Research Journal of Applied Sciences, Engineering and Technology 9(10): 876-885, 2015
DOI:10.19026/rjaset.9.2638
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 25, 2014 Accepted: January 23, 2015 Published: April 05, 2015

Research Article

Protecting E-healthcare Data Privacy for Internet of Things Based Wireless Body Area Network

[1]Anass Rghioui, [2]Aziza L'aarje, [1]Fatiha Elouaai and [1]Mohammed Bouhorma
[1]LIST, Faculty of Science and Technology of Tangier, Abdelmalek Essaadi University, Morocco
[2]Department of Cardiology, CHU Ibn Rushd of Casablanca, Hassan II University, Morocco

Abstract: This study aim to give an analysis of the threats to privacy in wireless sensors in the context of the Internet of things and we review the pros and cons of some of the proposed solutions in order to ensure privacy. We propose a solution for the management of security keys based on symmetric encryption, taking into account two important factors, the sensors resources constraints and their mobility being linked to the patient body that may move occasionally. Tests gave significant results confirm that our proposed solution is secure, energy efficient and unable to deal with mobility. The field of healthcare knew an important development due to the evolution of the technology used in its applications, from sophisticated equipment in the operating rooms, to diagnostic and analysis equipment offering accurate and effective results. Among devices that have contributed to the development of the field of healthcare is the mobile monitoring sensors that are placed on the patient's body. By the emergence of the Internet of Things, it became possible to access to them remotely, so the possibility of offering patients a continuous and real-time monitoring and keep track of his health condition wherever he goes, from inside his home, in the street, in the workplace, etc. However, the main drawback of these applications is the lack of consideration of data security and privacy. The nature of these sensors from a wireless connection and limited capacities, making them vulnerable to a range of attacks aimed at eavesdrop or tamper patients' personal information.

Keywords: E-healthcare, information security, internet of things, privacy, WBAN

INTRODUCTION

The healthcare is among the most important areas in which technology gives special attention due to its vital importance, the whole progress is based on improving the human life quality and provide better for him, it is normal that the field of healthcare has this advantage as it directly affects human life. Among the cutting-edge technology that aided the field of healthcare and contributed to its improvement is the wireless body sensors (Hao and Foster, 2008) that are placed on the body of the persons in need of care as patients, handicapped, elderly and children; in order to monitor their health state. Thanks to advances in sensor types and capabilities, it was possible to capture various information about the patient, about his physical, physiological, psychological and behavioral state. Its composition of cheap and mini materials contribute to its integration in all healthcare areas. Sensed data is sent to a medical central unit carried by caregivers or any authorized person. The medical central unit analyzes the received data and shows the caregivers the results about the monitored person health; to help them to understand his state and help them to intervene in the best moment.

Integrating these sensors to internet open a new horizons to the telemedicine domain (Atzori *et al*., 2010), giving the possibility of tracing the patient's condition frequently and in real time. Moreover, it will help by creating cooperative networks between them and the rest of the other sophisticated devices in order to benefit mutually from the capabilities of each and every one of them and improve the quality of tracking and diagnostics and analysis. It will contribute to the coordination between various healthcare professionals without moving from one place to another. In addition, these techniques will make the patient avoid the trouble of mobility and stand in queues. Wireless body sensors will provide in the context of the Internet of Things (Atzori *et al*., 2010) the possibility of continuous monitoring, early detection and rapid intervention in emergency conditions, in addition to a wide range of healthcare services.

As the health information is very sensitive and vital, it must be obtained correctly and accurately with the source authentication and among the largest gaps in the sensors is the issue of data protection from eavesdropping or tampering. Security must be ensured in all scenario parts of the health care application. Therefore, there is a need for mechanisms to ensure data

Corresponding Author: Anass Rghioui, Department of Computer Science, Faculty of Science and Technology of Tangier, BP: 416-Tangier, Morocco

end-to-end security and integrity; from the sensor to the medical central unit. Among the most important requirements of the security to be provided to these systems is to maintain privacy (Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications-Springer, 2014), the medical information is considered as a vital issue. Legally and ethically is one of the most confidential things binding preserved between the patient and the caregiver responsible for his condition, whether an individual as the doctor or a legal entity as the hospital. Moreover, it must be protected from tampering; sensed data is sent over the Internet to the medical central unit that stores it and analyze it in order to reveal the health status of the patient. Any error in these data will give wrong results; the caregiver could take wrong decisions making the life of the patient in danger.

Wireless body sensor is a miniature device consisting of mini elements for storage, computation and wireless transmissions. Its computation capabilities are very weak and its storage space and memory size are very small. Its batteries charge is limited, knowing that these devices designed to live for a long period (Hao and Foster, 2008). Therefore, any system that would lead to excess consumption of energy will not be effective. These features make them vulnerable to a range of easy compromising, tampering and eavesdropping attacks. They put the privacy of patient medical information at risk. Moreover, any change in the sensed data will give wrong information about the patient health status, which would have a negative impact on his health and possibly his life. These sensors must adopt a security system capable of maintaining the confidentiality and integrity of the sensed data. The best system that can ensure this task is the encryption system, but it is not easy to apply it as it should respect and take into account the specificity of these devices. The impact of security on the age of sensor must be taken into account when adding new services. This effect presented in the extra power consumed in order to carry out the encryption and decryption mechanisms and security data transfer and storage. For example, the security keys, which is a challenge to be applied in this type of devices, as the keys management of asymmetric cryptography is an energy-consuming and those relating to symmetric cryptography is unsafe when exchanging it despite being the optimal method regarding its speed and lack of energy consumption.

