Cluster Comput (2018) 21:469–480
https://doi.org/10.1007/s10586-017-0903-7

Energy efficient key agreement scheme for ubiquitous and continuous remote healthcare systems using data mining technique

Saleh M. Al-Saleem[1,2] · Aftab Ali[2] · Naveed Khan[3]

Received: 1 November 2016 / Revised: 5 April 2017 / Accepted: 2 May 2017 / Published online: 13 May 2017

Abstract Wireless body area networks (WBANs) based ubiquitous and fully automated healthcare systems provide a platform to share medical information. Energy efficiency and communication security will increase the confidence of the users in adopting such remote healthcare systems. Key agreement and authentication schemes play an important role in the security of remote healthcare systems. The nodes in a WBAN exchange information in order to complete the key agreement and authentication process. In the literature, numerous schemes have used heavy mathematical calculations or overloaded with excessive information exchange. This paper presents a bloom filter-based key agreement scheme using k-mean clustering for WBANs. The key agreement and authentication is performed in clustered environment using k-mean clustering. This makes the scheme more robust and energy efficient. The keys are generated from the EKG values of the human body. The proposed mechanism is energy efficient and secure, due to its more efficient key generation and less memory utilizations for remote healthcare systems. Moreover, the proposed scheme is analyzed and compared with a state-of-the-art scheme in terms of energy consumption, memory utilizations, processing complexity, and false positive rate (FPR). The results show that the proposed scheme outperform significantly the other scheme by consuming less energy and efficient memory utilization, while achieving a very low FPR and linear running complexity.

Keywords Body area network · Healthcare · Security · Privacy · Bloom filter · Key agreement

✉ Aftab Ali
aftab.ali@nu.edu.pk

Saleh M. Al-Saleem
salehms@ksu.edu.sa

Naveed Khan
khan-n5@email.ulster.ac.uk

[1] Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

[2] Department of Computerized-Based Testing, National Center for Assessment in Higher Education, Riyadh, Saudi Arabia

[3] School of Computing and Information Engineering, Ulster University, Coleraine, UK

1 Introduction

Information technology modernized the medical field, a good example is the use of wireless body area network (WBAN) for collecting human physiological data. A 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, where the nodes in WBAN measure the vital signs from the body and send this information to a remote medical server in the hospital. Moreover, this information or vital signs are further examined and evaluated by a physician in the hospital for diagnoses purposes.

There are several applications of WBANs, including Medical Healthcare, fitness monitoring, etc. healthcare applications consist of indoor and outdoor monitoring of elderly people and patients. The use of small biosensors in a WBAN causes the increase in mobility of patients i.e., as the small biosensors can be used to monitor the patient remotely, this allow the patient to move around with more flexibility. The other positive aspect of this scenario is the ubiquitous health care i.e., health monitoring anywhere and anytime.

All the communication in the WBAN is carried out by using wireless medium, this poses major security threats to

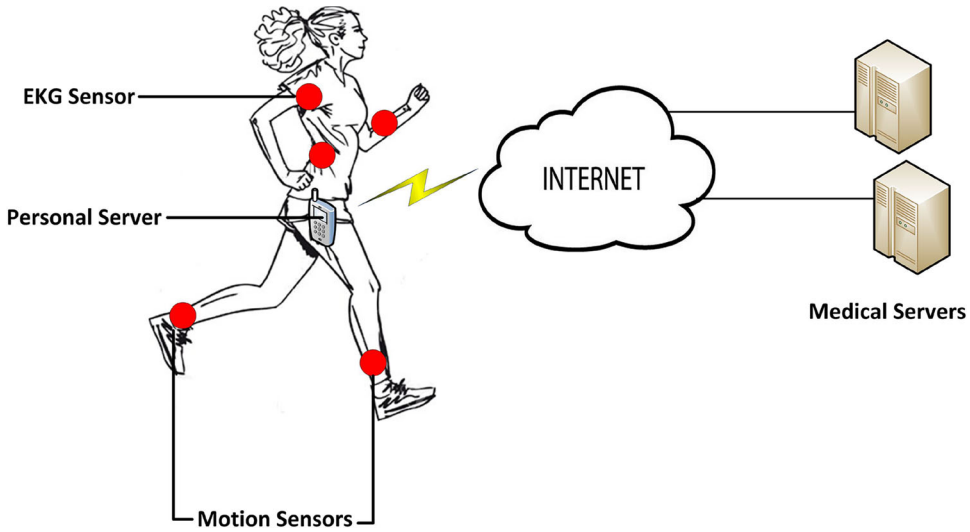


Fig. 1 A typical WBAN scenario [3]

WBAN. Securing WBAN communication is very important, this is because to provide 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]. For example, an intruder interrupted patients PVs during transmission, and got access to the actual PVs of the patient. The intruder can modify the PVs of that particular patient, which will misguide the physician and eventually will result in wrong diagnosis.

In this paper, we propose a bloom filter-based electrocardiogram (EKG) key agreement scheme for WBANs. The scheme provides plug-n-play security for inter-sensor communication in WBANs. The plug-n-play nature of the scheme eliminates the use of an explicit key distribution mechanism. The keys are generated from peak values of EKG signals of human body, because the EKG generated keys possess all the necessities, like the long, random, and time variant keys proposed in [2]. Moreover, to achieve the energy efficiency and to reduce the communication overhead this work uses bloom filter for EKG key generation. To the best of our knowledge, the proposed scheme is the first bloom filter-based EKG key agreement that is specifically designed for WBANs application in healthcare systems. A typical WBAN scenario with multiple biometric sensors is shown in Fig. 1.

