Trust Key Management Scheme for Wireless Body Area Networks

Mohammed Mana[1], Mohammed Feham[1], and Boucif Amar Bensaber[2]
(Corresponding author: Mohammed Mana)
STIC Lab., Department of telecommunications, University of Tlemcen, Tlemcen, Algeria[1]
Laboratoire de mathématiques et informatique appliquées LAMIA, Université du Québec à Trois-Riviéres[2]
C.P. 500 Trois-Riviéres, Québec, Canada G9A 5H7
(Email: manamed_alg@yahoo.fr, m_feham@mail.univ-tlemcen.dz, Boucif.Amar.Bensaber@uqtr.ca)
(Received Jan. 25, 2010; revised and accepted Feb. 17, 2010)

Abstract

With recent advances in wireless sensor networks and embedded computing technologies, miniaturized pervasive health monitoring devices have become practically feasible. In addition to providing continuous monitoring and analysis of physiological parameters, the recently proposed Wireless Body Area Networks (WBAN) incorporates context aware sensing for increased sensitivity and specificity. A number of tiny wireless sensors, strategically placed on the human body, create a WBAN that can monitor various vital signs, providing real-time feedback to the user and medical personnel. The wireless body area networks promise to revolutionize health monitoring. Since the sensors collect personal medical data, security and privacy are important components in this kind of networks. It is a challenge to implement traditional security infrastructures in these types of lightweight networks, since they are by design limited in both computational and communication resources. A key enabling technology for secure communications in WBANs has emerged to be biometrics. In this paper, we present an approach that exploits physiological signals (electrocardiogram (ECG)) to address security issues in WBAN: a Trust Key Management Scheme for Wireless Body Area Network. This approach manages the generation and distribution of symmetric cryptographic keys to constituent sensors in a WBAN (using ECG signal) and protects the privacy.

Keywords: Biometric security, ECG signal network, key management, privacy, wireless body area

1 Introduction

Recent technological advances in wireless networking, microelectronics integration and miniaturization, sensors, and the Internet allow us to fundamentally modernize and change the way health care services are deployed and delivered. Focus on prevention and early detection of disease or optimal maintenance of chronic conditions promise to augment existing health care systems that are mostly structured and optimized for reacting to crisis and managing illness rather than wellness [3].

Wearable systems for continuous health monitoring are a key technology in helping the transition to more proactive and affordable health care. They allow an individual to closely monitor changes in her or his vital signs and provide feedback to help maintain an optimal health status. If integrated into a tele-medical system, these systems can even alert medical personnel when life-threatening changes occur. In addition, the wearable systems can be used for health monitoring of patients in ambulatory settings [8]. For example, they can be used as a part of a diagnostic procedure, optimal maintenance of a chronic condition, a supervised recovery from an acute event or surgical procedure, to monitor adherence to treatment guidelines (e.g., regular cardiovascular exercise), or to monitor effects of drug therapy.

One of the most promising approaches in building wearable health monitoring systems utilizes emerging wireless body area networks (WBANs) [9]. A WBAN consists of multiple sensor nodes, each capable of sampling, processing, and communicating one or more vital signs (heart rate, blood pressure, oxygen saturation, activity) or environmental parameters (location, temperature, humidity, light). Typically, these sensors are placed strategically on the human body as tiny patches or hidden in user's clothes allowing ubiquitous health monitoring in their native environment for extended periods of time. Figure 1 illustrates a basic design of a health care system [21].

Security and privacy are important components in WBANs. A medical sensor network monitors humans. A human-centered sensor network has distinct features such as the sensitive nature of the data, the mobility of sensors, and the proximity to potential attackers, leading to these security challenges [17]:

