Oct 28th, 9:00 AM - Oct 30th, 5:00 PM

Security Analysis of Wireless BAN in e-Health

Romina Muka
Norwegian University of Science and Technology, romina.muka@ntnu.no

Sule Yildrim-Yayilgan
Norwegian University of Science and Technology, sule.yildirim@ntnu.no

Kozeta Sevrani
University of Tirana, kozeta.sevrani@unitir.edu.al

Security Analysis of Wireless BAN in e-Health

Romina MUKA[1], Sule YILDIRIM-YAYILGAN[1], Kozeta SEVRANI[2]

[1] Norwegian University of Science and Technology, Gjovik, Norway
[2] University of Tirana, Tirana, Albania
{romina.muka, sule.yildirim}@ntnu.no, kozeta.sevrani@unitir.edu.al

Abstract. The Wireless Body Area Network (WBAN) has gained popularity as a new technology for e-Health, and is considered as one of the key research areas in computer science and healthcare applications. WBAN collects patients' data, monitors constantly their physiological parameters, using small implantable or wearable sensors, and communicates these data using wireless communication techniques in short range. WBAN is playing a huge role in improving the quality of healthcare. Still, due to sensitive and concurrent nature of e-Heath systems, current research has showed that designers must take into considerations the security and privacy protection of the data collected by a WBAN to safeguard patients from different exploits or malicious attacks, since e-Health technologies are increasingly connected to the Internet via wireless communications. In this paper we outline the most important security requirements for WBANs. Furthermore, we discuss key security threats to avoid. Finally, we conclude with a summary of security mechanisms to follow that address security and privacy concerns of WBANs, and need to be explored in an increasingly connected healthcare world.

Keywords: WBAN, e-Health, information security, wireless.

1. Introduction

In a digital society, electronic healthcare is one of the services that will contribute in improving the life quality of citizens. Recently, the fast development of wireless communication and intelligent medical sensors, which can be implanted or worn on human body, has made the wireless body area networks (WBANs) a promising method that will revolutionize practices of healthcare [1–3]. The term of WBAN was first created by Van Dam et al. [4] and received the attention of numerous researchers from different fields [5-6]. WBANs simplify and accelerate processes of healthcare, such as emergency medical responses and clinical diagnosis, increasing significantly healthcare efficiency.

WBAN is a communication network between human and computers through wearable devices [7]. On the whole, we can distinguish two types of devices: sensors and actuators. The sensors measure externally or internally parameters of the human body, for example measuring the body temperature, the beat of the heart or recording a continued electrocardiogram (ECG). From the other side the actuators (or actors) perform some actions related to the data that sensors send to them or through communication with the user. A personal device, like a smartphone or a PDA, which serves as a data sink for the wireless device, generally conducts interactions with the patient or other users. Next, we present the architecture of a WBAN in Figure 1.

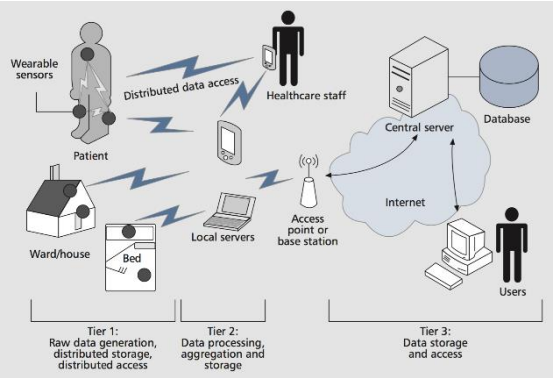

Fig. 1: WBAN Architecture.

The WBAN mostly contains small wireless sensor nodes that are positioned around, in or on a patient's body. These sensors constantly monitor vital signs of patients, like pulse, electrocardiogram (ECG), and blood pressure; or significant environmental parameters like humidity and temperature. Patient related data that are collected by sensors are transmitted to one or more servers or gateways, which can further perform data processing and distributed storage. The patient's data collected from all WBANs can be eventually sent to a centralized database for permanent healthcare records. Therefore, the authorized users of patient's data can access the data from the database remotely, or create a query to take information locally from the WBAN, depending on the application scenario.

