EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications

Aftab Ali[1] and Farrukh Aslam Khan[1,2*]

Abstract

Wireless body area networks (WBANs) are formed by using tiny health monitoring sensors on the human body in order to collect and communicate the human personal data. WBANs serve as a solution to facilitate the tasks performed in the medical sector, and minimize the chances of errors during the process of medical diagnosis. Due to the unreliable wireless media, the communication in a WBAN is exposed to a variety of attacks. These attacks pose major threats to WBAN security. In order to overcome these threats, several cryptographic techniques have been proposed in the recent past. Effectiveness of these cryptographic techniques largely depends on a good key management scheme. However, using an expensive key management scheme is not feasible in highly resource-constrained WBANs. Therefore, we propose and evaluate an energy-efficient key management scheme for WBANs that takes into account available resources of a node during the whole life cycle of key management. Our proposed scheme is a cluster-based hybrid security framework that supports both intra-WBAN and inter-WBAN communications. By using multiple clusters, energy-efficiency can be ensured. The cluster formation process itself is secured by using electrocardiogram (EKG)-based key agreement scheme. The proposed technique is hybrid because we use both preloading of keys and physiological value-based generated keys. We use highly dynamic and random EKG values of the human body for pairwise key generation and refreshment. The performance comparison of our proposed cluster-based key management scheme and low-energy adaptive clustering hierarchy (LEACH)-based key agreement scheme shows that the proposed scheme is secure, more energy-efficient, and provides better network lifetime.

Keywords: Wireless body area networks (WBANs); Energy-efficiency; Key management; Clustering

1 Introduction

Wireless body area network (WBAN) is a special kind of network, which is formed by putting the biometric sensors on the human body. In other words, a human body wearing the biometric sensor clothes forms the WBAN [1]. Due to resource limitations, WBANs need a number of sensor nodes to collect physiological data from the body of its wearer in a safe and secure manner. Each WBAN also contains a single centralized entity called personal server (PS), which gathers data from the sensor nodes using multi-hop communication. The PS acts as a gateway between the body on which it resides and the outside world. There are two types of communications in WBANs; intra-WBAN communication, and inter-WBAN communication. The on-body communication among the sensor nodes is called intra-WBAN communication. Inter-WBAN communication occurs between PSs residing on two or more bodies, i.e., WBANs.

The applications of WBANs include the monitoring of human health remotely. In this type of application, the health monitoring sensors are implanted on the human body. These sensors collect personal data from the host body and send it to remote medical servers located in the hospital. Similarly, inter-WBAN communication can be applied to the health monitoring system, for example, monitoring the health of patients while they are doing their normal routine work (i.e., somewhere in market, home, office, or even in the playground). In this case, WBANs (sensor-clothed bodies) will be scattered and

*Correspondence: fakhan@ksu.edu.sa
[1]National University of Computer and Emerging Sciences, A. K. Brohi Road, H-11/4 Islamabad 44000, Pakistan
[2]King Saud University, Riyadh 11653, Saudi Arabia

the sink or remote base station (RBS) will not always be in their range. Therefore, WBANs must cooperate with one another using hop-by-hop communication in order to reach the RBS (sink), and the RBS further communicates with the medical server (MS) through the internet. Another application scenario of inter-WBAN communication could be monitoring the health of soldiers in a battlefield. After deployment, nodes that are far away from the RBS, located in a safe zone, will have to communicate in a hop-by-hop fashion in order to reach the RBS. In this scenario, the nodes (WBANs) act as routers to forward data to the RBS. In both the applications, the WBAN (single human body) may not always be in the range of the remote MS or the RBS. So, along with intra-WBAN communication, there is a need for inter-WBAN communication in order to deliver data to the destination, i.e., through PS to MS. Securing intra-WBAN and inter-WBAN communications means securing the human lives because both kinds of communications involve the human personal data to be delivered to the medical server. Hence, the security of WBANs is essential.

WBANs are composed of small sensors that have limited memory and power sources. For such a special network, security, energy, and other requirements differ from ordinary wireless sensor networks (WSNs). The security protocols designed for WSNs cannot be applied to WBANs due to their energy and storage constraints. Moreover, the key management protocols for WSNs will not work as efficiently as the protocols specifically designed for WBANs [2,3], e.g., public key-based protocols will be computationally expensive to use in WBANs [4]. There are some symmetric key management strategies for secure trust establishment in WSNs, e.g., pre-deployment-based key management, communication-based key management, and public key-based key management schemes. Each of these schemes has its own limitations, e.g., limited memory, authentication from a centralized authority, and complex mathematics [5]. Table 1 summarizes the differences between WBANs and WSNs.

In this paper, we propose a secure cluster-based key management scheme for both intra-WBAN and inter-WBAN communications. In intra-WBAN communication, we use physiological value (PV)-based solution for establishing trust among sensor nodes. PV is a stimulus from human body, which is used for generating pairwise keys. The advantage of PV-based solution is that the generated keys on both sender and receiver sides are the same, because both the sender and the receiver use the same PVs for generating the key. We use electrocardiogram (EKG) as a PV to generate pairwise keys in intra-WBAN communication, which eliminates the key distribution process [5,8-10]. Due to the highly dynamic nature of the human body, it produces time-variant PV, i.e., EKG, which results in addition and removal of nodes without rekeying [11]. In intra-WBAN communication, the cluster formation is done on the basis of residual energy and distance [12]. The leader solicitations are made secure to avoid sinkhole-like attacks by using secure cluster formation using EKG-based keys. For secure cluster formation and exchange of EKG blocks in intra-WBAN communication, we use EKG-based generated pairwise keys using keyed-hashing digest. Keyed-hashing message authentication code (HMAC-MD5) [13] ensures the authenticity and integrity of the EKG blocks exchange process between communicating sensors in intra-WBAN communication. Securing communication among the sensors is done in two steps. In the first step, trust is established between the sensors, and in the second step, data communication is carried out on the basis of that trust. Trust establishment is the process of agreeing upon a common key for secure communication [14]. While in inter-WBAN communication, secure cluster formation and communication is done through preloaded pool of keys. The reason of using preloading-based keys is that existing PV based key management schemes of WBANs are designed by keeping in mind the characteristics of intra-WBAN communication, i.e., these networks are small in size and scale, and the communication is done over a single body. Whereas, in inter-WBAN communication, the communication involves two or more bodies (WBANs), therefore, EKG-based scheme cannot be applied in this case. Moreover, in inter-WBAN communication, the security requirements are totally different from those of intra-WBAN communication e.g., there is an additional risk of physical attacks in inter-WBAN communication such as node capture, tampering, as well as unknown pre-deployment network topology etc.

An important requirement of inter-WBAN communication is the efficiency of energy, which increases the lifetime of a network. For this purpose, we use an energy-efficient secure cluster formation technique in inter-WBAN communication. The PS acts as a single node and represents the whole WBAN in inter-WBAN communication. To communicate multiple WBANs, only the PS will communicate with another PS and will choose one PS as a cluster head (CH). For example, consider three WBANs A, B, and C having personal servers PS1, PS2, and PS3, respectively. Now if A wants to communicate with B or C, it will communicate through PS1 to PS2 or PS3 and the ordinary sensor nodes on A, B, and C will not take part in inter-WBAN communication. Our technique for clustering in inter-WBAN communication is based on the residual energy of the PS and the distance between PSs of two communicating WBANs. We use a pool of keys and then randomly select some keys from that pool. These randomly selected keys from CH are assigned to cluster members (CMs) in the pre-deployment phase.

Table 1 Difference between WBANs and WSNs [6,7]

Challenges	Wireless sensor network	Wireless body area network
Scale	Monitored environment (meters/kilometers)	Human body (centimeters/meters)
Number of nodes	Many redundant nodes for wide area coverage	Fewer, limited in space
Result accuracy	Large number of nodes provide accuracy	Few nodes, need to be robust and accurate
Node tasks	Node performs a dedicated task	Node performs multiple tasks
Node size	Small is preferred, but not important	Small is essential
Network topology	Very likely to be fixed or static	More variable due to body movement
Data rates	Most often homogeneous	Most often heterogeneous
Node replacement	Performed easily, nodes are even disposable	Replacement of implanted nodes is difficult
Node lifetime	Several years or months	Several years or months, smaller battery capacity
Power supply	Accessible and can be replaced easily and frequently	Inaccessible and difficult to replace in an implantable setting
Power demand	Likely to be large, energy supply easier	Likely to be lower, energy supply more difficult
Energy scavenging source	Most likely solar and wind power	Most likely motion (vibration) and thermal (body heat)
Biocompatibility	Not a consideration in most applications	A must for implants and some external sensors
Security level	Lower	Higher to protect personal information
Impact of data loss	Likely to be compensated by redundant nodes	More significant, may require additional measures to ensure QoS and real-time data delivery
Wireless technology	Bluetooth, ZigBee, GPRS, WLAN, etc.	Low power technology required
Key management support from application	No	Yes, sensor nodes not required to generate random numbers
Human intervention	Not possible in most cases	Possible rather inevitable in some cases

The main contributions of our work are summarized as follows: (1) We propose a cluster-based key management technique for intra-WBAN communication that uses PV-based (EKG) generated keys for secure cluster formation. (2) For inter-WBAN communication, the clustering is made secure by using the preloading-based lightweight key management scheme [15] that is divided into two phases. The first phase includes the communication between WBANs and the second phase includes the communication between WBAN and RBS. During the communication between WBAN and RBS, the WBAN might not be in the transmission range of the RBS. In this case the WBAN will communicate with another WBAN (WBAN-to-WBAN communication) to reach the RBS. (3) We also present a key refreshment mechanism for both intra-WBAN and inter-WBAN communications based on PVs. After presenting our scheme, its overhead is analyzed based on storage, energy, and security. (4) We compare our proposed secure cluster formation technique with the technique presented in [5]. The authors in [5] use PV-based security scheme in a WBAN, where low-energy adaptive clustering hierarchy (LEACH) [16] is used for secure cluster formation. Table 2 shows a list of notations used in the paper.

The remaining of the paper is organized as follows: In Section 2 the related work is explained. Section 3 presents the system model, while Section 4 describes our intra-WBAN communication security technique. In Section 5 the technique for inter-WBAN communication is explained. Section 6 presents the performance evaluation of our proposed technique, and Section 7 concludes the article.

2 Related work

Clinical prototypes for implantable and wearable health monitoring sensors have been designed recently. These devices are used for monitoring human body over long periods of time [17,18]. Most of the work concerns biocompatibility, power-efficiency, and reliability. Therefore, ensuring the security of communication among these devices is important [19,20]. Medical sensors used in a pervasive healthcare system have very limited capabilities.

