applied sciences

Article

Cryptographic Protocol with Keyless Sensors Authentication for WBAN in Healthcare Applications

Kevin Andrae Delgado-Vargas , Gina Gallegos-Garcia * and Ponciano Jorge Escamilla-Ambrosio

Centro de Investigación en Computación, Instituto Politécnico Nacional, Av. Juan de Dios Bátiz S/N, Nueva Industrial Vallejo, Gustavo A. Madero, Ciudad de México 07738, Mexico
* Correspondence: ggallegos@cic.ipn.mx

Abstract: Nowadays, technological advances provide people with more facilities and luxuries in life. Medicine is no exception; for example, different wireless sensors can be used to monitor patients' state of health. These sensors are used in the so-called Wireless Body Area Networks (WBAN), to improve the efficiency of doctor-patient activities at any time, in any body area, and anywhere. However, health data contains sensitive information that becomes a critical issue requiring special attention when transmitted within a WBAN. In other words, WBAN must be protected from malicious devices that intercept, alter or access without authorization or even deny the health information being transmitted. In this article, we present the design of a new cryptographic protocol that guarantees three security services, authentication, confidentiality, and integrity by securing sensitive information communication through a WBAN. We also consider a keyless sensors authentication method to distinguish whether or not the devices are placed on the same individual's body. A formal analysis of the protocol is carried out using cryptographic protocol verification tools to guarantee its correct construction and that it provides appropriate security.

Keywords: cryptographic protocol; medical approaches; WBAN; non-cryptographic authentication method

check for updates

Citation: Delgado-Vargas, K.A.; Gallegos-Garcia, G.; Escamilla-Ambrosio, P.J. Cryptographic Protocol with Keyless Sensors Authentication for WBAN in Healthcare Applications. *Appl. Sci.* **2023**, *13*, 1675. https://doi.org/10.3390/app13031675

Academic Editor: Arcangelo Castiglione

Received: 17 November 2022
Revised: 12 January 2023
Accepted: 24 January 2023
Published: 28 January 2023

1. Introduction

A wireless body area network (WBAN) is a wireless network of heterogeneous sensors placed in different parts of a human body [1]; the sensors can be wearable or implanted under the user's skin. WBANs will be relevant and helpful for monitoring the population's health. WBANs can be used not only on remote patients but also to enable the wireless monitoring of patients within hospitals. According to the World Health Organization (WHO), between the years 2000 and 2050, the population over 65 years old will go from 605 million to 2 billion people [2]. WBANs use low-power signals to reduce interference between devices, and the transmission distance is not greater than 2 or 3 m. Thanks to this, doctors can monitor patients' health in real-time; thus, their health records are always up to date. The Health Insurance Portability and Accountability Act (HIPAA) provides a series of regulations on securing a patient's information [3]. In such regulations, it is stipulated that privacy and confidentiality are essential characteristics to have on monitored patients. Despite this, security is often overlooked, and patients could be exposed to a cyberattack that could put their health and life in danger. In this context, several cryptographic protocols have been proposed that ensure authentication and only use confidentiality and integrity as support for maintaining authentication.

A WBAN is secure if it ensures privacy, confidentiality, integrity, and authentication. However, the limited power and infrastructure of WBAN systems provide a challenge in implementing such measures. Authentication is a very crucial aspect in any network of communicating devices. Traditionally, the authentication process has been related to pre-distributed secret keys among nodes in a network. Nevertheless, WBAN's users are usually security inexperienced, which requires high usability of the authentication process, minimization of key distribution/management, and needs to be automatic and transparent to users. Node authentication mechanisms in WBAN should have minimal reliance on cryptography. Finally, low-end medical sensors are extremely constrained in resources, while non-cryptographic authentication mechanisms mostly require advanced hardware [4,5] or significant modifications to the system's software. Node authentication in a WBAN is of great concern as it can compromise the privacy of the entire network. Hence, this paper presents a cryptographic protocol that guarantees the security services of authentication, confidentiality, and integrity applicable to WBAN. The research question considered in this approach can be stated as: Can cryptographic primitives combined with a key-free authentication method improve the security of transmitted data over a WBAN used by doctor-patients activities at any time, any body area, and anywhere? The proposed protocol makes use of a non-cryptographic sensor authentication method that does not depend on pre-shared secrets between nodes. In the same way, cryptographic primitives, such as the key encapsulation mechanism, digital signature, and hash functions, are used to guarantee security services on the information transmitted.

Current protocols use cryptographic primitives to preserve security services, mainly authentication and confidentiality. The main primitives used to preserve these services include encryption, key encapsulation mechanism (KEM), digital signatures, and hash functions. Cryptographic protocols help protect the information, minimize the confidence required between participants and face security breaches when these services are absent [6,7]. There are different types of attacks that can be made to protocols. These attacks usually involve obtaining a determined entity's values to pose as a legitimate source. Some of the possible attacks are [6]: (a) Man-in-the-middle attack, an external entity intercepts the communication between the authorized parties; (b) Repetition attack, an unwanted entity poses as a real one with information gathered from a previous execution of the protocol, or the same one with a different verification; (c) Parallel execution attack, this attack is achieved by making use of specific values obtained from one or more previous simultaneous executions. Security verification tools are used to verify that protocols can resist these different attacks. Protocols can be probed for security or semantic failures. Different tools exist to help formal verification of a protocol. The different tools verify the cryptographic primitives that each protocol has, in both its use and the security it provides under different scenarios.

The rest of the article is organized as follows: Section 2 presents a review of the work related to cryptographic protocols focused on medical care and their security verification. Section 3 introduces security in medical systems and those cryptographic primitives that help achieve their security, also describes the proposed protocol. Section 4 presents the proposed protocol's security verification results using protocol verification description tools. Finally, in Section 5 conclusions and future work are presented.

2. Related Work

The level of security required for medical devices depends on the function of each device. It is necessary to secure the information used by medical devices so that attackers do not obtain unauthorized information or control over them, as the main information transmitted by these devices is sensitive. Many of the devices used in medicine are embedded, and most are intended to be secure at the physical level; this opens the door to targeted cyberattacks focused on sharing of secrets, private certificates, passwords, open-source bugs, cryptography, and weak authentication [8]. Different protocols, systems, or cryptographic schemes have been proposed for Implantable Medical Devices (IMDs). There are different solutions to provide security to medical scenarios with a sensor network architecture. Research on security mechanisms for WBAN can be divided into cryptographic and non-cryptographic authentication mechanisms. Cryptographic authentication mechanisms adapt lightweight traditional cryptographic schemes. Non-cryptographic authentication approaches can be divided into biometric-based, channel-based, and proximity-based authentication schemes [9]. These solutions are well-defined protocols, with security tests using protocol verification tools. The cryptographic protocols reviewed in this section were chosen due to their application, in a medical scenario, within a sensor network architecture. Most use cryptographic primitives to guarantee security services: authentication, confidentiality, and integrity.

The work in [10] presents an efficient and practical authentication solution based on the scheme of Hwang and Li [11]. This solution uses smart card features and one-way functions. The solution presented changes the problem on which the security of Hwang's scheme rests, going from discrete logarithms to hash functions. The authors performed security and efficiency analysis tests, which showed that the change in the problem does not affect the security provided by the solution.

In [12], a WBAN authentication solution based on the Rabin scheme [13] and public key algorithms, is presented. The schemes used in this system are lightweight since the authors use their system on embedded devices with limited resources. The application scenario in which the solution works comprises a set of sensors and actuators connected to the WBAN and placed in the body of patients with different diseases. It has four participating entities: sensors, actuators, the node coordinator, and, a doctor. Each of these entities interacts with one another within the system.

The work presented in [14] proposes an upgrade from work done by Lu et al. [15] which is an authentication protocol used at Telecare Medic Information Systems (TMIS). The authors discovered that the original work was prone to diverse attacks. Through several tests with the ProVerif tool, they identified vulnerabilities related to the violation of the patient's anonymity, identity usurpation, and TMIS server attacks. Therefore, the developed protocol is resistant to those attacks and performance better, but at a computational cost.

