, information like the sender ID will be the main focus of the attacker. Leaking such information will open the doors for attacks like selective forwarding and denial of service. To prevent such attacks, the proposed scheme uses the challenge-response authentication and verification to verify whether or not the receiver is trustworthy.

The authentication and verification process is depicted by two messages. In msg_1, the PS of the WBAN broadcasts a message authentication code (MAC) by using the key generated by the EKG values of the human body. The MAC contains the ID of the PS, a challenge C, and the *nonce*.

$$msg_1 : PS \rightarrow * : MAC_{KPS,SNi}\ (ID_{PS}, C, nonce)$$
$$msg_2 : SN_i \rightarrow PS : MAC_{KPS,SNi}\ \left(ID_{SNi}, ID_{PS}, C', nonce\right)$$

In response to msg_1, each sensor node SN_i in the WBAN responds with msg_2 encrypted with the same key $K_{PS,\ SNi}$, its version of the challenge C' and *nonce*. The key is the same in the communicating parties because it is generated from the EKG values of the same body. In addition, the errors and differences are removed from the feature sets by using the set reconciliation scheme in order to generate the common key. If we recall the key agreement process described earlier in the same "Proposed Scheme" section, the main advantage of the scheme is to allow the nodes to agree upon a single common key with the exchange of minimal information. Upon the reception of msg_2, PS checks the ID of each sender (SN_i), its own ID, the challenge C', and compares these values with its own version of the challenge, *nonce*, and IDs for the authentication of sensor nodes in WBAN. In the case of a mismatch, the malevolent node is detected and removed from the list of WBAN member nodes by the PS.

f) **Node Joining and Leaving**

The joining and leaving of nodes in WBANs is very rare. This is because such joining and leaving occurs when a node dies, i.e., due to battery depletion or malfunction. A WBAN is a very small network, i.e., limited to a single human body. As a result of this small size, every node is in the range of PS and other nodes. Therefore, if a particular node is eliminated for any reason (leaving, failure, power shortage, etc.) the scheme will not be affected, because the connectivity will remain. The scheme will be affected only if, for example, a single node is measuring the EKG and that node fails for some reason. Then, an immediate replacement should be made; otherwise the scheme will not work. Fortunately, this is not the case in our proposed framework. In the proposed work, we assume that every node in the WBAN can measure the EKG values.

The WBAN joining is done by placing or replacing a sensor node, after which the newly joined node will send a *hello* message to the PS. Both the PS and the sensor node will start measuring the EKG values for the generation of the common key. The key generation and agreement process described earlier will then take place. Once both the PS and sensor node agree upon a common key, the PS authenticates the node by using the challenge-response-based authentication mechanism described above. Upon its successful authentication, the node is added to the list of WBAN nodes; otherwise, if the authentication fails, the node is rejected by the PS, and the PS broadcasts the ID of the node to the other sensor nodes claiming that the node is an attacker.

If a node leaves the WBAN for any reason, like a failure, power shortage, or malfunction, the PS sends some keep alive messages to the node in order to check for its existence. If the node does not reply in

a specific time window, then the node is considered to be dead or already gone from the network. The PS removes the node from its list and broadcasts a message to the whole network that the particular node has left the network.

g) **Key Refreshment**

Key refreshment is done after a fixed interval of time or when a node joins or leaves the network. As described earlier, node joining and leaving is not very frequent in WBANs. Thus, it will not add much burden to the proposed scheme. When a node leaves the network, the PS broadcasts the *KeyRef* message to the whole network. The nodes then start the reconciliation and key agreement process to generate a new common key.

Experiments and Results

This section provides the experimental setup, analysis, and discussion on the experiments and the generated results.

Experimental Setup

In order to test the scheme for various times taken for generating the results, the simulation is performed in UBUNTU and MATLAB for 2, 4, 8, and 10 nodes respectively. Similarly, to check the randomness and uniqueness of the generated keys and the EKG values, the simulation is tested for 30 different persons' physiological data taken from the MIT PHYSIO BANK. Moreover, for the energy-efficiency experiments, all the simulations are carried out using the same hardware settings for the proposed scheme and the schemes that are compared with the proposed scheme.