Table 2 Notations used in the paper

Symbol/notation	Description	Symbol/notation	Description
WBAN	Wireless body area network	K_{sk}	Secret key preloaded in all sensors
WSN	Wireless sensor network	MAC	Message authentication code
EKG	Electrocardiogram is the interpretation of the electrical activity of the heart for a specific period	K_n and $K_{n'}$	K_n is the key selected from the key pool, and $K_{n'}$ is the hashed key obtained as a result of the hash of K_n
PV	Physiological value is a biological characteristic of the body	EK_{SN_a,SN_b}	Pairwise key established between SN_a and SN_b
ID_{SN_a},ID_{SN_b}, ID_{ps}, ID_{SNs}	Identifiers of sensor nodes a, b, personal server, and network respectively	nonce	Random number generated during the communication process to check the transaction freshness
MS	Medical server located in hospital	KeyRef	Broadcast message used to refresh key in the network
RBS	Remote base station	P	Key pool
CH	Cluster head	S	Subset of P
CM	Cluster member	R	Key ring
Intra-WBAN communication	The on-body communication	K_i	Randomly selected key from the pool
Inter-WBAN communication	The communication between two or more WBANs	HMAC	Keyed-hashing for message authentication
SN_a	Sensor node 'a'	K_M	Master key
SN_b	Sensor node 'b'	$K_{i'}$	Hashed key
PS	Personal server	ICK	Integrity check key
E_{re}	Residual energy	K_{net}	Network key for broadcast authentication
$T(n)$	The number of competing nodes	P_r	Probabilities of occurrence of CH
E_0	Initial energy	d	Distance from RBS

Hence, in general, a complex, computationally intensive security mechanism such as public-key infrastructure [21,22] is not suitable for securing medical sensor communication in the context of pervasive healthcare. Similarly, authors in [23,24] present the pre-deployment-based strategy to protect the communication in distributed sensor networks. Techniques such as message-in-a-bottle [25] are also not suitable for WBANs as they involve the use of a Faraday cage, which increases the involvement of the host, i.e., the host will put the Faraday cage in the WBAN. A technique concerning the security of implantable devices is presented in [26], which describes the use of biometrics as a tool for generating cryptographic keys for secure inter-sensor communication. Due to the extremely dynamic properties of human body, it can produce many specific physiological values that are time-variant and difficult to guess. These time-variant properties for cryptographic purposes ensure strong security and eliminate key distribution [5,8-10]. Both sender and receiver can now measure the physiological values from their environment, generate pairwise keys, and use them for security purposes whenever they intend to communicate [26].

In [9,10] the authors use EKG as a physiological measure for generating cryptographic keys for secure inter-sensor communication. Both communicating sensors first sense the EKG values and then by applying certain hashing and watermarking technique, exchange these values for generating common keys for communication. In [27,28] the authors proposed a pairwise key management protocol which uses accelerometer (handheld device) data as a PV for generating the keys. The scheme works by physically shaking the communicating devices. After shaking the user has to press 'authenticate now' button to synchronize the accelerometer signal measurement process and execute the protocol. In [6] the authors propose a preloading-based scheme for key management in WBANs; however, the technique suffers from lack of variations. Key refreshment is also an issue with the preloading-based schemes. Also, most of the preloading-based schemes suffer from forward secrecy problems. In [29] the authors use PV-based keys for secure cluster formation. The idea of cluster-based secure key agreement protocol for WBANs is presented in [8]. The authors consider the WBAN as a single cluster and the PS is considered as the CH. The network is assumed to be a

heterogeneous WSN, which consists of a powerful high-end sensor (H-sensor) node and several low-end sensor (L-sensors) nodes.

Several techniques are available in the literature for selecting CH in a cluster. In [30] CH is chosen on the basis of node ID. In [31] a cluster-based protocol uses randomized rotation of local CHs to evenly distribute the energy load among sensors in the network. In [32] optimal CH selection is done using multi-objective particle swarm optimization. The above approaches do not consider security of the protocols or techniques that are used for cluster formation. Also in the context of WBANs, the above-mentioned techniques are very complex and expensive due to limited resources of the nodes in WBANs. In [33] the authors propose a secure cluster formation scheme, which is based on microTesla protocol. MicroTesla protocol uses pre-deployment and public-key cryptography which is expensive in WBANs. The scheme proposed in this paper presents a secure cluster-based approach to choose an optimal CH on the basis of residual energy and distance of nodes present in WBANs.

3 System model

We assume the WBAN as a network of sensor nodes implanted on the human body, with the ability to measure PVs of the body. We also assume that the sensors have the capability of measuring multiple types of PVs. Physiological monitoring sensors are mostly multimodal and are able to sense multiple types of stimuli [34,35]. Sensor nodes are ordinary devices with limited computation, communication, and storage capabilities. We consider that sensor nodes have different communication and storage powers and all the nodes are constrained in energy. PS is a powerful sensor node having high computation, communication, energy supply, and storage capabilities. The PS is preloaded with node identities and relevant keys before deployment. The proposed system architecture for intra-WBAN communication is shown in Figure 1.

Inter-WBAN communication involves CHs and CMs communication. CMs are PSs located on the body in WBANs to collect information or biometrics from sensors and then transmit to CHs. PSs are body base stations, which are more powerful devices attached to the human body. CHs are tamper-resistant devices that are well-protected against routing attacks and adversaries.

The proposed technique uses residual energy and distance [12] to choose the CHs for inter-WBAN as well as intra-WBAN communication using Equation 2. The residual energy and distance of each node in intra-WBAN communication is checked. If a node has an optimal value returned from the equation, it is selected as CH and the nodes within its transmission range are considered as its cluster members. Similarly, a PS on a body (WBAN) is selected as CH based on residual energy and distance in case of inter-WBAN communication by using the same equation. Figure 2 shows the architecture for inter-WBAN communication.

4 Intra-WBAN communication

The proposed technique uses EKG-based generated keys for secure cluster formation in intra-WBAN communication (Figure 3). Pairwise keys are used for key management, and a unique key is used for each communication between the sensor nodes. The *IDs* of nodes and the secret key K_{SK} are preloaded in all the sensors.

EKG values are used for the generation of keys. When SN_a wishes to communicate with SN_b, SN_a sends hello message with its ID in message 1.

$$m1 : \forall SN_a \varepsilon \{SN\} : SN_a \rightarrow SN_b : MAC(ID_{SN_a}, \text{Hello, nonce})$$

After receiving $m1$, SN_b calculates pairwise key with the required data and ID of SN_a and SN_b

$$K_{SN_a,SN_b} = \text{HMAC}(\text{Calculated EKG value} \parallel ID_{SN_a} \parallel ID_{SN_b}) \quad (1)$$

SN_b encrypts the data with K_{SN_a,SN_b} and computes the message authentication code (MAC) on ID of SN_a, nonce from SN_a, and data using the same key K_{SN_a,SN_b}. In $m2$, SN_b sends its ID, encrypted data and MAC to SN_a.

$$m2 : \forall SN_b \rightarrow SN_a : ID_{SN_b}, EK_{SN_a,Sn_b}\{ID_{SN_b}, \text{Data}\}, MAC_{K_{SN_a,SN_b}}(ID_{SN_b}, \text{Data, nonce})$$

When PS receives this $m2$, first it calculates the K_{SN_a,SN_b} by applying the keyed-hash function on the calculated EKG values, ID_{SN_a} and ID_{SN_b}. As EKG values are same on both sides, K_{SN_a,SN_b} generated by SN_a will also be same as that of SN_b. SN_a decrypts the message with K_{SN_a,SN_b} and compares ID_{SN_b} and received EKG values with the decrypted message ID_{SN_b} and EKG values on SN_a to ensure that both parties have generated the same key. The message authenticity is checked by SN_a through MAC verification with K_{SN_a,SN_b}. The communication between PS and sensor nodes is done through the ID_{PS}. PS broadcasts its ID to the whole network. Sensor nodes generate $K_{PS,SN}$ by applying keyed-hash function on ID_{SN}, ID_{PS}, and EKG values. SN encrypts data by $K_{PS,SN}$ and sends its ID, encrypted data, and MAC of these values to PS. PS then generates the key and decrypts the data. Authentication of PS is done by MAC.

4.1 Secure cluster formation in intra-WBAN communication

In this step the nodes with minimum energy and located far from PS are organized in a cluster to reduce the energy dissipation during the communication. The cluster formation process is based on the parameters of residual energy and distance from PS. The following equation is derived

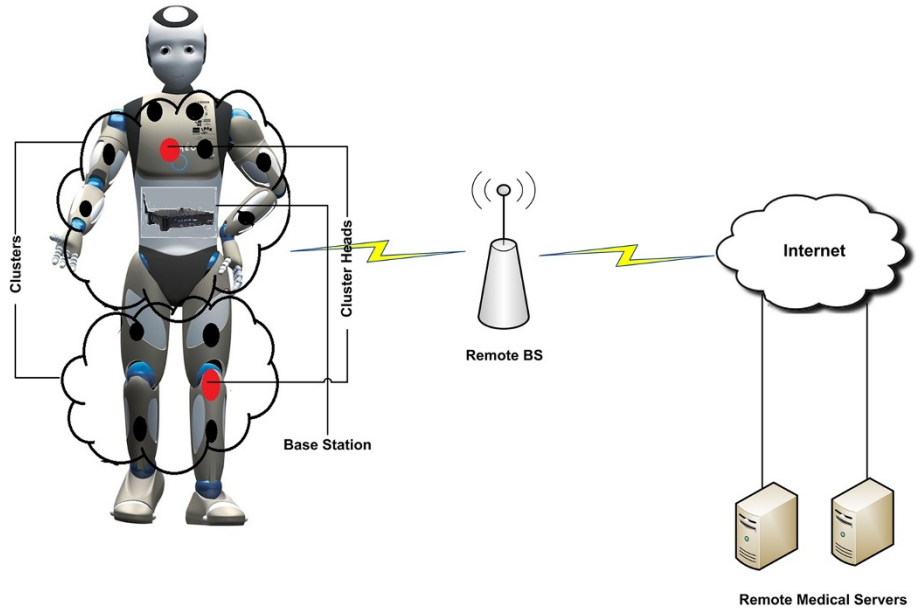

Figure 1 Intra-WBAN communication architecture.