We try to give in this study a solution for the management of keys protection for encrypted replication, being optimized for resource-constrained sensors, trying to avoid the past solutions gaps by respecting the requirements of these devices, as well as taking into account their mobility. We deal with the challenge of symmetric encryption in low power networks; the security keys management, because of a lack of a secure infrastructure where devices can through exchange the shared keys. It is unsafe to exchange a key without encrypting it; otherwise it would be susceptible to be captured. We decided in our solution avoid any exchange of keys between devices by providing a mechanism that makes the devices create a symmetric key through the exchange of some information, which it detection will not endanger any of the two devices. Our solution operates without pre-shared information as is the case in a set of proposed solutions. In addition of its adaption with the problem of mobility, which without it; it would be necessary to create and regulating device keys whenever the device gone, it is not practical as the sensors are linked to the body of the patient that move from one place to another.

Analysis and experiments that we have established gave good results showing that our solution in an energy efficient compared to the rest of the proposed solutions and the formal evaluation using AVISPA tool (Armando *et al*., 2005) confirms that our solution is secure.

OVERVIEW OF THE INTERNET OF THINGS CONCEPT

The Internet is among the largest and most important inventions of the last half century, which radically changed the lives of human beings and was able to touch all sectors and all segments of society. From an academic network connecting some computers (1969) to the global network used by nearly 3 billion users (2014), approximately 40% of the earth's population (BBC, 2014), moving from network computers used by human users, to network connecting everything at any time in any place (Fig. 1).

The open nature of the Internet and that no one, or a specific destination owned it, allowed for many actors from academics and researchers, companies and organizations, formal and informal, to be enriched with new ideas and recent developments, made it fertile ground and vital to scientific and technical research. The set of protocols work together in order to serve Internet and make it in the reality, these protocols are in a permanent and ongoing development, evolving development of the technology and come to meet the needs of the user, whatever its use, whether professional or recreational. Among the most important of these protocols, which have been linked closely connected to the Internet, is the IP protocol (Internet Protocol). It allows each device connect the Internet obtaining its own address that determine its position within the network that containing millions of nodes and allows the transfer of data packets through the methods of end-to-end communication.

Currently, the Internet is composed of two layers, the first layer form the infrastructure consisting of intermediary devices, routers and wired and wireless links, as well as servers and data centers. The second layer formed by the computers and phones, stamps and all machines associated with the direct use by users, constitute the boundaries of the online world, it ends at the machine with direct use by the user. The Internet of things, what it is called the Internet of the future, will bind the online world with the physical world and makes it an integral part of it. It will eliminate all boundaries

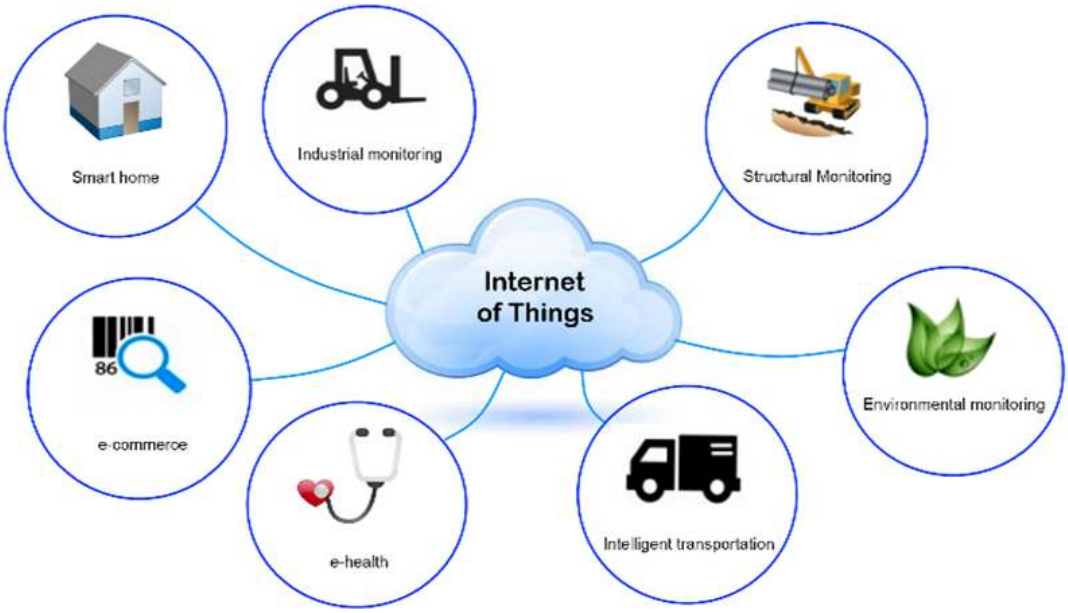

Fig. 1: Different internet of things applications

between them; everything and everyone will become linked directly to the Internet network. The Internet of Things consists of devices able to use the IP including sensors, machines, RFID, etc. The development of these devices and their associated technology progress on accelerated way in spite of all the challenges that it know. The fact that most of these devices are low power energy and resource constrained, it is difficult to provide systems and protocols that have been developed so far for other ordinary devices such as computers.