Analysis and Discussion

In this section, the proposed broadcast-based key agreement scheme using set reconciliation is tested and analyzed in terms of False Acceptance Rates (FARs), False Rejection Rates (FRRs), the effect of increasing the number of nodes on time consumption, communication overhead, and energy consumption.

Security Analysis

An attacker may attempt to launch replay attacks by sniffing packets sent by a victim, and injecting duplicate copies of the packets from other network locations. Those replayed packets will be discarded; this is because after a predefined time or upon some suspicious event, the key will be refreshed as described earlier in the paper. The newly generated key cannot be generated without proper authentication from the PS, and the unauthenticated nodes will be removed from the network. In the key refreshment phase, only those nodes can take part that are located or attached to the human/subject body. This is because without being coupled with the human body, it is very difficult to measure the EKG signal of that particular body. So, if a node cannot measure the EKG signal will not be able to take part in the key agreement process. Similarly, by using *msg1* and *msg2* in the Challenge-Response-based Authentication phase, these nodes will have no idea about the new EKG values from which the key is going to be generated. This is because of the fact that the EKG values are time-variant.

Similarly, an attacker may attempt to launch selective-forwarding attack by declining to send packets to the PS. The proposed scheme assumes that each node in the WBAN is in direct contact with the PS, as a WBAN has very short network area. Due to this property, if a particular node drops packets during the key agreement process then that node will be unable to get the updated key during reconciliation with the PS. Failing to get the key will make the node visible as unauthenticated node and the PS will remove that node from the network by stopping the conversation with that particular node.

Moreover, an attacker may also attempt to launch denial-of-service attack by sending too many packets to the network in a short interval of time. The authentication and verification mechanism described in the earlier section provides a remedy in such scenarios. The authentication and verification mechanism uses a challenge-response authentication system in order to disclose a node as legitimate or an attacker. The nodes that fail to provide proper credentials for the authentication process are considered as attackers, while the others are considered as legitimate nodes. After a node is considered as an attacker, the packets sent from that node are rejected by the PS.

For the security analysis, the proposed broadcast-based key agreement scheme using set reconciliation is tested and analyzed in terms of False Acceptance Rate (FAR) and False Rejection Rate (FRR). FRR is the probability that the keys generated on the same body fail to match, i.e., the nodes on the same body did not agree upon a common key. Similarly, the FAR represents the probability that two sensors at different WBANs successfully establish a common key. In addition, to measure the detection performance, the Half Total Error Rate (HTER) is used, which combines the FRR and FAR, and is defined in the following formula:

$$\mathrm{HTER} = \frac{\mathrm{FAR} + \mathrm{FRR}}{2} \tag{3}$$

The graphs of FAR and FRR visualize and demonstrate the probability that an unauthorized user is accepted as authorized, and that an authorized user is rejected as unauthorized.

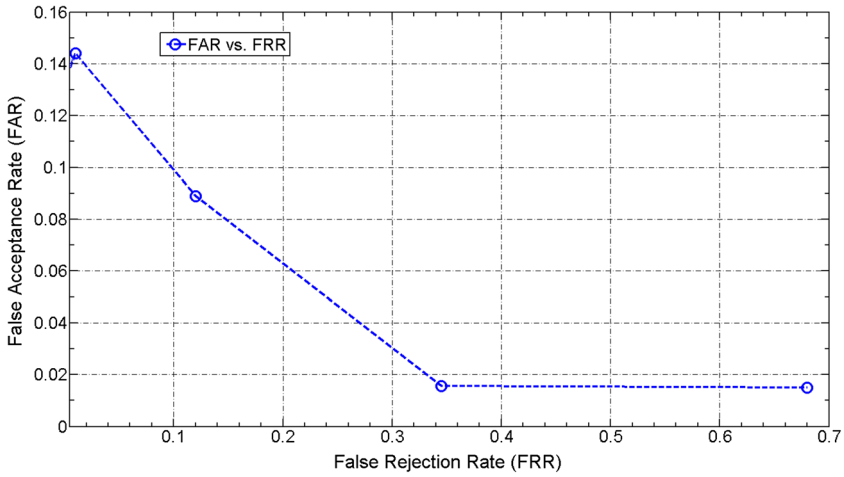

Fig. 3 FAR vs. FRR

As shown in Fig. 3, a decrease in FAR results in an increase in FRR, i.e., they are inversely related. The combined graph of FAR and FRR helps in determining the optimal threshold value for a practical biometric system. From Table 1, it is observed that when the difference threshold t increases, the FAR also increases. When greater differences in the features among the communicating sensors are tolerated, the possibility of matching two feature sets that do not belong to the same person increases, and hence the FAR increases. In contrast to the FAR, the FRR decreases when the threshold t increases. As a result of the increase in t, two feature sets from the same person are more likely to be matched. Thus, the probability of recovering one set using the other sets also increases.