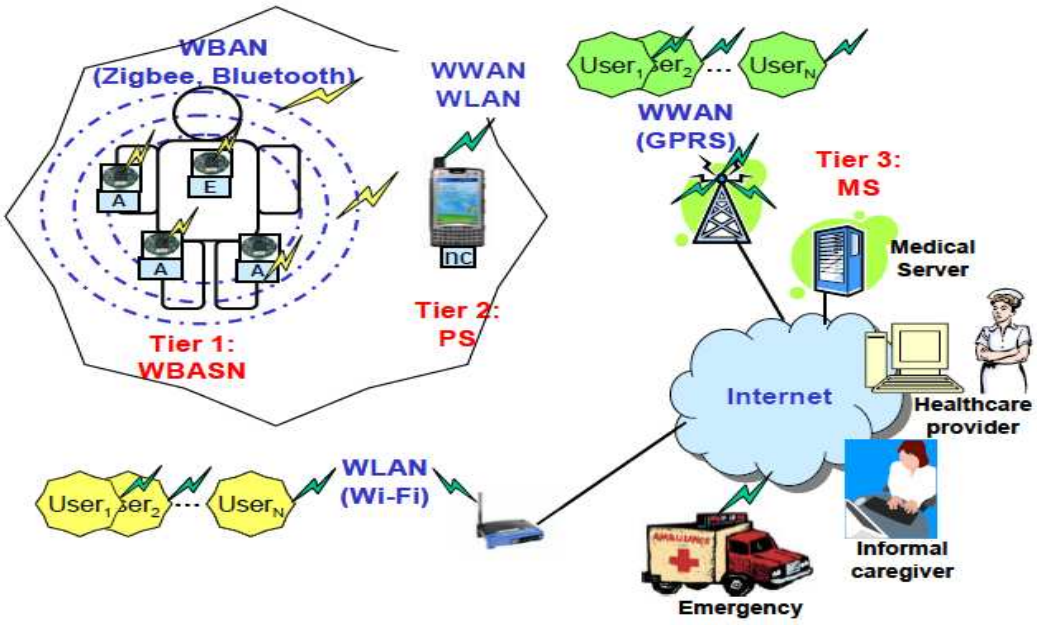

Figure 1: The basic design of a health care system

- How to ensure the privacy and integrity of the medical data, given that the wireless channel is easily subject to many forms of attacks?
- How to ensure that only authorized people can access the data?
- How to prevent someone from using captured sensors to recover sensitive medical information or inject false information?

Figure 1 illustrates the basic design of a health care system. There are three main components: the Wireless Body Area Network (WBAN), the external network and the medical server. The WBAN contains several sensors that measure medical data such as ECG, body movement, temperature etc. These sensors are equipped with a radio interface and send their measurements wireless to a central device called the personal server or the base station. This can be done either directly or via several intermediate hops. The base station is unique for each WBAN (and hence for every patient/user) and acts as a gateway between the WBAN and the external network. As it has more processing power than normal sensors, it can process the medical data and generate alarms if necessary. Each sensor shall only send its recorded data to the unique gateway it is linked with and this needs to be enforced by specific security mechanisms. The external network can be any network providing a connection between the base station and the medical server. The medical server securely stores, processes and manages the huge amount of medical bio-data coming from all of the patients. This data can then be observed and analyzed by medical staff.

What makes securing sensor networks more difficult than other types of networks is that wireless sensor nodes usually have limited resources, while conventional security mechanisms incur high costs in terms of CPU, memory, bandwidth, and energy consumption [17].

The contribution of our work is to secure communication links between sensor nodes using biometrics data. We propose to generate symmetric cryptographic keys from Electrocardiogram signal (ECG) and distribute them securely and efficiently between sensor nodes over the WBAN.

The remainder of this paper is organized as follows. Section 2 gives an overview of the security in WBANs. This is followed by a detailed descriptions for a trust key management scheme for wireless body area networks in Section 3. In Section 4, is given the analysis of our protocol in terms of security services and energy cost. Lastly, concluding remarks for future directions are given in Section 5.

2 Related Work

Security issues in WBAN are particularly important because sensitive medical information must be protected from unauthorized use for personal advantage and fraudulent acts that might be hazardous to a user's life (e.g., alteration of system settings, drug dosages, or treatment procedure).

The security mechanisms employed in Wireless Sensor Networks do generally not offer the best solutions to be used in Wireless Body Area Networks for the latter have specific features that should be taken into account when designing the security architecture. The number of sensors on the human body, and the range between the different nodes, is typically quite limited. Furthermore, the

Table 1: Security schemes used in health care architectures

System architecture	Hardware platform	Security scheme
Code Blue	Mica2	ECC & TinySec
ALARM-NET	Tmote Sky	Hardware Encryption
SNAP	Tmote Sky	Tiny ECC
WBAN	Tmote Sky	Hardware Encryption

sensors deployed in a WBAN are under surveillance of the person carrying these devices. This means that it is difficult for an attacker to physically access the nodes without this being detected. When designing security protocols for WBAN, these characteristics should be taken into account in order to define optimized solutions with respect to the available resources in this specific environment [22].

Several security solutions have been proposed in protecting biomedical sensor network. Following are presented the main approaches followed by the architectures mentioned in Table 1 [4, 5, 16, 27, 28].