Supply these devices with limited resources with IP is an important step that will enable the activation of the concept of Internet of Things in the real world, even though they constitute a sub-group within groups of other projects that involve within the concept of the wide Internet of Things concept, but it is considered the most challenging as it opens the door to many problems to be solved and one of the main groups that will allow the Internet of Things becomes a reality. But nowhere does the Internet of Things offer greater promise than in the field of healthcare (di Peri, 2014), where we find its principles are already being applied in order to improve and reduce the cost of care and offer to patients with difficulties a remote and real-time assistance.

A significant amount of recent research has been done in the field of wearable wireless body sensor networks in the Internet of Things context with many researchers proposing different solutions for healthcare monitoring. However, very little effort has been made to ensure the security and privacy of the patient data when dealing with the IP-based sensor networks.

E-healthcare WBAN applications in the internet of things context: In healthcare, Internet of Things (IoT) plays an important role in many applications that can be separated within three areas of intervention: clinical care, home care and healthcare assistance.

Automating data collection reduces the risk of human error. The caregivers in this case will obtain reliable information about the patient with a negligible error rate. This will improve the quality of diagnosis and will avoid human intervention that may collect or transmit false information, which can have a dangerous impact on patient health.

Clinical care: Sensors will help hospitalized patients to move freely within the hospital without having to commit to a certain rooms and been liked wired to certain machines, as well as avoiding the trouble moving from a pavilion to the other for examination and analysis. It will help as well as caregivers in the performance of their work, as will enable it to track the patient's condition remotely and help them to cooperate with each other in the diagnosis of the patient's condition between the various disciplines. Moreover, it will save the doctors' time from moving between patients to reveal their health status. It will help them for rapid intervention in an emergency and will enable them to cooperate with international hospitals to track a patient's condition.

Home care: We can take advantage of these sensors in the home monitoring for the elderly, people with special needs or the owners of chronic diseases such as diabetes, asthma, chronic obstructive pulmonary, congestive heart failure and memory decline ... etc. They will avoid trouble navigating to the hospital from time to time to

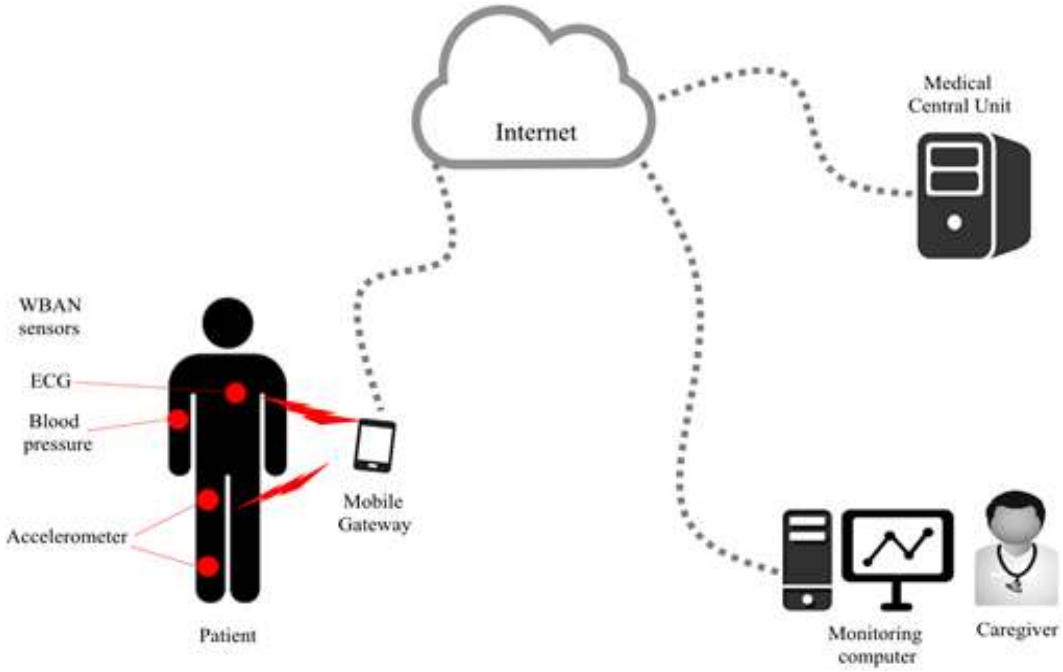

Fig. 2: Simplified example of an internet of things based e-healthcare system

check their health state. As they have an unstable condition that may develop to the worse at any moment, the sensors will warn the medical staff remotely in order to intervene. The patient can also use these sensors itself for tracking his health daily, as well as by its family, even remotely via the Internet.

Healthcare assistance: Wireless body sensors can be used as well as in personal care in order to maintain health and fitness. It can be used on a personal level in order to help take daily preventive measures to maintain health. Its connection to internet will enable it to obtain the necessary information and updates in order to help people organize their lives, which fall within the so-called smart devices that interact with the requirements and variables of its owner.

E-healthcare example:

Continuous cardiac monitoring: Cardiovascular diseases are the leading cause of death worldwide since more than twenty-two million people are affected (Go *et al*., 2013), this number should triple by 2020. This requires immense expenses for managing such disease. The looming health crisis attracts researchers and industry to look for optimal and rapid solution to perform cardiac remote monitoring, with medical records updates in real-time via the Internet, by economic solutions valid for the entire world.

