Development and Simulation of Enhanced Key Management Scheme for WBANs

Sufyan T. Faraj Al-Janabi
College of Computer,
University of Anbar
Ramadi, Iraq
sufyantaih@yahoo.com

Ali J. Dawood
College of Computer,
University of Anbar
Ramadi, Iraq

Ekram Habeeb Hassan
College of Computer,
University of Anbar
Ramadi, Iraq

Abstract— **The design and deployment of Wireless Body Area Networks (WBANs) have recently resulted from the use of sensors to measure the biometrics and movements of the human body. The development of such networks is imperative for modern telemedicine and e-health. Since WBANs are dealing with very sensitive information (i.e., medical data which has a direct impact on human life), security is an essential part of WBANs design. Indeed, key management plays pivotal role in ensuring security requirements in WBAN.**

In this paper, an enhanced version of a biometric-based distributed key management scheme is introduced. This scheme is designed for use in WBAN scenarios. It makes use of key refreshment schedules and distributes key management responsibility among all nodes in a WBAN in a fair manner. The scheme supports the use of biometric measurements to generate symmetric keys in WBANs via facilitating the work of biometric random number generators that can extract a random bit sequence from biological data to generate symmetric keys. A general description of the development of this scheme is given along with all phases of its operation. Furthermore, simulation results are presented with security analysis related to the resistance of the proposed scheme against some possible attacks.

Keywords— ***biometric randomness; e-health; key management; security; WBAN***

I. INTRODUCTION

Advances in wireless communication sensing technologies have been the motivation behind the development of Wireless Body Area Networks (WBANs). WBAN is a modern technology used to enhance health observance and alternative health care application systems. WBANs can offer efficient and simple ambulatory health monitoring for extended periods of time and almost real-time updates of patients' medical records through the Internet. Many interesting WBAN-based systems for health monitoring have been proposed during tha last decade. Each of these systems has its pros and cons (See for example [1]-[4]).

WBAN is faced with varied security problems like loss of information, authentication, and access control [5]. So, Security is necessary to protect WBANs against unauthorized use that could be dangerous to the life of the user (e.g. change of dosage of drugs or treatment procedures) [6].

Key management protocols or schemes are basic necessities to develop secure applications. These protocols are used to set up and distribute varied forms of cryptographic keys to nodes within the network to achieve sufficient security services. Dealing with WBAN facilitates the use of biometric methods in cryptography for authentication purposes. This is mainly achieved by using biological data for generating sequences of random bits [7]. WBAN network is small in size; each node in communication range of others and all sensors near personal server (PS). This makes all sensors communicate directly with PS and there is no need for cluster sensor to relay this communication. The PS usually communicates with a medical server (MS) via a reliable and secure link (e.g. VPN). Typically MS can be responsible to communicate with more than WBAN through their relative PSs.

The aim of this paper is to develop and simulate a biometric-based authentication and key management scheme for WBANs which relies on biometric symmetric cryptography. The remainder of this paper organized as follows: Section 2 gives a survey about significant related work. Then, our proposed key management scheme with all its phases and details are explained in Section 3. In Section 4, a review on the normal network operation in our developed simulation environments is given. Next, security analysis and services provided by this scheme are presented in Section 5. Simulation results are discussed in Section 6. Finally, the paper is concluded in Section 7.

II. RELATED WORK

Despite the fact that WBANs are a special type of Wireless Sensor Networks (WSNs), there are several differences between them from topology scale, the size of the operational area, and human intervention. These differences result in that most of the schemes for key

management which are generally efficient in WSN scenarios are not suitable for WBAN applications. Usually their designs are overly complex for WBAN scenarios. But, one the most important differences are that WBANs can use random biometric signals as cryptographic keys. Thus, many researchers focused in their work on application characteristics of WBANs and the usage of biometric properties as keys**.**

In 2010, Raazi et al [8] proposed a distributed key management scheme, which makes use of key refreshment schedules to distribute key management responsibility among all nodes in a WBAN in a fair manner. This scheme supports the use of biometric measurements to generate symmetric keys in WBAN scenarios. This scheme is considered to be very interesting key management scheme for WBANs. However, it does not have time synchronization, does not consider multiple sensing issues, and lacks some important security features.