We face a lot of new challenges when trying to develop a WBAN healthcare application, such as transmission of reliable data, appropriate distribution of data in the right time, power management, node computation and mobility support, middleware and fast detection of events [8-10]. Furthermore, the privacy of patient is vulnerable if security is not considered when implementing new technologies in healthcare applications [11,12]. Particularly must be guaranteed that patient related data are accessed only by authorized users; else, the patients' privacy could be compromised. However, since private data are stored in distributive manner in WBANs, they may be easily disclosed because of a physical compromise of a node. Consequently, to ensure patients' privacy, it is needed cryptographically enforced access and data encryption.

This paper gives contributions in presenting some security and privacy requirements in WBANs. We also discuss some WBANs security threats and initiate discussions on security mechanisms of WBANs to solve all the drawbacks and concerns regarding security and privacy. Next, in this paper is emphasized the need for the design of cryptographic methods that are reasonably resource optimal, low transmission overhead and storage, suggesting potential future directions for WBANs security. Finally, it concludes with some security mechanisms to follow that address WBANs security and privacy concerns, and need to be explored in an increasingly connected healthcare world.

2. WBAN Security and Privacy Requirements

It is essential to understand the security and privacy issues in WBANs, since they are two essential components for the system security of WBAN healthcare monitoring applications. In

this section we will discuss: (1) which would be the security requirements in WBAN before implementing suitable security mechanisms; and (2) e-health data privacy requirements.

Data confidentiality requirement is to protect the disclosure of e-health data. Sensor nodes, which send sensitive data in WBANs, can be compromised because of their not tampered proof nature. The compromise can lead to the disclosure of data if the whole data is encrypted and saved in one node both with its encryption key. The eavesdropping of communication can seriously harm patients because the attacker can use their data for criminal purposes. Encrypting the patient related data with a secret key attains data confidentiality, and this key must be shared on a secure communication channel between the sensor nodes and local servers.

Data Integrity requirement is to protect the modification of patient related data when communicated over a vulnerable WBAN. In WBANs altered data could lead to dangerous consequences, especially life-critical events. Appropriate data integrity mechanisms at the node and the local server certify that an attacker does not modify the received data. This can be attained by using data authentication protocols.

Data availability requirement guarantees that physicians could always obtain patient related data at the time when they require. The availability of a WBAN can be a target for an attacker. The attacker can capture or disable a sensor node, by resulting in loss of data availability. Consequently, it is necessary to maintain the operation of the sensor nodes in healthcare applications always on and shift the operation to another node in case of data availability loss.

It is not enough to guarantee data integrity and confidentiality, without considering also data freshness requirement. An attacker can get data in a transit and replay them later to fool the local server. Data freshness guarantees that patient data is fresh or contemporary, and the attacker has not replayed the old messages.

Data authentication is another WBAN security requirement for healthcare applications. It is essential for each sensor node and local server to prove that the data was sent by a trusted node, and not by an attacker that cheated the node or the local server to accept fake data. The sender of the e-health data must be authenticated and injection of data from outside the WBAN should not be allowed. Using symmetric techniques can attain data authentication in a WBAN.

Secure management requirement is required at the local server since it provides key distribution schemes to the sensor nodes in order to consent encryption and decryption operations.

Many users in a WBAN healthcare application such as physicians, nurses, doctors, insurance companies, pharmacists, social workers access patient's data. So, it is highly recommended to implement an access control mechanism based on roles in real time healthcare applications that can control the access of the patient's physiological data, and guarantee its privacy.

Patient permission requirement is necessary when a healthcare provider is distributing his/her health records to another healthcare authority, such as medical researcher, insurance company, and etc.

3. WBAN Security Threats

WBANs certainly improve the quality of care for patients, but the medical sensor devices sense the sensitive patient's data and uses wireless communication to transmit it. Therefore, it must be guaranteed the security and privacy for patient's physiological parameters from any security threats. Based on the security requirements, in the following we examine security threats that would be harmful for the WBAN healthcare applications.

Secrecy and Authentication Attacks: In this category are included threats such as eavesdropping and monitoring on patient vital parameters, spoofing of packets, or masquerade and packet replay attacks. Eavesdropping is the most common threat to e-Health systems. By snooping to patient's sensitive data, an attacker can easily track the activity of users from communication channel. Based on the patient related data he/she can analyze patients' activities. One case of authentication attacks in WBANs is faking of alarms on patient related data [30]. In a WBAN healthcare application an adversary can easily cheat a sensor node while patient related data is transmitted to the local server. In this attack, an illegal sensor node acts as a real one to the network. This can lead to false system alarms, for instance an emergency team can start an unnecessary rescue operation. A masquerade node can also create denial of service attacks, by interrupting the application functionality. Furthermore, if a masquerade sensor node gets the physiological parameters of a patient, this can pose a replay threat to a WBAN e-health application. Thus, attacks on secrecy and authentication endanger WBANs healthcare applications. Standard cryptographic techniques and Message Authentication Code (MAC) can safeguard the authenticity and secrecy of communication channels.