from the formula presented in [36], in which the node with optimal value of *T(n)* is selected as CH:

$$T(n) = \frac{E_{\text{re}}.P_r}{E_0.d} \tag{2}$$

where $T(n)$ represents the total number of competing nodes, E_{re} and E_0 are the residual and initial energies respectively, d is the distance while P_r is the probability of occurrence of the CH. The traditional cluster formation protocols can allow a malicious node to broadcast a false solicitation beacon claiming itself as a CH by advertising wrong residual energy and distance. When CM nodes receive this message, they consider the claiming node as their CH. This type of attack is called HELLO Flood attack [37]. The malicious node can easily launch sinkhole attack using HELLO Flood and claiming itself as CH. When a sinkhole is formed, all the information passing through it can easily be manipulated by the malicious node. In response, a malicious CM sends a join request to the CH and joins the network by claiming itself as a legitimate CM. In this case, the malicious CM can also manipulate and inject false data and alarms in the network. In intra-WBAN communication, the security is provided by computing the MAC. Every CH broadcasts its solicitation message by including a certificate in order to authenticate the CHs. When the CMs receive this message, they verify the certificate by using MAC. In the proposed scheme, the certificates are issued by the PS of the WBAN. For example, when CH_a wants to authenticate other nodes in the cluster formation process in intra-WBAN communication, CH_a will broadcast a message containing its certificate ($\text{CERT}_{\text{CH}_\text{a}}$) and will be of the following format:

$$\text{CERT}_{\text{CH}_\text{a}} = \text{EK}_{\text{CH}_\text{a}}[\,\text{ID}_{\text{CH}_\text{a}}||\text{Data}||T_{\text{sign}}||T_{\text{expire}}]$$

where T_{sign} and T_{expire} are issuance and expiry time for the certificate respectively. Also, *Data* contains the information of the node's residual energy and distance from PS of the WBAN. Upon receiving this message, every node in the WBAN verifies the certificate by using MAC. For renewal of the certificate, the T_{ref} is used and all certificates must be renewed within this T_{ref} time interval.

Nonce is a random number included in the request messages, as in Equation 3, to fix the replay problems. The replies to these request messages must carry the transformation of this number; otherwise, these are considered a replay attack. In the proposed work, nonces are included in the messages exchanged for key agreement, key refreshment, and node addition/revocation, etc., and only legitimate users can extract the nonce values from the MAC and hence protect the replay attack. For example, the message exchanged between the sensor nodes SN_a and SN_b contains the nonce in the MAC secured with key $K_{\text{SN}_\text{a},\text{SN}_\text{b}}$. Now node SN_a having this key will be able to extract the nonce and can transform this nonce in the reply message; otherwise, it will be considered as a replay attack.

$$\begin{aligned}\forall \text{SN}_\text{b} \rightarrow \text{SN}_\text{a} : \text{ID}_{\text{SN}_\text{b}}, \text{EK}_{\text{SN}_\text{a},\text{Sn}_\text{b}}\{\text{ID}_{\text{SN}_\text{b}}, \text{Data}\},\\ \text{MAC}_{K_{\text{SN}_\text{a},\text{SN}_\text{b}}}(\text{ID}_{\text{SN}_\text{b}}, \text{Data}, \text{nonce})\end{aligned} \tag{3}$$

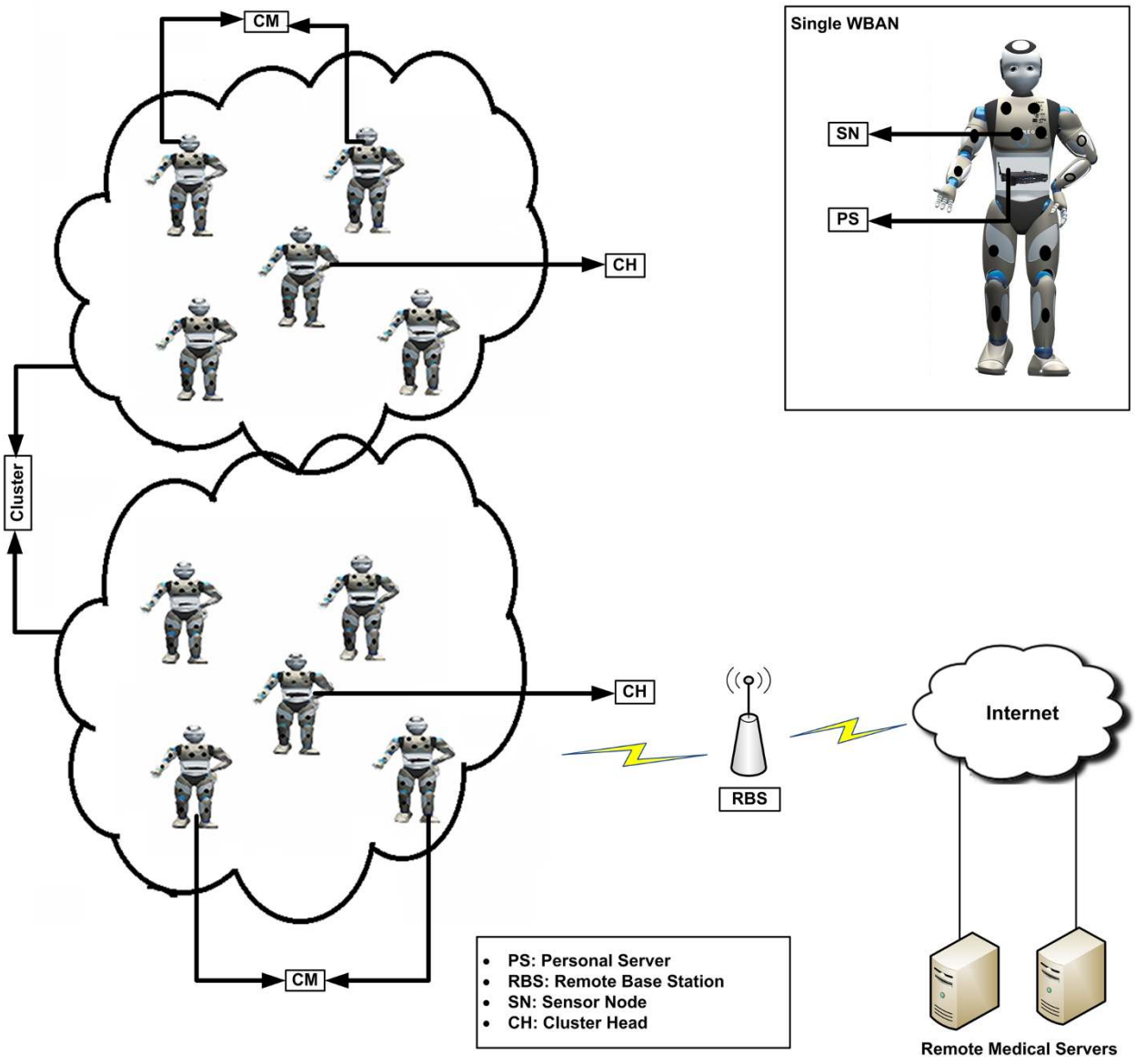

Figure 2 Inter-WBAN communication architecture.

4.2 Key refreshment in intra-WBAN communication

The keys are refreshed at regular intervals by using the plug-and-play nature of EKG-based key generation process. Due to the dynamic and highly random nature of EKG values of the human body, the key distribution process is eliminated because the generated keys are common on both the sender and the receiver sides [5,8-10], which makes the key refreshment process more powerful and robust. Key refreshment is also very important to maintain forward secrecy. Schemes that do not consider key refreshment suffer from forward secrecy problem [38]. To maintain this property, keys must be refreshed at regular intervals. Keys in intra-WBAN communication are refreshed at regular intervals. When PS wishes to refresh the key, it sends *KeyRef* message to the sensor nodes. Sensor nodes compute new key by the EKG values:

$$m1 : \mathrm{PS} \rightarrow * : \mathrm{KeyRef}(\mathrm{ID}_{\mathrm{PS}})$$

5 Inter-WBAN communication

The inter-WBAN communication is used for the delivery of data from PS to the remote sink. We consider the inter-WBAN communication as a hierarchical structure, in which more powerful sensors act as CH. The hierarchical structure has the advantage of local data processing,

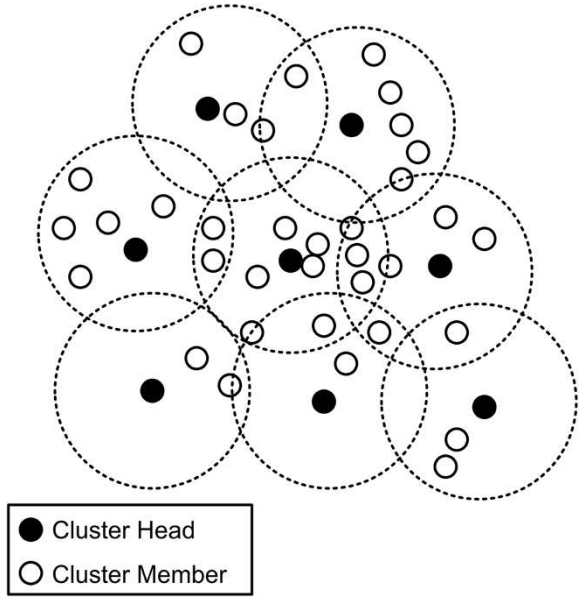

Figure 3 Cluster formation.

which reduces communication load in the network in order to provide a scalable solution.

5.1 Key pre-distribution

A key pool P is generated consisting of S number of random symmetric keys. These keys and IDs are stored in a CH. CH are high-end nodes with more storage and energy capabilities and have tamper-resistant hardware. The upper limit of S depends upon the storage and computational capabilities of the CH. As CHs are powerful nodes with high computational, communication, energy supply, and storage capabilities, the value of S is assumed to be a large number. Each key is assigned a unique ID. Further, a unique ID is assigned to each PS [15]. Before deploying the WBANs, each WBAN is loaded with its assigned key ring R. The assigning rules are as follows:

Step 1. For each PS, randomly select one key k_i from the key pool and generate a new key k_i^- by applying one-way hash function on the $\mathrm{PS_{ID}}$ and k_i. This newly generated key (k_i^-) is assigned the same key ID as that of k_i. Put k_i^- along with corresponding key ID into PS's memory.

Step 2. Each CH is preloaded with all S keys of the key pool. Further, RBS and each CH are loaded with a special key K_{M} known as the master key.