2.1 TinySec

TinySec is proposed as a solution to achieve link-layer encryption and authentication of data in biomedical sensor networks [10]. TinySec [24] is a link-layer security architecture for wireless sensor networks that is part of the official TinyOS release. It generates secure packets by encrypting data packets using a group key shared among sensor nodes and calculating a MAC for the whole packet including the header. TinySec by default relies on a single key manually programmed into the sensor nodes before deployment. This network-wide shared key provides only a baseline level of security. It cannot protect against node capture attacks. If an adversary compromises a single node or learns the secret key, she can gain access on the information anywhere in the network, as well as inject her own packets. This is probably the weakest point in TinySec, since, node capture has been proved to be a fairly easy process.

2.2 Hardware Encryption

As an alternative to TinySec, one could utilize hardware encryption supported by the ChipCon 2420 ZigBee complaint RF Transceiver, one of the most popular radio chip on wireless sensor nodes. Based on AES encryption using 128-bit keys, the CC2420 can perform IEEE 802.15.4MAC security operations, including counter (CTR) mode encryption and decryption, CBC-MAC authentication and CCM encryption plus authentication. It can also perform plain stand-alone encryption of 128 bit blocks [12]. The WBAN group, employed this method in their network infrastructure [15], where the personal server shares the encryption key with all of the sensors in the WBAN during the session initialization. Hardware encryption is also followed by ALARM-NET [22]. One limitation of the method is that it does not offer AES decryption, so transmitted information cannot be accessed by intermediate nodes if needed (e.g. for aggregation purposes). Any decryption can be performed only at the base station. Another drawback of the method is that it is highly dependent on the specific platform. Other sensor node hardware do not offer hardware encryption support, so a different approach has to be taken in this case.

2.3 Elliptic Curve Cryptography

Recently, elliptic curve cryptography (ECC) has emerged as a promising alternative to RSA-based algorithms, as the typical size of ECC keys is much sorter for the same level of security. There have been notable advances in ECC implementation for WSNs in recent years. Uhsadel et al. [23] propose an efficient implementation of ECC and Liu et al. developed TinyECC [7], an ECC library that provides elliptic curve arithmetic over prime fields and uses inline assembly code to speed up critical operations on the ATmega128 processor. Also lately, Szczechowiak et al. presented NanoECC [2], which is relatively fast compared with other existing ECC implementations, although it requires a heavy amount of ROM and RAM sizes. Even though elliptic curve cryptography is feasible on sensor nodes, its energy requirements are still orders of magnitude higher compared to that of symmetric cryptosystems. Therefore, elliptic curve cryptography would make more sense to be used only for infrequent but security-critical operations, like key establishment during the initial configuration of the sensor network [19].

2.4 Biometric Methods

A key establishment method to secure communications in biomedical sensor networks has emerged to be biometrics [18]. It advocates the use of the body itself as a means of managing cryptographic keys for sensors attached on the same body, if they measure a piously agreed physiological value simultaneously and use this value to generate a pseudo-random number, this number will be the same. Then it can be used to encrypt and decrypt the symmetric key to distribute it securely. The physiological value to be used should be chosen carefully, as it must exhibit proper time variance and randomness. The ECG (electrocardiogram) has been shown to be appropriate [20]. Several schemes are proposed to protect WBAN using ECG signal, authors in [1, 13, 28] proposed to generate the session keys from ECG signal and distribute them between nodes over the network. The disadvantage of these methods is that the accuracy of key recoverability is less than 100% at nodes over the network.

Our contribution aims to generate symmetric session keys from ECG signal. It also aims to establish securely and efficiently the generated keys between the sensor

nodes and the base station in order to secure end to end transmission. Our protocol is characterized by minimal resource consumption.

3 Our Contribution

In this section, we present our protocol (Trust key Management Scheme for Wireless Body Area Network) which secures keys exchange between sensor nodes and the base station with minimal resource consumption.

3.1 Assumptions

Before describing the protocol, let us identify the assumptions underlying our model. We assume that:

- The base station has more resources than a regular sensor node.
- The base station can keep a record of the keys it shares with each sensor node and can use these keys to send confidential messages to individual nodes.
- The base station can make long range radio transmissions to reach a node anywhere within the sensor network. However, in order for messages to travel from a sensor node to the base station, the message has to hop from node to node in order to maximize the energy conservation.
- The base station has a pair of keys (private and public key).
- Each sensor is capable to use symmetric and asymmetric encryption, by implementing (hard or soft) each of these operations.
- Each sensor node gets the public key of the base station before deployment from an off-line dealer.
- The base station gets a template reference (biometric features generated from the ECG signal of the user) before deployment from an off-line dealer.

