Proc. Of the 3rd International E-Conference on Advances in Engineering, Technology and Management - ICETM 2020

ISBN: 978-1-63248-190-0 DOI: 10.15224/978-1-63248-190-0-04

Wireless Medical Sensor Networks

Security issues for e-health applications

Romina Muka[1], Kozeta Sevrani[2]
[1,2]University of Tirana, Albania
{romina.muka, kozeta.sevrani}@unitir.edu.al

***Abstract*—E-health appears to be a highly interesting field expanding nowadays, as an indispensable utility for doctors to facilitate the process of tracing electronic healthcare records. The increased use of Wireless Sensor Networks (WSN) for healthcare applications has improved the life quality of patients and has increased the physician-patient efficiency. A main concern regarding WSN for e-health applications is related to security issues, dedicated to the sensitiveness and criticism of patient related data, tending to become even more serious as wireless networks are involved. The majority of these applications rely on the use of wireless sensor networks, interacting with a database, transferring the data collected from patients in distributed locations. The distributive nature of these systems represents a greater challenge in securing data, by making the individualization of security solutions a field of interest and further research. In this paper will be given a brief insight of security issues threatening WSNs for e-health applications and solutions proposed, in order to manage the existent security issues.**

***Keywords*—e-health, security, wireless medical sensor networks, electronic health records**

I. Introduction

Among other fields of study that are expanding lately, e-health occupies an important place, highly interesting and advantageous regarding the future development of medicine. E-health presents a whole different platform of managing patients' health records and collecting information about their real-time health state. Due to WSNs for healthcare applications, nowadays patients in distributed locations can be supervised. This new system provides the facility of transferring data detected by sensors located in the vicinity of the patients, then stored in a remote database server and monitored by healthcare professionals. The idea behind e-health works perfectly, until security issues are taken into consideration. As we all may know medical records contain critical data, which need to be provided with high level of security, so security mechanism should be incorporated to this system in order for it to become totally efficient.

This paper is structured in some different parts, each one giving an insight of some different aspects regarding e-health. The great benefit e-health has, is making the communication between healthcare professionals and patients real-timing, easy and secure. E-health is a very broad field with a lot of applications [1], awaiting to be further developed up to the present overview of the system that will be given in this paper, leaving opened all the possibilities for future research.

In the first part of this paper will be explained how a wireless medical sensor network is designed, including the main components of the system, associated with the dataflow of the collected information from patients. Furthermore, some security issues will be reviewed, along with their consequences. It seems logical to present the requirements needed for a system to be considered secure, before any solution is explained. In the last part of the paper, a solution addressing the security issues of the system is introduced. It includes the presentation of an architecture model, along with the explanation of the way it works and how it provides security, before the paper is concluded in Section VI.

II. An overview of WMSN

The aim of a wireless medical sensor network (WMSN) is to facilitate the communication between patients and doctors and to make their lives easier and more comfortable. WMSN is very important for both parties. Patients who suffer from different diseases can be monitored continuously, staying comfortable at their own home. On the other hand, doctors may need to monitor a high number of patients at the same time, but they cannot interact directly with all of them. In order to access health monitoring at any time and from everywhere without costs, different technologies and architectures regarding wireless sensor networks are being developed.

Figure 1. WSMN design [2]

These proposed technologies are based on three components: Body Area Networks or BAN, gateways and remote supervising system [3]. The BAN is the set of wireless sensors used to aggregate health data. Wireless sensor nodes are deployed on a patient's body or near to the patient's body to monitor physiological conditions or other vital conditions such as temperature, heart beats, blood pressure etc. These sensors, as we can see from the figure above, use the ZigBee

ISBN: 978-1-63248-190-0 DOI: 10.15224/978-1-63248-190-0-04

[4] protocol in order to carry data packets over short distances, with low power consumption, or Bluetooth for short-range wireless communication. Because of the limited communication range, a wireless gateway is needed. So, the BAN sends collected data wirelessly to the gateway. The function of a wireless gateway is to provide paths for sensor nodes to send or receive data to the server and to serve as a relay node to the supervising system. There are two types of wireless gateways; one is local and serves as a bridge between wireless sensors and the local server and the other gateway serves to connect remotely through the IP network. The server receives the data, stores it in the database and presents the data in an appropriate form on the interface. Then authorized doctors can view the user interaction interface, can make queries to retrieve health parameters and to check for anomalies. This technology can be lifesaving, because doctors can intervene at the exact time, when necessary. A lot of healthcare applications can benefit from WMSNs such as: monitoring in-hospital, ambulatory monitoring, clinical, ward monitoring, sports-person health monitoring etc.