5.2 Secure cluster formation in inter-WBAN communication

Traditional cluster formation protocols are vulnerable to attacks. The protocols work by choosing the CH after the deployment of nodes [39,40]. In inter-WBAN communication, the clusters are formed to efficiently deliver data to the remote sink. The proposed work chooses the CH on the basis of residual energy and distance from the RBS [12]. Each node calculates its position by using any technique such as positioning through global positioning system (GPS) or any of the GPS-free positioning techniques available in the literature [41-43]. Each node in the network broadcast its residual energy and distance. Nodes with optimal value of $T(n)$ in Equation 2 are selected as CHs. The CH selection process is shown in Figure 4, where CH selection in cluster B is done by measuring its distance from the RBS directly. Node 1 in cluster B is selected as a CH because it has the minimum distance from the remote base station and also has maximum residual energy as compared to the other members in the same transmission range. Similarly, node 4 in cluster A is selected as CH because its distance from the RBS is lesser and its residual energy is maximum within that transmission area. The distance between the sender node and the RBS will be the total cost of the path (summation of all distances on the path to RBS). After the CH is selected, the nodes within its transmission range with minimum distance from the CH are declared as CM for that particular CH. The cluster formation process is as follows:

- Each CH broadcast its solicitation beacon, which contains its ID and control information.
- Upon receiving the solicitation beacon, each CM decides to join the cluster of a CH such that the distance of the CM from this CH is minimum as compared to the distances from other CHs.
- Each CM now sends a join request to the CH whose cluster it wants to join.

5.3 Neighborhood discovery in inter-WBAN communication

After the completion of cluster formation, all the WBANs broadcast solicitation beacons in order to discover their neighbors in a cluster.

5.4 Inter-cluster and intra-cluster pairwise keys generation in inter-WBAN communication

After discovering its neighbors, each PS sends $m1$ to CH containing PS's ID, IDs of generated keys (kn'), nonce, and list of its neighbor WBANs.

$$m1 : \forall \mathrm{CH_a} \in \{\mathrm{CH}\} \forall \mathrm{PS}_i \in \{\mathrm{PS}\} : \mathrm{PS}_i \rightarrow \mathrm{CH_a} : \mathrm{ID_{PS_i}}, \mathrm{ID}_{kn'}, \mathrm{List\ (neighbors)}, \mathrm{Nonce_{PS_i}}$$

CH locates the corresponding key ID ($\mathrm{ID}_{kn'}$) from its key pool S. After locating the key, $\mathrm{CH_a}$ performs one-way hash function on the ID of PS_i and K_n.

$$kn' = f_{kn}(\mathrm{ID_{PS_i}}) \tag{4}$$

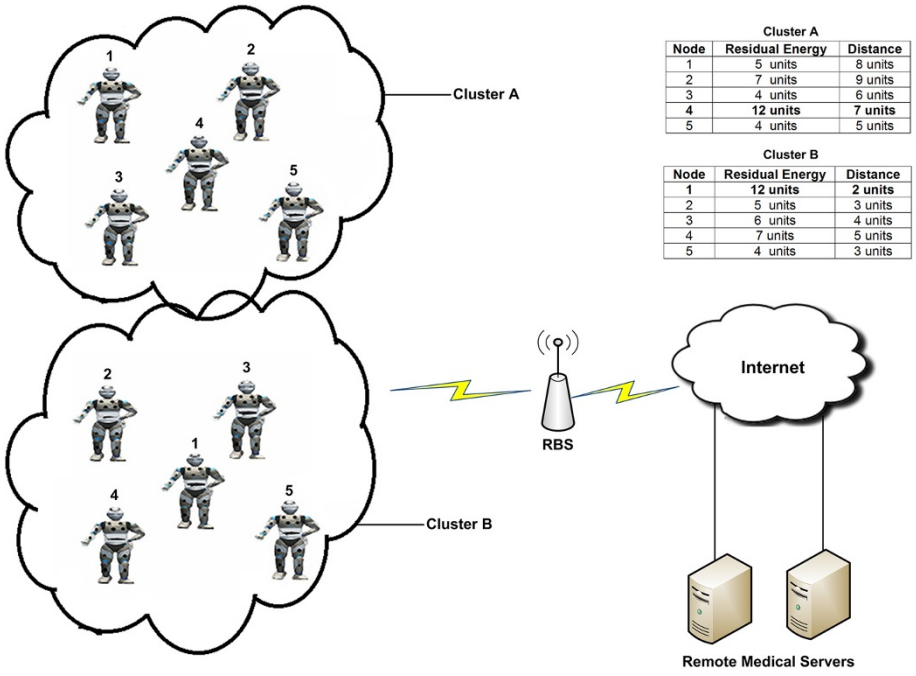

Figure 4 Cluster head selection process in inter-WBAN communication.

Network key (K_{net}) and integrity check key (ICK) is generated by CH_a by applying one-way hash function on ID of PS_i, ID of CH_a, nonce of PS_i, nonce of CH, and an integer (0 for ICK, 1 for K_{net}) using kn'.

$$\text{ICK}_{\text{PS}_i,\text{CH}_\text{a}} = f_{kn'}(\text{ID}_{\text{PS}_i}, \text{ID}_{\text{CH}_\text{a}}, \text{nonce}_{\text{PS}_i}, \text{nonce}_{\text{CH}_\text{a}}, 0) \tag{5}$$

$$K_{\text{net}_{\text{PS}_i,\text{CH}_\text{a}}} = f_{kn'}(\text{ID}_{\text{PS}_i}, \text{ID}_{\text{CH}_\text{a}}, \text{nonce}_{\text{PS}_i}, \text{nonce}_{\text{CH}_\text{a}}, 1) \tag{6}$$

CH_a sends its nonce and MAC calculated on ICK to PS_i so that PS_i can generate both keys, ICK, and K_{net}.

$$m2 : \forall \text{PS}_i \in \{\text{PS}\} : \text{CH}_\text{a} \rightarrow \text{PS}_i : \text{nonce}_{\text{CH}_\text{a}}, \text{MAC}(\text{ICK}_{\text{PS}_i,\text{CH}_\text{a}}, \text{nonce}_{\text{CH}_\text{a}})$$

After receiving $m2$ from CH_a, PS_i generates both ICK and K_{net} by extracting $\text{nonce}_{CH\text{a}}$. PS_i then authenticates these keys by checking the MAC value. Once MAC is authenticated, PS_i sends ready message to tell CH_a that it is ready to start using the new keys for encryption in $m3$.

$$m3 : \forall \text{PS}_i \in \{\text{PS}\} : \text{PS}_i \rightarrow \text{CH}_\text{a} : \text{ReadyMsg}, \text{MAC}(\text{ICK}_{\text{PS}_i,\text{CH}_\text{a}}, \text{ReadyMsg})$$

$m3$ includes a MAC so the CH_a can authenticate PS_i by verifying that it has a matching key kn'. CH replies with $m4$. PS_i waits for $m4$ before installing the keys.

$$m4 : \forall \text{PS}_i \in \{\text{PS}\} : \text{CH}_\text{a} \rightarrow \text{PS}_i : \text{AckMsg}, \text{MAC}(\text{ICK}_{\text{PS}_i,\text{CH}_\text{a}}, \text{AckMsg})$$

Once the message transfer is completed, both CH_a and PS_i install the keys and start encryption. After encryption is enabled and the keys are authenticated, CH_a sends pairwise keys to PS_i encrypting with network key K_{net} in $m5$.

$$m5 : \forall \text{PS}_i \in \{\text{PS}\} : \text{CH}_\text{a} \rightarrow \text{PS}_i : EK_{\text{net}_{\text{PS}_i,\text{CH}_\text{a}}}\{K_{\text{PS}_i,\text{PS}_j}, K_{\text{PS}_i,\text{PS}_k}, \ldots\} \text{MAC}(\text{ICK}_{\text{PS}_i,\text{CH}_\text{a}}, K_{\text{PS}_i,\text{PS}_j}, K_{\text{PS}_i,\text{PS}_k}, \ldots)$$

An inter-cluster communication between CHs is achieved through keys K_{CH_i} and K_{CH_j} generated by applying one-way function on ID_{CH_i} and ID_{CH_j} using key K_M. All data from CH to RBS are transferred through the master key K_M as given below:

$$K_{\text{CH}_i,K_{\text{CH}_j}} = f_{K_M}(\text{ID}_{\text{CH}_i}, \text{ID}_{\text{CH}_j}) \tag{7}$$

5.5 Re-clustering

In both types of communications, the CH performs long-distance communication and also performs some extra tasks due to which its energy reduces with higher ratios as compared to the CM nodes. Due to this issue, the cluster has to be reorganized at regular intervals by choosing CHs from CM nodes. Re-clustering will also be performed when a node is reconfigured as well as when the CH leaves especially in inter-WBAN communication.

5.6 WBAN addition

In inter-WBAN communication, in order to add a new PS, say PS_u to the cluster, e.g. cluster_i, the RBS assigns a new

ID to the PS_u and a unique master key K_M. The PS_u then generates a random nonce RN_u and sends the following message to its cluster head CH_i.

$$m1 : PS_u \rightarrow CH_j : (ID_{PS_u}, RN_u) \parallel MACK_M(ID_{PS_u} \parallel RN_u)$$

The cluster head CH_i simply forwards the received message from PS_u to its neighbor cluster head, if required. This message finally reaches the remote RBS via cluster heads.

$$m2 : CH_j \rightarrow BS : (ID_{PS_u}, RN_u) \parallel MACK_M(ID_{PS_u} \parallel RN_u)$$

The authentication of the new PS is done by using the RBS. The RBS validates the received message and computes the MAC on $ID_{PS_u} \parallel RN_u$ using the master key K_M. The RBS has the master keys of all sensor nodes. If computed MAC matches with the corresponding received MAC, the node PS_u is considered as a legitimate node.

5.7 WBAN eviction in inter-WBAN communication

PS eviction means that any PS in the cluster leaves its region for any reason (power consumption, node emigration, node capture, etc.). In this case, we propose two cases for PS eviction.

Case 1. Member PS eviction occurs when the CH does not receive the solicitation beacon from a certain PS for a specific duration. In this case, CH sends a query message to that PS and waits for a reply. If it does not receive a reply within a certain time, the CH sends a message to its entire member WBANs to inform them to delete the PS with a certain ID from the list of neighbors.

Case 2. In CH eviction when a CH leaves the cluster, two steps must be taken. First, the CH sends messages to its entire members to inform them that it is going to leave. Another PS is selected as CH by using the Equation 2. Secondly, if the CH leaves surreptitiously, the entire cluster members will not receive the CH beacon for a certain period, and then another PS is selected as CH by the same Equation 2.