In order to distinguish the physiological signals of one person from another so that no one can reproduce the keys from other than the subject's body, the input physiological signal must be universal, i.e., it should be measurable in everyone, and must possess the properties like, randomness, distinctiveness, and time variance. As can be seen from Figs. 4 and 5, sensors on the same body have a higher number of super-imposed lines (less blue bars are visible because they are hidden by the red ones) as compared to sensors on two different bodies. The lack of correlation between features of the physiological signals measured at two different subjects is due to the difference in the physiological signature of each person at any given time. This feature distinguishes two bodies, and makes it difficult for an attacker to guess or reproduce the signal of the host body.

Table 1 FAR and FRR calculations

t	FAR	FRR	HTER
1	0	0.022	0.011
2	0.0022	0.144	0.0731
3	0.0044	0.089	0.0467
4	0.0089	0.0156	0.01225
5	0.0156	0.015	0.0153

Scalability

The proposed scheme is highly scalable i.e., new nodes are introduced to the network without compromising security. As described earlier, a node can join the WBAN by just putting itself on the human body and it will start measuring the EKG values of the human body for generating the common key. This plug-n-play nature of the proposed scheme increases the scalability and usability of the proposed scheme. Figure 6 shows that when we increase the number of nodes in the network, it affects the overall running time, setup time, total communication time to agree upon a single common key, and the time taken by the reconciliation process to eliminate the differences between the values of the PS and the sensor nodes. This is because every node has to reconcile with the PS in order to generate a common key. Thus, increasing the number of nodes in the network increases the reconciliation time, setup time, running time, and communication time.

We compared our work with [9] and [22] in terms of the running time, communication overhead, and energy consumption. Figure 7 shows that the proposed scheme is better than the EKG-based key agreement scheme [9, 22] in terms of the time taken to agree upon a common key, as we increase the number of nodes. The schemes in [9] and [22] follow the same model, i.e., both the schemes exchange the whole feature set extracted from the EKG values of the body, in order to complete the key generation and agreement process. The

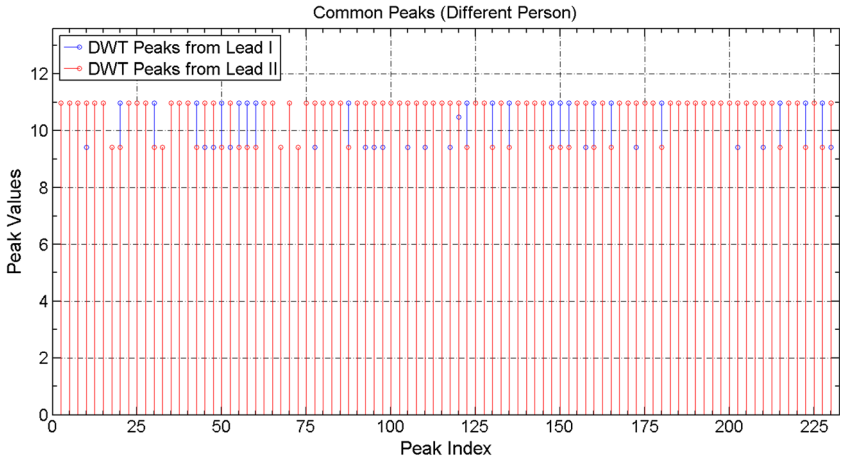

Fig. 4 DWT peaks for different persons

proposed scheme communicates only a small amount of information during the key agreement process. The proposed scheme only exchanges the evaluation points and the values of the characteristic polynomial at those points. This makes the proposed scheme more efficient than those presented in [9] and [22] in terms of the time taken to complete the key agreement process.