In the proposed scheme, the nodes are required to agree with the personal server (PS) upon a single common key, the PS constructs a bloom filter [4] from the feature set of EKG values extracted from the human body. Similarly, the communicating nodes also calculate and constructs the bloom filter from the EKG of the same human body. After construction the bit arrays are exchanged between the sensor nodes and PS. Further, the PS check the membership of each and every bit by comparing it with its own version of the stored bit array. Once the membership is confirmed, the key generation process starts. Moreover, representing the elements with a single bit makes the proposed scheme very secure and energy efficient. All the communications are made secure by using message authentication code (MAC) before sending it on the wireless channel. Due to very less information exchange during the key agreement process, the proposed scheme mitigates the attacks like, replay and denial-of-service. The proposed scheme is analyzed in terms of security, time complexity, energy efficiency, and memory overhead. The results and analysis of our experiments show that the proposed scheme is a better choice for resource constrained networks like, WBANs.

The remainder of this paper is organized as follows. In Sect. 2, the background and related literature is discussed. Section 3 elaborates on the proposed system model. Section 4 describes details about the proposed scheme. Section 5 presents the experimental analysis and results of our scheme, while Sect. 6 concludes our work.

2 Related work

The development of implantable device revolutionized the medical field. These implantable devices are used to form a WBAN. In a WBAN sensor nodes are connected to the PS, which acts as a gateway to forward the human physiological data to the medical servers for analysis and diagnosis [5]. As the potentially exploitable wireless communication in a WBAN involves the human personal data. This raises a huge concern about the security of WBAN [6,7]. However, because of limited resources of such medical devices, heavy cryptographic schemes, like Public Key Infrastructure (PKI) [8,9], cannot be used directly in WBAN.

Similarly, there are some schemes which have used predeployment strategies to implement the key agreement and

generation process in WBAN [10,11]. These scheme are also extensively heavy for the tiny sensor nodes used in WBAN, due to their memory and processing limitations [12]. In literature some approaches have properties like, received signal strength (RSS) [13], and human interaction channel [14], that can be used for the key agreement and generation in WBAN. Moreover, few schemes have used fuzzy logic for commitment and key agreement in WBAN [15].

There are schemes that uses biometrics or human physiological data for key agreement and generation process to secure the inter-sensor communication in WBAN [16]. According to [11], the advantage of using the physiological values as a mean for generating the cryptographic keys is that it possess time variant nature and high randomness. Moreover, most of the physiological value-based schemes require no key distribution due to the fact that each sensor is measuring the same physiological values from the same body, while small differences can be eliminated by using some error correction codes. These properties have formed physiological values an attracting choice for key agreement and generation in WBAN [17–20]. The authors in [21] have used an EKG to generate keys for secure intra-WBAN communication. Also, the authors in [22] have 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, which are exchanged between the communicating sensors for the generation of common keys for communication. The scheme in [3], has used set reconciliation-based scheme for key agreement and generation in WBAN. It takes EKG as a mean for generating the keys, while the small differences in the calculations are then reconciled among the communicating nodes in order to agree upon a single common key.

In the aforementioned physiological value-based schemes, few schemes have exchanged the whole feature set between the sensor nodes, that causes an increase in communication overhead. Some of the schemes have used heavy mathematical calculations which tends to have heavy processing overhead. Similarly, some schemes are much heavier in terms of memory consumption. All these properties have made these schemes very difficult to be applicable in a resource constrained networks like, WBAN.

In the first round of the scheme secure cluster formation is achieved by using a pre-deployed master key. Once the cluster formation by using *k-mean* clustering is finalized, the bloom filter-based scheme is further applied on peak points in the EKG signal to achieve maximum randomness. The scheme exchanges only the bit array formed by using the bloom filter as a mean for agreeing upon some common set of values among the cluster members. This reduces the communication overhead as well as the energy consumption of the proposed scheme. The *k-mean* cluster-based communication reduces the communication distance, which reduces the overall communication energy. Moreover, every element of the feature set is represented by a single bit in the bloom filter, which reduces the size of the transformed feature set (bit array). Additionally, another advantage of using the bloom filter for key agreement is that the running complexity or the search complexity is linear, i.e., $O(k)$. These properties of the proposed scheme make it secure and efficient as compared to the schemes discussed earlier. Moreover, only one key is stored in the whole network and is used by all the sensors to perform inter-sensor communication.

3 System model

We assume that WBAN is a network formed by sensor nodes attached to the human body, having the ability of measuring the human physiological values (PVs). These sensor nodes are ordinary resource constrained devices having limited memory, power and energy. We also assume that all sensor nodes and PS of the WBAN are synchronized. Furthermore, we assume that PS is a powerful sensor node which has high power, memory, and energy resources. A typical WBAN scenario is shown in Fig. 1, where the black circles represent the ordinary physiological measuring sensors, while a personal digital assistance (PDA) like device represents the PS.

3.1 Bloom filter

Bloom filter is a data structure having the ability of efficient and quick data searching [4], while using hash functions as a mean for data size reduction and security. The advantage of using bloom filter is that it can store large amount of data in a very small space, and also can efficiently check for the membership of the elements i.e., search for elements. A bloom filter is basically a bit array of 'm' bits that can easily check a finite set consists of 'n' elements for the membership of an element, i.e., whether the element is on the list or not. Bloom filter reduces the size of the data by reconstructing the data elements in to more manageable bits in the form of a bit array. This reconstruction using hash functions make the communications secure, this is because it requires proper authentication. Consequently, if an attacker node by any mean captures the data during the communication, the attacker will be unable to decrypt the hashed data due to the irreversible properties of the hash functions. The process is depicted in Fig. 2.

Where el_1, el_2, and el_n represents the feature set element number 1, 2 up to n, respectively. Similarly, $h_1(.)$, $h_2(.)$ up to $h_n(.)$ represents the corresponding hash functions.