III. Attacks

In this section, we present four different possible attacks in WMSNs, as described below:

Privacy Threats: The main concern in healthcare applications is patient's privacy. Although, WMSNs are beneficial to patients, they are vulnerable towards privacy [5]. The data collected by sensors should be kept private and no one that is unauthorized should be able to see patient's health data. Imagine someone who has signs of a disease and suddenly all the rest of the people get to know about it. This can be depressing for the person that is suffering. A possible scenario could be: while the data is transmitting from wireless sensors to a caregiver, an attacker is eavesdropping patient data. He/she can get the information he/she wants to get (if data is not encrypted or if it is easy to decrypt the encrypted data) and then he/she can post all that information in a social network. The patient will suffer the consequences. To avoid this, the architecture should be improved in order to not allow an attacker to determine the identity of a patient and patient's private health data.

Denial of Service (DOS) Threats: The aim of this attack is to disrupt services and to make a network resource unavailable to its legitimate users. The medical network needs to be always functional to provide health monitoring at any time from everywhere. These types of attacks can be critical because can cause the loss of patients' lives. There are some types of DOS attacks [6], for example tampering, where a malicious user steals the medical sensor and tries to extract information from this sensor. Collision attack is another type of DOS attacks where the attacker transmits the packets at same frequency, resulting in packet collision and degradation of the network performance. Flooding attack is designed to bring a network down by flooding it with large amounts of traffic.

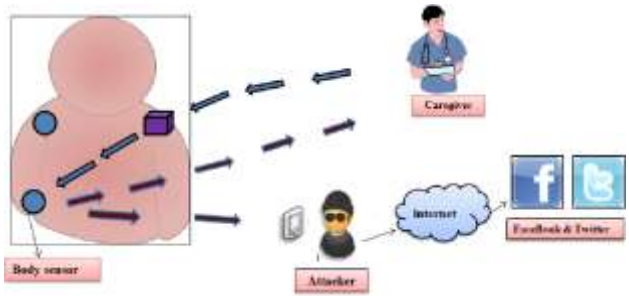

Figure 2. Threats against WMSNs [7]

Masquerade and Replay Threats: These types of attacks are very dangerous for real-time healthcare applications. The attacker can rouge a wireless rely point in a home care application while data is transmitting to the remote destination. Then the attacker can cause a masquerade. He can act as a real node to the network and can send false alarms to the remote location or cause disruption of different services. Since the treatment is based on fresh messages that are received by medical sensors, if the masquerade replays the old messages a lot of times this can cause medicine overdose and in the worst case can cause the loss of patient's life [7].

In Transit Threats: Interception is one type of in transit threats and it leads to an attacker accessing the sensor node data illegally, such as IDs or keys. The second type is message modification, so the message is altered in transit. The attacker captures wireless communication channels and extracts patient data. This attacker can tamper the data and send it to the destination (remote doctors). Since they don't have the correct information or signals from the patients, they will give less or more medicine to patients. In both cases, the results could be dramatic.

IV. Security requirements for WMSNs Healthcare Applications

Medical data are sensitive data, so it's not possible to design a wireless sensor network without taking into consideration the security. The architecture should guarantee confidentiality, integrity, availability, data freshness, and collision resistance [8].

Confidentiality: Health data should be confidential and should be accessed only by authorized doctors. In this way, an attacker cannot eavesdrop on the patient's data which are kept private. Confidentiality is ensured by encrypting data that are transmitted from the sensors to the intended destination, using symmetric encryption [9].

Integrity: It guarantees at the destination that the data has not been changed or modified in transit. Health data can be altered if an attacker exploits vulnerability in the system, for example: the broadcast nature of the sensor network. The integrity can be ensured by using the hash function for each packet sent between the server and the sensors.