Communication Overhead

In order to perform secure and efficient key agreement in the whole WBAN, the proposed scheme uses a single broadcast by the PS to the intended receivers. The receivers then calculate the differences in the measured EKG feature set and unicast it to the PS. These communicated values are small in number, that is why it does not affect the performance of the scheme. The proposed scheme is compared with the EKG-based key agreement scheme in [9] and [22] in terms of the communication overhead. Figure 8 shows that the proposed scheme performs better than the model followed in [9] and [22]. This is because these schemes must exchange the whole feature set for the key generation process to take place, while the proposed scheme only exchanges the evaluation points and the values of the characteristic polynomial at those points, instead of communicating the whole feature vector. In this way, the proposed scheme reduces the communication

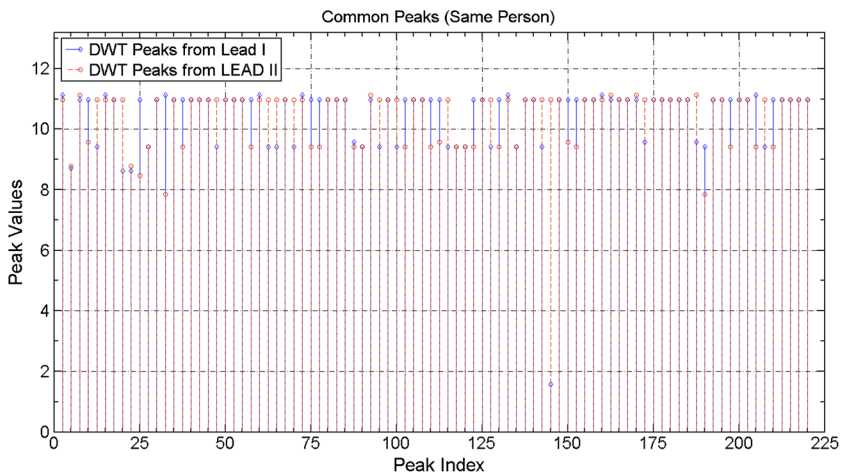

Fig. 5 DWT peaks for the same person

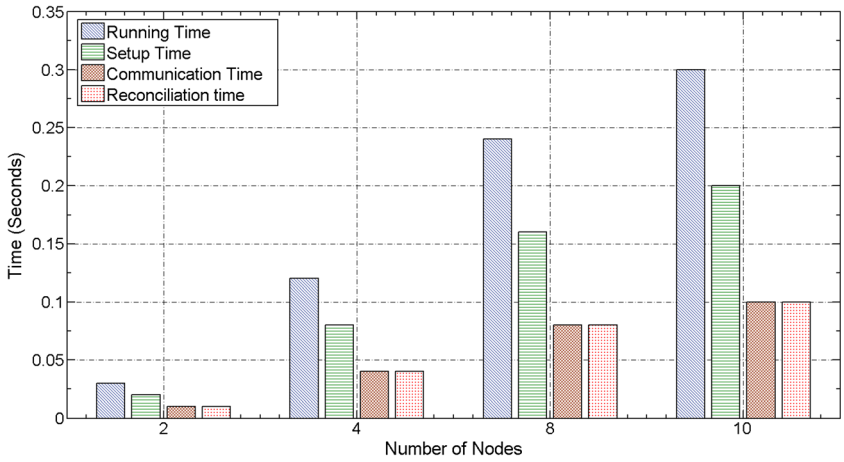

Fig. 6 Time vs. number of nodes

overhead by minimizing the number of bits broadcast over the medium. This reduction in the communication overhead will increase the energy efficiency and network lifetime of the proposed scheme, which will eventually boost the overall performance of the system.

Energy Consumption

The cost of using the communication channel largely impacts the energy consumption of the protocol, that is why involving too much communication increases the energy overhead of the protocol. According to [26], the Chipcon CC1000 radio used in Crossbow MICA2DOT motes consumes 28.6 and 59.2 μJ of energy to send and receive 1 byte of data, respectively. Using these values for receiving and transmitting a single byte, the total energy consumption is drawn in Fig. 9 for the proposed and EKG-based key agreement schemes. Figure 9 shows that the total energy consumption for the proposed scheme is significantly lower than the model used by [9] and [22] for the EKG-based key agreement. In [9] and [22], the hashes of the whole feature set are exchanged during the communication process, while in the proposed scheme, only the evaluation points and the values of the characteristic polynomial at those points are exchanged. This reduces the communication overhead, as well as the energy consumption, of the proposed scheme.