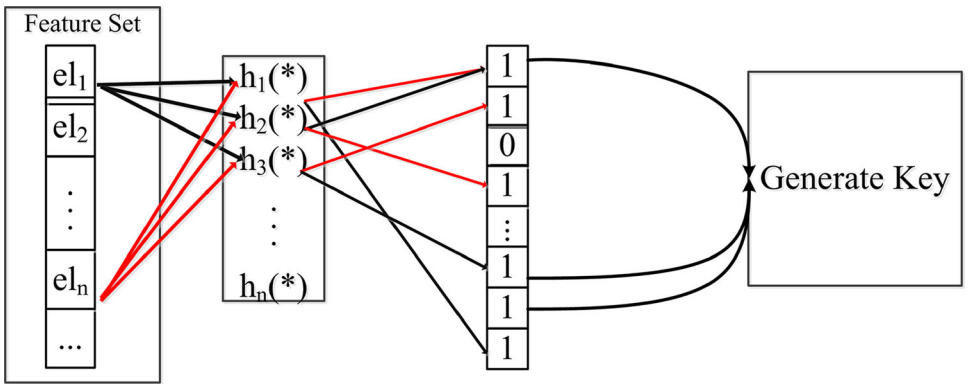


Fig. 2 Bloom-filter

4 Proposed scheme

Using the bloom filter as a mean for agreeing the nodes upon a single common key, we proposed a bloom filter-based key agreement scheme for WBANs. The proposed scheme has three main steps i.e., feature extraction and quantization, clustering mechanism, and a bloom filter-based EKG key agreement Scheme. Below each step is described in detail.

4.1 Feature extraction and quantization

In the feature extraction and quantization phase, each node in the WBAN extracts the physiological features from the EKG signal obtained from the human body. The signal is collected at a specific sampling rate and time duration, and then a discrete wavelet transform (DWT) is applied on the collected data. In order to extract the peaks from the collected data, it is passed through a peak detection mechanism. Once the peaks are finalized, each of the peak value along with the index pair is quantized for the formation of a feature set $FS = FS^1, FS^2, FS^3, , FS^n$, where FS^n represents the concatenated peak value and peak index pair of element 'n', and 'n' is the size of the feature vector.

4.2 Clustering mechanism

The *k-means* is an unspervised learning algorithm that has been used in literature to solve the clustering problem.The algorithm is used to classify a given set of sensor nodes through a certain number of clusters. The set of senor nodes is partitioned into k clusters using Euclidean distance mean, this results the maximization of intra-cluster similarity and the minimization of inter-cluster similarity. The *k-means* clustering algorithm [23] is iterative in nature and follows the steps given below:

Let $X = x_1, x_2, x_3, \ldots, x_n$ be the sensor nodes and $Z = z_1, z_2, z_3, \ldots, z_n$ be the set of centers

Step 1 Select cluster center 'c' randomly

Step 2 compute the Euclidean distance between each sensor node and cluster centers using the Eq. 1.

$$Dist(X_i, Z_i) = \sqrt{\sum_{i=1}^{n}(x_i - z_i)^2} \tag{1}$$

Step 3 Assign each sensor node to the cluster center whose distance is minimum to the cluster center in all cluster centers.

Step 4 Recalculate the new cluster center using Eq. 2

$$Z_i = (1/C_i)\sum_{i=1}^{C_i} x_i \tag{2}$$

where 'C_i' represnet the number of sensor nodes in the ith cluster.

Step 5 Recalculate the distance between each sensor node and newly obtained cluster centers.

Step 6 If no sensor node was reassigned then stop ,otherwise repeat step 3.

The following Fig. 5 shows the two clusters formed for a set of 16 sensor nodes using *k-means* cluster algorithm. The algorithm is fast, robust and easier to understand as discussed earlier. Also, the algorithm is relatively efficient and consumes less energy O(tknd), where n is the number of objects, k is the number of clusters, d is the dimension of each object and t is the iteration.

4.3 A bloom filter-based EKG key agreement scheme

A bloom filter-based key agreement scheme is proposed for healthcare system using wireless body area networks. In the proposed scheme, when the sensor node wants to communicate with PS, it will first agree up on a single common key with the PS. The sensor node will first calculate the EKG values from the human body and then extract the features from the collected physiological signal. After performing the quantization, the sensor node will apply the bloom filter on

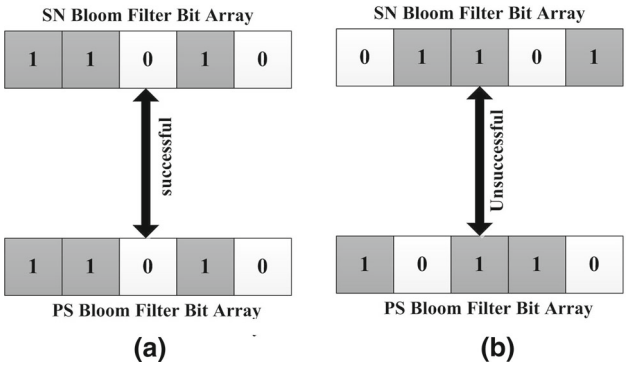


Fig. 3 Bit arrays comparison

the quantized blocks, and the filter will be stored as a bit array on the sensor node. Furthermore, the sensor node sends this bit array to the personal server for confirmation i.e., whether the array calculated on the PS are the same or not. In order to preserve privacy the array is exchanged using MAC. It is worth mentioning here, that the PS and sensor nodes resides on same body and are synchronized, so each sensor node calculate similar physiological values from the human body [1,3]. Moreover, when the PS receives the sensor nodes bit array, it calculates its own version of the feature set from the same EKG signal simultaneously. After that the PS apply the bloom filter on the quantized blocks, stores the filter as a bit array. However, for verification purpose, to check whether the received bit array and that calculated by the PS are similar or not, the PS performs a membership check function by using hash comparison. Once this is confirmed that the bit arrays calculated at the PS and sensor node are the same, then comes the final key generation step. In the proposed scheme the actual data is not exchanged during the key agreement process, rather bit arrays are exchanged. This reduces the communication overhead and energy consumption, as well as strengthen the security of the scheme by not exposing the actual data in the communication process.