Availability: It ensures that services and health data are constantly available whenever they are required by legitimate

Proc. Of the 3rd International E-Conference on Advances in Engineering, Technology and Management - ICETM 2020

ISBN: 978-1-63248-190-0 DOI: 10.15224/978-1-63248-190-0-04

users, even if there are a lot of requests. So, the architecture should be resilient to Denial of Service attacks.

Data freshness: It guarantees that an attacker has not replayed the old messages so that the patient's psychological signs are fresh. Use a strong freshness to give a total order on a request-response pair and to carry time-delay information [10].

Collision resistance: The architecture should resist against collision attacks in order to not allow unauthorized access to medical data.

v. Secure solution for WMSNs

As mentioned in the previous section, there are a lot of security challenges, yet to be overcome, in order for this service to be secure. Since the basis of it is composed from patients' health records, which are critical and highly sensitive data in need of maximum confidentiality, then solutions to these security challenges are mandatory for a proper implementation. Even though, e-health represents a relatively new field of study, its importance, in providing to patients immediate health support, is fascinating, but on the other hand the altering of patients' records can be fatal for their lives. Taking this into consideration, in this part of the paper will be discussed an architecture as the solution regarding WSN for medical applications security issues proposed in the work of [11] and [12], to provide a secure method of transferring patients' health state.

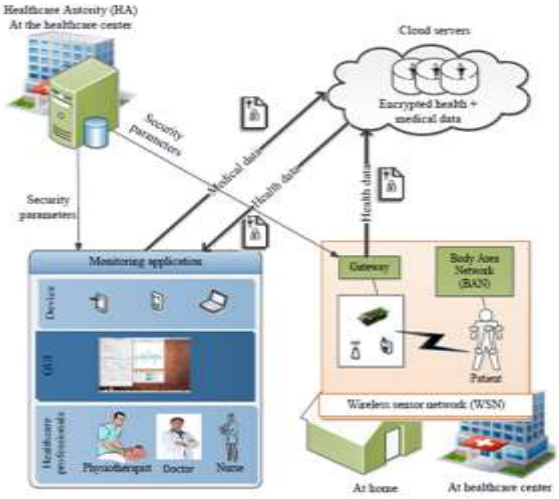

Figure 3. New proposed architecture

As a starting point for presenting this new architecture, it's essential the individualization of the security needs, which are: securing data during transmission and storage, implied from their nature, which should be confidential, only presented to authorized personnel and not altered (integrity) [13]. Also, the state of patients is not stable during all the time, which makes the emergency cases another matter of concern. In terms of security, the traditional method for handling emergency cases by allowing emergency staff to access all the medical records of the patient, achieved by the disabling of the security system, is intolerable. In this architecture is involved a new secure way to access information during critical health status of patients, as well as cloud computing technology [14] to manage the large amount of data needed to be transferred and offering scalability also.

The proposed architecture illustrated in Figure 3 [12] classifies users as healthcare professionals and patients, composed by 4 main components:

WSN - located in the patients' vicinity, responsible for collecting health information from them.

Monitoring applications - located in the healthcare professionals' vicinity, responsible for showing the information collected to the authorized doctors.

Healthcare Authority - responsible for the security policies of all the architecture.

Cloud servers - responsible for storing large amount of data, in this case encrypted, also as the management of servers' complexity.

As mentioned here, the data stored in the cloud servers will be encrypted, more specifically: the encryption will include a combination of symmetric cryptography and ABE (Attribute Based Encryption) [15]. The files containing the data from the patients will be encrypted using an RSK (Randomly generated Symmetric Key) and then the RSK will be encrypted with ABE, both stored in the cloud servers. On the other hand, decryption will be successful, if the user's key, by satisfying the ABE access policy, will decrypt the RSK key, meaning that he will after be able to decrypt the file. If the access policy, which determines the access rights of each user changes, only the RSK should be re-encrypted, not the whole file, as previous solutions implied because they used to encrypt the whole file using ABE.