A wearable WBAN is efficient for this mission. It can be placed on specific places of the body of the patient to continuous measure its Electrocardiograms signs (ECG) and transmit them to the hospital supervisor medical central unit in real-time. Thus, it can monitor patient under natural physiological states of health in the long term without constraining their normal activities. These sensors are able to gather information from Implantable Cardiac Defibrillators (ICDs) to detect and treat ventricular tachyarrhythmia and prevent Sudden Cardiac Death (SCD) (Ullah *et al*., 2009) (Fig. 2).

Privacy issues in e-health applications:

Security threats: In e-healthcare applications, privacy is an indispensable objective that must be ensured by any system that maintains it. In security, it may be confusion between the confidentiality and privacy. Confidentiality is regarding the data in general, while privacy concerning personal information. However, people are allowed access to the WBAN data, but we can ban them of some of the data pertaining to the personal life of the patient and cannot be accessed except for one who is allowed to do so. As the subject of our study, data are collected by the sensor from patients, professionally and ethically considered confidential, shall not be entitled only for caregivers to revise them. They can share it with other caregivers in order to access to treatment for the patient, but they cannot share it with the patient family (except in certain cases), only if he allowed them to do so, here we are talking about privacy.

Internet of Things resource constrained devices creates a problem for privacy, in addition to the ease of access to attackers due to the weak nature of the wireless devices in the above; the Internet of Things allows

remotely access to the sensor, thus the expansion of the circle of danger.

Among the most serious attacks against privacy are eavesdropping operations through access to the device itself or by undertaking the flow of data sent from the device. Also, tampering data sent from the sensor to the medical central unit via the Internet.

The attacks may be carried out by powerful hosts and from anywhere in the world via the Internet. End-users can access to WBAN sensors connected to the Internet and thus access to the data illegally. When the sensor completes the connection to the medical central unit via Internet, the attacker can eavesdrop data flow between them, or tampers it and displays its integrity, causing reception of wrong information. Since most of the actual IP hosts are powerful machines, it can exploit this thing to launch an attack to damage the WBAN, trying to form a pressure upon the exhaustion of its capacity, even cause its destruction.

Threats model: The architecture of an e-healthcare system may vary depending many requirements and constraints, but generally the system is composed by three major component; the wireless body sensors, the medical central unit and the gateway that links the sensors by the Internet, it may be a router, PDA, Smartphone, etc.

We assume that both the gateway and the medical central unit are secure and trustworthy, as they are full resources devices; implemented by the performant security protocols.

We assume an ideal network where no message is lost exchanged and all messages are sent and received instantly by the communicated devices. Moreover, all communication channels are assumed public.

The attacker cannot intervene by an active attack by capturing or compromising a node from the WBAN in the bootstrapping phase during the network deployment, but he can execute a passive attack like eavesdropping the flow between the wireless sensors and the gateway in this phase. Thus, it is not possible to take into account the time that the attacker make to execute its attacks.

If the attacker compromise a node, he can reveal the key stored in it, but it will obtain only the key of the current session. He can encrypt and decrypt messages by the key in his possession and he is capable of storing, deleting, build and send all the messages with this key.

We assume the used cryptography, even the symmetric or the asymmetric, is perfect. Encrypted messages can only be read if the decryption key is available in the node.

LITERATURE REVIEW

Applying cryptography in WBAN must take into consideration characteristics and constraints of the sensors, such as low power battery, low storage ability and low computing capacity, to optimize resources and provide to nodes longer life lasting.

Even if efficient key management systems exist in today's internet, but their underlying cryptographic algorithms are either too heavy to run on resource-constrained nodes, or do not provide a satisfactory security level.

Several recommendations and solutions (Meingast *et al*., 2006; Liu *et al*., 2012; Medaglia and Serbanati, 2010; Rghioui *et al*., 2013; Barakah and Ammad-Uddin, 2012) propose the use of key management protocols based on symmetric shared keys instead of the asymmetric for such limited resources networks since its operation does not consume a lot of energy. However, a leading issue that must be addressed is the mechanisms used for establishing these shared keys in the first place.

Existing solutions are based either on pre-shared information between nodes of the same network or depends on a trusted third party that manages the security keys between these nodes.

In the pre-shared based solutions, we find the use of a secret master key pre-shared between all nodes in the same network to use it as a basis for generation of session keys between them. Other solution based on multiple pre-shared keys that if a network gather N nodes, each node will hold N-1 pairwise key shared with network nodes. In addition, there are solutions that use a random sharing key and depends on probability functions or nodes location to find at least one shared key between two nodes on the same network. Yet there are solutions that use a trusted third party to manage security keys, usually it is the medical central unit or a local powerful nodes.

These solutions deal only with local networks. However, IoT WBAN networks are open to outside communications, with external IP-hosts, also its corresponding nodes from other IP networks cannot be predicted in advance; consequently, these keys will need to be established after the network is deployed.