Service Integrity Attacks: In this type of attacks is included threat to information when in transit. In WBAN healthcare applications, sensor devices capture patient related data and send it to the local server or the hospital server. While the data is in transit, it may be attacked. This can trigger a false alarm or can hide the true state of a patient, leading to a disaster event. Message alteration threatens the integrity of WBAN sensor nodes. Service integrity attacks don't occur only during transmission times, but also during storing times. WBANs can be protected from these attacks if implemented Message Authentication Code techniques.

Network Availability Attacks: Network availability attacks are referred also as Denial of Service (DoS) attacks. DoS attacks try to make unavailable to its users the network resource and affect network's capacity and performance. DoS threat can be even more disrupting in WBAN healthcare applications since it is necessary for the network to be always on to monitor the patient health. Since WBANs are a type of wireless sensor networks (WSN), most of their DOS attacks are inherited from WSN, but, because of the unique features of WBAN, there exist certain differences between DOS attacks that can happen in WBAN compared to WSN.

4. WBAN Security Mechanisms

There exist a lot of security mechanisms recommended for Wireless Sensor Networks (WSN), however few of them can be implemented in a WBAN that has low power computation. For instance, the IEEE 802.15.4 is a standard designed for Wireless Personal Area Networks with low data rate, so we can call it a low power standard. Control layers that IEEE 802.15.4 standard specifies are media access and physical ones, and it focuses on low speed and cost pervasive communication between devices. This is a very relevant standard for WBANs since it supports applications with low data rate and cost power consumption. For this reason it is implemented by many researchers and designers to develop security mechanisms and protocols for Wireless Body Area Networks. The IEEE 802.15.4 security modes are classified into null, encryption only (AES-CTR), authentication only (AES-CBC-MAC), and encryption and authentication (AES-CCM).

4.1. AES-CTR

Sensor nodes, to encrypt the data and to provide confidentiality protection, use the Counter (CTR) mode (also known as Integer Counter Mode) by using Advance Encryption Standard (AES) block cipher. In this mode the plaintext is broken into 16-byte blocks b_1, b_2, ..., b_n, and the ciphertext is computed in the sender side: $c_i=b_i$ XOR $E_k(x_i)$, where c_i is the ciphertext, b_i is the data block, and $E_k(x_i)$ is the encryption of the counter x_i. Figure 2 shows the process of encryption and decryption of CTR.

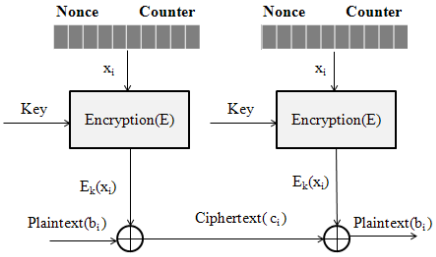

Fig. 2: CTR encryption and decryption process.

4.2. AES-CBC-MAC

A secure authentication and message integrity protection is required in a WBAN. A Cipher-Block Chaining Message Authentication Code (CBC-MAC) mode indicates that an n-block message B = b_1, b_2, ..., b_n will be authenticated between two parties involved that share a secret key, K, for the block cipher, E. The sensor nodes can compute a 32, 64, or 128 bit MAC. Only parties that have symmetric key can compute the MAC.

In this mode, the plaintext is XORed with the previous encrypted text until the final MAC is achieved. In this moment the ciphertext is generated by $c_i= E_k(b_i$ XOR $c_{i-1})$ and plaintext can be generated by $b_i= D_k(c_i)$ XOR c_{i-1}. The sender pairs the plaintext with the calculated MAC. The receiver located in Tier 2 authenticates the message by calculating its own MAC and compares it with the received MAC of sensor nodes. The body sensor network coordinator (receiver) accepts the packet if both MACs are similar. The block diagram of a CBC-MAC operation is shown in Figure 3.