All of the above experiments and results show that the proposed scheme is highly robust, secure and efficient. This is because the proposed scheme has the tendency to exchange very little information during the

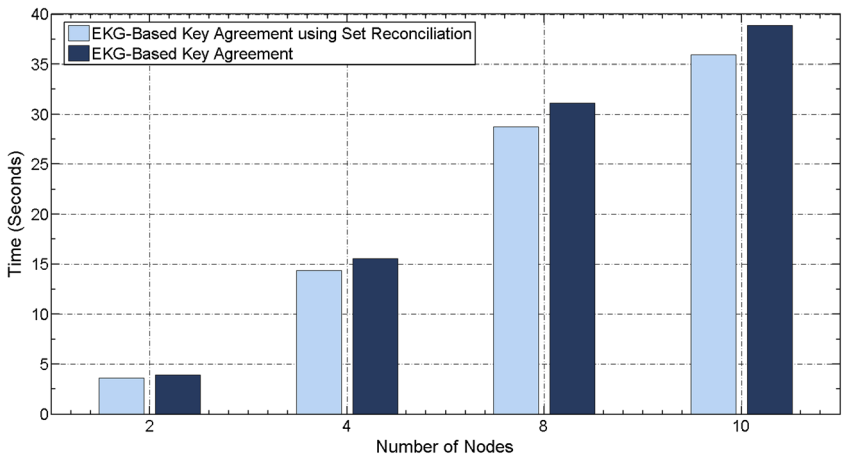

Fig. 7 Comparison of time vs. number of nodes for proposed and EKG-based key agreement scheme

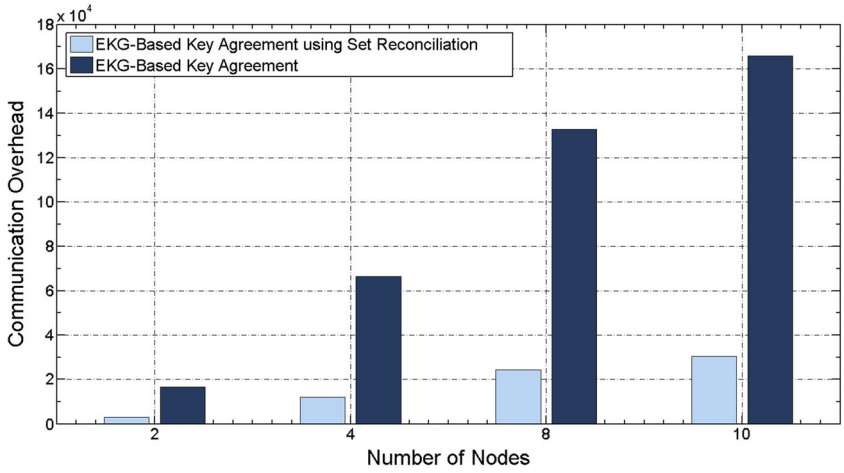

Fig. 8 Communication overhead comparison

key agreement and authentication process, which makes it a good choice for the practical use. The property of minimal information exchange results in energy efficiency, communication efficiency, and also increases the security of the proposed scheme. The proposed scheme also has some weaknesses such as key length and running complexity problem i.e., taking more time for agreeing the nodes upon a single common key. Due to small size of the WBAN, the running complexity problem does not affect the performance of the scheme severely. Another problem can be the length of the key where the proposed scheme produces 128-bit long key from the EKG data. Long and random keys can be produced by combining two different physiological values i.e., EKG and EEG, which we plan to work on in our future work.