As already mentioned in the previous paragraph, in the case of IoT WBAN networks, we need solutions that guarantee the end-to-end communication security such aIPsec (Seo and Kent, 2014) and its key management protocol IKE (Eronen *et al*., 2014), which are used to secure IP-based communications, yet they are very greedy for resource-constrained networks as they are based on asymmetric cryptography. Many contributions have proposed lightweight implementations of asymmetric solutions in networks with constrained-resources as for example whose based on ECC (Elliptic Curve Cryptography) that demonstrations have shown that a key ECC 160-bit provides the same level of security than RSA 1024-bit key, while having a lower energy consumption and faster time calculation than RSA. However, the use of ECC in highly constrained-nodes, like WBAN sensors, still expendable.

As the IoT is a recent under developing concept, there is no many security solution are proposed yet. Our contribution aim to propose a key management scheme with a security solution that benefit from symmetric advantages, as it is energy efficient, trying to guarantee the end-to-end security establishment between the sensors and the medical central unit. The challenge we address is to maximize IoT WBAN networks privacy performance while minimizing nodes resource consumption.

KEY MANAGEMENT PROPOSED SOLUTION

We deal in this study with the case of e-healthcare monitoring where the patient carries a set of WBAN devices and can move from a place to another, but still always on the reach of the gateway that bind the sensors with the medical central unit. These devices communicate remotely through the Internet with a monitoring medical central unit installed in a healthcare center (hospital, clinic …) responsible for monitoring patient's health status. Caregivers can connect through the Internet via computers or mobile devices (Smartphones, PDA …) to the medical central unit to supervise patient data processed and analyzed by dedicated applications. The object of study is to address the data privacy of the mobile WBAN sensors exchanged with the remote medical central unit.

Our scheme is based on the symmetric cryptography with a session key management system and a node authentication model with an identifier ID. Each node has a unique identifier stored in the server database, which must be kept secret and must never be communicated in plaintext.

Assumptions: The paper supposes that IoT healthcare system consists of the following units: a medical central unit MCU, a gateway G and WBAN sensors. Each one of WBAN sensor has a unique identifier ID that must be already registered on the MCU. Or registered by the user at the time of the WBAN deployment. And a secret number N_S that must never be disclosed.

WBAN sensors are implemented on patient body, they must still always on the area of the G, which can be immobile, fixed in one place like the routers, or mobile that the patient can have on like the PDA, the Smartphone or any mobile device.

In the MCU, there is a database of WBAN sensors that the patient will wear, it is implemented by data concerning these devices. The both information necessary for our solution are the identifier ID and the secret number N_S.

We deal with mobility in the case of the WBAN sensors move from a gateway to another, in this case, the sensor must preserve the address of his ex-gateway and every gateway must keep the mobile sensor information for a moment after his disconnection from its network (Table 1).

Table 1: Acronyms used for protocol description

Entity	Description
MCU	Medical center unit
G	Gateway
K_{MCU-ID}	Individual shared key between the MCU and the WBAN sensor
K_G	Group key shared between the gateway and WBAN sensors
S_{MCU}	Generated seed by the MCU
S_G	Generated seed by the G
ID	Unique sensor identifier
Ts	Timestamp
Te	Time expiration of the Ts
N_S	Unique sensor secret number

Our solution is based on symmetric cryptography, we chose to use AES (Advanced Encryption Standard) algorithm because it is efficient, fast and it does not consume energy. The AES algorithm is able to operate on three variants of encryption key; 128, 192, or 256 bits, but since we are limited by WBAN sensors computation capacity and memory size, we chose to use 128 bits variant. We chose the AES-CCM mode as it provides data encryption and integrity.

Key establishment: Every sensor will obtain two symmetric keys; one unique shared with the MCU that the sensor will use to encrypt sensed data and the other is a group key shared with the G that will be used only to encrypt non sensitive updates of the system.

At the deployment phase, firstly the G gets establish a secure connection with the MCU. As they are full resources devices, they use the asymmetric cryptography to secure their exchanged messages. We suggest the use of the Host Identity Protocol (Henderson *et al*., 2014) that use IP sec in order to establish a secure end-to-end communication, also its advantage that is self-certifying identifiers; no certificates and trusted third party are required. It provides identifier ownership and makes difference between the identifier and the locator and supports mobility and IP changing as it does not bind to the IP address.

After establishing the connection with the MCU, the G generates a seed S_G and broadcast it to the WBAN sensors with a Timestamp Ts and a its time expiration Te in order to avoid replay attacks. Every sensor uses the received S_G and combined with is secret number N_S to generate its unique symmetric key K_{MCU-ID}. After that each node encrypts its secret number and sends in a message containing its ID to the G.

Then, G sends the S_G and the received messages from WBAN sensors to the MCU in a secure way (Fig. 3) using the HIP protocol mechanisms. As the MCU holds a database that contains all the WBAN sensors related to it, it searches every sensor using its ID, when the MCU finds the related sensor, it uses the received S_G and