In this paragraph, further details (see Figure 4) regarding the main component responsible for ensuring security, Healthcare Authority (HA), will be provided. It is the HA, which defines the security policies of the system, by generating the related security parameters, which include a pair of access structure and secret key. HA is also responsible for distributing them to each user. The access structure defines the privileges of each user in accessing data, while the secret key is generated from the attributes of these users, which at the same time represent their privileges [16]. The RSK decrypted with ABE, ensures that only the users with the right attributes can read a file, because only them have the privileges (right key) to decrypt the RSK key. Patients have a personal WSN and a gateway, which encrypts all the collected information from the sensors using RSK, then encrypted using the access structure obtained from HA. Regarding the healthcare professionals, they are allowed to add medical data to the patient's records, encrypted from the Monitoring Application using an RSK and the ABE provided by HA. The Healthcare Authority is assumed to be trusted, so the keys it distributes are encrypted by using its private key, sent to the cloud server along with its digital signature.

ISBN: 978-1-63248-190-0 DOI: 10.15224/978-1-63248-190-0-04

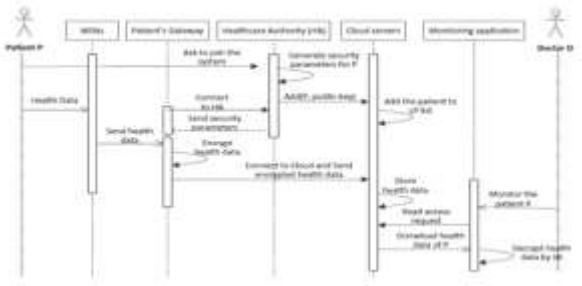

Figure 4. Detailed picture of the architecture [12]

Compared to the systems used until now, HA is considered innovative, because it is a dedicated structure that handles all the security requirements, leaving out of this responsibility patients and healthcare professionals. The last part of the description of this architecture will be dedicated to the management of emergency cases, critical health state of the patient. There are two scenarios that might happen during an emergency case:

- **Proactive scenario**: This scenario implies that the detection of the emergency situation is a merit of the analysis of the collected data from the WSN, which enables the system to identify the emergency staff, by providing them the access rights to the patient's data.
- **Passive scenario**: The emergency case is reported by someone else, who might be a relative of the patient, so the emergency staff needs to request temporary access to the patient's data to the HA.

In both scenarios, the first step includes the identification of the emergency case, then the responders should get access rights and at the end the rights should be revoked to their original pattern. This architecture's solution, as mentioned before, presents a new way of providing access rights to the emergency staff during emergency situation, not by disabling the whole security system. The HA generates two different access structures, one dedicated to normal cases and one for emergency cases, which is also pre-built and stored in HA or to a patient's devices. The overall rule is, the file data of the patient can be decrypted if the regular access rights or the emergency access rights are compatible with the ABE. Also, the emergency key, except from the attributes of the regular cases needs extra attributes-EC, in order to identify the actual emergency and the required data, such as a patient's ID, so the data of other patients will remain secured and the emergency staff won't be able to access them. As soon as the emergency case is resolved, the emergency keys should be revoked, because the emergency staff should no longer have the rights to access this patient's medical records. As the revoke process is complicated, an alternative solution is presented. Emergency keys have to be expiring, and as a validation, check the date they are used. The RSK of the actual files should be re-encrypted with a new date, so the validation date will change.

VI. Conclusion

In this paper, we discussed the importance of wireless medical sensor networks in real-time healthcare applications and we explained the way a simple WMSN works and its functionalities. We have outlined some security issues that researchers have found while implementing healthcare monitoring systems using medical sensors.

Since medical data are highly sensitive data, WMSNs should guarantee confidentiality, integrity, availability, data freshness and collision resistance. Furthermore, it's very important for patients to feel safe and protected so their health data should be kept private. The architecture should accomplish all of these security services because otherwise attackers will exploit vulnerabilities in the system and the patient will suffer the consequences.

To sum up, the idea of this paper is to have a secure architecture, not a complicated one. To accomplish this, we presented a solution regarding WSN for medical application security issues. In future works, we plan to put this system in practice to see whether it is feasible for real-time healthcare applications and we will try to improve the security mechanisms of this system in order to minimize its vulnerabilities and to improve the security.