In 2015 [16], a lightweight key-handling protocol was proposed. This protocol establishes secure communication between a node with limited resources and a remote server. To ensure the protocol is secure, the authors use the AVISPA verification tool [17]. The protocol proposed by the authors considers the use of 3 entities: (1) Sensors or the restricted node (CN), (2) Remote server (UN), and (3) Third entities (TP_i). The three entities divide the secret among themselves. The protocol uses algorithms based on symmetric cryptography to provide confidentiality; for authentication, digital signatures are used; and hash functions are employed with Message Authentication Code (MAC) to ensure integrity. This protocol has 5 phases, and the results indicate that the protocol is secure in certain scenarios but also obtain an inconclusive result, which, according to the tool manual, does not imply that an attack has been detected.

In 2019, an authentication protocol [18] for TMIS use was introduced based on the protocol developed by Das et al. [19]. The authors analyzed the security of the protocol using protocol verification tools, starting with AVISPA [17], in which two of the scenarios provided by the tool were analyzed. Similarly, the protocol is verified using the Scyther tool [20,21]. The proposed protocol is developed with four main entities: (1) Medical Record Server (MRS), (2) Medical Server (MS), (3) Patient Server (PS), and (4) Patient Unit (PU). If a server is controlled directly by a doctor, then it is a PS; otherwise, it is an MS. The protocol works with one server at a time. The proposed revised protocol contains 9 phases, unlike the 6 phases in the one by Das. The verification results with AVISPA indicate that the protocol is safe against some attacks that the tool verifies. The results of Scyther show that the principal values used to generate keys in different phases remain secret, and in the same way, the entities remain authenticated. Therefore, the protocol provides authentication of the entities, confidentiality, and integrity to the data handled.

In 2020, the work in [22] was presented, in which the authors propose a protocol for IMD. The protocol is functional, does not risk the life of the patient who uses it, and was evaluated for protection against denial-of-service attacks. The protocol was subjected to safety tests using the AVISPA tool [17]. If the attacker has complete control of the communication channel, the system can be analyzed to determine if it meets certain security requirements. The environment in which the protocol is developed considers four entities:

(1) Smart card (C) for the user (U), (2) Hospital server (S), (3) Implant (I), and (4) Reader (R). Entities C and S provide the protocol with security services: non-repudiation, access control, and user authentication. This protocol has 4 phases to provide the services of confidentiality, integrity, non-repudiation, access control, and user authentication. The protocol has two ways of working. The first one considers that all entities have an internet connection. When this is not possible, the protocol enters the second model, which proposes the exchange of keys between only three entities, preventing the server from being the one that sent the keys. Vulnerabilities against man-in-the-middle and, repetition attacks are sought. The analysis yielded results by phase, showing that some phases do not comply with all security services.

In 2020, work at [23] presented an efficient privacy-preserving protocol with anonymous authentication to provide information security and privacy to users with low computational and communication costs. The protocol maintains communication between a network manager, sensors placed on the patient's body, a controller device, and a medical server. Communication is done in three main phases: (1) System initialization. (2) Registration of sensors. (3) anonymous authentication between patient to doctor and doctor to patient. One of the characteristics of this protocol is that the records are made personally between the patient and the doctor with the network manager. The protocol guarantees the security services of confidentiality, authentication, and integrity. The protocol is analyzed in three ways: (1) informal security analysis, (2) formal security analysis based on BAN logic, and (3) formal security analysis using the AVISPA [17] tool. The results of applying AVISPA and the informal analysis show that the protocol is safe and even ensures it is safer against impersonation attacks.

In 2020, the work in [24] presented a key agreement and authentication protocol based on hash and XOR functions. The protocol proposed by the authors has protection features against intermediate node compromise, sensor node spoofing, and base station compromise attacks, in addition to the security features proposed by Kompara et al. [25]. The protocol is executed between 3 main entities: Sensor Node (N), Intermediate Node (IN), and a Hub Node (HN). The protocol contemplates three primary phases to achieve authentication. The security assessment is performed with the help of the AVISPA [17] tool. The results thrown by the tool showed that the proposed protocol is secure in the different ways that can be reviewed.

In 2020 the authors of [26] presented a lightweight ECC-based end-to-end authentication protocol for WBAN to overcome the vulnerabilities in the protocol of Li et al. [27]. The proposal considers three entities: the User (U), the Network Manager (NM), and the Application Server (AS). The protocol contemplates the communication between the entities along three main phases to guarantee authentication. The authors present a security analysis using the AVISPA [17] tool. The results showed that the protocol is secure in the different scenarios in which it was simulated. In the same way, an informal analysis is presented, showing that the proposal is secure against different attacks, unlike the resistance presented by the protocol of Li et al.

2.1. Security Mechanisms for WBAN

Research on security mechanisms for WBAN can be divided into cryptographic and non-cryptographic authentication mechanisms. Cryptographic authentication mechanisms adapt lightweight traditional cryptographic schemes. Non-cryptographic authentication approaches can be divided into biometric-based, channel-based and proximity-based authentication systems [9].

2.1.1. Cryptographic Authentication Methods

Cryptographic authentication methods are computationally power-hungry, making them infeasible for constrained WBAN sensor nodes. Elliptic curve cryptography has been successfully deployed in wireless sensor networks. Although these systems are feasible for WBAN, elliptical curve cryptosystems consume higher energy when compared to symmetric cryptosystems [28]. TinySec [29] is an approach for providing authentication in WBAN. In this scheme, every sensor is programmed with a common key before the deployment of the sensor network. Further communication in the network, as a message or packet encryption, is done using a common key. The main drawback of this system is that a compromised sensor can cause the leakage of complete information from the sensors network; hence, the whole system will be at risk. Accordingly, the traditional authentication schemes mentioned above lack security and require high computational power; therefore, they are infeasible for WBANs.

2.1.2. Biometric-Based Authentication Mechanisms

Biometric-based authentication mechanisms aim to find a unique feature from the human body and then use these traits as an authentication identity. Said features are derived from behavioral or physiological characteristics exhibited by a human. Common primitives used by biometrics systems are fingerprint, face, hand geometry, iris, and voice. These systems overcome the problem of distributing pre-shared keys among sensors. In [30,31], researchers have exploited physiological parameters such as electrocardiogram (ECG), photoplethysmogram (PPG), heartbeats, and fingerprints. The efficiency of these authentication mechanisms lies in the correlation coefficient of physiological parameters calculated at the sender and receiver. The main reason for dissimilar physiological signals is due to the position of sensors at different parts of the human body. Biometric-based systems require specialized sensing hardware, which is an overhead for the miniature on-body sensors.

2.1.3. Channel Characteristic-Based Authentication Mechanisms

Channel Characteristic based Authentication mechanisms are also known as location-based authentication systems; they are built based on variations in Received Signal Strength (RSS). Researchers have leveraged the variations in RSS over time to authenticate WBANs. Body Area Network Authentication (BANA) [9] is a lightweight authentication scheme built on the observation that RSS variations are distinct for on-body and off-body communication channels. An extended version of this approach is ASK-BAN [32], which works concurrently within a wireless channel to generate a key and node authentication. A static channel for authentication and a dynamic channel for key generation are employed. This system takes around 12 s for authentication and 15.9 s for key generation. ASK-BAN requires additional nodes between the Control Unit (CU) and the sensor node. In addition, sensor nodes on the body are deployed half a wavelength from each other to verify the viability of the multi-hop relay node security system. On the other hand, during the authentication phase of the system, the subjects cannot perform any bodily movement.

3. Protocol Design and Description

In the previous section, different protocols focused on protecting WBASNs and TMIS were presented. These protocols are primarily focused on ensuring the authentication of entities. The protocol presented below focuses on guaranteeing not only entities' authentication but also information. In the same way, the confidentiality and integrity of sensitive information that travels through the network are guaranteed. This is achieved by using four cryptographic primitives to ensure secure communication between the entities participating in the WBASN. Therefore, sensitive information that is transmitted between nodes is protected. Likewise, the protocol applies a key-free or non-cryptographic method of authentication of the nodes, which makes it possible to distinguish whether the sensors are on the patient's body.