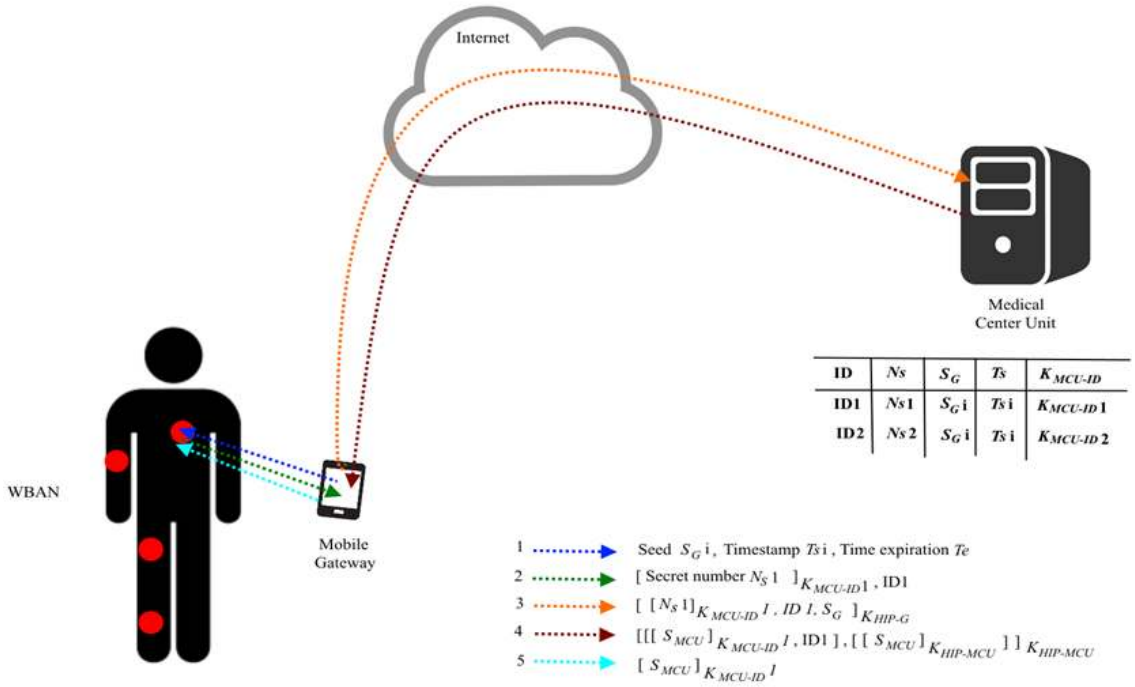

Fig. 3: Key agreement and establishment exchanged messages

the sensor secret number N_S to generate the symmetric key K_{MCU-ID}. To authenticate the sensor, firstly it decrypts the received message by the generated K_{MCU-ID}. If it success, it compares the S_N containing in the message by the stored S_N, if they match, the MCU saves the key and declares the sensor as legitimate. If not, it informs the G to begin revocation procedures explained later.

At this time, from the sensors received messages; the G saves some information about WBAN sensors as their ID and MAC address to update its routing table, but no sensed data is communicated yet.

In the second phase, after that the MCU authenticates all the sensors, it generates a new seed S_{MCU} and encrypt it by each node symmetric key K_{MCU-ID} and also by the G key. It sends them all to the G using a Ts and its Te. The G will redirect these messages, everyone to its destination.

Both the G and the sensors uses the S_{MCU} to generate the group key K_G shared by all of them to exchange updates information with the G. No sensed data will be encrypted by this K_G and no sensor will use it to communicate with another sensor.

Key update: Rekeying contributes in improving the system protection by changing the security keys in a specific time interval.

All the old session keys must be deleted after generating the new key, but only after checking that it worked.

The constraint in the rekeying is the good choice of changing key frequency. A change in a very short time interval will consume nodes resources and the choice of a longer period will offer to attackers more time to compromise the keys.

Even if that the G will be responsible to renew the sensors keys by sending new generated seed S_G. From time to time, without informing the gateway G, the MCU updates the sensors secret numbers N_S and records the old secret numbers, so if it receives a message with an old N_S, it will understand the node was compromised or its secret number was divulged.

Like that, with updated session keys and different secret numbers, even in the case of the compromised node or in the case of divulged keys, it will be difficult to an intruder to use them for launching tampering attacks or for eavesdrop the sensor data as they change frequently and in a period of time they will be out-of-date.

Node revocation: In the case of that the MCU detects a compromised node or an intruder, firstly it marks it as malicious in its database and signal an alarms about it. After that, it informs the G by its ID and sends to it a message; encrypted by the key used by this malicious node; containing a small program that will flash the device system and make it unusable. The G will records also in its table the node as malicious and redirects the message to the destination node. This latter, by decrypting the message and executes the program, it will loss all the stored information like the key, cryptography

mechanism and secret number, its system will be flashed.

Then, the G also will update its key and informs all the other nodes by the malicious nodes to avoid any message becoming from it.

Integrity: This objective is to preclude any changing to be made by an unauthorized intruder and to assure that the data coming from the sensor have not been tampered by this intruder.

The CCM mode of the AES algorithm ensures data origin authentication and integrity, by using a Message Integrity Code (MIC) also named as Message Authentication Code (MAC) that is appended to the message. It is created encrypting parts of the data using its generated key of the current session. Upon receiving the message, the receiver will decrypt it and generates the MAC for the received data and compares it with the MAC received in the message, if they match, it confirms that the message is authenticated and has not been altered by an intruder.

