SEKES (Secure and Efficient Key Exchange Scheme for wireless Body Area Network)

Mohammed MANA[†], Mohammed FEHAM[†] and Boucif AMAR BENSABER[††],

STIC Lab., Department of telecommunications, University of Tlemcen, Tlemcen, Algeria[†]
Department of Computer Science, university of Quebec, Quebec, Canada[††]

Summary

The development of Wireless Body Area Networks (WBANs) for wireless sensing and monitoring of a person's vital functions, is an enabler in providing better personal health care whilst enhancing the quality of life. A critical factor in the acceptance of WBANs is providing appropriate security and privacy protection of the wireless communication. 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.

In this paper we propose and analyze an approach which exploits physiological signal to address security issues in WBANs, a secure and efficient key exchange scheme for WBANs (SEKES). SEKES manages the generation and distribution of symmetric cryptographic keys to constituent sensors in a WBAN and protects the privacy.

Key words:
Biometrics Security, ECG biometric, Wireless Body Area Network, Security and Privacy, key exchange.

1. Introduction

The pervasive interconnection of autonomous and wireless sensor devices has given birth to a broad class of exciting new applications in several areas of our lives, where health care is being one of the most important and rapidly growing one. The emergence of low-power, single-chip radios has allowed the design of small, wearable, truly networked medical sensors. These tiny sensors on each patient form a Wireless Body Area Network (WBAN). Medical readings from sensors on the body are sent to servers at the hospital or medical centers where the data can be analyzed by professionals. These systems reduce the enormous costs associated to ambulant patients in hospitals as monitoring can take place in real-time even at home and over a longer period. Fig. 1 [4] shows the general overview of a health care architecture. There are three main components: the Wireless Body Area Network (WBAN), the external network and the back-end 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 wirelessly to a central device called the medical hub or base station. This can be done either directly or via several intermediate hops. The medical hub (base station) is unique for each WBAN (and hence for every patient) 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 medical hub and the back-end server. In most cases, the communication between the external network and the medical hub will be wireless. The back-end 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.

Security and privacy are important components in WBANs. Existing sensor networks researches have mainly focused on monitoring the physical environment. However, 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[3]:

- 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?

What makes securing sensor networks more difficult than other types of networks is that wireless sensor nodes usually have limited resources, while conventional security

Manuscript received November 5, 2009
Manuscript revised November 20, 2009

mechanisms incur high costs in terms of CPU, memory, bandwidth, and energy consumption[3].

The contribution of our work is to construct a secure and efficient key exchange scheme for WBANs. Our scheme aims to establish securely and efficiently symmetric session keys between sensor nodes and the base station to secure end to end transmission. It also aims at securing communication links between sensor nodes themselves using biometric data.

The remainder of this paper is organized as follows. Section 2 gives an overview of the related work. This is followed by a detailed descriptions for a secure and efficient key exchange scheme for wireless Body Area Network in Sec. 3. In sec. 4, is given the analysis of our protocol in terms of security services, energy cost and biometric key recoverability. Lastly, concluding remarks for future directions are given in Sec. 5.

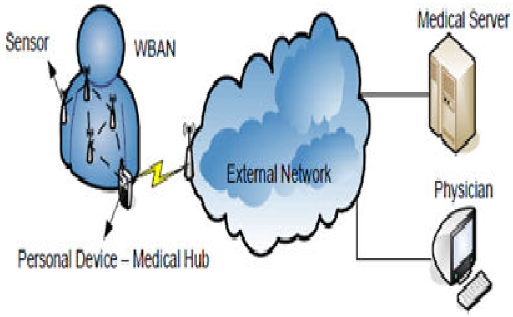

Fig.1 General overview of a health care architecture

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 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[4].

Several security solutions have been proposed in protecting biomedical sensor network. Following are presented the main approaches followed by the architectures mentioned in the table 1[37][38][39][40].

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	TinyECC
WBAN	Tmote Sky	Hardware Encryption

2.1 TinySec

TinySec is proposed as a solution to achieve link-layer encryption and authentication of data in biomedical sensor networks [8]. TinySec [9] 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 [10]. The WBAN group, employed this method in their network infrastructure [7], 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 [4]. 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. [11] propose an efficient implementation of ECC and Liu et al. developed TinyECC [12], 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 [13], 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[41].