Once the comparison is successful the PS then broadcast a keygen message to all the sensor nodes. Upon receiving the keygen message all the sensor nodes generate the key from the same quantized blocks. While in case if the comparison is unsuccessful, the PS directs all the sensor nodes to recalculate the EKG signal and the whole process is repeated. This exchange and hash bit array comparison process for both successful and unsuccessful bit arrays are shown in Fig. 3a, b, respectively, while the whole key agreement and generation process is depicted in Fig. 4.

4.3.1 Challenge response based authentication

To secure the wireless communication in WBAN, the nodes must be authenticated before communicating the human personal data. This will mitigate and deny the attacks like, replay and denial-of-service attack. For this purpose the proposed scheme uses a challenge response-based authentication mechanism to distinguish between the legitimate sensor nodes and the attackers.

The authentication process is shown by two simple messages communicated between the sensor nodes and the PS of the WBAN. In msg_1, the PS of the WBAN broadcasts a 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.

$$msg_1 : PS \rightarrow * : MACK_{PS,SN_i}(ID_{PS}, C, nonce)$$

$$msg_2 : SN_i \rightarrow PS : MACK_{PS,SN_i} (ID_{SN_i}, ID_{PS}, C, nonce)$$

In msg_2 every sensor node reply to the PS by encrypting it with the same key K_{PS,SN_i} , its own version of the challenge C , and nonce. The communicating sensors share the same human body i.e., both sender and receiver sensors are located on the same body. The key generated at a particular time from the EKG of a particular person will be the same, this is because it is generated from the same EKG signal of the same human body in a synchronized environment. 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.

4.3.2 Cluster member joining and leaving

The node joining and leaving is very rare in a WBAN due to their fixed position on the body. The nodes can only leave or join when nodes are replaced due to energy depletion or performs malfunctions. Moreover, due to the small size of the WBAN, joining and leaving will not affect the scheme, because every node in the network is directly connected to the cluster head. When a node is place or replaced in a WBAN, the newly joined node will send a hello message to the cluster head. Then the cluster head and the node will start measuring the EKG signal in a synchronized manner. After that the key agreement and generation process described above will take place. Once both the cluster head and sensor node agree upon a single common key, the cluster head authenticates the node by using the challenge-response-based authentication mechanism described above. Upon successful authentication, the node is added to the list of WBAN nodes; otherwise, the node is rejected by the cluster head, and the cluster head broadcasts the ID of the node

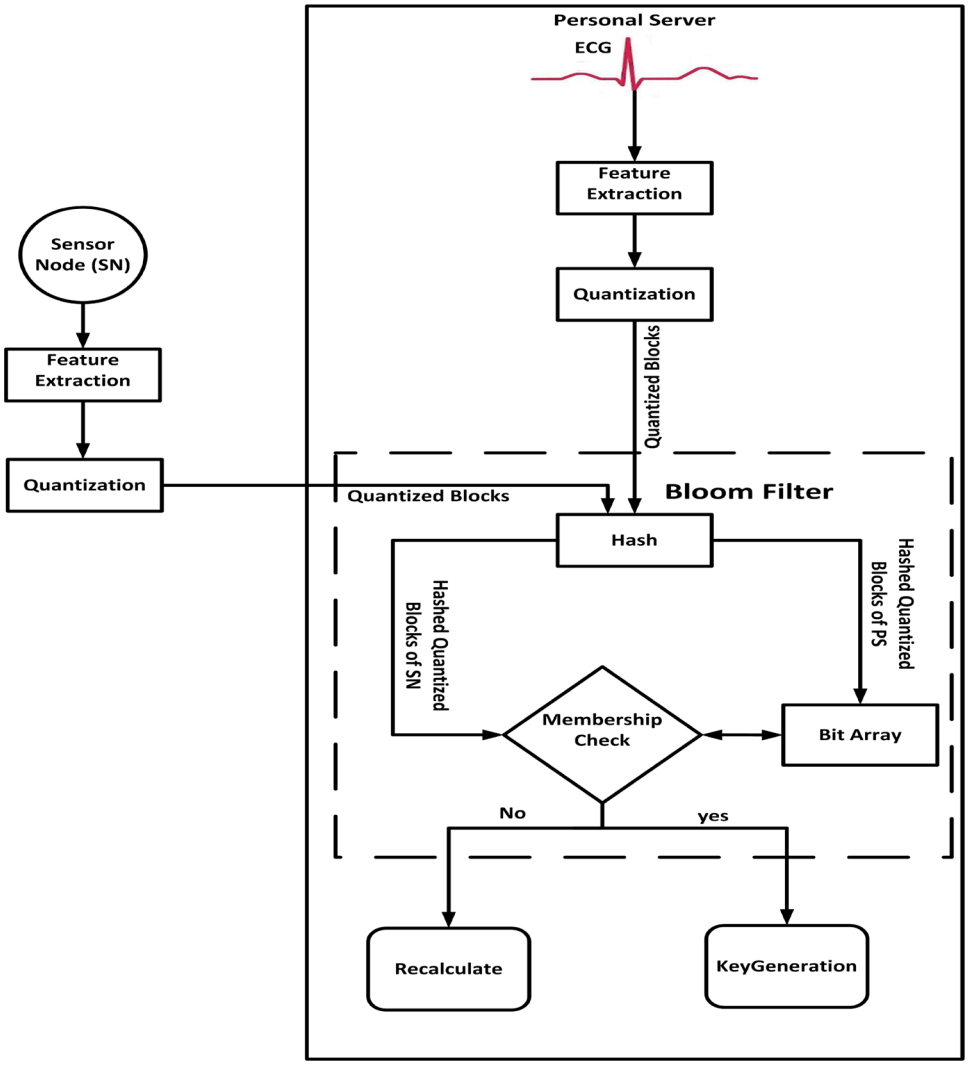


Fig. 4 Proposed key agreement scheme

to the other cluster members claiming that the node is an attacker.

If a node leaves the WBAN for any reason, like a failure, power shortage, or malfunction, the cluster head 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 moved from the network. The cluster head removes the node from its list and broadcasts a message to the whole network that the particular node has left the network.