3.2 Notation

We will use the following notation to illustrate different primitives in our cryptographic operations:

- **Biokey:** is the ECG-generated key.
- $Biokey_{Ref}$**:** is the template reference. It is used to authenticate sensor nodes by the base station.
- $E_k(M)$: an encryption of message M with a symmetric key K.
- $E_{Pub}(M)$: is an encryption of message M with the Base station's public key.
- Id: is a node's identifier.

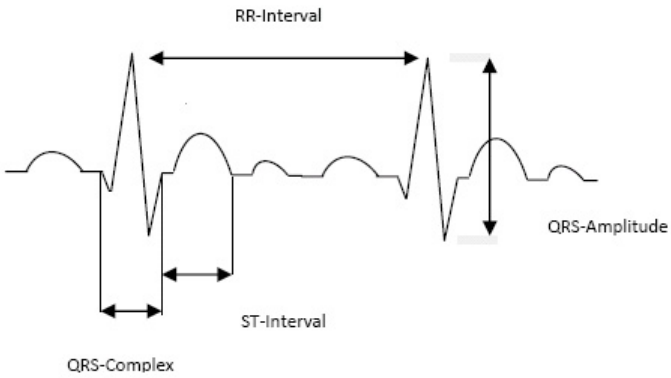

Figure 2: ECG signal

- A, B, C: are examples of node Ids.
- cmp_1, cmp_2, ...: are examples of a counter (initialized to some random values).
- $N_A, N_B, N_C, \ldots$: are examples of a nonce generated by nodes A, B, C, ..., respectively.

3.3 The Protocol

The protocol is divided in four steps, key generation phase, key setup phase, key authentication phase and key update phase.

1) Key Generation Phase:
While many physiological features can be utilized as biometrics, the ECG has been found to specifically exhibit desirable characteristics for WBAN applications. More specifically, it has delivered promising prospects for security in the WBAN settings. In this emerging area of research, the relevant ECG techniques ostensibly appear to be mere examples of fiducial methods. Fiducials are essentially points of interest on a heartbeat. The P, PQ, QRS, QT, T and RR time intervals as well as the amplitudes of P, R and T fiducials Figure 2 can be used to provide security in WBAN.

Good cryptographic keys need a high degree of randomness, and keys derived from random time varying signals have higher security, since an intruder cannot reliably predict the true key. This is especially the case with ECG, since it is time-varying, changing with various physiological activities [14]. More precisely, heart rate variability is characterized by a (bounded) random process [25].

Following is given a description of our strategy for generating cryptographic keys from the ECG signal Figure 3.

From a cryptographic perspective, the ECG-generated binary sequence (in our work, it is noted Biokey), is already suitable for a symmetric encryption scheme. However, we use its morphed version using a morphing block (here we use the MD5 function