2.4 Biometric Methods

A key establishment method to secure communications in biomedical sensor networks has emerged to be biometrics [16]. 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 [17]. Several schemes are proposed to protect WBAN using ECG signal, authors in [35][36][37] 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 consists to establish securely and efficiently symmetric session keys between the nodes and the base station in order to secure end to end transmission. It also aims to use biometric keys (generated from ECG signal) to secure communication links between the nodes themselves with 100% accuracy of keys recoverability at the nodes over the network. Our protocol is characterized by minimal resource consumption.

3. SEKES Protocol Design

In this section, we present SEKES (Secure and Efficient Key Exchange Scheme for wireless Body Area Network). As mentioned in the above paragraph, SEKES aims to achieve the two proposals. In this regard, we first state our security assumptions.

3.1 Security Assumptions

This section aims to address the security of the entire system (shown in Fig.1), and the WBAN in particular. The most security critical device in the entire architecture is the back-end server. This server, which is managed by the hospital or medical center, will receive the medical data sent by all active WBANs. It is assumed that this server is physically protected (e.g., put in a secure place in the hospital where it cannot be stolen or tampered with), and that an adequate access control system is implemented (i.e. only authorized medical personnel has (partial) access to the server through appropriate identification/authentication mechanisms). The back-end server is considered to be a trusted third party, which means that it is known and trusted by all other devices in the network after a successful authentication, it performs all tasks correctly and will not tamper with the data its receives.

Since potentially security critical data will be transferred through the external network, end-to-end security between the medical hub (base station) and the back-end server is necessary. For efficiency reasons, it is assumed that both devices share a symmetric session key to secure their communication. This symmetric session key can be manually installed (e.g., pre-installed during manufacturing), or (preferably) established via a symmetric key establishment protocol. The description of such protocols can be found in the ISO 9798-2 standard, and is out of scope of this article. The symmetric session key is updated regularly. The end-to-end channel between base station and back-end server should also be anonymized using temporary pseudonyms. This avoids privacy problems like (location) tracking.

In the remainder of the paper, it is assumed that the secure end-to-end channel between base station and back-end server is already established after a successful mutual authentication. As mentioned before, each base station belongs to a specific WBAN (i.e. a patient, who is carrying this device). To enforce this, the base station is registered in advance at the back-end server. We also make some assumptions about the trust requirements of our sensor nodes. First, we assume that the sensor nodes are created with a Unique device Identifier (UId), which is known only by that particular sensor node. The UId of all the nodes has to be manually programmed into the base station and each UId acts as an initial shared secret between that device and the base station. The UId is used only during the bootstrapping process and is never exchanged in clear text, hence ensuring that this identifier is never explicitly disclosed to any other sensor node. Device tamper resistance mechanisms might have to be employed in order to ensure that the memory is flushed if any attempt is made to physically manipulate the device in order to retrieve this data. In addition, we assume that the base station has a pair of keys (private and public key). The base station's public key has been pre-deployed within the sensors. Sensor nodes can conveniently be programmed with this key before their actual deployment in the field. This obviates the need for a reliable, omnipresent Certification Authority (CA).

3.2 Notation

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

- Biokey: is the binary sequence obtained from encoding the inter pulse interval sequences (IPIs).
- 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.
- Idt: is a temporary identifier assigned by the administrator to a node for a particular network topology.
- Cmp: is an example of a counter (initialized to some random value).
- N: is an example of a nonce generated by a node.
- M1||M2: is the concatenation of messages M1 and M2.

3.3 ECG as Biometrics

The ECG has recently generated immense interest in the sensor networking research community. 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 (see figure 2) can be used to provide security in WBAN.

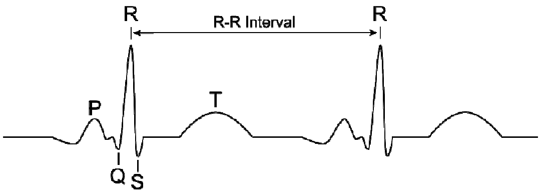

Fig.2 The ECG features

According to [16], the relevant ECG feature in a WBAN is the so-called inter pulse interval (IPI) sequence, which is a sequence of times between R-R intervals. It has been reported also in [16] that a sequence of 128 bits can be generated from 67 IPIs sequence obtained from an ECG signal sampled at 1000 Hz, and for each 128-bits sequence captured at a particular time instant, sensors within the same WBAN have Hamming distances less than 22 bits; by contrast, sensors outside the WBAN typically result in Hamming distances of 80bits or higher. The following figure illustrates the hamming distance for same and different person.