3.1. Cryptographic Primitives Election

Once security services and the cryptographic primitives that help to preserve them have been reviewed, it is necessary to specify which of these primitives will be used in the future. It is sought that three security services will be preserved: confidentiality, integrity, and authentication, through four cryptographic primitives. Encryption: used to provide confidentiality to the information [6], so it can travel securely. Digital signature: fundamental primitive to provide authentication, any entity that receives information can know its identity [7]. Key Encapsulation Mechanism (KEM): an agreement that encrypts the information using techniques designed to secure the keys of symmetric cryptography for transmission using asymmetric algorithms. Hash functions: it maps binary strings of information of an arbitrary length and converts them into binary strings of fixed length [6]. It is computationally simple to get from any input to any output. However, getting from any input to a hash value is computationally impossible.

These primitives are used to take advantage of the capabilities of each device. Before fully defining the location of each of these primitives, it is necessary to know the capabilities of the entities that will be used in the protocol. In [33,34], the minimum capabilities that the used equipment must have, are presented, as well as their different characteristics, such as the range of data that they handle, the frequency at which they work, and the range of data presented by each of the devices.

3.2. Choice of devices

In [35], a study of the different standards for the devices used in the medical field is presented. Derived from this, the following entities are proposed:

- Medical server (A): this entity must have the computational capacity to perform the most complex cryptographic operations. It is proposed that this entity is a desktop or laptop computer with an x86 processor. It is assumed that the patient's physician controls this entity. The entity must read the data from the other entities and generate instructions or commands to be executed by the corresponding actuator.
- Coordinator node (B): This entity has limited resources compared to the server. It will be with the patient at all times. The entity can be a smart cell phone, an embedded system, or a device with an ARM processor. It must perform the cryptographic operations necessary to fulfill the purpose of the protocol. This entity will be in constant communication with the sensors, actuators, and server.
- Sensors (C): They will be placed on the patient's body taking specific measurements. They must be able to take the measurements and send them to B. The transmission is assumed to be over a secure channel.
- Actuators (D): They will be on the patient's body waiting for a command. They must have the capability to perform their normal and inexpensive operations.

Inspired by the work presented in [12], the architecture seen in Figure 1 is proposed. The architecture shows the position of entities A, B, C, and D, and their interactions. The direction of the communication indicates whether the information is encrypted or signature-protected.

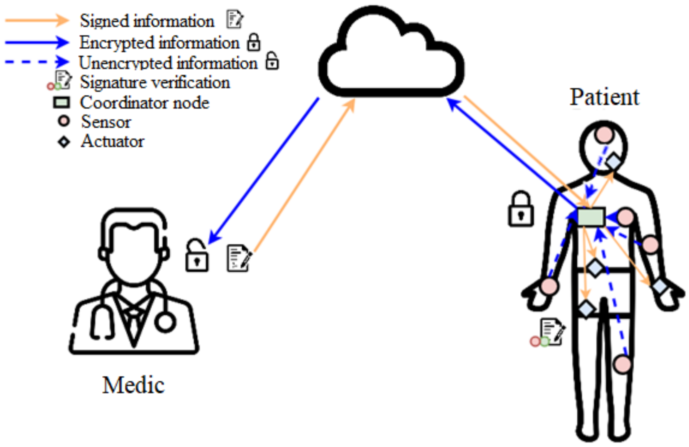


Figure 1. Proposed medical scenario WBAN architecture.

3.3. Description of the Protocol Phases

Figure 2 shows the protocol sequence diagram. It shows the messages to be sent between the entities and the functions to be performed. The protocol is divided into four main phases.

The five phases that make the protocol can be described in terms of their function and their inputs and outputs:

- Phase 0—Setup and sensors authentication: Generates the movement data of $B_{(Acc,Gyro)}$, $C_{(Acc,Gyro)}$ and $D_{(Acc,Gyro)}$. The output is the acceptance or denial of access to the WBAN.
- Phase 1—Key generation: Generates a key pair (P_{KA}, S_{KA}) and sends P_{KA} to B and D.
- Phase 2—Sensing, encrypting, and sending information: C sensors register and send the encrypted information to B.
- Phase 3—Decryption of the information, signing, and sending instructions: B receives the encrypted information, decrypts it, and generates instructions and a digital signature that is sent to D.
- Phase 4—Verification of the signature and application: A verification function determines if it is safe to apply the instructions received based on the signature that came with the instructions.

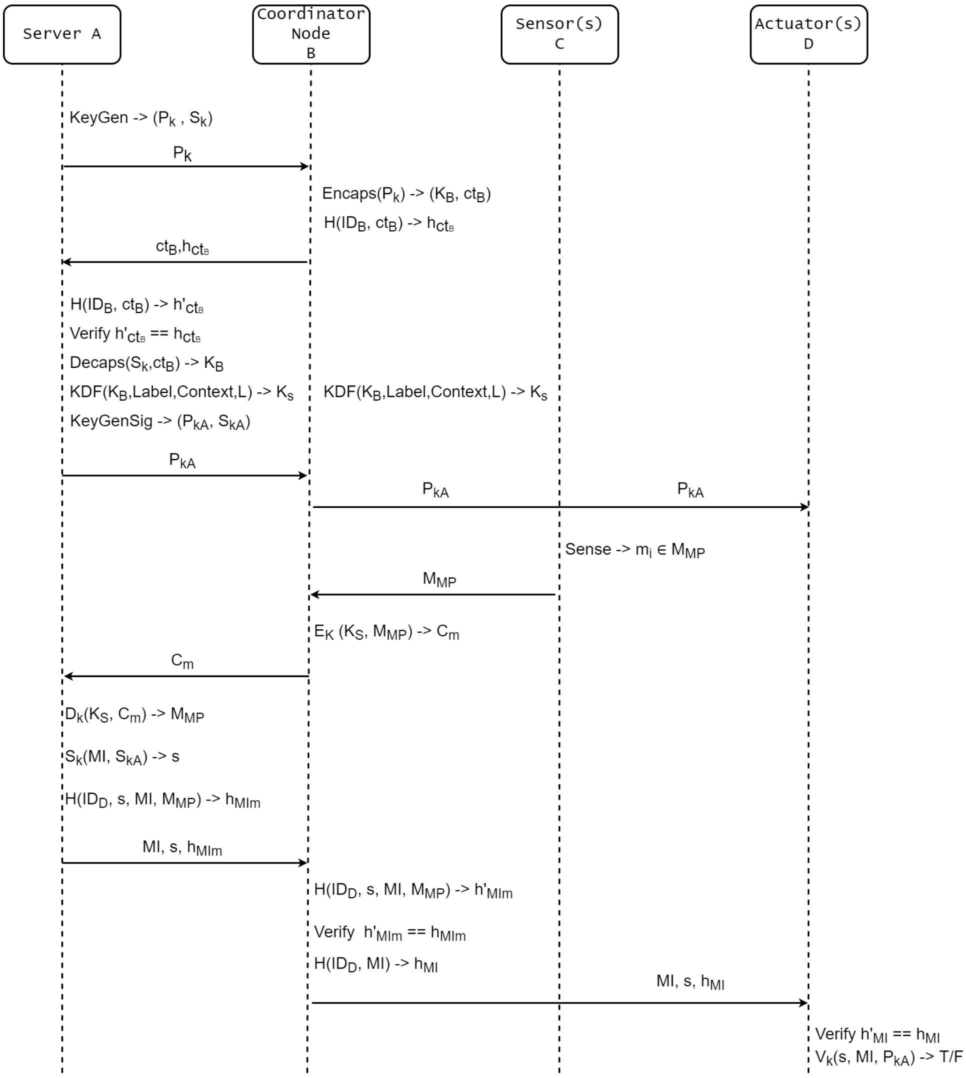

Server A
Coordinator Node B
Sensor(s) C
Actuator(s) D
KeyGen -> (P_k , S_k)
P_k
Encaps(P_k) -> (K_B, ct_B)
H(ID_B, ct_B) -> h_{ct_B}
ct_B,h_{ct_B}
H(ID_B, ct_B) -> h'_{ct_B}
Verify h'_{ct_B} == h_{ct_B}
Decaps(S_k,ct_B) -> K_B
KDF(K_B,Label,Context,L) -> K_s
KDF(K_B,Label,Context,L) -> K_s
KeyGenSig -> (P_{kA}, S_{kA})
P_{kA}
P_{kA}
P_{kA}
Sense -> $m_i \in M_{MP}$
M_{MP}
E_K (K_S, M_{MP}) -> C_m
C_m
D_k(K_S, C_m) -> M_{MP}
S_k(MI, S_{kA}) -> s
H(ID_D, s, MI, M_{MP}) -> h_{MIm}
MI, s, h_{MIm}
H(ID_D, s, MI, M_{MP}) -> h'_{MIm}
Verify h'_{MIm} == h_{MIm}
H(ID_D, MI) -> h_{MI}
MI, s, h_{MI}
Verify h'_{MI} == h_{MI}
V_k(s, MI, P_{kA}) -> T/F

Figure 2. Interaction between participant entities and functions of the protocol.