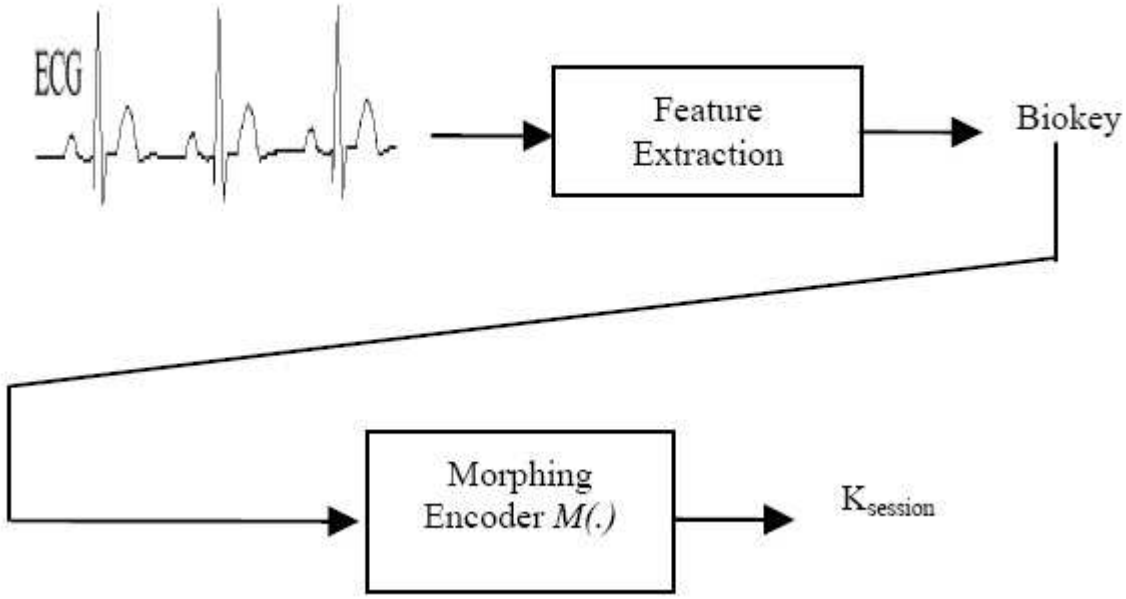

Figure 3: Key generation from ECG-signal

for the morphing function M(.)) to ensure user privacy and confidentiality. As noted in [15], for privacy reasons, any signals, including biometrics, generated from physiological data should not be retraceable to the original data. The reason is because the original data may reveal sensitive medical conditions of the user, which is the case for the ECG. Therefore, a morphing block serves to confidently remove obvious correlations between the generated key and the original medical data.

In the next section, is given how to exchange securely the generated session keys ($K_{session}$) between each sensor node and the base station.

2) Key Setup Phase:
The node closest to the BS (base station) initiates the key setup phase by issuing the "join- network" message. In our sample topology shown in Figure 4, node A and node B are the closest to the BS. Using the process discussed above in Key Generation, each node should:

- Generates the biometric key "Biokey".
- Computes the session key using Biokey and the morphing encoder (Ksession = M(Biokey)).
- Encrypts the Biokey with the base station's Public key, then transmits it to the Base Station.

Let us assume node A initiates the key exchange phase:

$$A \rightarrow BS : Id_A, E_{pub}(Biokey_A), \\ MAC(K_{sessionA}, Id_A||Biokey_A).$$

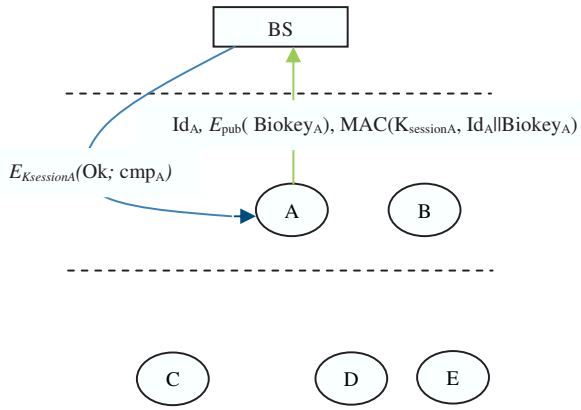

Figure 4: Node A initiates the key setup phase

The base station decrypts the received message with its corresponding private key, compares the received $Biokey_A$ to the template reference $Biokey_{Ref}$. On confirming the validity of the device (i.e. the check is successful), the base station computes the session key $K_{sessionA}$ using the received $Biokey_A$. It uses this key ($K_{sessionA}$) to check the MAC message and to send the following encrypted information to node A: an Ok message and a counter cmp_A, initialized to some random value. The counter is used to assure freshness. Every time the counter is used, the value gets incremented by 1.

$$BS \rightarrow A : E_{K_{sessionA}}(Ok, cmp_A).$$

The first nodes that manage to complete the key setup procedure with the base station act as gateways for the other nodes in the network. The next sensor node (assume C as shown in Figure 5) wishing to join the network performs the same sequence of steps performed by node A:

- Generates the biometric key $Biokey_C$.
- Computes the session key $K_{sessionC}$, ($K_{sessionC} = M(Biokey_C)$)
- Encrypts the $Biokey_C$ with the base station's Public key. The request "join- network" is then broadcast by the node C.

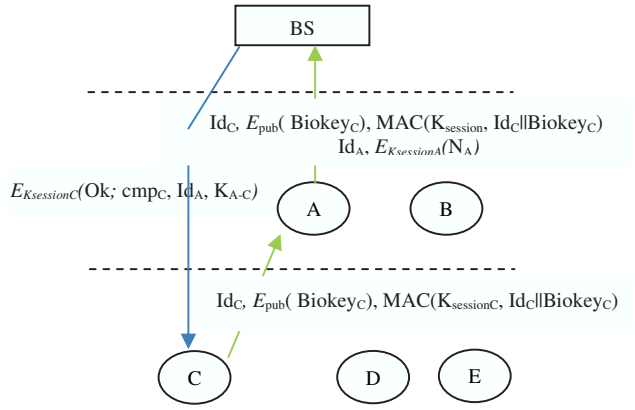

Figure 5: Node C initiates the key exchange phase

In our sample topology, the request will be received by the node A.