In 2010, Yao et al [9] proposed a highly flexible authentication and key establishment protocol based on electrocardiogram (ECG) signals and fuzzy commitment, namely ESKE. The idea behind using ECG is that the uniqueness of ECG signals guarantees ESKE can provide long, random, low latency, distinctive, and temporal variant keys. The fuzzy commitment assures that ESKE scheme can tolerate the high degree of noise and variability inherently in ECG signals. When the control unit (CU) authenticates a biosensor, CU will send a message including the real biometric data and some chaff points. The biosensor will calculate the similarity between its own set of points and the set of points from CU. If a sufficient number of points can match within a certain threshold, the biosensor will be proved as legal. At last a session key would be established

In 2011, Mana et al [10] proposed a trusted key management scheme that exploits ECG to address security issues in WBAN. They made use of the ECG-generated binary sequence for a symmetric encryption scheme. However, they used its morphed version using a morphing block (using the MD5 function for the morphing function). This approach also managed the distribution of symmetric cryptographic keys to constituent sensors in a WBAN and protected the privacy.

In 2012, Sivaprasatham et al [11] proposed a secure key management (SKM) technique for WBAN, The proposed architecture is constructed that include a set of WBANs connected to the master server which connected with backend server using authentication channel. Backend server and master server use a shared symmetric key. This is performed with the help of private and authenticate out-of band channel. In order to ensure authentication of the Backend Server (BS), we use three types of keys which are: Message Key (K_{msg}) which is used for communicating with backend server and other nodes, Master Key (K_{mas}) that is used for refreshing the message key by scheduling the re-keying intervals, and Secret key (K_{sec}) which is shared with the master server and this key is unique for each node.

III. PROPOSED KEY MANGEMENT SCHEME

The proposed scheme is a distributed key management scheme in which Key management responsibility is distributed among all sensors in WBAN in a secure and fair manner and it is not limited on one sensor. Every node takes its turn according to key refreshment schedule issued by a *PS* which issues a dedicated turn and time out for every sensor. *PS* also issues new key refreshment schedule periodically. Every node refreshes the key in the slot allotted to it. The scheme supports the use of biometric measurements as symmetric keys because they exhibit sufficient randomness properties, long, time variant and are distinctive for different people .This proposal has adapted symmetric cryptography because asymmetric operations are very expensive in terms of resource consumption and are not very suitable for the sensor networks. In this scheme, every sensor is responsible about generating its required keys. The main phases of the proposed system are depicted in Figure1. In the next subsections, we will describe each phase alone.

A. Initial Deployment Phase

In this phase, before the network is deployed, sensors are initialized by loading them (e.g., during manufacturing) with identities and authentication codes (***ID, Auth-code***) respectively, where "*ID*" represents the sequence of sensor in the network and "*Auth-code*" is used to authenticate each of these sensors. These *Auth-cods* enable every sensor to be known and trusted by others. Every sensor in the network has unique *ID* and *Auth-code*.

Sensor nodes come pre-loaded with *Auth-code*s of all nodes in the network, *ID* and *Auth-code* of all nodes are pre-loaded in the PS according to the database. On the other hand, PS and MS have their own special authentication codes, so that they can be trusted in the network. Also, PS is assumed to be equipped with specific biometric recognition system to authenticate authorized person for using PS. The initial default number of sensors that are considered in the network simulation is 9 sensors. This number can be increased (or decreasd) according to specific scenarios.These sensors are associated to one PS.

After the initialization procedure, sensors are ready to put on the patient's body. The PS is usually deployed firstly, connected with MS through an external secure communication channel (such as a secured connection or VPN on the internet), and then sensors are deployed in various parts of the patient's body sequentially.

B. Basic Biomedical Readings and Signals

The second phase includes generating the required medical readings. Every sensor is specialized to one medical measurement or reading. Table 1 shows physiological signals that our simulation is supposed to be dealing with and their parameter range.