3.3.1. Phase 0—Authentication of Corporal Sensors

The security levels and protocol parameters are agreed upon in the initial phase. In the same way, the sensors and actuators must be registered with the coordinator node and later with the server. In this way, both the server and the coordinating node know the identities of all the sensors and actuators participating in the WBAN. From this moment, the communications of A with C and D must be through B. However, it is known that one of the most vulnerable aspects of WBANs is wireless communication since it can allow unwanted third-party entities to transmit information passing through authentic sensors. Therefore, it is necessary to provide a method to authenticate corporal sensors. The proposed method is based on the use of the acceleration vector and gyroscope correlation-based authentication proposed in [36]. This method uses a coordinator node (CN) and different sensor nodes; each has a 3D-axis accelerometer and a 3D-axis gyroscope. Sensors are placed on different parts of the patient's body to measure patient-specific physiological data and transmit them to the CN that is placed on the chest. The location of the sensors is shown in Figure 3. The authentication process begins with the sending and receiving of information, where the CN analyzes the received data. For this, the information provided by the accelerometers of both parties is used. To carry out authentication, this method calculates the correlation between the accelerometer data flow of the new sensor and the coordinator node. If the sensor and the coordinator node are in the same body, the magnitude of the accelerometer vector will be highly correlated. The method will approve the connection if the correlation value is high between them, otherwise, it will reject it. Figure 4 presents the flow diagram of the proposed authentication method.

Algorithm 1 presents the authentication process described in [36], where b is the new detected sensor. A_{CN}, A_b, G_{CN}, andG_b are the accelerometer and gyroscope readings of the CN and the sensor, respectively. C_{ACC}, C_{GYR}, are the results of the calculation of the correlation between the data of the CN and the sensor using the accelerometer and the gyroscope measurements, respectively. LD is the decision limit to accept the sensor or reject it. If the sensor is accepted, it can freely send data to the CN; if rejected, the sensor is deleted, and access to the network is denied.

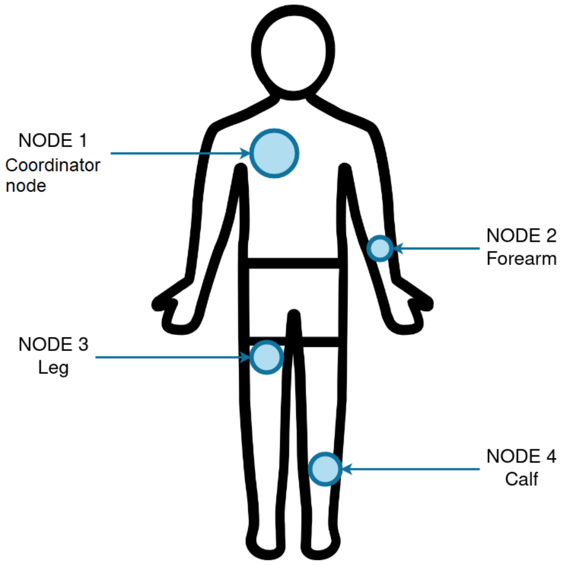


Figure 3. Sensors' location within a WBAN.

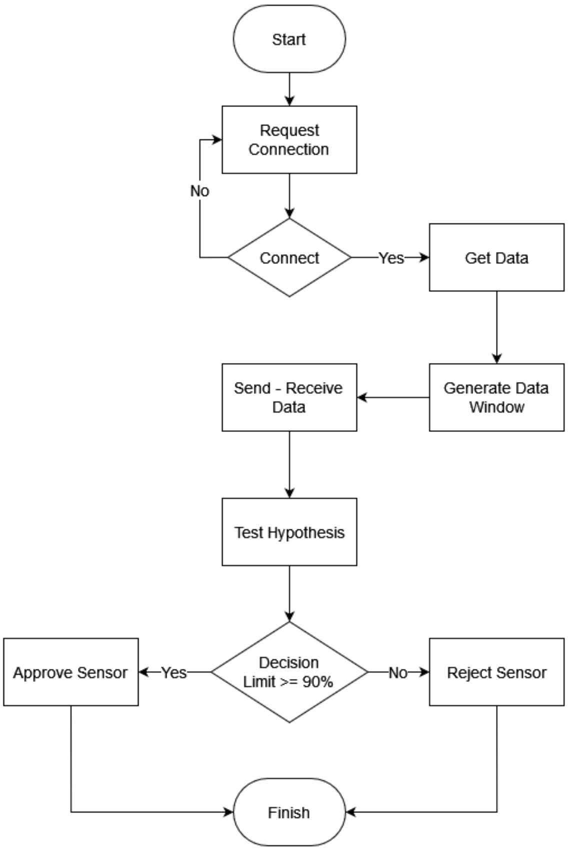


Figure 4. Data flow of authentication method.

Algorithm 1 Calculus of *first hop*.

```
while True do
    if b := newSensorDet() then
        mark new sensor as unauthenticated
        $A_{CN}$:= readData(t)
        $A_b$:= readData(t)
        $G_{CN}$:= readData(t)
        $G_b$:= readData(t)
        $C_{ACC}$:= computeCorrelation(UC,b)
        $C_{GYR}$:= computeCorrelation(UC,b)
        if computeConditionalAverage($C_{ACC}, C_{GYR}) \geq LD$ then
            markSensorAsAuthenticated(b)
            sendDataCN(b)
        else
            deleteSensor(b)
```

Nodes and actuators register with the coordinator node and then with the server so that the server knows all WBAN participants. From this point on, C and D communicate with A via B. All entities have an ID_x identifier stored during this phase by the server. Figure 5 shows the diagram referring to phase 1 of the protocol.

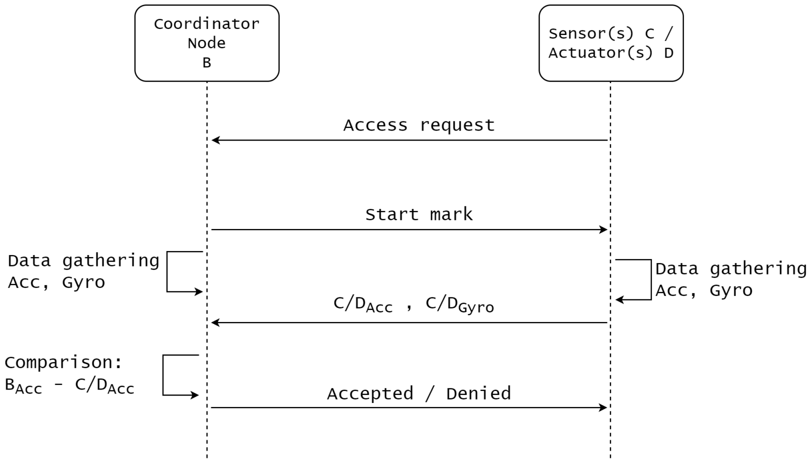


Figure 5. Phase 0: Interaction diagram with keyless authentication using accelerometer and gyroscope data.

3.3.2. Phase 1—Key Generation

The input variables used may change depending on the scheme used. Generally, the keys require primes p and q and a generator g. These values are agreed upon in phase 0.