$$C \rightarrow A : Id_C, E_{pub}(Biokey_C), MAC(K_{sessionC}, Id_C||Biokey_C).$$

Node A generates a nonce N_A and encrypts it with its session key. It appends its identifier Id_A and the encrypted N_A to the request. The request is finally forwarded to the BS:

$$A \rightarrow BS : Id_C, E_{pub}(Biokey_C), MAC(K_{sessionC}, Id_C||Biokey_C), Id_A, E_{KsessionA}(N_A).$$

The base station performs the routine validity checks on the sensor node and sends node C the information it needs to be a part of the network. In addition to the Ok message and the counter cmp_C the base station also sends node C the identifier Id_A of node A and the key authentication K_{A-C}[1] ($K_{A-C} = M(K_{sessionA}||N_A)$) to inform it that node A is its gateway to reach the base station.

$$BS \rightarrow C : E_{KsessionC}(Ok, cmp_C, Id_A, K_{A-C}).$$

[1] K_{A-C} is used to secure communication link between node A and node C.

Once this information is available at node C, it attempts to authenticate its gateway A as described in the next section.

Node C is setting up a secure key with the base station. The gateway node A has already successfully complete the key setup procedure with the base station.

3) Key Authentication Phase:
On receiving the Id_A and the key authentication K_{A-C}, node C attempts to authenticate its gateway A using a challenge response. To do so, node C generates a nonce N'_C, encrypts it with the key authentication K_{A-C} and transmits it to the node A. Node A, on receiving an "authenticate me" message, computes its own copy of $K_{A-C} = M(K_{sessionA}||N_A)$ and responds with the original nonce N'_C and a new nonce N'_A, both encrypted with the newly agreed key K_{A-C}. To complete node C's authentication, node C responds with the nonce $N'A$ encrypted with the shared key K_{A-C}.

$$\begin{aligned} NodeC \rightarrow NodeA &: Id_C, E_{KA-C}(N'C). \\ NodeA \rightarrow NodeC &: Id_A, E_{KA-C}(N'C, N'A). \\ NodeC \rightarrow NodeA &: Id_C; E_{KA-C}(N'A). \end{aligned}$$

The same process is then carried out for all the remaining sensor nodes as they join the network.

4) Key Update Phase: a key update tries to prevent long term attack aiming to extract the encrypting keys by analyzing the encrypted traffic over the network for long time. In a WBAN an automatic key update must be defined, since a network can be deployed for many days or months. In our approach, we propose a periodic key update for each established session key.

The key update is initiated by the base station by launching a key update request. On receiving the key update request, each sensor node generates a new biometric key Biokey', Encrypts it with the base station's public key and sends the encrypted message to the base station.

$$Node \rightarrow BS : E_{Pub}(Biokey').$$

On receiving the encrypted message, the base station decrypts it, checks the node's validity, computes the new session key from Biokey' (the new key $K'_{session} = M(Biokey')$), updates the session key and sends an Ok message and a new counter cmp' to the node.

$$BS \rightarrow Node : E_{K'session}(Ok, cmp').$$

The period of the key update is relative to the key length and the complexity of the used algorithm which means that this period is fixed by the administrator of the WBAN.

4 Analysis

4.1 Security Services

- **Confidentiality:** This aspect is ensured by the use of symmetric encryption to encrypt the exchanged traffic between the base station and sensor nodes. The confidentiality is enforced using automatic key update to prevent long term attacks.
- **Integrity:** The integrity in our approach can be ensured using MAC (Message authentication codes) computed and joined to each sent packet between the base station and any sensor over the network.
- **Authentication:** Authentication between sensor nodes over the WBAN as well as between each sensor node and the base station is ensured using the ECG-generated keys.
- **Data freshness:** the use of the counter avoids replay attacks and ensure data freshness.

4.2 Energy Cost Analysis

The energy cost of any key management scheme is determined by the energy required for the execution of cryptographic primitives and the energy needed for transmitting the encrypted data. According to [26], the transmission of a single byte of data requires 59, 2muJ and 28, 6μJ for reception.