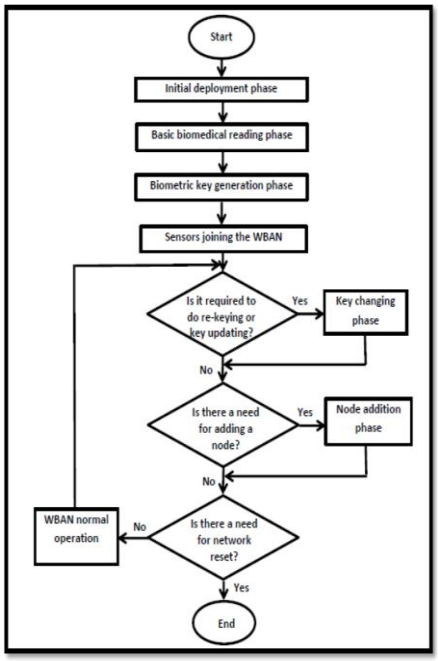

Fig. 1. Main phases of the proposed scheme

TABLE I. TYPICAL PARAMETER VALUES OF SIMULATED PHYSIOLOGICAL DATA

Physiological Signal	Parameter Range
Respiratory Rate	2 - 50 breaths/min
Blood Pressure (BP)	10 - 400 mmHg
Body Temperature	32 - 40° c
EEG	3µv-300µv
Glucose sensor	140-100 mlg\dl
Electrocardiography (ECG)	0.5-4mv
Blood flow	1 - 300 ml/s
Heart beat rate	60-80 beat\mint
Galvanic skin Reflex(GSR)	30µv-3mv

Every sensor measures the same biometric signal more than once (as required) in order to generate the keys relative to it. In this phase, it has been hypothesized that every sensor sense or measure its biometric only ten times to generate one key. So, to generate the required four keys for each sensor, the sensor must read the same biometric approximately 40 times. Since these measurements need not to be correlated among sensors, there is no need for error-correcting codes to correct errors in measurements.

C. Biometric Keys Generation Phase

Biometric key generation is the process of calculating a binary sequence extracted from biometric reading as cryptographic keys. This phase has applied the method "last digit fluctuation" (See Algorithm 1) to generate random sequence from biometric data and extract the least significant bit from every reading. A number of mathematical transformations are then applied on the biometric measurement before keeping the most right bit (or the least significant bit) of each measurement which exhibit sufficient randomness. The fundamental idea of this method is that the least significant bit from every reading has a sufficient randomness [7]. Since this technique does not involve complex mathematical operations, it has been assumed that key generation will solely be done by sensor nodes.

Algorithm 1: Last Digit Fluctuation Method
Input: *10 numbers// variant*
Output: *sequence of binary number //variant*
Step1: Let $\{x_i\}^{n}_{i=1}$ *where n=number of reading from every sensor*
Strep2: Calculate average of these readings.

$$av=1\backslash n \quad \sum_{i=1}^{n} x_i \qquad (1)$$

Step3: Calculate the standard deviation for these readings

$$S=\sqrt{1\backslash n-1\sum_{i=1}^{n}(xi-av)}^{2} \qquad (2)$$

To eliminate the large fluctuations in the data, this improves the performance of the method. This means that we record only those measurements which are not too far from the average.
Step4: $1 \leftarrow r$ *; where r is parameter of the order of 1.*
Step 5: $r*s \leftarrow rs$
Step 6: $av\text{-}rs \leftarrow h1$; $av+rs \leftarrow h2$
Step7: $h2\text{-}h1 \leftarrow l$.
Step8: For i=h1+1 to h2 do

$$L^i=\lfloor (xi-av-rs\backslash 2rs)*l \rfloor \qquad (3)$$

Step9: $b^i=l^i \bmod 2$.
b^i *sequence of binary number where k=bi*
Return k

Every sensor applies the same algorithm to generate keys relevant to it. It is worth mentioning every sensor has four keys, these keys as following:

1. Communication Key (K_{comm}): It is a network wide key and it is used to transfer data through the network in a secure manner through normal case for work of

network. Given that PS is more capable than a sensor node, it also participates in key management. K_{comm} is managed by the PS itself. Since K_{comm} is used very frequently.

2. Administrative Key (K_{admin}): It is the master key in the proposed scheme used to refresh K_{comm}. K_{admin} is also a group key but it is not used as frequently as K_{comm}. Naturally, K_{admin} is less exposed as compared to K_{comm}.
3. Basic Key (K_{bsc}): This key is only shared with the personal server and don't know by another sensor. Despite the fact that there are lesser chances of malicious activities in WBAN, but it is important to cover all possibilities. Thus, in order to prevent malicious activities K_{admin} needs to be refreshed through K_{bsc} at some point in time.
4. Secret Key ($K_{SN, MS}$): This Backup key is shared only with medical server (MS). It is important and is essential to recover from the compromise of PS or K_{bsc}.

These four keys are generated in the same method for every sensor. In spite of that the number of readings to generate keys is equal for every sensor but these keys are different in length according to the range value of physiological data; whenever was the range bigger the key length longer. These keys contain high random proposition. After every sensor generates its keys, it sends K_{comm}, $K_{admin,}$ and K_{bsc} to personal server to store them, and $K_{SN, MS}$ to medical server, using a secure "out-of-band" channel. The creation of a private and authenticate channel is based on the physical characteristics of the sensor nodes. Using this technique, the data can be sent through the channel confidentially such that data integrity and authenticity are also protected.