The first key to be generated is the symmetric key. It is based on asymmetric cryptography, where the KEM will act as the key agreement protocol. It is performed between A and B using the KeyGen algorithm executed by the server to generate a key pair (P_k, S_k). P_k is sent to B as input to $Encaps(P_k)$, which returns the values K_B and ct_B. ct_B is the input to the hash function along with the identifier of B: ID_B, such that $H(ID_B, ct_B) \rightarrow h_{ct_B}$. The output h_{ct_B} of this function and the value ct_B are sent back to entity A. In this way, A can verify that the received value is integer; subsequently, the $Decaps(S_k, ct_B)$ algorithm is executed to obtain K_B. Once both entities know K_B, using a Key Derivation Function (KDF), the symmetric key is derived by applying the function $KDF(K_B, Label, Context, L)$, where $Label$ contains the purpose of using KDF, $Context$ is a binary string with K_B information, and L is the length of the output key. All the above values must be equal in both entities to have the symmetric key K_s. After this, the server must generate a new key pair (P_{kA}, S_{kA}) using $KeyGen$ from the digital signature scheme to obtain the key that will sign subsequent phases. When the public key (P_{kA}) is obtained, it is sent to B, and D. Figure 6 shows the diagram referring to phase 1 of the protocol.

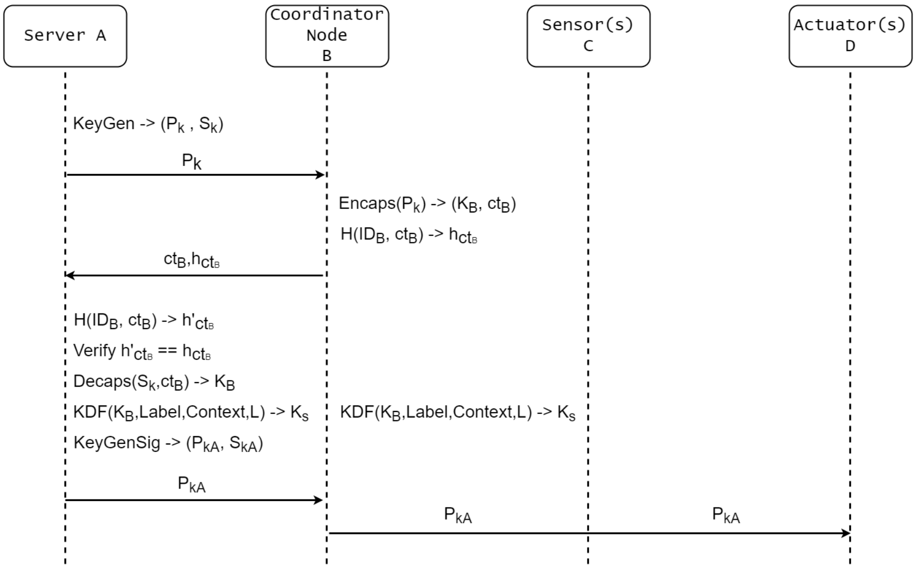


Figure 6. Phase 1: Symmetric key generation between A and B. Asymmetric keys generation from A for subsequent distribution to B and D.

3.3.3. Phase 2—Sensing, Encryption, and Sending of Information

After the devices in the WBAN initiate communication and register, the C-sensors can start their function. The information is calculated per unit time, m_i, to form the final message, M_{MP} , a data set such that $M_{MP} = m_0, m_1, m_2, m_3, \ldots, m_n$. When complete, it is sent to B. K_s is used to encrypt the information in M_{MP} using the encryption algorithm E_k that obtains the encrypted message C_m that is sent from B to A. Figure 7 shows the diagram of phase 2, which shows the information path and the functions used in this phase.

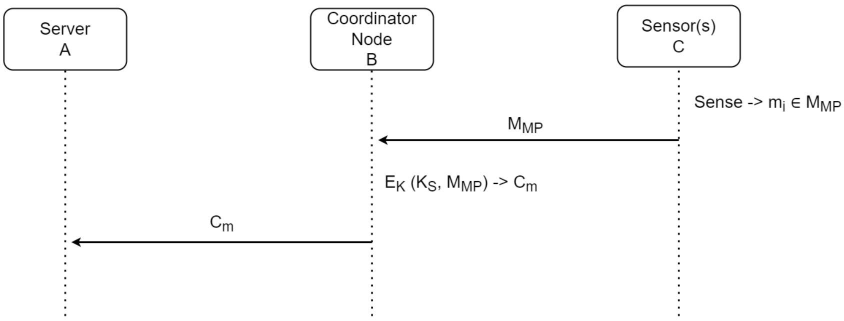


Figure 7. Phase 2: Transmission of sensed data in plaintext from entity C to entity B. Transmission of encrypted sensed data from entity B to entity A.

3.3.4. Phase 3—Verification of the Signature and Application of the Instructions

Figure 8 shows phase 3 of the protocol, where the functions performed by each entity and the messages sent are shown. This phase has as inputs K_s, S_{KA}, C_m, and an instruction message MI which is formed at the discretion of the physician's interpretation. The decryption function $D_k(K_s, C_m) \rightarrow M_{MP}$ allows A to know the original message generated by C. Upon learning M_{MP}, A proceeds to generate and sign MI using a function S_k of the digital signature scheme. The function $S_k(MI, S_{kA}) \rightarrow s$ delivers a value s which is the digital signature. The actuator identifier ID_D, the message MI, the message M_{MP}, and the signature s enter the hash function, such that $H(ID_D, s, MI, M_{MP}) \rightarrow h_{MIm}$. The resulting value is sent together with the value MI and the signature s to entity B. Finally, when these values reach B, it must verify these received values utilizing the hash function. If they are complete, they must be sent to the corresponding entity D, considering the ID_D to identify the target actuator. When entity D receives the signature and instructions, phase 3 ends, and phase 4 begins.

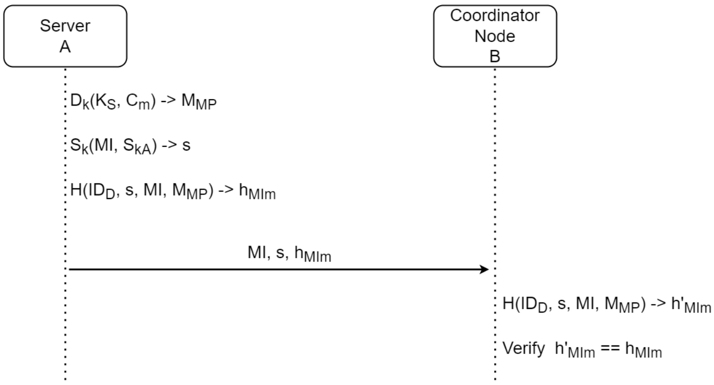


Figure 8. Phase 3: Decryption of the information received from the sensors, signature generation of entity A from the MI data, hash value generation of the previous signature, the decrypted data, and the identifier of B.

3.3.5. Phase 4—Verification of the Signature and Application of the Instructions

The last phase of the protocol begins when entity B uses a hash function with the values of the identifier of entity D(ID_D) and the message MI, such that $H(ID_D, MI) \rightarrow h_{MI}$. The output of this function is sent together with the signature and the message MI to entity D. Subsequently, entity D must verify the hash value it receives with the one it calculates, to verify the integrity of the information. Once this has been checked, s, P_{kA}, and MI are taken as inputs to give as output a Boolean value determined by the verification function $V_k(s, MI, P_{kA}) \rightarrow T/F$ that defines if the signature is authentic and therefore safe to be applied by the actuators on the patient's body. Figure 9 shows the phase diagram, where all the functions performed by each of the entities can be seen.

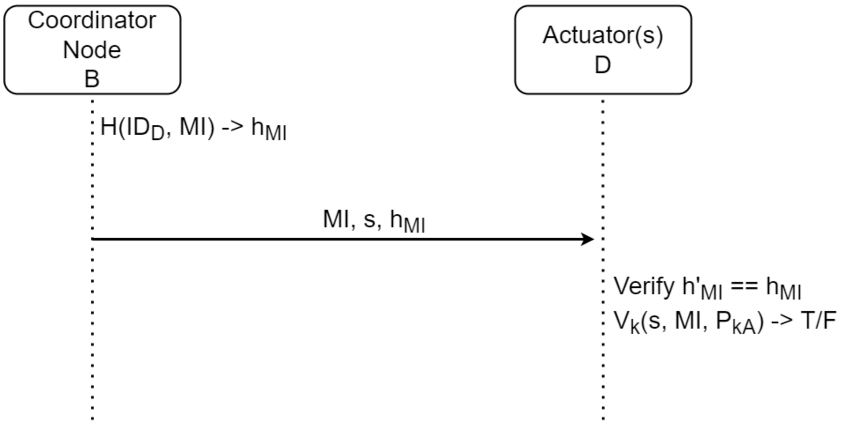


Figure 9. Phase 4: Transmission of MI data from entity B to D for signature verification issued by entity A.