References

[1] Ko, J., Lu, C., Srivastava, M. B., Stankovic, J. A., Terzis, A., & Welsh, M. (2010). Wireless sensor networks for healthcare. Proceedings of the IEEE, 98(11), 1947-1960.

[2] Ghamari, M., Janko, B., Sherratt, R. S., Harwin, W., Piechockic, R., & Soltanpur, C. (2016). A survey on wireless body area networks for ehealthcare systems in residential environments. Sensors, 16(6), 831.

[3] Darwish, A., & Hassanien, A. E. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. Sensors, 11(6), 5561-5595.

[4] Huang, Y. M., Hsieh, M. Y., Chao, H. C., Hung, S. H., & Park, J. H. (2009). Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. IEEE journal on selected areas in communications, 27(4), 400-411.

[5] Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, 36(1), 93-101.

[6] Ng, H. S., Sim, M. L., & Tan, C. M. (2006). Security issues of wireless sensor networks in healthcare applications. BT Technology Journal, 24(2), 138-144.

[7] Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. sensors, 12(1), 55-91.

[8] Othman, S. B., Bahattab, A. A., Trad, A., & Youssef, H. (2014, May). Secure data transmission protocol for medical wireless sensor networks. In 2014 IEEE 28th International Conference on Advanced Information Networking and Applications (pp. 649-656). IEEE.

[9] Mohan, M., Kavithadevi, M. K., & Prakash, V. J. (2016). Improved Classical Cipher for Healthcare Applications. Procedia Computer Science, 93, 742-750.

[10] Kumar, P., Ylianttila, M., Gurtov, A., Lee, S. G., & Lee, H. J. (2014). An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor network-based applications. Sensors, 14(2), 2732-2755.

[11] Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2012, July). Secure and scalable cloud-based architecture for e-health wireless sensor

ISBN: 978-1-63248-190-0 DOI: 10.15224/978-1-63248-190-0-04

networks. In 2012 21st International Conference on Computer Communications and Networks (ICCCN) (pp. 1-7). IEEE.

[12] Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2016). Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. Future Generation Computer Systems, 55, 266-277.

[13] Doroodgar, F., Razzaque, M. A., & Isnin, I. F. (2014). Seluge++: A secure over-the-air programming scheme in wireless sensor networks. Sensors, 14(3), 5004-5040.

[14] Swathi, B. S., & Guruprasad, H. S. (2014). Integration of wireless sensor networks and cloud computing. International Journal of Computer Science, 2(5), 49-53.

[15] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). Association for Computing Machinery, New York, NY, USA, 89–98. DOI:https://doi.org/10.1145/1180405.1180418

[16] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In 2010 IEEE 3rd International Conference on cloud Computing (pp. 268-275). IEEE.

PhD Candidate Romina Muka holds a bachelor's degree in Business Informatics and a Master of Science in Information Systems in Economy from University of Tirana (UT), Albania. She is also a lecturer at UT since 2015. Romina has been a guest lecturer in several international universities in Europe, and has been the contact person of different projects funded by Erasmus+, Interreg IPA BCC, Ministry of Science and Education in Albania, and Industry. Her research interests include security of WBANs in IoT and optimal deployment of sensors and controllers for the operation of the smart distribution grid (with new intelligent electronic devices).

Prof. Dr. Kozeta SEVRANI has graduated the Faculty of Natural Science in 1984. She is a Professor of Computer Science and Management Information Systems at the Faculty of Economy, University of Tirana, Albania. Her research interests include: information security; data science; digital divide; issues and solutions in building information infrastructure, e-business, e-learning, e-government/e-business and e-services in developing countries, particularly in Albania. She is in the Editorial Board of several international journals and does an extended work in consulting private companies and government agencies in Albania. Also, she has presented her work in numerous national and international conferences. Her work has been published in several journals and she has co-authored four one monograph and four books. Professor Sevrani has been awarded many important prizes among them "The Academic of the Year" from the ICT Award Albania in 2014. She is currently the head of Statistics Council of Albania and Head of Commission for promoting academic titles in University of Tirana.