D. Sensor Joining the WBAN

This phase includes two main steps:

1. Soon after every sensor terminates generating its keys, it sends HELLO or a discovery message to PS, a HELLO message is structured in the following way:

$$m1: \forall i : SN^i \rightarrow PS: E_{Kadmin}\{ID^i|Auth\text{-}Code^i|HV\}$$

After all sensors send their discovery messages, every sensor is being part of WBAN. In order to prevent the PS from waiting forever, there is a timer which its period is as soon as the last expected node's discovery message is received or the timer expires. Then PS calculates the initial key refreshment schedule and broadcasts message *m2* as shown in the next step.

2. PS calculates the initial key refreshment schedule (See Figure 2) to update K_{admin}. According to this schedule the turn and time are allocated for every sensor to update K_{admin}. The refreshment schedule is broadcasted as follows:

$$m2: PS \rightarrow *: K_{admin}\{Key\text{-}Ref\text{-}Schedule|Auth\text{-}Code^{PS}|Timestamp|HV\}$$

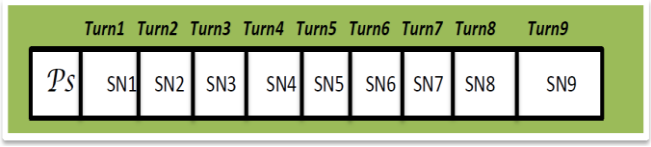

Fig. 2. Initial key Refreshment Schedule

The time assigns for update K_{admin} is divided between sensors equally. In this simulation, it has been hypothesized that every sensor needs "5000 ms" to update key specific to it. Through this interval the sensor must compute new values for the key and encrypted it with old value then broadcasts update in the network. This phase is summarized in Figure 3.

E. Key Change Phase

The aim of this phase is to achieve (when needed) the replacement of a key with another key that performs the same function**.** This is achieved by either re-keying or by key update, where the "value" of the new key is dependent on the value of the old key. This is called key update function. When the value of the new key is independent of the "value" of the old key, the process is known as re-keying. These two techniques have been adapted in this proposal as follows:

1. PS participates in key management, so it is responsible about re-keying K_{comm} for all sensor nodes. In order to refresh K_{comm}, the PS does not have to generate a key, it just needs to randomly select a value from already existing biometric measurements that have been measured by sensor nodes and forward to it. Since K_{comm} is frequently used, it needs to be refreshed rapidly. So, PS encrypts the new value of K_{comm} with K_{admin} and broadcasts it into the network as follows:

$$m3: PS \rightarrow *: E_{Kadmin}\{K_{comm}|Auth\text{-}Code^{PS}|HV\}$$

2. Every sensor is responsible about updating its K_{admin}. When the turn of sensor node *i* arrives, sensor node *i* waits for a certain period of time, computes a new value for K_{admin} from biometrics and broadcasts it in the network as follows:

$$m4: SN^i \rightarrow * : E_{Kold\ admin}\{K_{newadmin}|Auth\text{-}Code^i|HV\}$$

Every sensor will be equipped with a timer. In simulation, the interval property for every timer has been assigned at "5000 ms". When the timer for the first sensor expires, this declares terminating the turn of first sensor and beginning the turn of the second sensor by starting the timer of the second sensor, while other sensors wait for their turn, and so on (See Figure 4).