4. Test and Results

Protocols are instructions that follow a strict sequence to generate good communication between entities. In a cryptographic protocol, the information travels protected using some cryptographic primitive. In this context, protocols are intended to provide confidentiality, entity authentication, information integrity, and non-repudiation. Protocols can be prone to security or semantic failures. Hence, different tools help in the formal verification of protocols. These tools verify the cryptographic properties of protocols, including their semantics and security, under certain scenarios raised in the tools. The methodology used by verification tools is specified in [37]. This methodology uses security services, the protocols designed together with the properties to be tested, and the model of the attackers. In this way, verification tools can obtain proof of the security of a protocol or the description of the attacks that can be performed on it. Therefore, it is possible to know if the protocol is well constructed or not. Figure 10 shows this methodology graphically. Some tools, in the results, provide information about the attacks that can be performed on the protocol to correct security breaches.

The tools for protocol verification vary depending on how the verification can be performed. Among the tools considered in this work, some are automatic since they can analyze the security of the protocols and the semantics of the security properties that are verified. In addition, they provide results that can be used to improve the protocol itself, if necessary.

As shown in Figure 10, automatic verification tools take as input the cryptographic protocol and the security properties it must comply with. Subsequently, the tool analyzes the security by taking these inputs and performing attacks. If the protocol is found insecure, the tool reviews the type of attacks performed. Otherwise, the protocol is found to be secure. A representation of this process can be seen in Figure 11. The tool used for this purpose is Scyther [19,20].

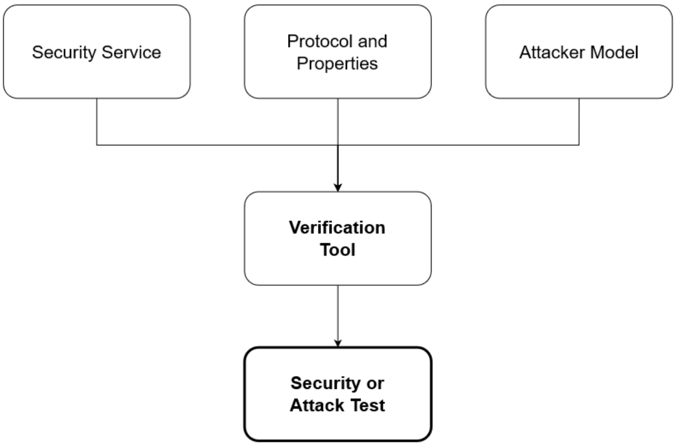


Figure 10. Protocol verification methodology.

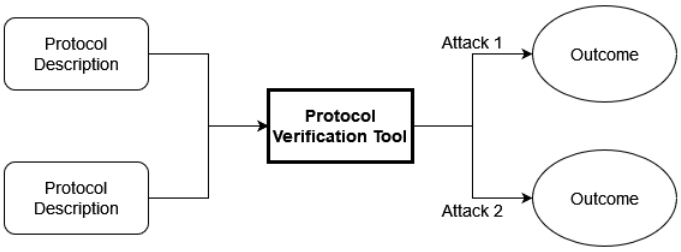


Figure 11. Cryptographic protocol verification block diagram.

4.1. Scyther

Scyther performs the verification with an unlimited number of protocol executions. It was developed by Cas Cremers in 2006 [19,20]. The scenario in which the protocol is analyzed is not required to be specified. Scyther provides a graphical interface in which the protocol description and security parameters must be entered. As an output, it delivers a report of the resulting analysis and a graph for each attack. It can review all possible scenarios. In case one or more attacks are found during the verification, the tool creates and displays a tree, as shown in Figure 11, where possible attacks can be observed. It is capable of verifying man-in-the-middle attacks and characterization. In the same way, it can perform a protocol characterization analysis.

Scyther uses the Security Protocol Description Language (SPDL). The language allows the verification of claims, manually and automatically, which allows the tool to be requested to validate certain aspects of the protocol (e.g., the secrecy of a value). This provides confidentiality or certain properties necessary for authentication. Finally, the protocol can be analyzed from the point of view of each role, so the tool takes a finite number of possibilities in the execution of the protocol.

4.2. AVISPA

Automated Validation of Internet Security Protocols and Applications (AVISPA) [16], is a cryptographic protocol verification tool. It was developed in the artificial intelligence laboratory at the University of Genoa, Italy, in conjunction with other institutions. The architecture used by the tool can be seen in Figure 12, which indicates that the protocol must enter the High-Level Protocol Specification Language (HLPSL), then the analysis model must be chosen for the tool to check the protocol; finally, the output returns the result of testing the protocol on the model. Each of these models is specified below.

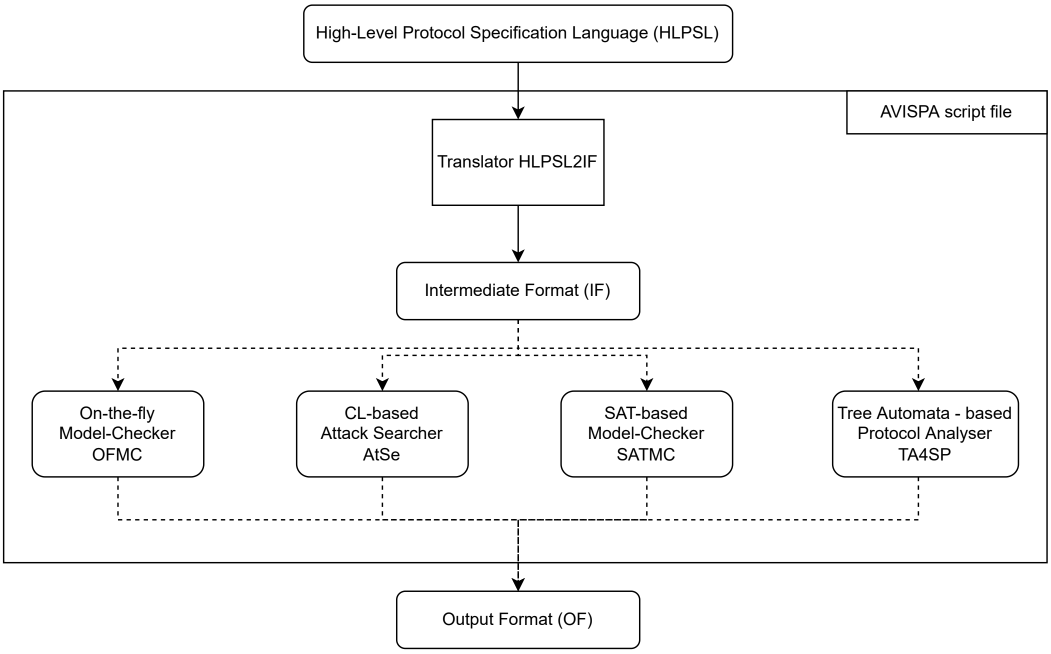

High-Level Protocol Specification Language (HLPSL)
AVISPA script file
Translator HLPSL2IF
Intermediate Format (IF)
On-the-fly Model-Checker OFMC
CL-based Attack Searcher AtSe
SAT-based Model-Checker SATMC
Tree Automata - based Protocol Analyser TA4SP
Output Format (OF)

Figure 12. AVISPA tool architecture.

All the protocols verified in the AVISPA tool must be specified in the HLPSL language. This language is based on roles: the basic roles of representation of each entity and the role in which they are specified to represent the scenario. Each of the roles is independent of the others and has initial information or parameters of the entities, and the communication one has with others. A complete specification of the language is presented in [16].