5.8 Key refreshment in inter-WBAN communication

Key refreshment in inter-WBAN communication is done in two phases. The first phase includes intra-cluster key refreshment and the second phase includes inter-cluster key refreshment. For intra-cluster key refreshment, CH_a randomly selects one ID from the assigned key ring of PS_i and sends its own ID and selected ID to PS_i.

$$m1 : \forall CH_a \in \{CH\} \forall PS_i \in \{PS\} : CH_i \rightarrow PS_a : ID_{CH_i}, ID_{kn}$$

After receiving ID from CH_a, PS_i locates the corresponding key of that ID and generates new key $K_n^{'}$ by applying one-way hash function on the ID of CH_a and K_n.

$$Kn' = f_{kn}(ID_{CH_a}) \tag{8}$$

ICK and K_{net} are refreshed by CH_a by applying one-way hash function on newly generated key Kn', ID of PS_i, ID of CH_a, nonce of PS_i, and nonce of CH_a, (0 for ICK, 1 for K_{net}).

$$ICK_{PSi,CH_a} = f_{kn'}(ID_{PS_i,CH_a}, nonce_{PS_i}, nonce_{CH_a}, 0) \tag{9}$$

$$K_{net_{PSi,CH_a}} = f_{kn'}(ID_{PS_i,CH_a}, nonce_{PS_i}, nonce_{CH_a}, 1) \tag{10}$$

CH_a sends the $nonce_{CH_a}$ and MAC calculated by newly generated ICK, so that PS_i can refresh ICK and network key K_{net}.

$$m2 : \forall PS_i \in \{PS\} : CH_a \rightarrow PS_i : nonce_{CH_a}, \\ MAC(ICK_{PS_i,CH_a}, nonce_{CH_a})$$

After receiving $m2$, PS_i generates ICK and K_{net} by extracting $nonce_{CH_a}$, and the keys are verified by checking the MAC value. Master key K_M is refreshed by RBS. RBS sends random integer r to CH for the refreshment of K_M; CH generates new K_M by applying hash function on r and the old K_M.

6 Results and analysis

In this section, the proposed cluster-based WBAN technique is analyzed with respect to security, storage, and energy consumption of nodes. Both intra-WBAN and inter-WBAN communications involve routing, in which the nodes (CMs) transmit data to the CH, which relays the information to the RBS and then to the MS. All experiments were performed using MATLAB (Mathworks, Natick, MA, USA). For key generation, the EKG data of 31 patients are taken from the MIT Physiobank database [44]. Clustering is performed for ten rounds for both proposed and LEACH-based schemes.The simulation area is kept as 100 × 100 m for 60, 100, and 300 nodes.

6.1 Security analysis

In this subsection, the security analysis of the proposed scheme is demonstrated based on (a) resilience against routing attacks, and (b) personal server compromise.

6.1.1 Resilience against routing attacks

Routing attacks include spoofed, altered, or replayed routing information; selective forwarding; sinkhole attack; Sybil attack; and wormhole attack etc. Detailed description of all these attacks can be found in [35]. In the following, we discuss how the proposed technique defends against these attacks.

Sybil attack involves the attack in which a single node appears with multiple identities. The communication between two PSs in a WBAN is done through pairwise keys. When PS_i wishes to send data to PS_j, MAC is computed by using the shared pairwise key between PS_i and PS_j. These pairwise keys are only known to PS_i and

PS_j so no adversary can pretend to be PS_i unless PS_i is compromised. Thus, Sybil attack can be prevented.

The proposed cluster-based routing in WBAN includes two types of routing in inter-WBAN and intra-WBAN communications i.e., intra-cluster routing, and inter-cluster routing. For intra-cluster routing, all CMs send data only to the CH. For inter-cluster routing, the data packets are forwarded only through CH in the cluster. Other nodes in the cluster do not participate in routing. An adversary is not able to route in the proposed routing structure, therefore, the proposed technique is well protected against wormhole and sinkhole attacks. Also in intra-WBAN communication, the sinkhole is prevented by applying MAC using the EKG-based keys.

The routing information is distributed by the CH. Since CH in the WBAN is a high-end device, has tamper-resistant hardware, and is well protected against routing attacks, it cannot be compromised by an adversary. A CH appends keyed MAC to each routing control message. Only the intended CM and CH know the key used to generate MAC so the adversary is unable to inject false information in the WBAN. Due to these factors, selective forwarding attacks cannot be launched on CH. To defend the selective forwarding attack on PS in WBAN, *PacketID* is used. Each PS is responsible to confirm that its successor has successfully forwarded the packet by overhearing the transmission.

6.1.2 Dieharder tests for randomness

In the proposed work, keys are generated for 25 different subjects using the EKG data taken from MIT Physiobank. The Dieharder [45] testing suite is applied on the keys generated from the EKG data. Dieharder includes tests from DIEHARD [46] battery of tests, Statistical Test Suite developed by the National Institute for Standards and Technology, and also new tests developed by the Dieharder team.

For each statistical test, a set of P value is produced. The P value is the probability of obtaining a test statistic larger than the one observed if the sequence is random. Hence, small values are interpreted as evidence that a sequence is unlikely to be random. The decision rule in this case states that 'for a fixed significance value α, a sequence fails the statistical test if it's P value $< \alpha$'. A sequence passes a statistical test whenever the P value $\geq \alpha$ and fails otherwise. Authors in [32] assume 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. It results in a 95% confidence interval of P values between 0.0001 and 0.9999.

Table 3 shows the average P value of keys generated from the PVs of 25 subjects and their respective assessments. Similarly, Figure 5 shows the P values of the total tests of the Dieharder suite. It is evident from Table 3 and Figure 5 that none of the P values is violating the condition given in [47]. The average P value is far away from the boundaries defined in [47] for all the tests.

The sts serial, rgb bitdist, and rgb minimum distance are the set of tests. For the sts serial test, the value of N-tuple is from 1 to 16 and produces the P value between 0.424347 and 0.674048. Similarly, rgb bitdist have the value of N-tuple ranging from 1 to 12 and produces the P value between 0.438929 and 0.647891. The generated keys pass each and every test in the suite, which shows the degree of its randomness.

6.1.3 Personal server compromise

The proposed technique for inter-WBAN communication shows a strong resilience against node capture. To check the randomness of the generated keys in an inter-WBAN communication, the 'Birthday Paradox' analysis is performed, i.e., if r keys are selected at random, what is the chance that no two keys will have the same value? Let Pr be this chance. If keys are independently and uniformly distributed between 1 and m, then the probability equation will be as follows [48,49]:

$$P_r = \frac{(m)_r}{m^r} = \frac{m!}{m^r(m-r)!} \approx e^{\frac{-r^2}{(2m)}} \tag{11}$$

The purpose of this analysis is to assess the repetition of the keys. For 64-bit key length, there are 2^{64} different combinations of keys that can be generated. Applying the formula of 'Birthday Paradox', the probability of repeating a key is 0.5 in 2^8 attempts, which is a big number because the inter-WBAN communications have lesser number of nodes in the network. Hence, the probability of repeating a key in the network is very small. The threshold of the probability of repeating a key falls within the range of 1 to 0.99999. Figure 6 demonstrates the probability of repetition of keys. At the initial stage, the probability of keys to be unique remains closer to one. After the initial stage, the curve starts declining and then approaches to zero. In case of PS compromise, the secret key K_{SK} is used to authenticate the sensor nodes and the communication is done by deploying new PS in the cluster.

6.2 Storage overhead analysis

The proposed scheme supports a large number of nodes with a small number of keys, i.e., a few key pairs can support secure communication for a very large network. In other words, the proposed scheme reduces the number of keys required for a secure communication, thereby affecting the memory consumption of the sensor node. The graph in Figure 7 is drawn on logarithmic scale, because the number of nodes that can be supported increases exponentially with respect to the number of keys used. Figure 7 substantiates the exponential increase in the

Table 3 Dieharder testing suite results for randomness of EKG generated keys

Test name	N-tuple	t Sample	P sample	Average P value of 25 keys	Assessment
diehard_birthdays	0	100	100	0.58498	Passed
diehard_operm5	0	1,000,000	100	0.524797	Passed
diehard_rank_32 × 32	0	40,000	100	0.58725	Passed
diehard_rank_6 × 8	0	100,000	100	0.620069	Passed
diehard_bitstream	0	2,097,152	100	0.480387	Passed
diehard_opso	0	2,097,152	100	0.583141	Passed
diehard_oqso	0	2,097,152	100	0.534111	Passed
diehard_dna	0	2,097,152	100	0.512451	Passed
diehard_count_1s_str	0	256,000	100	0.60379	Passed
diehard_count_1s_byt	0	256,000	100	0.443534	Passed
diehard_parking_lot	0	12,000	100	0.493756	Passed
diehard_2dsphere	2	8,000	100	0.627908	Passed
diehard_3dsphere	3	4,000	100	0.605787	Passed
diehard_squeeze	0	100,000	100	0.600487	Passed
diehard_sums	0	100	100	0.141058	Passed
diehard_runs	0	100,000	100	0.603007	Passed
diehard_craps	0	200,000	100	0.683825	Passed
marsaglia_tsang_gcd	0	10,000,000	100	0.641335	Passed
sts_monobit	1	100,000	100	0.553621	Passed
sts_runs	2	100,000	100	0.593961	Passed
sts_serial	1 to 16	100,000	100	0.424347 to 0.674048	Passed
rgb_bitdist	1 to 12	100,000	100	0.438929 to 0.647891	Passed
rgb_minimum_distance	2 to 5	10,000	1000	0.326321 to 0.534724	Passed
rgb_permutations	2	100,000	100	0.561426	Passed
rgb_permutations	3	100,000	100	0.617997	Passed
rgb_permutations	4	100,000	100	0.621495	Passed
rgb_permutations	5	100,000	100	0.525111	Passed
rgb_lagged_sum	0 to 32	1,000,000	100	0.420681 to 0.737265	Passed
rgb_kstest_test	0	10,000	1000	0.484288	Passed
dab_bytedistrib	0	51,200,000	1	0.411422	Passed
dab_dct	256	50,000	1	0.5766	Passed
dab_filltree	32	15,000,000	1	0.532675	Passed
dab_filltree	32	15000000	1	0.512094	Passed
dab_filltree2	0	5,000,000	1	0.478207	Passed
dab_filltree2	1	5,000,000	1	0.539234	Passed
dab_monobit2	12	65,000,000	1	0.570357	Passed

number of supported nodes while using very limited number of keys. In Equation 12 *'k'* is the total number of keys, *'m'* represents the number of keys required to support a particular number of nodes, and *'n'* is the total number of nodes supported.

$$n = \frac{(k+m)!}{k!\,m!} \tag{12}$$

6.3 Communication and computation complexity

In intra-WBAN communication each time a key is refreshed, the whole process is repeated, i.e., the features are extracted and quantized, and then the keys are generated after the feature exchange process between the communicating sensors. Also in intra-WBAN communication, the key establishment latency (join and leave latency) occurs very rarely, as the node leaving and joining