To join network, a sensor node needs to send one message to the base station containing its identifier (1 bytes), the biometric key (16 bytes) and the MAC message (16 bytes) added 12 bytes of protocol headers. Thus the size of the sent packet is 45 bytes, the energy needed for transmitting such packet is 2,67 mJ. In reception, added to the protocol headers the sensor node receives an Ok message (2 bytes) and a counter (4 bytes) added one bytes of gateway's identifier and 16 bytes of the key authentication if the sensor node is far from the base station and cannot directly communicate with it, the energy needed for reception is 1,01 mJ at max. In addition, the energy needed to encrypt the message using the base station's public key is 22, 82 mJ and that needed to decrypt the received message sent by the base station is 0,054 mJ according to [26] if the used algorithm is AES and using 128 bits key length. Therefore the total energy cost is 26, 56 mJ.

To complete mutual authentication, a sensor node needs a 1, 57 mJ to complete the challenge response.

Consequently, the total energy cost of our protocol is 28, 13mJ.

Compared to other schemes based ECC-160 bits (Table 2, Figure 5) like simplified SSL protocol [6] or simplified Kerberos protocol [11] where their energy costs are respectively 39 mJ and 39.6-47.6 mJ, our scheme is more energy saving which make it very suitable for wireless body area network.

Table 2: Energy cost comparison

Schemes based ECC	Energy cost (mJ)
SSSL	39
SKERBEROS	39,6 -47,6
Our protocol	28,13

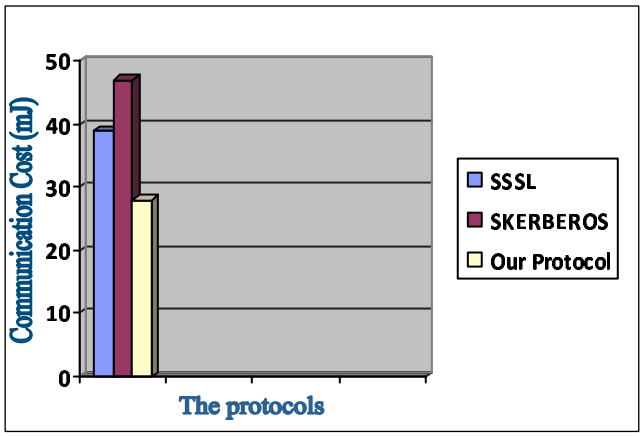

Figure 6: Energy cost consumption

5 Concluding Remarks

Wireless Body Area Networks (WBANs) are an enabling technology for mobile health care. These systems reduce the enormous costs associated to patients in hospitals as monitoring can take place in real-time even at home and over a longer period. A critical factor in the acceptance of WBANs is the provision of appropriate security and privacy protection of the wireless communication medium. The data traveling between the sensors nodes should be kept confidential and integrity protected. Certainly in the mobile monitoring scenario, this is of uttermost importance.

In this paper, we have presented a trust key management scheme for wireless body area network. Our protocol attempts to solve the problem of security and privacy in WBANs. It also aims to securely and efficiently generating and distributing the session keys between the sensor nodes and the base station to secure end to end transmission. It also allows to secure communication links between the nodes themselves.

Compared to other approaches, our approach is more suitable for wireless body area network because it is efficient and energy saving.

Acknowledgments

The research is developed in STIC (System and Technology of Information and Communication) Laboratory, Department of telecommunications, University of Tlemcen, Tlemcen, Algeria.

References

[1] S. D. Bao, C. Y. Poon, Y. T. Zhang, and L. F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Transactions on Information Technology in Biomedicine*, pp. 772-779, 2008.

[2] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," *Proceedings of the 32nd International Conference on Parallel Processing*, pp. 432-439, 2003.

[3] E. Dishman, "Inventing wellness systems for aging in place," *IEEE Computer*, vol. 37, no. 5, pp. 34-41, May 2004.

[4] M. R. Doomun and K. M. S. Soyjaudah, "Analytical comparison of cryptographic techniques for resource-constrained wireless security," *International Journal of Network Security*, vol. 9, no. 1, pp. 82-94, July 2009.

[5] J. GrosschLadl, "TinySA: A security architecture for wireless sensor networks (extended abstract)," *Proceedings of the 2nd International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2006)*, Lisbon, Portugal, December 4–7, ACM Press, 2006.

[6] J, GrosschL adl, Alexander Szekely, Stefan Tillich, " The Energy Cost of Cryptographic Key Establishment in Wireless Sensor Networks (Extended Abstract)", *ASIACCS '07*, pp. 380-382, Singapore, Mar. 20-22, 2007.

[7] M. Guennoun, M. Zandi, and K. E. Khatib, "On the use of biometrics to secure wireless biosensor networks," *Information and Communication Technologies: From Theory to Applications*, pp. 1-5, 2008.