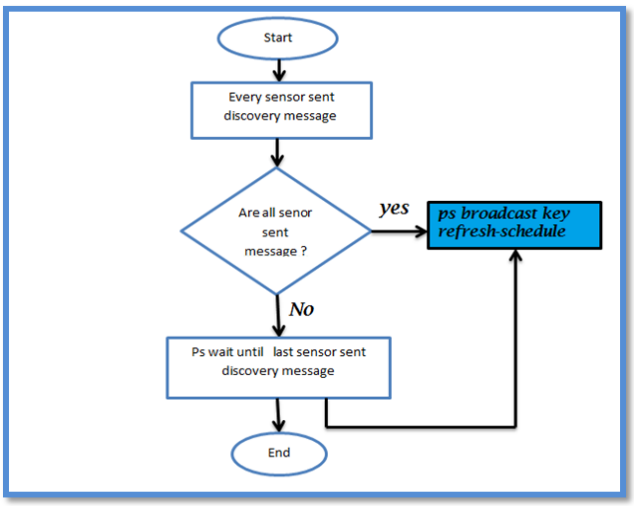

Fig. 3. Sensor Join WBAN

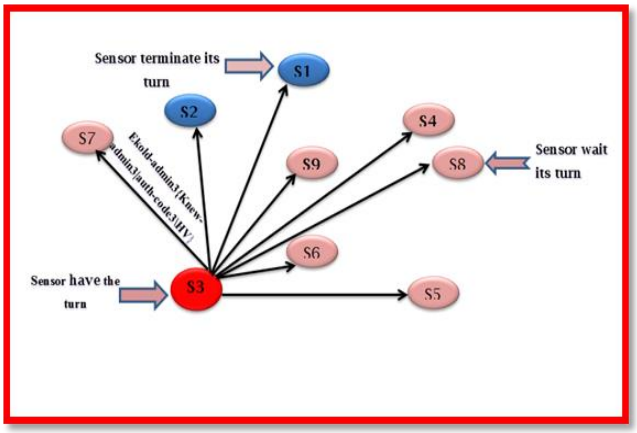

Fig. 4. Updating K_{admin}

Administrative key is refreshed periodically, therefore when the key refresh schedule is expired; the PS calculates the new schedule and broadcasts in the network as follows:

m5: PS → *: K_{admin} {Key-Ref-Schedule\|AuthCode^{ps}\|Timestamp\|HV}

This phase is recurring phase. So, assuming operating the network for two minutes; therefore, every minute the PS broadcasts a new key refreshment schedule. Figure 5 shows sequence of sensors according to second key refreshment schedule. This phase is summarized in Figure 6.

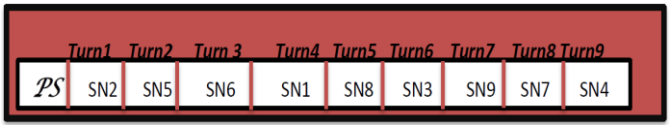

Fig. 5. Second Key Refreshment Schedule

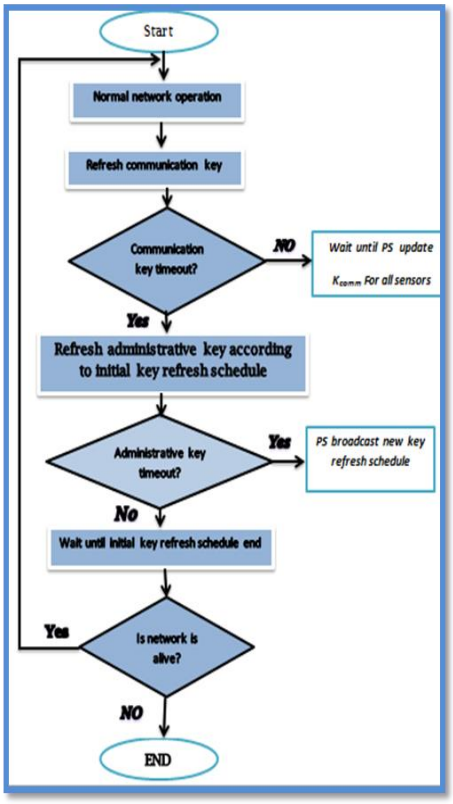

Fig. 6. Key Change Phase

F. *Node Addition Phase*

In some cases, there is an urgent need to add a new node to the network. One possible scenario for adding node: Replacing unemployed sensor which may be suffering from mechanical malfunction or power exhaustion, so the existing node stop working. Under such circumstances new node is added to the network instead of another. The new node takes same *"ID"* of old sensor but new "*Auth-code*" specialized to it and come pre-loaded with all *Auth-code*s for other sensors. PS declares in the network it is about to add a new node. *Auth-code* of replaced the sensor is deleted from the memory of other sensors and from the database in PS, and a new one is added instead. Figure 7 and Figure 8 represent a depicted simulation example of this case.