4.3. Test

The security tests were performed using the automatic protocol verification tools described above. Both Scyther and AVISPA tools verified the security of the protocol. Both tools were downloaded from their official web pages. Both tools are used in a Linux environment. In the case of Scyther, a Linux distribution must be installed; therefore, Ubuntu 21 was used as the operating system, and, as it was also required, Python 2.7 was installed. For its part, AVISPA also uses an Ubuntu environment; however, this environment only can be run on a virtual machine. In order to use the tools, it is necessary to encode the protocol. Each tool has its own language, Scyther uses the SPDL language, and AVISPA uses the HLPSL language. Once the protocol described in the previous section had been codified, the tests were carried out on each tool.

In Scyther, the tool checks for claims searched for in the protocol. In our case, we want the protocol to comply with the entity authentication properties provided by *Niagree* and *Nisync*. Hence, for the *secrecy* of some of the values used, for example, the key, we look for the secrecy property. The tool will then verify that the described protocol complies with these properties. For this, the tool is configured to search for all possible attacks.

The results of the tool helped determine if the protocol has security gaps and can be attacked. The results are displayed with the claim made followed by the verification result. If an *OK* is observed, then it would mean that the property has no attack; otherwise, Fail would mean that the property has failed, and the number of attacks that can be made on this property will be displayed in the comments. If this happens, a button is displayed showing the attack tree. If this is the case, the protocol must be adapted to cover such gaps.

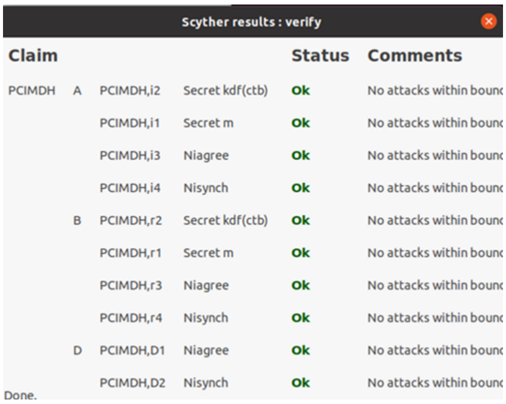
Unlike Scyther, AVISPA does not require the properties to be checked to be specified, but the mode in which the protocol is to be checked must be specified. Therefore, once the protocol is encoded, it is fed into the tool and checked in all modes it allows. The results of the tool show a summary indicating whether the protocol is $safe$ or $unsafe$. This result can be translated as to whether the protocol is secure or insecure. In the same way, it shows the execution times, and in case the protocol is not secure, the tool allows the user to see the attack carried out on the protocol step by step. Similarly, the user can see how the protocol behaves between entities.

4.4. Security Results Obtained from Protocol Verification Tools

The results of the security tests carried out on the protocols using the protocol verification tools are presented in the same order in which they were reviewed in the previous sections. Hence, the results thrown by Scyther are presented first, followed by those thrown by AVISPA. Both tools were configured with the environment in which the protocol was tested. Each of them had different configurations. Scyther was configured with a minimum of five runs, which is the default for the tool. In the same way, the tool was chosen to search for all possible attacks on the protocol with a maximum number of ten patterns per claim. On its part, in AVISPA, the user only needs to choose the model on which the protocol will be tested. These models, as seen in Figure 12, are On-the-fly Model-checker (OFMC), CL-based Attack Searcher (AtSe), SAT-based Model-Checker (SATMC), and Tree Automata-based Protocol Analyzer (TA4SP), the specific description of them can be found in [16]. In this case, the protocol was run for each of these modes.

Some of the results obtained with Scyther are shown in Figure 13. The results are displayed in columns; the first column specifies the name given to the protocol. In such case, is an acronym for "Cryptographic Protocol for Medical Information in Heterogeneous Devices"; the second column shows the entity; the third column shows the communication within the protocol, that is, the side of the communication between the entities being reviewed. The next column shows the claim that is being sought; in the case of secrecy, the data that is sought is also shown, whether it is secret; in our case, it will be the symmetric key that is being obtained with a *KDF* function and the value ct_b and the message. The last two columns show the result of the claim and the comments on the claims. The results produced by the tool show only *Ok*, indicating that the property that was demonstrated has been verified. In the comments, the legend *No attacks within bounds* is shown, meaning that there are no attacks within the limits specified in the tool.

These results show that the protocol covers the security services of authentication, confidentiality, and integrity. This is achieved using encrypted primitives, digital signature, KEM, and hash functions.



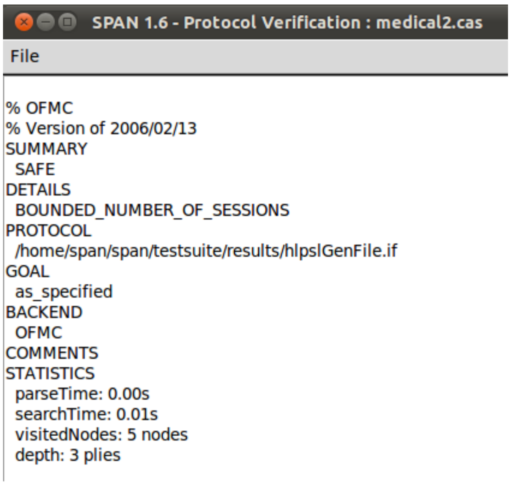
Claim				Status	Comments
PCIMDH	A	PCIMDH,i2	Secret kdf(ctb)	Ok	No attacks within bounc
		PCIMDH,i1	Secret m	Ok	No attacks within bounc
		PCIMDH,i3	Niagree	Ok	No attacks within bounc
		PCIMDH,i4	Nisynch	Ok	No attacks within bounc
	B	PCIMDH,r2	Secret kdf(ctb)	Ok	No attacks within bounc
		PCIMDH,r1	Secret m	Ok	No attacks within bounc
		PCIMDH,r3	Niagree	Ok	No attacks within bounc
		PCIMDH,r4	Nisynch	Ok	No attacks within bounc
	D	PCIMDH,D1	Niagree	Ok	No attacks within bounc
		PCIMDH,D2	Nisynch	Ok	No attacks within bounc

Done.

Figure 13. Results obtained by SCYTHER for the verified protocol.

Figure 14 shows the results of the AVISPA tool. Summarizing, these results indicate that the protocol is "SAFE". Details specify that it is safe in a limited number of sessions. In the same way, it is shown the number of nodes that were visited during the evaluation with the tool. In this case, there are five nodes, and the search time taken by the tool was 0.01s. As mentioned above, no claims are specified in this tool for the tool to be checked. However, the model in which the protocol is to be verified must be specified. The results indicate that the protocol is secure in the specified mode. Similarly, it is observed that the protocol meets the specified objectives.