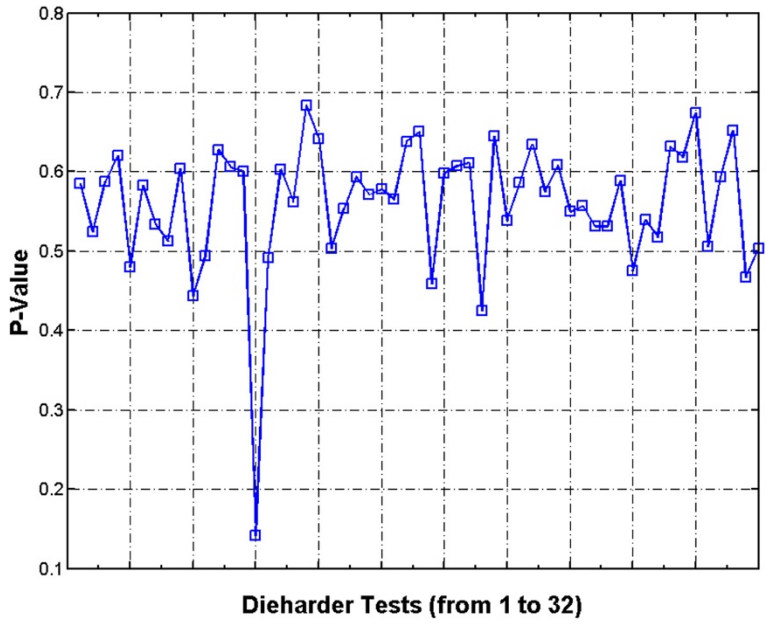

Figure 5 *P* **values of EKG-generated keys for each test.**

occurs only when the node failure happens, e.g., due to power failure or malfunctioning. Hence, due to these properties of intra-WBAN communication, its communication and computation costs are relatively minimal.

Due to the availability of powerful devices and high resources, inter-WBAN communication resembles the communication in WSNs. Therefore, we compare our proposed inter-WBAN communication scheme with LEAP+ [6], which is a lightweight extensible authentication protocol for WSN security. In inter-WBAN communication, the WBAN (node) joining and leaving may occur very frequently, so the keys need to be refreshed regularly thereby affecting the computation and communication costs of the scheme. The computation cost depends upon the total number of encryptions and decryptions taking place in the key agreement process.

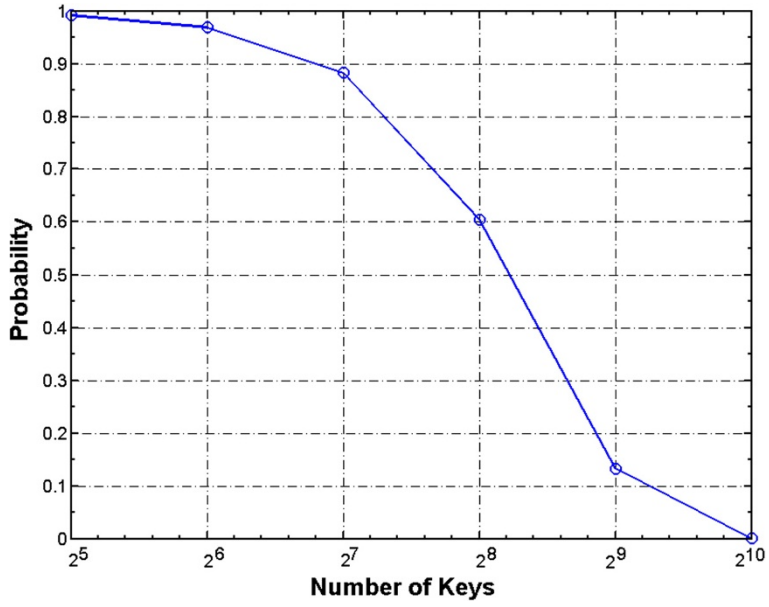

Figure 6 Probability of keys.

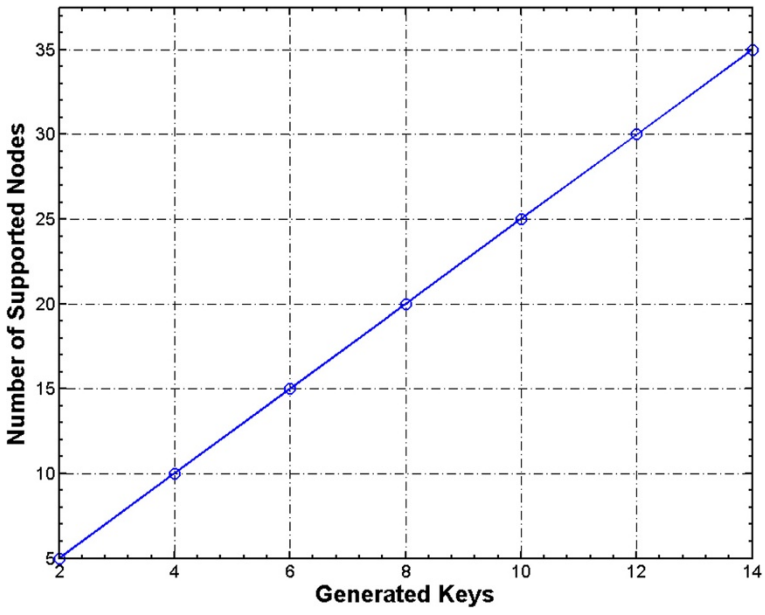

Figure 7 Storage overhead analysis.

In a cluster-based key agreement scheme, the number of decryptions is equal to the network size *(N)* because every node has to decrypt the message. Also in cluster-based schemes, CH encrypts the message once for all its CMs. Thus, the total number of encryptions depends upon the network size and can be at most *N*. So, for a network of size *N*, the average number of symmetric key operations a node performs during cluster key generation and updating is $(2S/N)$ [6], where *S* is the sum of all encryptions and decryptions, while *N* is the network size. So the computation complexity of the proposed work is dependent upon the degree of connectivity (*d*) and network size *N* and can be given as $O(d^2/N)$. Table 4 shows that the computation and communication complexity of both the schemes are same, but the number of messages sent by the proposed scheme are less than that of the LEAP+, which reduces the computation as well as the communication costs of the protocol. This is because the communication cost is the sum of all costs incurred during transmission and reception of the messages for the key agreement, key refreshment, and node addition and revocation. In cluster-based key agreement, the communication cost is dependent upon the degree of connectivity of the nodes, i.e., the increase in the connectivity will increase the communication cost. The communication cost is the same as the computation cost because every node has to send and receive keys for cluster key revocations. However, in case of communication cost, the number of messages transmitted will affect the total cost and the proposed scheme sends lesser number of messages than the LEAP+ scheme. This is because the message overhead is a much bigger concern than the computation overhead. It has been shown that the energy for computing one MAC is equivalent to transmitting only a single byte [50]; as for every message received, the node will have to calculate the MAC and will update its neighbor table.

Table 4 Communication and computation complexity

Protocol	Number of message exchanges	Computation cost	Communication cost
LEAP+	15	$O(d^2/N)$	$O(d^2/N)$
Proposed scheme	9	$O(d^2/N)$	$O(d^2/N)$

In the key refreshment phase, the CH refreshes the keys by selecting a random ID of a key from the key pool and sends this ID along with its own ID to all the members in the cluster. The members locate the key against the selected ID and apply one-way hash function to generate a new key. The key IDs will have 2 bytes size, so transmitting two IDs will take 4 bytes for key refreshment to take place, i.e., CH's own ID and ID of the PS. Transmitting 4 bytes will not affect the communication cost. Also, one-way hash function (HMAC-MD5) is used for the key refreshment to take place securely. To generate the hashes for 'HELLO' message, HMAC-MD5 takes 0.0003 msec/operation on a P4 machine [51]. The generation of hashes for the IDs of the communicating sensors will take less time and hence will consume fewer resources.

6.4 Energy consumption

The energy consumption in intra-WBAN communication is calculated for both LEACH and the proposed scheme. The energy is dependent on the distance between the PS of a WBAN and the sensor nodes. As the distance between PS and CHs increases, its energy consumption also increases. The energy consumption is calculated by using the following formula [31]:

$$\text{Energy} = \text{data\_packet} * (2 * e\_\text{elect} + e\_\text{emp} * \text{distance}) \quad (13)$$

In Equation 13, data_packet represents the number of packets transmitted during the cluster formation process, e_elect represents the energy consumed in the electronics, while e_emp is the energy consumption in amplifier. LEACH divides the network into clusters and the operation in LEACH is divided into rounds. In the first round, the CH is elected among the number of nodes. The election of CH uses probabilistic approach. LEACH introduces randomized rotation role of CH between member nodes to balance the energy conservation among nodes.

WBANs are highly resource-constrained networks and need energy-efficient and secure solutions for communication. Figure 8 shows the energy consumption comparison of the proposed scheme with LEACH-based scheme [5] in WBAN communication. The proposed scheme consumes lesser energy as compared to LEACH-based scheme because it uses hop-by-hop communication between CHs to reach the sink (PS in case of intra-WBAN communication) while LEACH uses direct communication between CHs and the sink (long-distance communication). It is apparent from Figure 8 that when we increase the number of nodes, the energy consumption also increases. In case of the proposed work, the energy consumption varies between 0.029 and 0.05 mJ, while in case of LEACH-based scheme, the energy consumption is above 0.1 mJ.

In cluster-based solutions, the energy consumption during CH selection process affects the performance of the overall system. The CH selection process must be optimal and energy-efficient. Figure 9 shows the comparison of energy consumption during the CH selection process in each round, where the proposed scheme consumes less energy than the LEACH-based scheme. The proposed scheme outperforms LEACH based solution due to the small-distance communication in the CH selection process. Figure 9 illustrates that the energy consumption in CH selection process in the proposed work varies between 0.04 and 0.07 mJ, while the LEACH-based scheme consumes energy between 0.1 and 0.19 mJ in CH selection process. The energy consumption of the LEACH-based scheme is very high as compared to the proposed scheme in case of CH selection process.