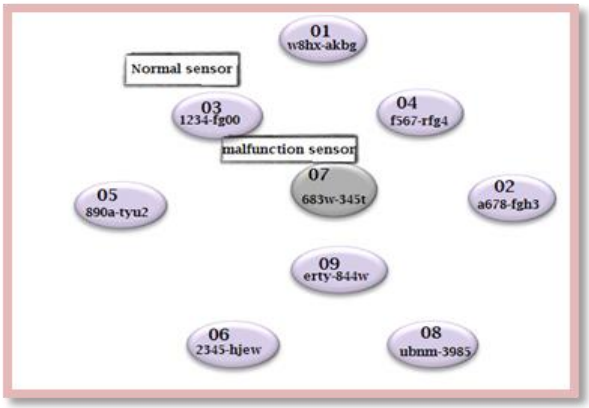

Fig. 7. Malfunction Sensor

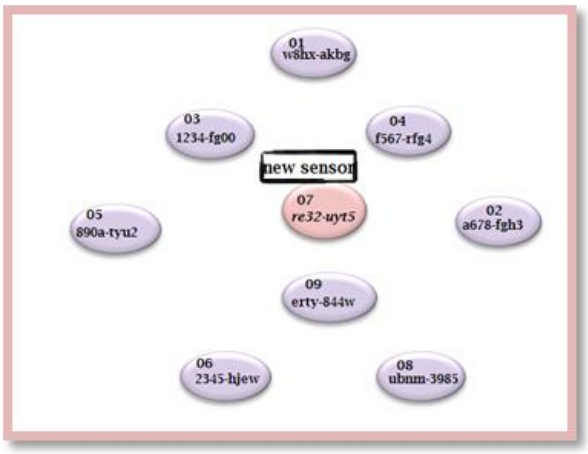

Fig. 8. New Added Sensor

The second possible scenario for adding a new sensor is the deployment of a new one to monitor some new biometric. In this case, MS informs PS about the new deployments by sending *ID* and *Auth-code* of new nodes to the PS:

$$MS \longrightarrow PS: \{ID^{j} | Auth\text{-}Code^{j} | Auth\text{-}Code^{ms}\}$$

where ***j*** represents new node that is added to the network. After the new node joining the WBAN, PS informs the new node by its turn in key refreshment by broadcasts the remaining key refreshment schedule. Also, PS takes upon the task of informing the network about new sensor, by broadcast the *ID*, *Auth-code* and turn of new sensor on the network. Other sensors store *Auth-code* for a new node. Newly deployed node can participate in key refreshment procedure after the next key refreshment schedule is issued by the PS including turn of the new sensor. According to this, node addition phase can be considered as occasional task.

IV. NORMAL NETWORK OPERATION

After completing the demonstration of key management, this section is dedicated to explaining the normal WBAN operations. As mentioned above, every sensor measures certain physiological data or signals. Supposing that we are dealing with following readings and signals: electrocardiography (ECG), blood flow, body temperature, blood pressure (BP), heartbeat, glucose in blood, galvanic skin reflex (GSR), nerve potential, and respiratory rate, as explained in Table 1. This involves a patient under monitoring of these sensors which continuously read data and transmit it wirelessly into PS (See Figure 9).To transmit these readings in a secure manner, sensors transmit them in an encrypted form by K_{comm} to PS as follows:

$$m6: \quad \forall\ i\ SNi \longrightarrow ps: Ek_{comm}\{Physiological\ signal\ |Auth\text{-}code^{i}|HV\}$$

In turn, the PS retrieves data and processes it before transmitting it to MS which analyze data, then based on this analysis MS returns recommendation to patients.

V. SECURITY ANALYSIS

Here we will emphasize some security services that are provided by the proposed scheme as well as important attacks that are avoided, as follows:

- ***Authentication:*** The proposed scheme provides authentication by using *Auth-code* in all communications. In this way, all receiving sensors know the origin of a message. If a message does not have a valid authentication code or does not contain *Auth-code*, it is discarded and malicious activity is indicated. On the other hand, the authentication in WBAN is enforced by using biometric keys. Also, the PS has its own *Auth-Code* and any unauthorized change in this *Auth-Code* is considered as compromising activity.
- ***Confidentiality:*** This aspect is ensured using symmetric encryption algorithms to encrypt all messages mutual between sensors and between the sensors and PS. To avoid cryptanalytic attacks or long term attack, keys are refreshed at regular intervals.
- ***Integrity:*** In the proposed scheme, integrity is provided by applying the SHA1 algorithm to generate 160 bits joined to each exchanged messages so as to ensure that messages have not been modified through transmission.
- ***Replay Attacks:*** To avoid this attack, timestamps have been applied in all communications. Using the timestamps also ensures data freshness.
- ***Routing Attacks:*** In WBAN, PS is in direct communication range of many nodes. Therefore, WBAN is not much vulnerable to routing attacks such as selective forwarding, sinkhole, Sybil, and wormhole attacks**.**