4.3.3 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 common 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 bloom filter-based key agreement process to generate a new common key.

5 Results and analysis

This section provides the experimental setup, and analysis on the evaluation of experimental results.

5.1 Experimental setup

For experiments and analysis the EKG data for 30 different persons' are taken from MIT PHYSIO BANK [24]. The simulation is performed in UBUNTU version 12.04 LTS and MATLAB version 7.0.1 for 2, 4, 8, and 10 nodes respectively. In the simulations both the hardware settings and environments are kept the same for proposed scheme and

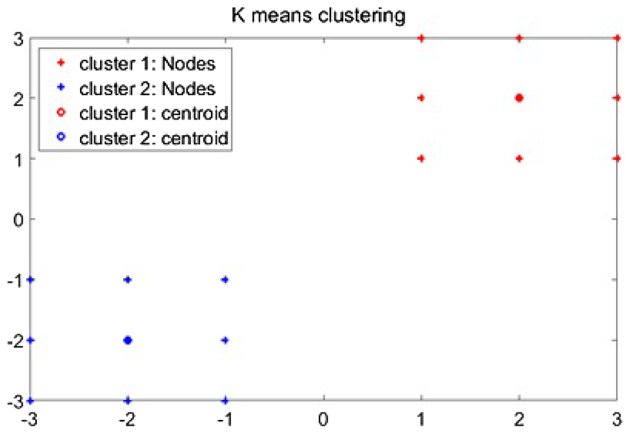


Fig. 5 Cluster formation in WBAN

set reconciliation-based scheme [3], as both the schemes are simulated on an Intel (R) Core (TM) i5 system with and 8GB RAM and Windows 7 Professional.

5.2 Analysis and discussion

In this subsection, the proposed bloom filter-based key agreement scheme is analyzed in terms of running complexity, false positive rate (FPR), memory consumption, and energy consumption. The proposed scheme is tested for the aforementioned parameters by increasing the number of nodes in the WBAN.

5.2.1 Cluster formation

The *k-means* clustering algorithm is used for cluster formation in WBAN. The scheme first select the centroid which acts as a cluster head. The remaining nodes are examined in terms of Euclidean distance to the cluster mean, and are allocated to the closest cluster. This can be seen in Fig. 5, where two cluster heads are selected on the basis of Euclidean distance, while the rest of the nodes are allocated to the best suitable cluster.

5.2.2 Security analysis

Due to the wireless communication involvement in the WBAN key agreement process, it is susceptible to some attacks. For example an attacker can launch a replay attack by sniffing some packets during the communication, and injecting duplicate copies of the packets. To remedy this situation, the proposed scheme discards the replayed packets; because the key is refreshed in the network after a predefined time. This key cannot be generated by the attackers, there are several reasons to support this statement. First, the attacker cannot measure the EKG values accurately without having contact with the subject body. Secondly, the generation of new key require proper authentication from the PS in the network. Due to these restrictions a node will be unable to participate in the key agreement process illegitimately.

Similarly, an attacker can launch denial-of-service (DoS) attack by sending excessive packets to the PS in a short time interval. To participate in the network the proposed scheme first authenticate the node in order to check the legitimacy of the node. This authentication makes it difficult for a node to perform DoS attack. This is because every packet sourced by an unauthentic node will be dropped by the proposed scheme.

For the sake of usability and applicability of the proposed scheme, it is analyzed in terms of false positive rate (FPR). FPR is the percentage of incorrectly identified bits in a bloom filter, i.e., those bits which are not present in the bloom filter, but when asked for the membership the scheme erroneously identify it as member bits. The identification of these bits will show how much the scheme is applicable and adaptable in a crucial healthcare application. For example, if the scheme erroneously identifies high amount of bits as member bits, this will lead to a scenario where anyone will be able to generate the key from similar EKG data. This scenario will provide unauthorized access to the WBAN, and will eventually create a security loophole. The FPR of bloom filter is dependent on the value of 'k' and 'm' and can be calculated by the following equation:

$$FPR = (1 - e^{-kn/m})^k \tag{3}$$

where ' k' represents the number of hash functions, 'm' is the number of bits required for the bloom filter, and n is the total number of elements. As evident from Eq. 3, increasing the value of 'k' will decrease the FPR value, but increasing the number of hash functions (i.e., k) will increase the processing overhead of the scheme. Similarly, increasing the number of bits for the bloom filter will cost memory consumption. Hence, the scheme should use optimal values for both ' k ' and ' m '; in order to get maximum applicability and usability in such constrained environment.

The proposed scheme is compared with the set reconciliation based scheme [3] in terms of FPR and number of nodes. Taking a 5 s ECG window yields a 2 kb (kilo byte) feature set after applying discrete wavelet transform for feature extraction. In simulations keeping the number of hash functions as 3, and number of bits 7158.3351, we get the FPR as low as 0.007. In Fig. 6, we can see that for set reconciliation based scheme increasing the number of nodes in the network increases the FPR, this is because when the number of nodes increases in the network, then the number of differences in the feature set for key generation also increases. This reduces the performance of set reconciliation-based scheme. It is evi-

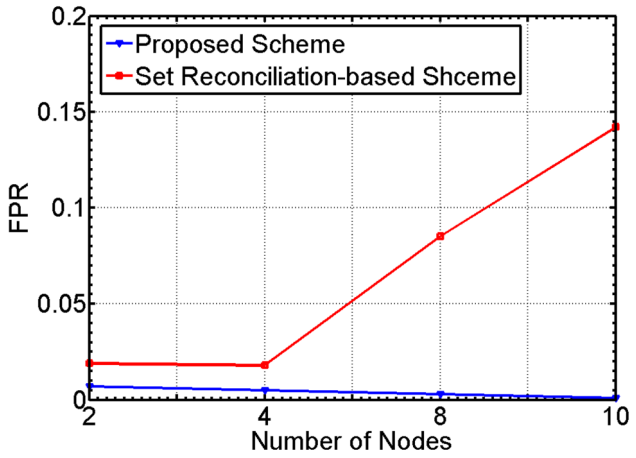


Fig. 6 FPR comparison of the proposed scheme and set reconciliation-based scheme

dent from Fig. 6, that increase in the network size does not affect the performance of the proposed scheme, because the scheme is not exchanging the features, rather it is communicating the bit array.