We define the lifetime of a network as the duration of time until the first node failure occurs due to battery depletion. In order to increase the productivity and usability of the proposed system, the network lifetime must be increased. The decrease in network lifetime will automatically decrease the usability, which will eventually affect

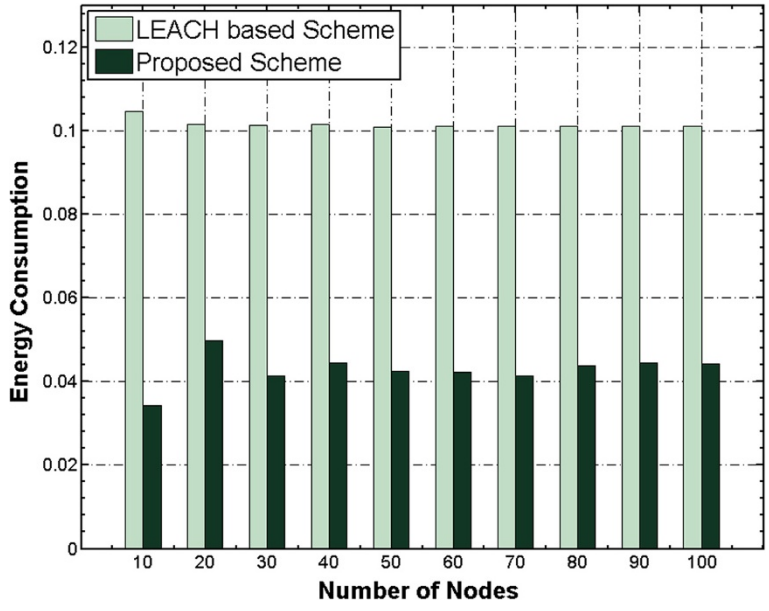

Figure 8 Energy consumption analysis as the number of nodes increases.

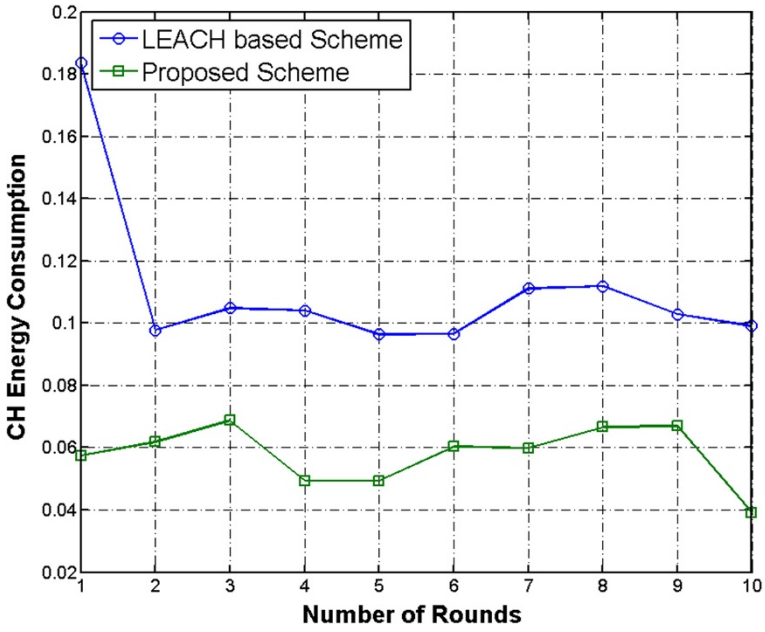

Figure 9 Energy consumption during CH selection process.

the productivity of the overall system. Figure 10 shows the network lifetime comparison of the proposed and LEACH-based schemes where the proposed scheme has a greater lifetime than the LEACH-based scheme. The proposed scheme has the ability to perform small-distance communication (CH to CH forwarding to reach the sink node) which consumes less energy and increases the network lifetime. The energy consumption of the proposed scheme fluctuates between 160 and 200 units, while that of the LEACH-based scheme is between 145 and 170 units.

The survivability of the proposed scheme depends upon the time it takes to reach the completely dead network status, i.e., when no node remains alive. As WBAN is a small-sized network, less number of nodes can sustain the connectivity in the network. Figure 11

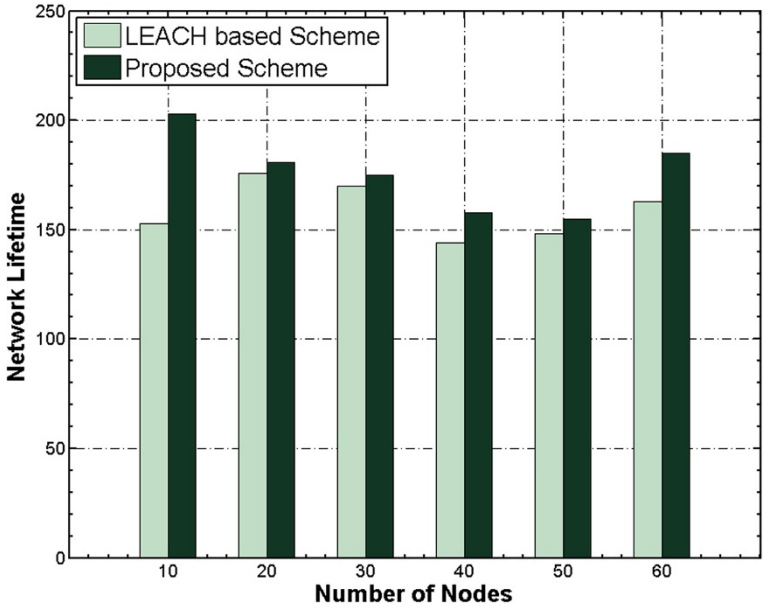

Figure 10 Effect of increasing number of nodes on network life time.

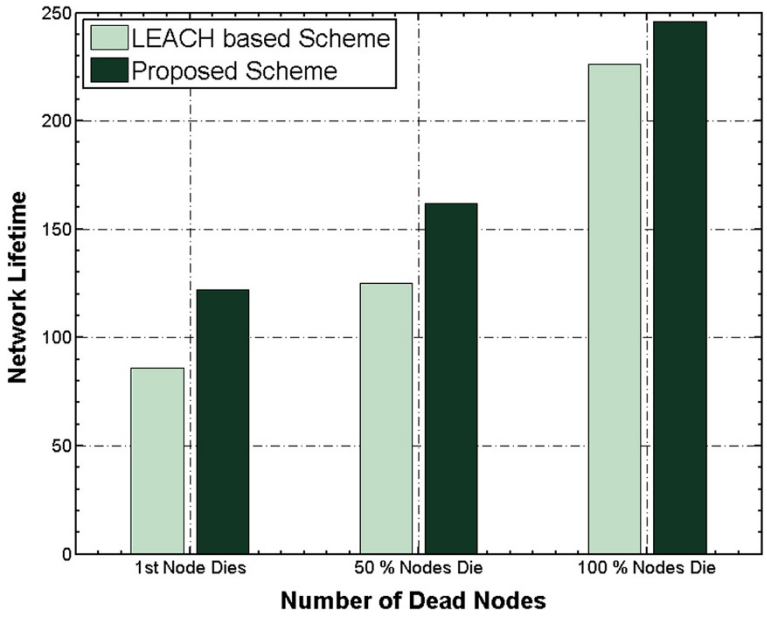

Figure 11 Total time from death of 1st node to 100% nodes.

depicts the comparison of how much time the proposed and LEACH-based schemes take when the first node, 50% nodes, and 100% nodes die. The proposed scheme has a greater time in each of the case due to lesser energy consumption in each phase. The increase in number of dead nodes results in a lesser-connected or half-connected graph. Hence, the number of dead nodes affects the connectivity in the network and eventually decreases the performance of the system.

The cluster formation for short-range communication like in WBANs will result in more clusters. As the communication distance is decreased for a particular network area like WBAN, the energy consumption in the communication process will also decrease. Figure 12 shows the effects of increasing the number of nodes on the cluster

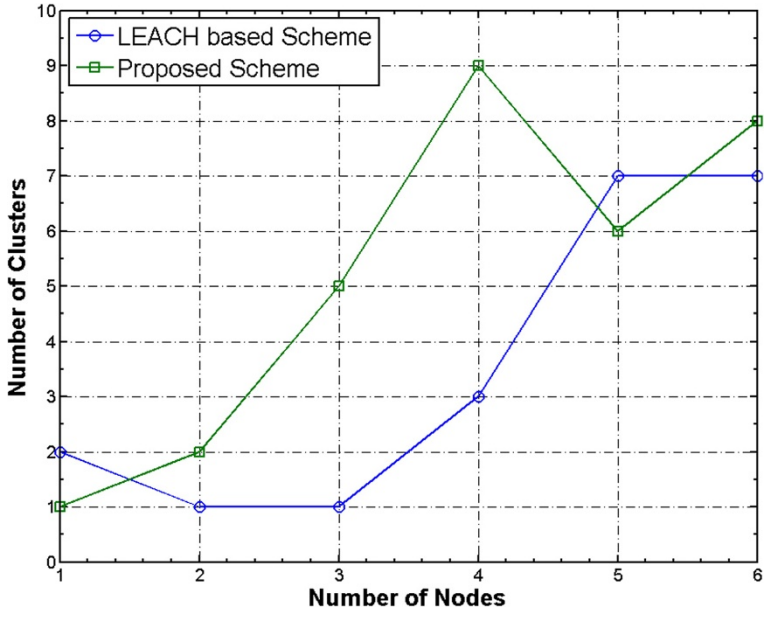

Figure 12 Effects of number of nodes on clusters.

formation process. The proposed scheme on average performs better than the LEACH-based scheme when we increase the number of nodes. Due to random deployment of nodes, sometimes the deployment is worse for a given experiment. In the figure the performance of the proposed scheme is less efficient than LEACH-based scheme when the number of nodes reaches 50 as well as in the case of bootstrapping. This is due to the random deployment of nodes in the network.

The above figures and discussion clearly show that the proposed scheme performs better than the LEACH-based scheme in case of energy consumption, network lifetime, and cluster formation.

7 Conclusions

WBANs play an important role in providing better healthcare services by using continuous and real-time monitoring of health information. Before using WBANs on real test beds, one must address the essential security and energy consumption requirements of WBANs as these requirements increase the usability and usefulness of WBANs. The technique presented in this paper uses clustering in both types of communications, i.e., intra-WBAN and inter-WBAN. In intra-WBAN communication, secure cluster formation is done by using PV-based generated pairwise keys. Introducing secure cluster topology formation to intra-WBAN communication makes the communication energy-efficient and increases the network lifetime. In intra-WBAN secure cluster formation, we compare the proposed scheme with the LEACH-based scheme presented in [5]. The results of our analysis show that the proposed scheme produces better results in terms of energy consumption, cluster formation, and network lifetime. In inter-WBAN communication, the cluster formation process is secured by using pre-deployed keys. The analysis of our proposed inter-WBAN communication scheme in terms of storage and energy efficiency shows that the proposed scheme uses very small number of keys per node, which reduces the storage overhead. Also, the cluster formation process in inter-WBAN communication brings energy efficiency to the scheme.