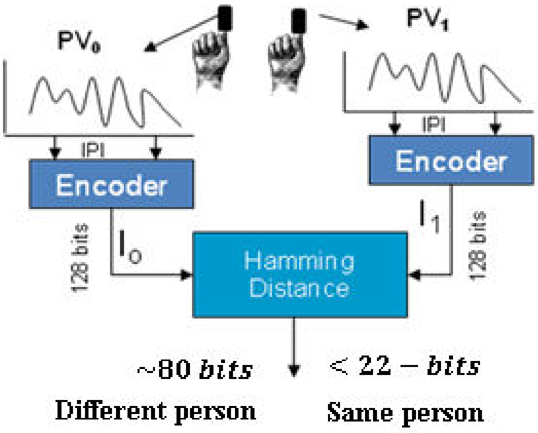

Fig.3 Hamming distance between
ECG-generated keys (intra and inter person)

3.4 Biometric Key Generation

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 [23]. More precisely, heart rate variability is characterized by a (bounded) random process[24].

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 for the morphing function *M(.)*) to ensure user privacy and confidentiality. As noted in [27], 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. Figure 4 depicts the key generation scheme.

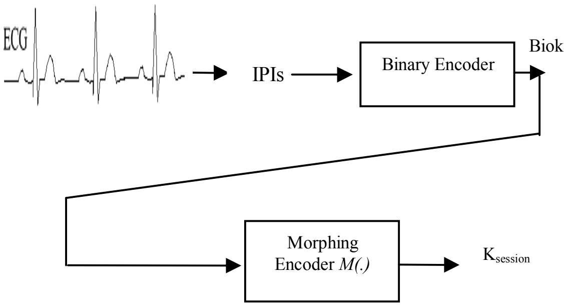

Fig.4 Key generation from ECG-signal

In our scheme, the biometric keys will be used to secure communication links between sensor nodes over the wireless body area network as illustrated below in node to node handshake.

3.5 Node to Base Station Handshake

This handshake aims to establish securely and efficiently symmetric session keys between the nodes and the base station.

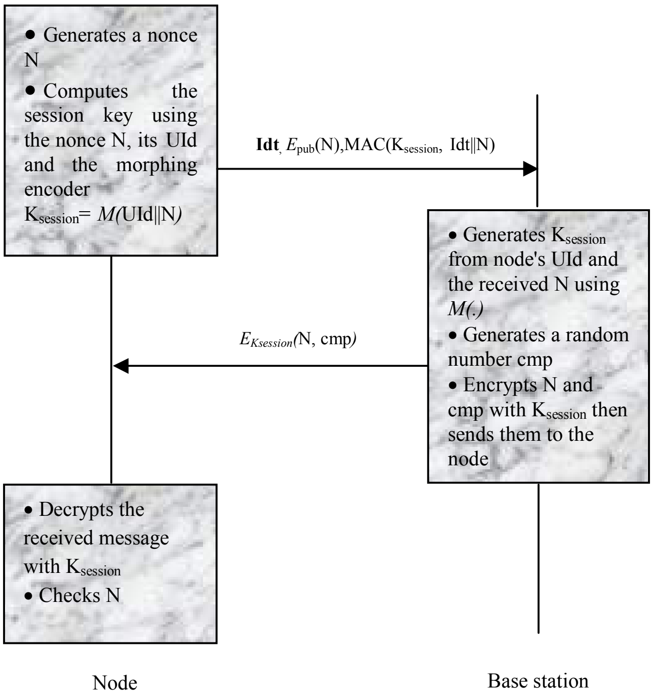
• Generates a nonce N
• Computes the session key using the nonce N, its UId and the morphing encoder $K_{session}$= *M(*UId||N*)*
Idt, E_{pub}(N),MAC($K_{session}$, Idt||N)
• Generates $K_{session}$ from node's UId and the received N using *M(.)*
• Generates a random number cmp
• Encrypts N and cmp with $K_{session}$ then sends them to the node
$E_{Ksession}$(N, cmp)
• Decrypts the received message with $K_{session}$
• Checks N
Node
Base station

Fig.5 Node to base station handshake

A node aiming to establish a symmetric session key with the base station performs the following steps (as depicted in figure5):

- **Step 1:** generates a nonce N
- **Step 2:** generates the session key from its UId and the nonce N using the morphing function *M(.)*,
  $K_{session}$= *M(*UId||N*)*
- **Step 3:** encrypts the nonce N with the base station's public key
- **Step 4:** computes the MAC (Message Authentication Code) over the node Idt and the nonce N.