Randomness To check the randomness, DIEHARDER [25] testing suite is applied on the generated keys from the ECG data. The decision rule in this scenario says that a test is considered failed if it outcomes a P value less than or equal to 0.0001 or greater than or equal to 0.9999. As we can see from Table 1, that all the P values generated by the DIEHARDER testing suite successfully passes the above mention
criteria.

5.3 Asymptotic complexity

Similarly, the set reconciliation-based scheme uses the scheme in [26] for key agreement between the nodes. The nodes reconcile the differences between the elements of their individual feature sets. Table 2 shows the asymptotic complexity of proposed and set reconciliation-based scheme. The proposed scheme is better than the set reconciliation-based scheme in terms of running complexity, the proposed scheme has a linear complexity compared to the cubic complexity of the set reconciliation-based scheme.

5.4 Memory consumption

The proposed scheme is also compared to the set reconciliation based scheme in terms of memory overhead. It can be observed from Fig. 7, that the proposed scheme is more efficient in memory consumption than the set reconciliation-based scheme. This is because the proposed scheme uses a single bit representation for every element of the feature set. While in contrast the set reconciliation-based scheme uses the complete bits (i.e., 8 bits for integer values) to store each element.

5.5 Communication overhead

The communication overhead is calculated for two scenarios, i.e., when both the sensors have 50% differences in their respective feature sets, and when the feature sets are totally different from each other, as depicted in Fig. 8. As feature sets are calculated from the EKG signal of the human body, the differences can occur while different sensors calculate the same EKG signal. These differences can be due to the noise, or even distance from the heart location can also affect the readings of EKG. When the differences in the feature sets are 50%, then the set reconciliation scheme has to at least reconcile half of the set elements. Similarly, in the worst case scenario, when the sets are totally different from each other the set reconciliation-base scheme will have to reconcile the whole feature set, which increases the communication overhead. While the proposed scheme for 50% differences only exchanges the bit array created for only half of the elements, where each element is represented as a single bit. Similarly, in case of hundred percent mismatch of the feature set, the proposed scheme only exchanges the bit array for the whole set. This bit array representation hugely reduces the communication overhead of the proposed scheme.

5.6 Energy consumption

As the energy consumption of a node is mainly dependent on the sending and receiving of information. According to [27], the Chipcon CC1000 radio have used in Crossbow MICA2DOT motes consumes 28.6 and 59.2 J of energy to send and receive 1 byte of data, respectively. Using these parameters, the energy consumption for the proposed and set reconciliation-based scheme are calculated for two scenarios, i.e., when there are 50% differences in the elements of the feature set, and when the difference is 100% (Worst case). It can be seen in Fig. 9, that the proposed scheme again outperform the set reconciliation-based scheme. This is because when the differences in the feature set increases the set reconciliation based scheme will use the whole feature set to be exchanged in the key agreement process, while in case of the proposed scheme it will represent the elements as bit array and will exchange it with the other communicating party.

The above results and discussions show that the proposed scheme is very efficient in terms of memory utilization, energy consumption, and communication overhead. This is because the proposed scheme is using the reduced sized bit arrays as a mean for exchanging the information between the communicating nodes. Moreover, the bit arrays exchange

Table 1 DIEHARDER testing suite results for ECG generated keys

Test name	ntup	t-sample	p-sample	Average P-value of 25 keys	Assessment
diehard_birthdays	0	100	100	0.5850	Passed
diehard_operm5	0	1,000,000	100	0.5248	Passed
diehard_rank_32x32	0	40,000	100	0.5872	Passed
diehard_rank_6x8	0	100,000	100	0.6201	Passed
diehard_bitstream	0	2,097,152	100	0.4804	Passed
diehard_opso	0	2,097,152	100	0.5831	Passed
diehard_oqso	0	2,097,152	100	0.5341	Passed
diehard_dna	0	2,097,152	100	0.5125	Passed
diehard_count_1s_str	0	256,000	100	0.6038	Passed
diehard_count_1s_byt	0	256,000	100	0.4435	Passed
diehard_parking_lot	0	12,000	100	0.4938	Passed
diehard_2dsphere	2	8000	100	0.6279	Passed
diehard_3dsphere	3	4000	100	0.6058	Passed
diehard_squeeze	0	100,000	100	0.6005	Passed
diehard_sums	0	100	100	0.1411	Passed
diehard_runs	0	100,000	100	0.6030	Passed
diehard_craps	0	200,000	100	0.6838	Passed
marsaglia_tsang_gcd	0	10,000,000	100	0.6413	Passed
sts_monobit	1	100,000	100	0.5536	Passed
sts_runs	2	100,000	100	0.5940	Passed
sts_serial	1–16	100,000	100	0.4243–0.6740	Passed
rgb_bitdist	1–12	100,000	100	0.4389–0.6479	Passed
rgb_minimum_distance	2–5	10,000	1000	0.4389–0.6479	Passed
rgb_permutations	2	100,000	100	0.5614	Passed
rgb_permutations	3	100,000	100	0.3263–0.5347	Passed
rgb_permutations	4	100,000	100	0.6214	Passed
rgb_permutations	5	100,000	100	0.5614	Passed
rgb_lagged_sum	0–32	1,000,000	100	0.6180	Passed
rgb_kstest_test	0	10,000	1000	0.6215	Passed
dab_bytedistrib	0	51,200,000	1	0.5251	Passed
dab_dct	256	50,000	1	0.4207–0.7372	Passed
dab_filltree	32	15,000,000	1	0.5327	Passed
dab_filltree	32	15,000,000	1	0.4843	Passed
dab_filltree2	0	5,000,000	1	0.4114	Passed
dab_filltree2	1	5,000,000	1	0.5766	Passed
dab_monobit2	12	65,000,000	1	0.5327	Passed