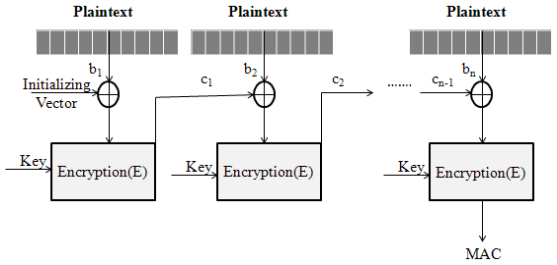

Fig. 3: CBC-MAC operation.

4.3. AES-CCM

The Counter with CBC-MAC (CCM) security mode is a combination of CTR and CBC modes that addresses a high-level security, including both encryption and data integrity. The sensor nodes first apply the integrity protection to the header and data payload of the MAC frames using AES-CBC-MAC mode and then encodes the frames using AES-CTR mode. It can be used to communicate sensitive information, for instance to update programs in implantable cardiac defibrillators and pacemakers.

Conclusion

A Wireless Body Area Network is estimated to be a very valuable technology with potential to provide a broad range of profits to patients, a continuously monitoring of health and give real time feedback to the patient or medical personnel. Security is an essential feature for the implementation of WBANs. The implementation of WBANs must fulfill the rigorous security and privacy requirements. However, designing security practices results to be a complicated process because of the limitations and features of WBAN's environment. The common security methodologies are not relevant for WBANs. An appropriate security mechanism in a WBAN must be low cost and lightweight in the view of resource consumption. Furthermore, we must not forget that, however, normally noise concerns are associated to quality of service, but they can lead to serious consequences related to security threats in WBANs. Therefore, a proper security mechanism for WBANs must take into considerations vulnerability of WBANs to the noise and implement an efficient and powerful error recovery method to reduce/stop this weak point.
WBAN is increasing fast but up to now there is no solid and unified security framework for these types of networks. The research in data security and privacy of WBANs is still in its beginning nowadays; more studies and researches are needed in this area.

References

1. Jovanov, E., Milenkovic, A., Otto, C., and C. de Groen, P. (2005). A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and Rehabilitation*, 2(6). DOI: 10.1186/1743-0003-2-6
2. Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., and Maisel, W. H. (2008). Security and privacy for implantable medical devices. *IEEE pervasive computing*, *7*(1), 30-39.
3. Lorincz, K., Malan, D. J., Fulford-Jones, T. R., Nawoj, A., Clavel, A., Shnayder, V., ... and Moulton, S. (2004). Sensor networks for emergency response: challenges and opportunities. *IEEE pervasive Computing*, *3*(4), 16-23.

4. Van Dam, K., Pitchers, S., and Barnard, M. (2001). Body area networks: Towards a wearable future. In *Proceedings of WWRF kick off meeting*, Munich, Germany, March 6–7, 2001.
5. Otto, C., Milenkovic, A., Sanders, C., and Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of mobile multimedia*, *1*(4), 307-326.
6. Jurik, A. D., and Weaver, A. C. (2008). Remote medical monitoring. *Computer*, *41*(4), 96-99.
7. Singh, A., Kumar, A., and Kumar, P. (2013). Body Sensor Network: A Modern Survey & Performance Study in Medical Perspect. *Network and Complex Systems*, 3(1), 12-17, Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications.
8. Gravina, R., Guerrieri, A., Fortino, G., Bellifemine, F., Giannantonio, R., & Sgroi, M. (2008, October). Development of body sensor network applications using SPINE. In *Systems, Man and Cybernetics, 2008. SMC 2008. IEEE International Conference on* (pp. 2810-2815). IEEE.
9. Lorincz, K., Chen, B. R., Challen, G. W., Chowdhury, A. R., Patel, S., Bonato, P., & Welsh, M. (2009, November). Mercury: a wearable sensor network platform for high-fidelity motion analysis. In *SenSys* (Vol. 9, pp. 183-196).
10. Lee, S. C., Lee, Y. D., & Chung, W. Y. (2008, November). Design and Implementation of Reliable Query Process for Indoor Environmental and Healthcare Monitoring System. In *Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on* (Vol. 1, pp. 398-402). IEEE.
11. Leon, M. D. L. A. C., Hipolito, J. I. N., & Garcia, J. L. (2009, September). A security and privacy survey for WSN in e-health applications. In *Electronics, Robotics and Automotive Mechanics Conference, 2009. CERMA'09.* (pp. 125-130). IEEE.
12. Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008). Security and privacy for implantable medical devices. *IEEE pervasive computing*, *7*(1), 30-39.