Mobility case: We created our solution to deal with mobility, as the sensor is linked directly to the medical center unit MCU by its symmetric key, so even if it changes the gateway, the service will continue working normally and the data still always secured. As in the case of in a hospital, it will be used a lot of routers implemented everywhere as gateways. If the patient changes the place so it will change the gateway, in this case, every WBAN sensor will sent a join request to this new gateway G' containing its ID and its secret number N_S encrypted by its symmetric key shared with the MCU. We claim that G' is already establishing a secure connection with MCU using the HIP protocol mechanism. The MCU authenticates the sensors and send after that a seed S_{MCU} as explained before to the G' and the WBAN sensors to generate the group key $K_{G'}$. Then, the G' uses this key to secure the seed $S_{G'}$ that will generate to initiate a new session.

In the join request, the sensors will include the address of the MCU. So even in the case of WBAN was found with the gateway that was not already established a connection with the MCU, it will find it directly using its address and start the same processes of keys establishment as the bootstrapping and deployment phases.

Post deployment operations: In each designed security key management protocol proposed for resource-constrained networks, it must respect and take into consideration a set of requirements and constraints for being an applicable and effective protocol.

Resiliency: Our scheme supports two types of key: an individual and unique key for each WBAN sensor, shared with the medical center unit MCU and another shared between the sensors and the gateway G. Therefore, in case of a compromised node, it will not affect other nodes in the network because everyone has a unique key and a unique secret number N_S that is the basis for the generation of the key. And the group key is used only to authenticate and check the integrity of updates from the gateway; it is prohibited to be used by the sensors to communicate between them.

Thus, most existing solutions are hypothesized no node is compromised or malicious node is introduced during the bootstrapping phase. However, this phase is dangerous because the establishment of all the network and protocols is done in this phase. Our scheme takes into account the security of this phase by the designated sharing key mechanism, no node communicates with another before its authentication by the MCU. Thus, no sensor that it is not recorded in the MCU database will have the possibility to establish a key.

Scalability: Our scheme is flexible regarding changes in network topology and supports scalability, it suffices that the sensor been stored in the database of the MCU to make it able to join the WBAN network.

If a new sensor wants to join the network, it sends its request to the gateway placed in its zone. The gateway that receives this request establishes the same mechanism of key establishment with the mobile sensor.

In case the G loses its connection with the main and secondary MCU servers, it will not accept any new sensor. It puts it in standby state and prohibits other sensors to communicate to it until its authentication.

Key connectivity: It is determined by the number of keys that every node must have to ensure the stability of communications within the network.

Each node has two different types of keys: the first is a single and unique K_{MCU-ID}, the unique key shared between each sensor and the MCU. The second type concerns the group key shared between the sensors and the gateway. So even in the case of mobility, the data flow between the sensors and the MCU will still stable as it is not depending to its relation with the local gateway. In any place where exist a gateway, the sensor can establish a secure connection with the MCU using only their shared symmetric key K_{MCU-ID}. This key will help also sensors to establish a rapid connection with any gateway.

PERFORMANCE EVALUATION

Energy cost: We use the energy model described in de Meulenaer *et al*. (2008) to analyze the energy cost of the key agreement of our proposed scheme and give an estimation of total energy cost; the energy required for the execution of the cryptographic instructions and the energy required for transmitting and receiving the used information for key establishment mechanisms, based

on estimates for the TelosB platform. We focus only for the energy cost of WBAN sensors as the other devices are not resource constrained.

According to the used energy model, the energy required to exchange one bit of data for a TelosB sensor is 0.72 uJ for transmitting and 0.82 uJ for receiving. For encryption, AES algorithm cost for 8 blocks of 128 bits is 144 uJ.

In our scheme, to establish the security keys, a sensor has to receive firstly the seed S_G from the gateway G in order to generate its K_{MCU-ID} key and the seed S_{MCU} from the medical center unit MCU. In addition, the sensor has to transmit its secret number encrypted by its K_{MCU-ID} to the MCU for authentication.

The first message is the one sent by G containing the seed S_G (32 bits), the timestamp (64 bits), the time expiration (8 bits) and the message protocols header (96 bits), so the total of bits the sensor receives is 200 bits; that mean it costs 144 uJ.

The second one is for authentication, the sensor must encrypt its secret number N_S (16 bits), i.e., 17.5 uJ and transmit a message containing this encrypted N_S and its ID (16 bits), in addition of the protocols header, so it transmits 128 bits, which costs 92.16 uJ, plus 17.5 uJ, that gives 109.66 uJ.

The last one is the message containing the encrypted seed S_{MCU} to generate the key K_G . Firstly, the sensor decrypts the message, which cost 113.7 uJ. The message length is the same as for the first message, i.e., 200 bits, so the total between the cost of decryption and reception is 304.7 uJ.

We observe that the total cost of the keys agreement to establish the two symmetric keys; the individual key K_{MCU-ID} and the group key K_G; in addition of sensor authentication, is 812.52 uJ about 0.81 mJ. The result is very interesting and energy efficient compared to other schemes.

Formal validation: To prove the fulfillment of the objectives desired security of the proposed systems, we used AVISPA tool to conduct a formal security analysis. AVISPA is a push-button that analyzes the security protocols based on formal methods to check whether the candidate protocol is secure or not. In the case of detection of a vulnerability, it offers the attack track and the step where that was made possible. The tool implements the Dolev-Yao intruder model [] able to modify traffic passing through, intercept messages, eavesdrop, or insert bogus data.

AVISPA implements four different automatic protocol analysis techniques for protocol falsification: OFMC (On-the-Fly Model-Checker), (CL-AtSe) (Constraint-Logic based Attack Searcher), SATMC (SAT-based Model Checker) and TA4SP (Tree Automata based on automatic approximations for the analysis of Security Protocols).