In this case, only the results of the OFMC model are shown, but it should be noted that in the remaining models that the tool can verify, the protocol also has "SAFE" results.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.01s
  visitedNodes: 5 nodes
  depth: 3 plies
```

Figure 14. Obtained results by AVISPA to the verified protocol.

The protocol covers the security services of authentication, confidentiality, and integrity. The protocol uses encryption primitives, digital signature, KEM, and hash functions. Hence, the protocol designed in this work has proven to be completely secure and well-constructed regarding cryptographic primitives.

5. Conclusions

In this work, the design of a novel cryptographic protocol that guarantees the security services of confidentiality, authentication, and integrity to keep secure the information transmitted in a WBAN in medical applications has been presented. Security services in the proposed protocol were verified through automatic protocol verification tools. From the design point of view of the protocol, different primitives that help to achieve the security services mentioned before were considered. In addition, using a keyless authentication method provides the protocol with the advantage that generating additional cryptographic key pairs is not required. The results obtained through protocol verification tools show that the designed protocol is secure in the sense of three security services. In the same way, the results of the verification analysis confirm that the protocol design does not present flaws in its logic of sending messages. Results show that the construction of the protocol focuses on keeping the patient's sensitive data confidential and complete. Also, it was shown that the data communicated between the considered entities when they reached their destination were authentic and complete. Authentication between sensors is performed by ensuring they are placed on the same human body. Unlike the protocols presented in the related work, the developed protocol here is designed not to expose data during key generation, preventing attackers from obtaining information needed to perform spoofing attacks, resulting in security flaws found in previous protocols.

Author Contributions: Conceptualization, G.G.-G.; Formal analysis, K.A.D.-V.; Investigation, K.A.D.-V.; Writing—original draft, K.A.D.-V. and G.G.-G.; Writing—review & editing, P.J.E.-A.; Supervision, G.G.-G.; Funding acquisition, G.G.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by CONACyT grant number 321068, SIP-20221427 and SIP-20221495.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: If necessary please contact the authors.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. IEEE 802.15, Working Group for WPAN & Task Group 6. Available online: http://www.ieee802.org/15/pub/TG6.html (accessed on 20 June 2021).
2. Organización Panamericana de la Salud, La Cantidad de Personas Mayores de 60 años se Duplicará para 2050; se Requieren Importantes Cambios Sociales. 1 de Octubre de 2015. Available online: https://www.paho.org/par/index.php?option=com_content&view=article&id=1434:la-cantidad-de-personas-mayores-de-60-anos-se-duplicara-para-2050-se-requieren-importantes-cambios-365sociales&Itemid=255 (accessed on 7 May 2021).
3. Lee, W.B.; Lee, C.D. A cryptographic key management solution for HIPAA privacy/security regulations. *IEEE Trans. Inf. Technol. Biomed.* **2008**, *12*, 34–41. [PubMed]
4. Zeng, K.; Govindan, K.; Mohapatra, P. Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. *IEEE Wirel. Commun.* **2010**, *17*, 56–62. [CrossRef]
5. Cai, L.; Zeng, K.; Chen, H.; Mohapatra, P. Good Neighbor: Ad hoc Pairing of Nearby Wireless Devices by Multiple Antennas. In Proceedings of the 18th Annual Network and Distributed System Security Symposium, San Diego, CA, 6–9 February 2011; pp. 1–15.
6. Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*, 1st ed.; CRC Press: Boca Raton, FL, USA, 1997.
7. Ferguson, N.; Schneier, B. *Practical Cryptography*; Wiley Publishing, Inc.: Indianapolis, IN, USA, 2003.
8. Instituto Nacional de Ciberseguridad de España M.P. SA. Available online: https://www.incibe-cert.es/blog/introduccion-los-sistemas-embebidos (accessed on 10 July 2021).
9. Varshavsky, A.; Scannell, A.; LaMarca, A.; de Lara, E. Amigo: Proximity-based authentication of mobile devices. In Proceedings of the International Conference on Ubiquitous Computing, Hong Kong, China, 11–13 July 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 253–270.
10. Sun, H.M. An efficient remote use authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2000**, *46*, 958–961.
11. Hwang, M.S.; Li, L.H. A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.* **2000**, *46*, 28–30. [CrossRef]
12. Hayajneh, T.; Vasilakos, A.V.; Almashaqbeh, G.; Mohd, B.J.; Imran, M.A.; Shakir, M.Z.; Qaraqe, K.A. Public-key authentication for cloud-based WBANs. In Proceedings of the 9th International Conference on Body Area Networks, London, UK, 29 September–1 October 2014; pp. 286–292.
13. Rabin, M.O. Digitalized Signatures and Public-Key Functions as Intractable as Factorization. Technical Report MIT/LCS/TR-212, Laboratory for Computer Science, MIT, 1979. Available online: https://apps.dtic.mil/sti/pdfs/ADA078415.pdf (accessed on 25 June 2021).
14. Chaudhry, S.A.; Mahmood, K.; Naqvi, H.; Khan, M.K. An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *J. Med. Syst.* **2015**, *39*, 1–12. [CrossRef] [PubMed]
15. Lu, Y.; Li, L.; Peng, H.; Yang, Y. An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *J. Med. Syst.* **2015**,*39*, 1–8. [CrossRef] [PubMed]
16. Abdmeziem, M.R.; Tandjaoui, D. An end-to-end secure key management protocol for e-health applications. *Comput. Electr. Eng.* **2015**,*44*, 184–197. [CrossRef]
17. Avispa a Tool for Automated Validation of Internet Security Protocols. Available online: http://www.avispaproject.org (accessed on 20 December 2021).
18. Amin, R.; Islam, S.H.; Gope, P.; Choo, K.K.R.; Tapas, N. Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. *IEEE J. Biomed. Health Inform.* **2018**,*23*, 1749–1759. [CrossRef] [PubMed]
19. Das, A.K.; Odelu, V.; Goswami, A. A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS. *J. Med. Syst.* **2015**, *39*, 1–24. [CrossRef] [PubMed]
20. Cremers, C.J. The Scyther Tool: Verification, falsification, and analysis of security protocols. In Proceedings of the International Conference on Computer aided Verification, Princeton, NJ, USA, 7–14 July 2008; pp. 414–418.
21. Cremers, C.J. *Scyther: Semantics and Verification of Security Protocols*; Eindhoven University of Technology: Eindhoven, The Netherlands, 2006.
22. Siddiqi, M.A.; Doerr, C.; Strydis, C. Imdfence: Architecting a secure protocol for implantable medical devices. *IEEE Access* **2020**, *8*, 147948–147964. [CrossRef]
23. Jegadeesan, S.; Azees, M.; Babu, N.R.; Subramaniam, U.; Almakhles, J.D. EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). *IEEE Access* **2020**, *8*, 48576–48586. [CrossRef]
24. Rehman, Z.U.; Altaf, S.; Iqbal, S. An efficient lightweight key agreement and authentication scheme for WBAN. *IEEE Access* **2020**, *8*, 175385–175397. [CrossRef]
25. Kompara, M.; Islam, S.H.; Hölbl, M. A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. *Comput. Netw.* **2019**, *148*, 196–213. [CrossRef]
26. Sowjanya, K.; Dasgupta, M.; Ray, S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *Int. J. Inf. Secur.* **2020**, *19*, 129–146. [CrossRef]
27. Li, X.; Peng, J.; Kumari, S.; Wu, F.; Karuppiah, M.; Choo, K.K.R. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. *Comput. Electr. Eng.* **2017**, *61*, 238–249. [CrossRef]

28. Szczechowiak, P.; Oliveira, L.B.; Scott, M.; Collier, M.; Dahab, R. NanoECC: Testing the limits of elliptic curve cryptography in sensor networks. In Proceedings of the European Conference on Wireless Sensor Networks, Bologna, Italy, 30 January–1 February 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 305–320.
29. Karlof, C., Sastry, N., Wagner, D. TinySec: a link layer security architecture for wireless sensor networks. In Proceedings of the 2nd international Conference on Embedded Networked Sensor Systems, Baltimore, India, 3–4 November 2004; pp. 162–175.
30. Venkatasubramanian, K.; Gupta, S. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sens. Netw. (TOSN)* **2010**, *6*, 1–36. [CrossRef]
31. Xu, F.; Qin, Z.; Tan, C.; Wang, B.; Li, Q. IMDGuard: securing implantable medical devices with the external wearable guardian. In Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, China, 2011; pp. 1862–1870.
32. Shi, L.; Yuan, J.; Yu, S.; Li, M. ASK-BAN: Authenticated secret key extraction utilizing channel characteristics for body area networks. In Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, Budapest, Hungary, 17–19 April 2013; pp. 155–166.
33. Khan, J.Y.; Yuce, M.R. Wireless body area network (WBAN) for medical applications. In *New Developments in Biomedical Engineering;* InTechOpen: London, UK, 2010, pp. 1–39.
34. Alam, M.M.; Hamida, E.B.; Rehmani, M.H.; Pathan, A.S.K. Wearable wireless sensor networks: Applications, standards, and research trends. In *Emerging Communication Technologies Based on Wireless Sensor Networks: Current Research and Future Applications*; CRC Press: Boca Raton, FL, USA, 2016; pp. 59–88
35. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access* **2018**, *6*, 36611–36631. [CrossRef]
36. Elyazidi, S.; Escamilla-Ambrosio, P.J.; Gallegos-Garcia, G.; Rodríguez-Mota, A. Accelerometer based body area network sensor authentication. In *Smart Technology*; Springer: Cham, Switzerland, 2018; pp. 151–164.
37. Formal Methods in Security Protocols Analysis. Available online: http://webpages.uncc.edu/wwang22/Research/projects/CCLI-I/AutoProtoVeri.pdf (accessed on 5 January 2022).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.