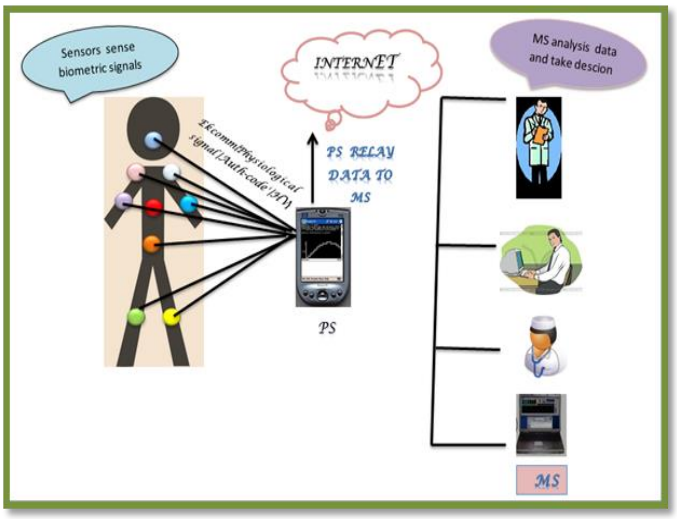

Fig. 9. Normal Network Operation in Secure Manner

VI. SIMULATION RESULTS

The simulated system prototype can be operated depending on two options of symmetric encryption.The first one is using the RC4 stream cipher, while the second one depends on a specific block cipher mode of operation of the AES algorithm (Using AES-CFB mode). More details about these two algorithms can be found in [12].

A simulation software package has been developed using Microsoft Visual C#, that exploits a suitable Graphical User Interface (GUI) to represent the network, Communication, and computation operations among sensors and PS. This language gives the programmer the flexibility to build large systems efficiently.

As known, WBAN deals with more sensitive data (biomedical data) associated with human life. So, one of the most important factors that we must take into account (besides security) is the execution time for this scheme. The system should consume less execution time as possible to be suitable to deal with this important data which must transfer as soon as possible to maintain the patient's life. So, execution time for many phases of this system was computed in milliseconds. Figure 10 represents a comparison between execution time for sensor join WBAN phase in RC4 algorithm with any key length for every sensor and key length of 128 bits, 192 bits and 256 bits in AES-CFB. According to this figure, RC4 algorithm takes less time and in the case of AES-CFB with the different key lengths there are slight differences.

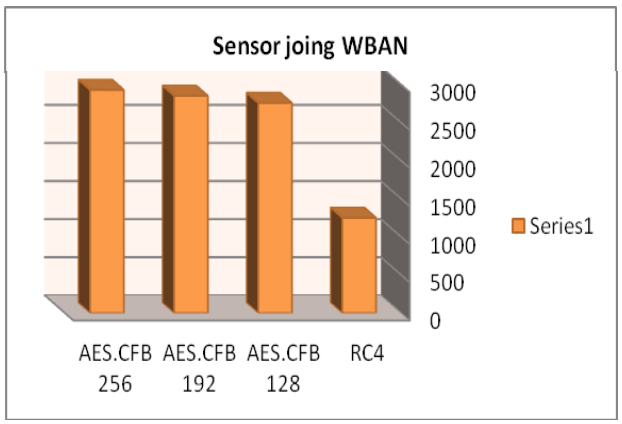

Fig. 10. Execution Time for sensor joining WBAN

Figure 11 shows execution time consumed by PS for updating K_{comm} in different cases mentioned above. The figure explains that AES-CFB with three key lengths takes time that is increasing asymptotically, but RC4 takes less time.

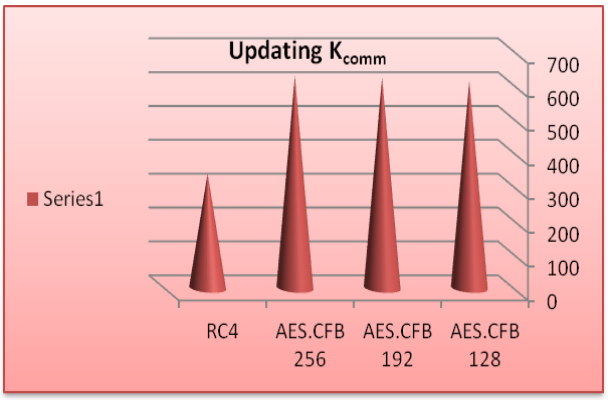

Fig. 11. Execution Time for Re-key Kcomm by PS

Figure 12 shows execution time for updating K_{admin} by all sensors in the network, where also RC4 take less time. As a result, it can be deduced that RC4 algorithm is more suitable for our system; especially it offers more than adequate security for such applications.