- **Step 5:** appends to its Idt the encrypted nonce N and the MAC, then transmits the entire message to the BS (base station).

$$\text{Node} \longrightarrow \text{BS: Idt}, E_{Pub}(\text{N}), \text{MAC}(\text{K}_{\text{session}}, \text{Idt}||\text{N})$$

On receiving the message, the base station generates $\text{K}_{\text{session}}$ from UId and the received nonce N using the morphing function *M(.)*. Then, it checks the MAC. If the check is successful, the base station uses this key ($\text{K}_{\text{session}}$) to send the following encrypted information to the node: the received nonce N and a counter cmp initialized to some random value to avoid replay attacks.

$$\text{BS} \longrightarrow \text{Node: } E_{Ksession}(\text{N, cmp})$$

3.6 Node to node handshake

After the establishment of the session key between each node and the base station, we suppose that some nodes need to establish a secure channel between them for any purpose.

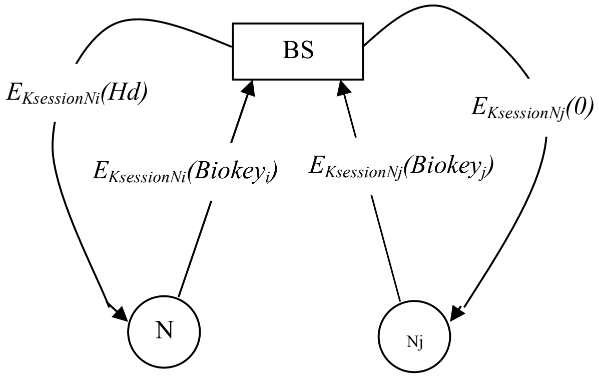

Fig.6 Node to node handshake

Let us assume two nodes Node_i and Node_j wish establish a secure channel between them. To do so, both the base station and the nodes execute the following steps (as shown in figure 6):

- **Step 1:** each node generates a biometric key from its reading ECG signal, then encrypts it with its session key shared with the base station and sends the encrypted biometric key to the base station.

$$\text{Node}_\text{i} \longrightarrow \text{BS: } E_{\text{Ksession-Nodei}}(\text{Biokey}_{\text{Nodei}})$$

$$\text{Node}_\text{j} \longrightarrow \text{BS: } E_{\text{Ksession-Nodej}}(\text{Biokey}_{\text{Nodej}})$$

- **Step 2:** on receiving the encrypted biometric keys, the base station decrypts each one with the corresponding session key of each node and computes the hamming distance between them. If the hamming distance is less than 22bits, then the base station returns to one of them the result Hd and to the other a null value.

For example, we suppose that node_i will receive the Hd and node_j will receive the null value.

$$\text{Hd}= \text{Biokey}_{\text{Nodei}} \oplus \text{Biokey}_{\text{Nodej}}$$

$$\text{BS} \longrightarrow \text{Node}_\text{i} \text{ :} E_{\text{Ksession-Nodei}}(\text{Hd})$$

$$\text{BS} \longrightarrow \text{Node}_\text{j}\text{: } E_{\text{Ksession-Nodej}}(0)$$

- **Step 3:** on receiving the result Hd and the null value, the nodes perform the following operations to recover the same key at each one:

-The node receiving the Hd, computes:

$\text{K}_{\text{Nodei-Nodej}}=\text{M}(\text{Biokey}_{\text{Nodei}}\oplus\text{Hd})$ where M(.) is the morphing function (figure 4).

-The node receiving a null value, computes:

$\text{K}_{\text{Nodei-Nodej}}= \text{M}(\text{Biokey}_{\text{Nodej}})$

$\text{K}_{\text{Nodei-Nodej}}$ is used to secure communication link between Node_i and Node_j.

3.7 Key update

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 nodes by launching a key update message including a new nonce N' encrypted, using the old session key.

Node $\longrightarrow$ BS: E_{Ksession}(N')

On receiving the key update message, the base station decrypts it, computes the new session key from UId and N', updates the session key and sends the encrypted received nonce N' to the node.

BS $\longrightarrow$ Node: $E_{\text{newKsession}}$(N')

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.

3.8 Joining the Network

If a new node wants to join the network, the administrator of this network must:

- Load the node's UId into the database of the base station

After loading its UId into the database of the BS, the new node can automatically initialize a Node to Base Station Handshake and join the network if there is any report to send.

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 and authenticity: The integrity and authenticity can be ensured using MAC (Message authentication codes) computed and joined to each sent packet between the base station and any node over the network.

- 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 [30], the transmission of a single byte of data requires 59, 2µJ and 28, 6µJ for reception.