The security analysis of the proposed intra-WBAN communication scheme shows resilience against different attacks e.g., sinkhole attacks are prevented by using the PV-based generated keys. In addition, replay attacks are prevented by using nonce and time stamps. Similarly, in inter-WBAN communication scheme, the generated keys are random and the probability of repetition of the keys is minimum. The proposed scheme is lightweight and is highly suitable for WBAN applications.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for the 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.

Received: 31 January 2013 Accepted: 31 July 2013
Published: 27 August 2013

References

1. R Paradiso, G Loriga, N Taccini, A wearable health care system based on knitted integrated sensors. Proc. IEEE Trans. Info. Technol. Biomed. **9**(3), 337–344 (2005)
2. D Djenouri, L Khelladi, N Badache, A survey of security issues in mobile ad hoc and sensor networks. IEEE Commun. Surveys and Tutorials. **7**(4), 2–28 (2005)
3. Y Wang, G Attebury, B Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun. Surveys and Tutorials. **8**(2), 2–23 (2006)
4. A Perrig, R Szewczyk, JD Tygar, V Wen, D Culler, SPINS: security protocol for sensor networks. Wireless Netw. **8**(5), 521–534 (2002)
5. KK Venkatasubramaniam, SKS Gupta, Physiological value-based efficient usable security solutions for body sensor networks. ACM Trans. Sens. Netw. (TOSN). **6**(4), 60–68 (2010)
6. SMKUR Raazi, H Lee, S Lee, YK Lee, BARI+: a biometric based distributed key management approach for wireless body area networks. Sensors. **10**, 3911–3933 (2010)
7. O Aziz, B Lo, AraDarzi, GZ Yang, in *Body Sensor Networks*. Chapter 1. Body sensor networks - introduction (Springer-Verlag, London, 2006)
8. A Ali, S Irum, K Firdous, FA Khan, A cluster-based key agreement scheme using keyed hashing for body area networks. Multimedia Tools and Applications. **66**(2), 201–214 (2013)
9. A Ali, FA Khan, in *Proceedings of International Conference on Information Security & Assurance (ISA'10)*. An improved EKG-based key agreement scheme for body area networks, Springer Berlin Heidelberg (Miyazaki, June 2010)
10. KK Venkatasubramaniam, A Banerjee, SKS Gupta, in *Proceedings of the 2nd IEEE INFOCOM Workshop on Mission Critical Networks*. EKG-based key agreement in body sensor networks (New York, April 2008)
11. BJ West, *Where Medicine Went Wrong: Rediscovering the Path to Complexity (Studies of Nonlinear Phenomena in Life Science*. (World Scientific Publishing Company, Singapore, 2006)
12. B Zarei, M Zeynali, VM Nezhad, Novel cluster based routing protocol in wireless sensor networks. Int. JComput. Sci. Issues(IJCSI). **7,4,** 32–36 (2010)
13. H Krawczyk, M Bellare, R Canetti, HMAC: keyed-hashing for message authentication. (RFC2104., HMAC, February 1997)
14. F Adelstein, SKS Gupta, G Richard, L Schwiebert, *Fundamentals of Mobile and Pervasive Computing*. (McGraw Hill, New York, 2005)
15. F Kausar, MQ Saeed, A Masood, in *4th IEEE International Conference on Wireless and Mobile Computing, (Networking and Communications (SecPriWiMob 2008)*. Key management and secure routing in heterogeneous sensor networks (Avignon, 12–14 October 2008)
16. WR Heinzelman, A Chandrakasan, H Balakrishnan, in *Proceedings of IEEE 33rd Hawaii International Conference on System Sciences (HICSS-33)*. Energy-efficient communication protocol for wireless microsensornetworks (Hawaii, 4–7 January 2000)
17. K Van Laerhoven, BPL Lo, JWP Ng, et al., in *3rd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications (UbiHealth) [Online]*. Medical healthcare monitoring with wearable and implantable sensors. Available: http://www.healthcare.pervasive.dk/ubicomp2004/papers/final_papers/laerhoven.pdf
18. A Darwish, AE Hassanien, Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors. **11**, 5561–5595 (2011)
19. P Kumar, HJ Lee, Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors. **12**(1), 55–91 (2012)
20. G Selimis, L Huang, F Massé, I Tsekoura, M Ashouei, F Catthoor, J Huisken, J Stuyt, G Dolmans, J Penders, H De Groot, A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design. J. Med. Syst. **35**, 289–1298 (2011)

21. D Balfanz, DK Smetters, P Stewart, H Chi Wong, in *Proceedings of the Symposium on Network and Distributed Systems Security*. Talking to strangers: Authentication in ad-hoc wireless networks (San Diego, California, February 2002)
22. RV Sampangi, S Dey, SR Urs, S Sampalli, A security suite for wireless body area networks. Int. J. Netw. Secur. & Its Appl. (IJNSA). **4,1,** 97–116 (2012)
23. ZHU S, S Setia, S Jajodia, LEAP+: efficient security mechanisms for large-scale distributed sensor networks. ACM Trans. Sens. Netw. **2,4,** 500–528 (2006)
24. L Eschenauer, VD Gligor, in *CCS Proceedings of the 9th ACM Conference on Computer and Communications Security*. A key-management scheme for distributed sensor networks (ACM, New York, 18–22 November 2002)
25. C Kuo, M Luk, R Negi, A Perrig, in *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems (SenSys '07)*. Message-in-a-bottle: user-friendly and secure key deployment for sensor nodes (ACM, New York, 6–9 November 2007)
26. KK Venkatasubramaniam, SKS Gupta, S Cherukuri, in *Proceedings of IEEE International Conference on Parallel Processing Workshops*. BioSec: A biometric based approach for securing communication in Wireless networks of biosensors implanted in the human body (Kaohsiung, 6–9 October 2003)
27. R Mayrhofer, in *Proceedings of the 4th European conference on Security and Privacy in Ad-hoc and Sensor Networks (ESAS'07)*. The candidate key protocol for generating secret shared keys from similar sensor data streams (Berlin, July 2007)
28. R Mayrhofer, H Gellersen, in *Proceedings of the 5th International Conference on Pervasive Computing (PERVASIVE'07)*. Shake well before use: authentication based on accelerometer data (Berlin, 13–16 May 2007)
29. KK Venkatasubramaniam, SKS Gupta, in *Proceedings of IEEE International Conference on Intelligent Sensing and Information Processing (ICISIP '06)*. Security for pervasive health monitoring sensor applications (Bangalore, 14–16 December 2006)
30. D Baker, A Ephremides, The architectural organization of a mobile radio network via a distributed algorithm. IEEE Trans. Commun. **29,11,** 1694-1701 (1981)
31. WR Heinzelman, A Chandrakasan, H Balakrishnan, An application -specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun. **1**(4), 660–670 (2002)
32. H Ali, W Shahzad, FA Khan, Energy-efficient clustering in mobile ad hoc networks using multi-objective particle swarm optimization. Appl. Soft Comput. **12**(7), 1913–1928 (2012)
33. K Sun, P Ning, C Wang, in *Proceedings of Annual Computer Security Applications Conference (ACSAC '06)*. Secure distributed cluster formation in wireless sensor networks (Washington, DC, December 2006)
34. V Laerhoven, H Gellersen, in *Proceeding of the 8th International Symposium on Wearable Computers*. Spine versus porcupine: a study in distributed wearable activity recognition (Washington, DC, 31 October to 4 November 2004)
35. K Ouchi, T Suzuki, M Doi, in *Proceedings of the 22nd International Conference on Distributed Computing Systems Workshop*. Lifeminder: A wearable healthcare support system using user's context (Vienna, July 2002)
36. O Younis, S Fahmy, HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. Proc. IEEE Trans. mobile comput. **3**(4), 366–379 (2004)
37. C Karlof, D Wagner, in *Proceedings of 38th International Conference on Communication*. Secure routing in wireless sensor networks: attacks and countermeasures (New York, 7–9 September 2003)
38. X Du, Y Xiao, Energy efficient chessboard clustering and routing in heterogeneous sensor network. Int. J. Wireless and, Mobile Comput. **1**(2), 121–130 (2006)
39. K Deb, A Pratap, S Agarwal, T Meyarivan, A fast and elitist multi-objective genetic algorithm: NSGA-II. IEEE Trans. Evol. Comput. **6**, 182–197 (2002)
40. YD Valle, GK Venayagamoorthy, S Mohagheghi, JC Hernandez, Particle swarm optimization: basic concepts, variants and applications in power systems. IEEE Trans. Evol. Comput. **122**, 171–195 (2008)
41. S Capkun, M Hamdi, JP Hubaux, *GPS-free positioning in mobile ad hoc networks*, vol. 5, 2, (2002), pp. 157–167
42. S Capkun, M Hamdi, JP Hubaux, in *Proceedings of the IEEE 34th Annual Hawaii International Conference on System Sciences (HICSS-34)*. GPS-free positioning in mobile ad-hoc networks (Washington, DC, 2008)
43. GM Bar, B Fidan, DO Anderson, 2007 Wireless sensor network localization techniques. Comput. Netw. **51**, 2529–2553 (2007). doi:10.1016/j.comnet.2006.11.018
44. NIH, NIBIB, National Institute of General Medical Sciences, PhysioBankArchive. http://www.physionet.org/physiobank/database/. Accessed 15 October 2012
45. RG Brown, Dieharder: a random number test suite. http://www.phy.duke.edu/~rgb/General/dieharder.php Accessed 23 October 2012
46. G Marsaglia, *DIEHARD Statistical Tests*, (Florida State University, 1995)
47. Intel Platform Security Division, The Intel random number generator. Intel Technical Brief, (1999). http://citeseer.ist.psu.edu/435839.html Retrieved 6 December 2012
48. W Feller, *An Introduction to Probability Theory and Its Applications*, 3rd edn, vol. 1. (Wiley, NewYork, 1968)
49. BS KaliskiJr, RL Rivest, AT Sherman, Is the data encryption standard a group? (results of cycling experiments on DES). J. Cryptol. **1**, 3–36 (1988)
50. D Liu, P Ning, in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03)*. Establishing pairwise keys in distributed sensor networks (ACM, New York, 2003), pp. 52–61
51. D Raffo, PhD Thesis, Chapter 6: cryptosystems for the ad hoc environment. Université Paris 6, 2005. http://perso.crans.org/raffo/papers/phdthesis/thesisch6.html. Accessed 28 May 2013

doi:10.1186/1687-1499-2013-216
Cite this article as: Ali and Khan: **Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications.** *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:216.