Table 2 Running complexity analysis

Schemes	Running complexity
Set reconciliation based scheme	$O(d^3)$
Proposed scheme	$O(k)$

between the communicating nodes is made secure by using the hash functions, which increases the security of the whole key agreement process and makes it difficult for an attacker to get the information about the key. The communication overhead and energy consumption comparison of the proposed scheme and set reconciliation-based key agreement

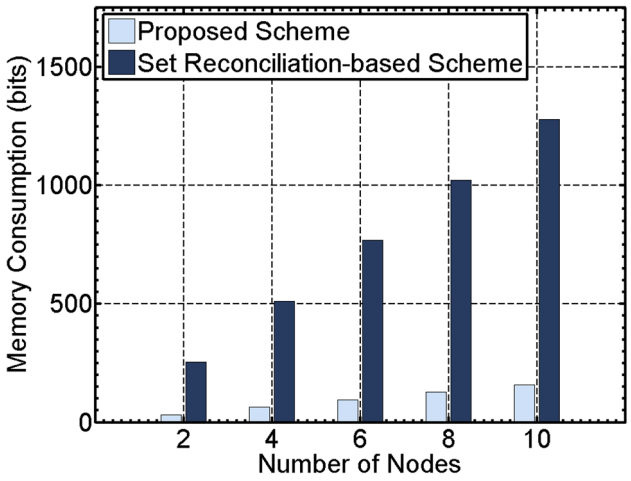


Fig. 7 Memory overhead

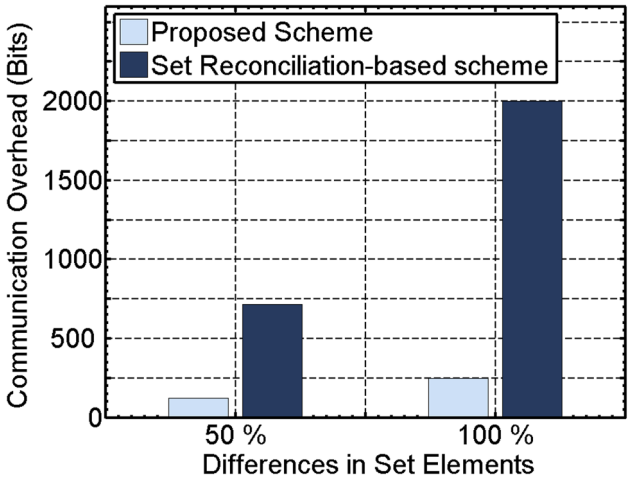


Fig. 8 Communication overhead

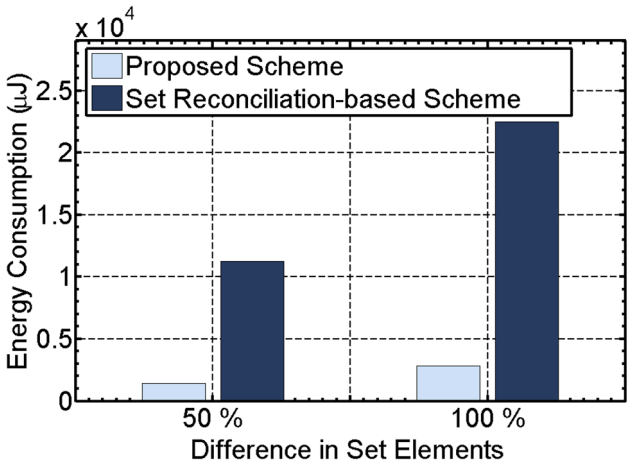


Fig. 9 Energy consumption analysis

scheme show the applicability and its suitability for applications where network connectivity and life time is of high importance. Similarly, memory consumption and running complexity are critically important in applications where tiny sensor devices are used for monitoring such as healthcare. It is evident from all the results and comparisons that the proposed scheme performs much better than the set reconciliation-based key agreement scheme.

6 Conclusion

Security and privacy concerns put a huge impact on the usability and applicability of any remote healthcare system. This is because the wireless communication in remote healthcare systems involves the human personal data that makes such systems more security conscious. Exchanging excessive information during the key agreement process itself is a security risk. The proposed bloom filter-based key agreement scheme uses very less information exchange during the key agreement process, this is because each member of the feature set is represented by a single bit in a bloom filter bit array, and that list is further exchanged. The proposed scheme mitigates denial-of-service and replay attacks by using bloom filter-based key agreement and authentication mechanism. Our proposed scheme shows very prominent results as compared to the set reconciliation-based key agreement scheme in terms of security and privacy, false positive rate (FPR), running time complexity, memory overhead, and energy consumption.

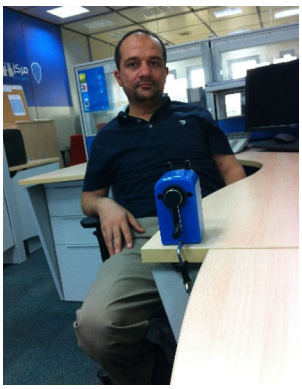
Acknowledgements The authors appreciate financial support from KSU deanship of scientific research represented by the research chair of Enterprise Resource planning and business process management.