To join network, a sensor node needs to send one message to the base station containing a nonce N encrypted with the base station's public key (8 bytes), 16 bytes of the MAC and 12 bytes of protocol headers. Thus the size of the sent packet is 36 bytes, the energy needed for transmitting such packet is 2,13 mJ. In reception, added to the protocol headers the sensor node receives a counter (8 bytes) and its transmitted nonce (8 bytes), the energy needed for reception is 0,80 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 0,039 mJ according to [30] if the used algorithm is AES and using 128 bits key length. Therefore the total energy cost is 25,79 mJ.

To setup a secure link between nodes, a node sends message containing its identifier (1 byte), the encrypted biometric key (16 bytes) and the MAC message (16 bytes), then receives the result of the hamming distance or the null value. Thus, the energy needed to transmit the message and receive the result is 3,62 mJ.

Consequently, the total energy cost of SEKES is 29,41mJ.

Table 2: Energy cost comparison

Schemes based ECC	*Energy cost (mJ)*
SSSL	39
SKERBEROS	39,6-47,6
Our proposition (SEKES)	29,41

Compared to other schemes based ECC-160 bits (table2) like simplified SSL protocol [42] or simplified Kerberos protocol [43] 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.

4.3 Biometric key recoverability

By involving the base station to secure link communication between two sensor nodes, the biometric keys are recoverable with very high fidelity with 100% accuracy.

The following table compares the performance of our scheme to that of schemes proposed by authors in [16] and [35]. The performances are evaluated by two types of errors, FRR (False Rejection Rate) and FAR (False Acceptance Rate)

Table 3: Performance comparison

	FRR (False Rejection Rate)	***FAR (False Acceptance Rate)***
Scheme proposed in [16]	4.20	0.02
Scheme proposed in [35]	0.00	0.03
Our scheme	0.00	0.00

Compared to the other schemes, our approach is more efficient.

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 secure and efficient key exchange for wireless body area network called SEKES. This latter attempts to solve the problem of security and privacy in WBANs. It also aims at 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 using biometric data. Compared to other approaches, SEKES is more suitable for wireless body area network because it is efficient and energy saving.

Acknowledgement

The research is developed in STIC Laboratory, Department of telecommunications, University of Tlemcen, Tlemcen, Algeria.

References

[1] V. Shnayder, B. Chen, K. Lorincz, T. Jones, and M. Welsh, "Sensor networks for medical care", in SenSys '05: Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, 2005.

[2] Tassos Dimitriou, Krontiris Ioannis, "Security Issues in Biomedical Wireless Sensor Network", Applied Sciences on Biomedical and Communication Technologies, 2008. ISABEL '08. First International Symposium on Publication Date: 25-28 Oct. 2008 On page(s): 1-5

[3] Kriangsiri Malasri, Lan Wang, "Addressing Security in Medical Sensor Networks", HealthNet'07,June 11, 2007, San Juan, Puerto Rico, USA.

[4] Dave Singelée, Benoît Latré, Bart Braem, Michael Peeters, Marijke De Soete, Peter De Cleyn, Bart Preneel, Ingrid Moerman and Chris Blondia, "A Secure Low-Delay Protocol for Multi-hop Wireless Body Area Networks", in Ad-hoc, Mobile and Wireless Networks 20 September 2008.

[5] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks". In CCS '02: Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47, New York, NY, USA, 2002. ACM.

[6] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and security in wireless body area network infrastructures," in Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2005, pp. 3837–3840.

[7] S. S. Marci Meingast, Tanya Roosta, "Security and privacy issues with health care information technology," in EMBS '06: Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, August 2006, pp. 5453–5458.

[8] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), November 2004, pp. 162–175.

[9] M. Healy, T. Newe, and E. Lewis, "Efficiently securing data on a wireless sensor network," Journal of Physics: Conference Series, vol. 76, 2007.

[10] L. Uhsadel, A. Poschmann, and C. Paar, "Enabling Full-Size Public- Key Algorithms on 8-bit Sensor Nodes," in Proceedings of European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2007), ser. LNCS, vol. 4572. Springer-Verlag, 2007, pp. 73–86.

[11] 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 (IPSN 2008), vol. 0, pp. 245–256, 2008.

[12] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve

cryptography in sensor networks," in Proceedings of the 5th European conference on Wireless Sensor Networks (EWSN), ser. Lecture Notes in Computer Science, vol. 4913. Springer, 2008, pp. 305–320.