VII. CONCLUSION

WBANs consist of resource constrained sensing nodes. Key management plays a pivotal role to achieve the security services. In fact, a key management scheme is useless if it does not fulfill security requirements of the target network. One of the most important properties of WBANs can be the possibility of using random biometric measurements as keys. Our developed scheme makes benefit of this fact. The time factor is most important when dealing with WBAN. Hence, introduce an adequately secure scheme with small execution time is important. Our future work might include investigating the accurate time and energy consumed by the proposed biometric-based key generation technique when applied on actual sensing nodes.

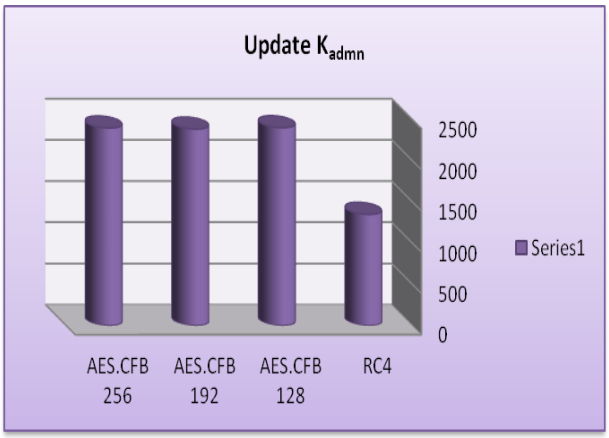

Fig. 12. Execution Time for Update Kadmin by all Sensors

REFRENCES

[1] E. Jovanov, A. Milenkovic, C. Otto, P. Groen, B. Johnson, S. Warren, and G. Taibi, "A WBAN System for Ambulatory Monitoring of Physical Activity and Health Status: Applications and Challenges," 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS 2005), China, pp. 3810-3813, Jan. 2006.

[2] C. Otto, E. Jovanov, and A. Milenkovic, "A WBAN-based System for Health Monitoring at Home," 3rd IEEE/EMBS International Summer School on Medical Devices and Biosensors, USA, pp. 20-23, Sept. 2006.

[3] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and Security in Wireless Body Area Network Infrastructures," Proceedings of the 27th Annual Conference of Engineering in Medicine and Biology, IEEE, Shanghai, China, Sept. 2005.

[4] Changle Li, Huan-Bang Li, and R. Kohno, "Performance Evaluation of IEEE 802.15.4 for Wireless Body Area Network (WBAN)", IEEE International Conference on Communications. ICC Workshops, Germany, pp.1-5, June 2009.

[5] Ramesh Kumar and Rajeswari Mukesh, "State Of The Art: Security in Wireless Body Area Networks", *International Journal of Computer Science & Engineering Technology (IJCSET)*, Vol. 4 No. 05 May 2013.

[6] Jingwei Liu and Kyung S. Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", *The Second International Conference on Ubiquitous and Future Networks (ICUFN)*, 2010.

[7] J. Szczepanskia, E. Wajnryba, J.M. Amigo´, Maria V. Sanchez-Vives, and M. Slater, "Biometric random number generators", *Computers & Security*, No. 23, pp. 77-84, 2004.

[8] Syed Muhammad Khaliq-ur-Rahman Raazi, Heejo Lee, Sungyoung Lee, and Young-Koo Lee, "BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks", *Sensors Journal*, Vol. 10, No. 4, pp. 3911-3933, MDPI, April 2010.

[9] Lin Yao, Bing Liu, Kai Ya, Guowei Wu, and Jia Wang, "An ECG-Based Signal Key Establishment Protocol in Body Area Network", *7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC)*, pp. 233-238, China, Oct. 2010.

[10] Mohammed Mana, Mohammed Feham, and Boucif Amar Bensaber, "Trust Key Management Scheme for Wireless Body Area Networks", *International Journal of Network Security*, March 2011.

[11] Venkatasubramanian Sivaprasatham and Jothi Venkateswaran, "A secure key management technique for wireless body area networks", *Journal of Computer Science*, Science Publications, 2012.

[12] William Stallings, *Cryptography and Network Security Principles and Practice*, Prentice Hall, 5th ed., 2011.