References

1. Venkatasubramanian, K., Gupta, S.K.S.: Security for pervasive health monitoring sensor applications. Proceeding of the 4th International Conference Intelligent Sensing & Information Processing. Bangalore pp. 197–202 (2006)
2. Yong, W., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutor. **8**, 2–23 (2006)
3. Ali, A., Khan, F.A.: A broadcast-based key agreement scheme using set reconciliation for wireless body area networks. J. Med. Syst. **38**(5), 1–12 (2014)
4. Bloom, B.H.: Space/time trade-offs in Hash coding with allowable errors. Comm. ACM **13**(7), 422–426 (1970)
5. 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 (2004)
6. Kumar, P., Lee, H.J.: Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors **12**, 55–91 (2011)

7. Selimis, G., Huang, L., Mass, F., Tsekoura, I., Ashouei, M., Catthoor, F., et al.: lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design. J. Med. Syst. **35**, 1289–1295 (2011)
8. Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C.: Talking to strangers: authentication in ad-hoc wireless networks, Proceeding of the Network and Distributed System Security Symposium, San Diego, pp. 1-13 (2002)
9. Sampangi, R.V., Saurabh, D., Urs, S.R., Sampalli, S.: A security suite for wireless body area networks. Int. J. Netw. Secur. Appl. (IJNSA) **4**, 97–116 (2012)
10. He, D., Chen, C., Chan, S., Bu, J., Zhang, P.: Secure and lightweight network admission and transmission protocol for body sensor networks. IEEE J. Biomed. Health Inform. **17**(3), 664–674 (2013)
11. Hu, C., Zhang, N., Li, H., Cheng, X., Liao, X.: Body area network security: a fuzzy attribute-based signcryption scheme. IEEE J. Sel. Areas Commun. **31**(9), 37–46 (2013)
12. Ali, A., Khan, F.A.: Key agreement schemes in wireless body area networks: taxonomy and state-of-the-art. J. Med. Syst. **39**, 115 (2015)
13. Wu, Y., Sun, Y., Zhan, L., 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)
14. Xin, H., Bangdao, C., Markham, A., Qinghua, W., Zheng, Y., Roscoe, A.W.: Human interactive secure key and identity exchange protocols in body sensor networks. IET Inf. Secur. **7**(1), 30–38 (2013)
15. Juels, A., Sudan, M.: A fuzzy vault scheme, Proceeding of the International Symposium Information Theory, IEEE, Lausanne pp. 408 (2002)
16. Cherukuri, S., Venkatasubramanian, K.K., Gupta, S.K.S.: Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, Proceeding of the Parallel Processing Workshops, Kaohsiung, pp. 432–439 (2003)
17. Ali, A., Khan, F.: An improved EKG-based key agreement scheme for body area networks, Proceeding of the 4th International Conference on Information Security and Assurance (ISA 2010). Miyazaki, Japan, CCIS, vol. 76, pp. 298–308 (2010)
18. Ali, A., Irum, S., Kausar, F., Khan, F.: A cluster-based key agreement scheme using keyed hashing for Body Area Networks. Multimed. Tools Appl. **66**, 201–214 (2013)
19. Orlitsky, A.: Worst-case interactive communication. I. Two messages are almost optimal. IEEE Trans. Inf. Theory **36**(5), 1111–1126 (1990)
20. Venkatasubramanian, K.K., Gupta, S.K.S.: Physiological value-based efficient usable security solutions for body sensor net- works. ACM Trans. Sens. Netw. **6**, 1–36 (2016)
21. Irum, S., Ali, A., Khan, F.A., Abbas, H.: A hybrid security mechanism for intra-WBAN and inter-WBAN communications. Int. J. Distrib. Sens. Netw. **2013**, 11 (2013)
22. Ali, A., 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)
23. Kanungo, T., Mount, D.M., Netanyahu, N.S., Piatko, C.D., Silverman, R., Wu, A.Y.: An efficiant kÅmeans clustering algorithm: analysis and implementation. IEEE Trans. Patern. Anal. Mach. Intell. **24**, 881–892 (2002)
24. MIT PhysioBank.: http://www.physionet.org/physiobank/database/ecgiddb/. Accessed 24 Nov 2016
25. Brown, R.G.: Dieharder: a random number testing suite, http://www.phy.duke.edu/rgb/General/dieharder.php. Accessed 1 Nov 2016
26. Minsky, Y., Trachtenberg, A., Zippel, R.: Set reconciliation with nearly optimal communication complexity. IEEE Trans. Inf. Theory **49**, 2213–2218 (2003)
27. Wander, A.S., Gura, N., Eberle, H., Gupta, V., Shantz, S.C.: Energy analysis of public-key cryptography for wireless sensor networks, Proceeding of the Pervasive Computing and Communications, PerCom 2005, Kauai, pp. 324–328 (2005)

Saleh M. Al-Saleem Associate Professor in College of Computer and Information Science, King Saud University. He received his PhD from Wayne State University, Michigan, USA, 2001, in the field of computer science (Evolutionary Computation). He received his Master degree in computer science from Ball State University, IN, USA 1996, and His BS degree in computer science from College of education, King Saud University, Saudi Arabia 1991. He served as the dean of admission & registration in Shaqra University, and also served as the head of IT and e-Learning in Shaqra University. Previously he worked as head of Information Technology department at the Arab Open University, and before that he worked as the head of Computer Technology department and faculty member in Riyadh College of Technology. Dr. Al-Saleem current research interests includes: evolutionary computation, Text Classification, ERP, BPM, e-Learning, and Open Source.



Aftab Ali received his MS and PhD degrees in Computer Science from National University of Computer and Emerging Sciences, Islamabad, Pakistan in 2009 and 2015 respectively. He is currently working as an information security consultant in the computerized testing department at National Center for Assessment (NCA), Riyadh, Saudi Arabia. Prior to joining NCA, Dr. Ali worked as Researcher at the Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia. Dr. Ali is a Technical Program Committee Member and reviewer for several international journals and conferences. His research interests include Wireless Body Area Networks, Key Management, Cyber Physical Systems security, E-Health, and Cloud Computing.

Naveed Khan received his B.Sc. degree in Computer Science in 2006 from Hazara University, Pakistan, and M.S degree in Computer Science in 2012 from King Saud University, Saudi Arabia. In September 2012, He joined the Department of Computer Science at King Saud University, Saudi Arabia as a Research Assistant and started working on Wireless Body Area Networks. Currently, He is doing his PhD degree in the field of Computer Science from the School of Computing and Information Engineering, Ulster University, Northern Ireland, UK. His current area of research is change detection in health sensor data.