Conclusion

In order to provide instant and reliable healthcare facility or disaster management services, security and privacy is of primary concern. In the absence of security, a healthcare system will bring danger to its user, because of the leakage of human personal data. In addition, the exchange of too much information makes a Wireless Body Area Network (WBAN) vulnerable to different attacks, like denial-of-service (DoS), selective forwarding, and replay. The proposed work uses a set reconciliation process with optimal communication complexity to allow the nodes in a WBAN to agree upon a single common key. The proposed scheme is broadcast-based and allows the whole WBAN to agree upon a single common key, which reduces the memory consumption. Since WBAN is a small network, the broadcast will not affect the performance of the

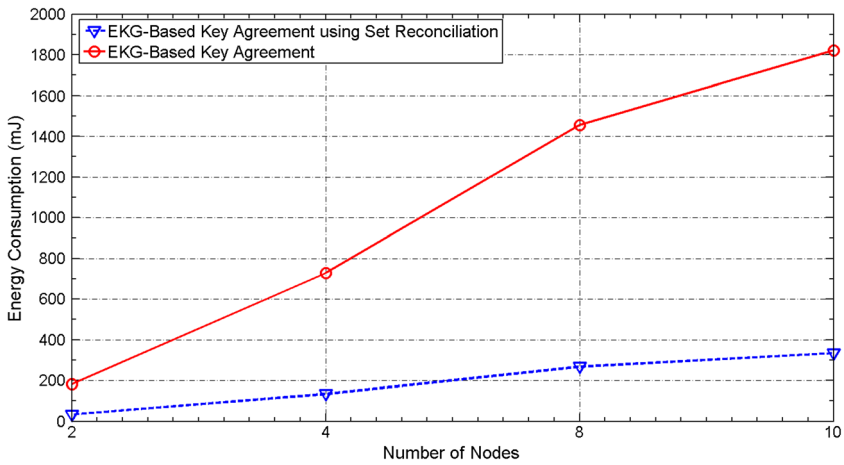

Fig. 9 Energy consumption during key agreement process

scheme. The proposed scheme mitigates denial-of-service, selective-forwarding, and replay attacks by using a challenge-response-based authentication mechanism. The proposed scheme shows good results in terms of security, communication overhead, and running time complexity as compared to the existing EKG-based key agreement scheme.

Acknowledgements 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. The authors would also like to thank the Higher Education Commission (HEC), Pakistan, for its support through the indigenous PhD fellowship program.