[8] R. S. H. Istepanian, E. Jovanov, and Y. T. Zhang, "Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 4, pp. 405-414, Dec. 2004.

[9] E. Jovanov, A. Milenkovic, C. Otto, and P. C. D. Groen, "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," *Journal of NeuroEngineering and Rehabilitation*, vol. 2, no. 6, Mar. 2005. (http://www.jneuroengrehab.com/content/2/1/6)

[10] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," *Second ACM Conference on Embedded Networked Sensor Systems*, pp. 162-175, Nov. 2004.

[11] T. Landstra, S. Jagannathan, and M. Zawodniok, "Energy-efficient hybrid key management protocol for wireless sensor networks," *International Journal of Network Security*, vol. 9, no. 2, pp. 121-134, Sep. 2009.

[12] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," *Proceedings of the International Conference on Information Processing in Sensor Networks*, pp. 245-256, 2008.

[13] K. Lorincz, D. J. Malan, T. R. F. F. Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16-23, 2004.

[14] S. Lu, J. Kanters, and K. H. Chon, "A new stochastic model to interpret heart rate variability," *Proceeding of the 25th EMBS Annual International Conference*, pp. 17-21, 2003.

[15] S. S. M. Meingast and T. Roosta, "Security and privacy issues with health care information technology," *Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 5453-5458, Aug. 2006.

[16] K. Malasri, and L. Wang, "Addressing security in medical sensor networks," *Proceedings of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments*, pp. 7-12, ACM, 2007.

[17] K. Malasri and L. Wang, "Addressing Security in Medical Sensor Networks," *HealthNet '07*, pp. 7-12, San Juan, Puerto Rico, USA, June 11, 2007.

[18] M. Manzo, T. Roosta, and S. Sastry, "Time synchronization attacks in sensor networks," *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 107-116, 2005.

[19] Md. M. Haque, A. S. K. Pathan, and C. S. Hong, " Securing U-healthcare sensor networks using public key based scheme", *ICACT '08*, pp. 1108-1111, Feb. 17-20, 2008.

[20] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," *BT Technology Journal*, vol. 24, no. 2, pp. 138-144, 2006.

[21] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of multimedia*, vol. 1, no. 4, pp. 307-326, 2006.

[22] D. Singelee, B. Latre, B. Braem, M. Peeters, M. D. Soete, P. D. Cleyn, B. Preneel, I. Moerman, and C. Blondia, "A secure low-delay protocol for multi-hop wireless body area networks," *Ad-hoc, Mobile and Wireless Networks*, pp. 94-107, Sep. 20, 2008.

[23] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," *Proceedings of the 5th European conference on Wireless Sensor Networks*, LNCS 4913, pp. 305-320, Springer-Verlag, 2008.

[24] L. Uhsadel, A. Poschmann, and C. Paar, "Enabling full-size public- key algorithms on 8-bit sensor nodes," *Proceedings of European Workshop on Security in Ad-Hoc and Sensor Networks*, LNCS 4572, pp. 73-86, Springer-Verlag, 2007.

[25] K. Venkatasubramanian and S. S. Gupta, *Physiological Value Based Security.* (ftp. cs. rochester. edu/ security-privacy-overview-and-biosensors.ppt)

[26] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," *IEEE Conference on Computer Communications Workshops*, pp. 1-6, 2008.

[27] 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 International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 3837-3840, 2005.

[28] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, *ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring*, Department of Computer Science, University of Virginia, Technical Repport, CS-2006-1, 2006.

Mohammed Mana received his engineer degrees in computer science from the University of Tlemcen, Algeria in 2003, and his M.S. degrees in networks and telecommunication systems within of the same University in 2007. Member of STIC laboratory in the University of Tlemcen. Now he is an assistant professor in computer science at the university of Saida, Algeria. His recent work is dealing with mobile wireless networks, their applications, their security, routing and management.

Mohammed Feham received his PhD in Engineering in optical and microwave communications from the university of Limoges, France in 1987, and his PhD in science from the university of Tlemcen, Algeria in 1996. Since 1987 he has been assistant professor and professor of microwave and communication engineering his research interest is in telecommunication systems and mobile networks.

Boucif Amar Bensaber received his PhD in computer science from the university of Rene Descartes (Paris V), France in 1998. In 1999, he worked as a scientist research associate at the research and evaluation center in diagnostics (RECD), CHUS Sherbrooke (Canada). Since 2000, he has been professor at the university of Quebec (UQTR), Canada. His research interest is in wireless networks, multicast protocols, distributed architectures, information and communication technologies and data mining.