[13] M. Guennoun, M. Zandi, and K. El-Khatib. "On the use of biometrics to secure wireless biosensor networks", in Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd

[14] Sriram Cherukuri, Krishna K. Venkatasubramanian, and Sandeep K. S. Gupta, "Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body", in Proc. IEEE Conf. Parallel Processing Wksp., 2003, pp. 432–39.

[15] 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," in Proceedings of the Workshop on Wireless Security and Privacy (WiSPr), International Conference on Parallel Processing Workshops, 2003, pp. 432–439.

[16] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," EURASIP J. Adv. Signal Process, vol. 8, no. 2, pp. 1–16, 2008.

[17]] M. Manzo, T. Roosta, and S. Sastry, "Time synchronization attacks in sensor networks," in SASN '05: Proceedings of the 3rd ACM wo

[18] 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.

[19] A. Liu, P. Kampanakis, and P. Ning. TinyECC: "Elliptic Curve Cryptography for Sensor Networks". http://discovery.csc.ncsu.edu/software/TinyECC/.

[20] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo. "Applicability of identity-based cryptography for disruption-tolerant networking". In MobiOpp 2007

[21] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO 2001

[22] U. Uludag et al., "Biometric Cryptosystems: Issues and Challenges," Proc. IEEE, vol. 92, no. 6, June 2004, pp. 948–60.

[23] Jaakko Malmivuo and Robert Plonsey, "Bioelectromagnetism:Principles and Applications of Bioelectric and Biomagnetic Fields", Oxford University Press, New York, 1995

[24] Sheng Lu, Jorgen Kanters, and Ki H. Chon, "A new stochastic model to interpret heart rate variability," in Proc. 25th EMBS Annual International Conference of the IEEE, 2003, pp. 17–21.

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

[26] John G. Proakis, Digital Communications, McGraw Hill, fourth edition, 2001.

[27] A. Cavoukian and A. Stoianov, "Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy," Information and Privacy Commissioner/Ontario, Mar. 2007.

[28] Dave SINGELEE, thesis "Study and Design of a Security Architecture for Wireless Personal Area Networks", December 2008

[29] Chris Otto, Aleksandar Milenkovic, Corey Sanders, Emil Jovanov, "System Architecture of a Wireless Body Area Sensor Network for Ubiquitous Health Monitoring," Journal of Mobile Multimedia, Vol. 1, No. 4, 2006, pp. 307-326

[30] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," Proceedings of PerCom, pp. 324-328, 2005.

[31] Krishna Kumar Venkatasubramanian, Ayan Banerjee, and Sandeep K. S. Gupta," EKG-based Key Agreement in Body Sensor Networks", Networks. In IEEE Conference on Computer. Communications Workshops (INFOCOM), pages 1–6. IEEE, 2008

[32]I. Krontiris, T. Dimitriou, and T. Giannetsos, "LIDeA: A distributed lightweight intrusion detection architecture for sensor networks," in Proceeding of the fourth International Conference on Security andPrivacy for Communication (SECURECOMM '08), September 2008.

[33]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", in Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on, pages 432–439, October 2003.

[34] S.D. Bao, Y.T. Zhang, and L.F. Shen, "A novel key distribution of body area networks for telemedicine", in Proc. IEEE Workshop on Biomedical Circuits and Systems, 2004.

[35] C.C.Y. Poon, Z. Yuan-Ting, and B. Shu-Di. "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health", IEEE Communications Magazine, 44(4):73–81, April 2006.

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

[37] K. Lorincz, D. J. Malan, T. R. F. Fulford-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.

[38] 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, Tech. Rep. CS-2006-1, 2006.

[39] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in HealthNet '07: Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments. ACM, 2007, pp. 7–12.

[40] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and security in wireless body area network infrastructures," in Proceedings of the 27th Annual International Conference of the IEEE

Engineering in Medicine and Biology Society, 2005, pp. 3837–3840.

[41] J. Großsch¨adl, "TinySA: A security architecture for wireless sensor networks (extended abstract)," in Proceedings of the 2nd International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2006). ACM Press, 2006.

[42] Md. Mokammel Haque, Al-Sakib Khan Pathan, and Choong Seon Hong, " Securing U-Healthcare Sensor Networks using Public Key Based Scheme", ICACT 2008 Feb. 17-20, 2008.

[43] Johann Großsch¨ adl, Alexander Szekely, Stefan Tillich, " The Energy Cost of Cryptographic Key Establishment in Wireless Sensor Networks (Extended Abstract)", ASIACCS'07, March 20–22, 2007, Singapore.

Authors

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.