References

1. Venkatasubramanian, K., and Gupta, S. K. S., *Security for pervasive health monitoring sensor applications*. Proc. 4th Intl. Conf. Intelligent Sensing & Information Processing. Bangalore, India, pp. 197–202, 2006.
2. Eschenauer, L., and Gligor, V. D., *A key-management scheme for distributed sensor networks*. Proc. 9th ACM Conf. Computer and Communication Security, Washington, DC, USA, pp. 41–47, 2002.
3. Zhu, S., Setia, S., and Jajodia, S., LEAP+: efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sens. Netw. (TOSN)* 2(4):500–528, 2006.
4. Djenouri, D., Khelladi, L., and Badache, N., A survey of security issues in mobile ad hoc and sensor networks. *IEEE Commun. Surv. Tutorials* 7:2–28, 2005.
5. Yong, W., Attebury, G., and Ramamurthy, B., A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutorials* 8: 2–23, 2006.
6. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., and Culler, D. E., SPINS: security protocols for sensor networks. *Wirel. Netw* 8:521–534, 2002.
7. Venkatasubramanian, K. K., Banerjee, A., and Gupta, S. K. S., PSKA: usable and secure key agreement scheme for body area networks. *IEEE Trans. Inf. Technol. Biomed.* 14:60–68, 2010.
8. Poon, C. C. Y., Yuan-Ting, Z., and Shu-Di, B., A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Commun. Mag.* 44:73–81, 2006.
9. Venkatasubramanian, K. K., Venkatasubramanian, A., Banerjee, K. K., and Gupta, S. K. S., "*EKG-based key agreement in Body Sensor Networks*," Proc. IEEE INFOCOM Workshops, Phoenix, AZ, 2008.
10. Minsky, Y., Trachtenberg, A., and Zippel, R., Set reconciliation with nearly optimal communication complexity. *IEEE Trans. Inf. Theory* 49:2213–2218, 2003.
11. Kristof, L., LoBenny, P., Jason, N. G., et al., "*Medical healthcare monitoring with wearable and implantable sensors*". Presented at 3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications (UbiHealth), Nottingham, UK, 2004.
12. Kumar, P., and Lee, H.-J., Security issues in healthcare applications using wireless medical sensor networks: a survey. *Sensors* 12:55–91, 2011.
13. Selimis, G., Huang, L., Mass, F., Tsekoura, I., Ashouei, M., Catthoor, F., et al., A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design. *J. Med. Syst.* 35:1289–1298, 2011.
14. Balfanz, D., Smetters, D. K., Stewart, P., and Wong, H. C., "*Talking to strangers: authentication in ad-hoc wireless networks*," Proc. Network and Distributed System Security Symposium, San Diego; CA; USA, 2002.
15. Sampangi, R. V., Saurabh, D., Urs, S. R., and Sampalli, S., A security suite for wireless body area networks. *Int. J. Netw. Secur. Appl. (IJNSA)* 4:97–116, 2012.
16. He, D., Chen, C., Chan, S., Bu, J., and Zhang, P., Secure and lightweight network admission and transmission protocol for body sensor networks. *IEEE J. Biomed. Health Inform.* 17(3):664–674, 2013.
17. Hu, C., Zhang, N., Li, H., Cheng, X., and Liao, X., Body area network security: a fuzzy attribute-based signcryption scheme. *IEEE J. Sel. Areas Commun.* 31(9):37–46, 2013.
18. Wu, Y., Sun, Y., Zhan, L., and Ji, Y., Low mismatch key agreement based on wavelet-transform trend and fuzzy vault in body area network. *Int. J. Distrib. Sens. Netw.* 2013:1–16, 2013.
19. Juels, A., and Sudan, M., "*A fuzzy vault scheme*," Proc. Int. Symp. Inf. Theory, IEEE, Lausanne, Switzerland, pp. 408, 2002.
20. Xin, H., Bangdao, C., Markham, A., Qinghua, W., Zheng, Y., and Roscoe, A. W., Human interactive secure key and identity exchange protocols in body sensor networks. *IET Inf. Secur.* 7(1):30–38, 2013.
21. Cherukuri, S., Venkatasubramanian, K. K., and Gupta, S. K. S., "*Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body*", Proc. Parallel Processing Workshops, Kaohsiung, Taiwan, pp. 432–439, 2003.
22. Venkatasubramanian, K. K., and Gupta, S. K. S., Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sens. Netw.* 6:1–36, 2010.
23. Ali, A., Irum, S., Kausar, F., and Khan, F., A cluster-based key agreement scheme using keyed hashing for Body Area Networks. *Multimed. Tools Appl.* 66:201–214, 2013.
24. Ali, A., and Khan, F., *"An improved EKG-based key agreement scheme for body area networks", Proc. 4th International Conference on Information Security and Assurance (ISA 2010)*. Miyazaki, Japan, CCIS Vol. 76, pp. 298–308, (Springer) 2010.
25. Orlitsky, A., Worst-case interactive communication. I. Two messages are almost optimal. *IEEE Trans. Inf. Theory* 36(5): 1111–1126, 1990.
26. Wander, A. S., Gura, N., Eberle, H., Gupta, V., and Shantz, S. C., "*Energy analysis of public-key cryptography for wireless sensor networks*", Proc. Pervasive Computing and Communications, PerCom 2005, Kauai, Hawaii, pp. 324–328, 2005.
27. Irum, S., Ali, A., Khan, F. A., and Abbas, H., A hybrid security mechanism for intra-WBAN and inter-WBAN communications. *Int. J. Distrib. Sens. Netw.* 2013:11, 2013.
28. Ali, A., and Khan, F. A., Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP J. Wirel. Commun. Netw.* 2013: 216, 2013.
29. Shi, J., Lam, K.-Y., Gu, M., Li, M., and Chung, S.-L., Energy-efficient key distribution using electrocardiograph biometric set for secure communications in wireless body healthcare networks. *J. Med. Syst.* 35(5):745–753, 2011.
30. Shi, J., Lam, K.-Y., Gu, M., and Li, H., BodySec: synchronized key distribution using biometric slots for wireless body sensor networks. *SIGMOBILE Mob. Comput. Commun. Rev.* 14(1):22–24, 2010.