AVISPA uses High Level Protocol Specification Language (HLPSL) to illustrate the protocols to be analyzed. It is a special input language used to model the security protocols.

We modeled our proposed solutions using the HLPSL to analyze our protocol, we used AVISPA web tool [] to evaluate our solution, the result in the output was:

AVISPA Tool Summary
OFMC: SAFE
CL-AtSe: SAFE
SATMC: SAFE
TA4SP: INCONCLUSIVE

As we see, OFMC, CL-AtSe and SATMC tools have reported that our solution is safe. However, the TA4SP has reported that our solution is INCONCLUSIVE; that is because the case of the existing of compromised nodes in the network, that is clear, cryptography alone cannot provide a complete solution to any system, we have to choose other systems in parallel to solve the shortcomings of cryptography, such as intrusion detection systems.

CONCLUSION

We presented a settlement security keys for symmetric cryptography in order to ensure the privacy of the WBAN sensors in the context of IoT. This model is based on the establishment of two security pair wise keys in order to secure communication between the sensors and the medical center unit MCU in a side and the sensors and the gateway G from the other side.

This model ensures the confidentiality, privacy and sensors authentication as no intruder cannot get a false identity or set the security key to integrate the network without being registered in the MCU database and carry the secret number N_S. The analysis showed that our scheme meets the measures that must be taken into account for WBAN networks, such as energy conservation and adaptation for network flexibility and scalability.

From the result of the energy cost estimation and the formal verification using AVISPA tool, we can claim that our solution is secure and energy efficient in comparison with other proposed schemes.

REFERENCES

Armando, A., D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.C. He´am, O. Kouchnarenko, J. Mantovani, S. M¨odersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan`o and L. Vigneron,2005. The AVISPA tool for the automated validation of internet security protocols and applications. Lect. Notes Comput. Sci., 3576: 281-85.

Atzori, L., A. Iera and G. Morabito, 2010. The internet of things: A survey. Comput. Netw., 54(15): 2787-2805.

Barakah, D.M. and M. Ammad-Uddin, 2012. A survey of challenges and applications of Wireless Body Area Network (WBAN) and role of a virtual doctor server in existing architecture. Proceeding of the 3rd International Conference on Intelligent Systems, Modelling and Simulation (ISMS), pp: 214-219.

BBC, 2014. The Web: Vital Statistics.SEC Technology, Retrieved from: http://news.bbc.co.uk/2/hi/ technology/8552415.stm.

De Meulenaer, G., F. Gosset, O.X. Standaert and O. Pereira, 2008. On the energy cost of communication and cryptography in wireless sensor networks. Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB'08), pp: 580-585.

Di Peri, D., 2014. Body Area Networks and Healthcare. In: Salvatore Gaglio and Giuseppe Lo Re (Eds.), Advances onto the Internet of Things. Advances in Intelligent Systems and Computing. Springer International Publishing, NY,260:301-310.

Eronen, P., C. Kaufman, Y. Nir and P. Hoffman, 2014. Internet Key Exchange Protocol Version 2 (IKEv2).Retrieved from: http://tools.ietf.org/html /rfc5996 (Accessed on: August 27).

Go, A.S., D. Mozaffarian, V.L. Roger, E.J. Benjamin, J.D. Berry, W.B. Borden, D.M. Bravata *et al*., 2013. Heart disease and stroke statistics--2013 update: A report from the American Heart Association. Circulation, 127(1): e6-245.

Hao, Y. and R. Foster, 2008. Wireless body sensor networks for health-monitoring applications. Physiol. Meas., 29(11): R27.

Henderson, T., P. Jokela, P. Nikander and R. Moskowitz, 2014. Host Identity Protocol. Retrieved from:http://tools.ietf.org/html/rfc5201 (Accessed on: September 10).

Liu, C.H., Y.F. Chung, T.S. Chen and S.D. Wang, 2012. The enhancement of security in healthcare information systems. J. Med. Syst., 36(3): 1673-1688.

Medaglia, C.M. and A. Serbanati, 2010. An Overview of Privacy and Security Issues in the Internet of Things. In:Daniel Giusto, Antonio Iera, Giacomo Morabito and Luigi Atzori (Eds.),The Internet of Things.Springer, New York,pp: 389-395.

Meingast, M., T. Roosta and S. Sastry, 2006. Security and privacy issues with health care information technology. Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society and IEEE Engineering in Medicine and Biology Society Conference, 1: 5453-5458.

Rghioui, A., M. Bouhorma and A. Benslimane, 2013. Analytical study of security aspects in 6LoWPAN networks.Proceeding of the 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M), pp: 1-5.

Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications-Springer, 2014. Retrieved on: http://link.springer.com/article/ 10.1007/s 10916-010-9449-4/fulltext.Html#CR11 (Accessed on: April 17).

Seo, K. and S. Kent, 2014. Security Architecture for the Internet Protocol.Retrieved on: http://tools.ietf.org/ html/rfc4301 (Accessed on: August 27).

Ullah, S., P. Khan, N. Ullah, S. Saleem, H. Higgins and K.S. Kwak, 2009. A review of wireless body area networks for medical applications. Int. J. Commun. Netw. Syst. Sci., 2(8): 797-803.