Secure and reliable patient body motion based authentication approach for medical body area networks

Nawel Yessad, Siham Bouchelaghem, Farah-Sarah Ouada, Mawloud Omar

Secure and reliable patient body motion based authentication approach for medical body area networks

Nawel Yessad, Siham Bouchelaghem, Farah-Sarah Ouada, and Mawloud Omar

Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.

Abstract

Medical Body Area Network (MBAN) has emerged as a promising solution for monitoring patient activities and actions, and supports a lot of healthcare applications. A MBAN includes a set of sensor nodes deployed such, they can be located on, in, or around the patient body. They are used to monitor physiological signs, which are transmitted then to medical servers without hampering the patient activities. Security is one of the main challenging issues in MBANs since the data nature is highly sensitive. In order to ensure the reliable gathering of patient critical information, it is vital to provide authentication to prevent an attacker from impersonating legitimate sensor nodes. In this paper, we propose a patient body motion based authentication solution. The routine activities, as walking or running, are characterized through a generic model allowing to identify the patient sensor nodes. Through the security analysis, we show its robustness against the well known attacks. In addition, we develop an analytical model to measure the impact of physical and logical attacks on the proposed solution with comparison to the existing protocols. We also evaluate the proposed solution through simulations with respect of important criteria, namely the transmission overhead, response time and energy consumption. The proposed solution demonstrates the best results in performance with comparison to the existing protocols. Furthermore, we have developed a prototype of the proposed solution, where it demonstrates promising results in terms of true acceptation and false rejection.

Keywords: Security, Authentication, Body-motion, Healthcare, MBAN.

1. Introduction

Medical Body Area Networks (MBANs) are a major asset in the design of health monitoring applications. They are considered as a promising technology for collecting and gathering physiological signals to monitor the patient health. In MBANs, special nodes are designed as lightweights, miniaturized sensors that could be placed on, in, or around the patient body as tiny intelligent devices. They monitor the patient body and collect different physiological parameters like heart rate, glucose level, blood oxygen level, etc. The collected health information is then transmitted to a local processing unit referred as a sink, which relays them to the hospital or any healthcare system for diagnostic and permanent record. The collected medical data from the sensors must be accessible anytime and anywhere. For instance, the Internet of things (IoT)

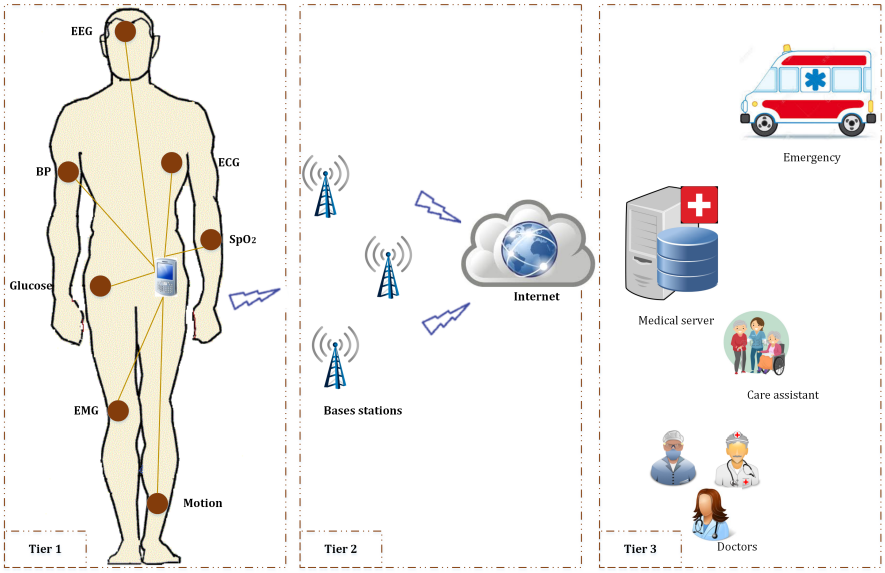

Figure 1: MBAN general architecture.

[7, 8, 9] is a well adapted infrastructure for such applications. The MBANs address several challenges in the health sector, such as the medical staff availability, the medical resource limitation, the real time monitoring restriction and the growing health cost. The MBANs have a huge potential to revolutionize the health sector and to provide a comfortable life mode, where the patients are efficiently remote monitored during their daily activities. With MBANs, the emergency aspect is improved, where the pathologies can be detected early, and the health staff has the opportunity to monitor continuously the health status of many patients simultaneously.

MBANs need to stay connected to other networks by using other technologies in order to ensure that the patients data can reach the center of treatment, while the subject is in a different place and the sensed data from the WBAN may ultimately be sent to a centralized healthcare repository for permanent records. Figure 3 illustrates the MBAN general architecture. A typical MBAN architecture includes the first tier (i) "Intra-MBAN" which refers a small network around the patient body (about 1-2 meters) equipped a gateway (sink) bridging to another network types that can be another node with some routing and data aggregate features, the second tiers (ii) "Inter-MBANs" represent a wide network that can be an Internet network, where the sink forwards the collected data to the base station after processing and aggregation and the third tier (iii) "Extra-MBAN" consists on several applications with server medical or other healthcare personnel. Moreover, MBAN applications span a wide area in the healthcare applications like Patients monitoring indoor Hospital environment, Continuous and Remote healthcare, Real-time home care service with emergency supporting, Body posture analysis in patient-aid rehabilitation, Preventing and managing chronic diseases and Remote assistance and long term monitoring for patient under disabilities, etc. For more details about the research effort in wireless communication standards for healthcare environments, kindly refer to [19, 12, 11].

The MBAN applications have emerged as a successful paradigm. Unfortunately,

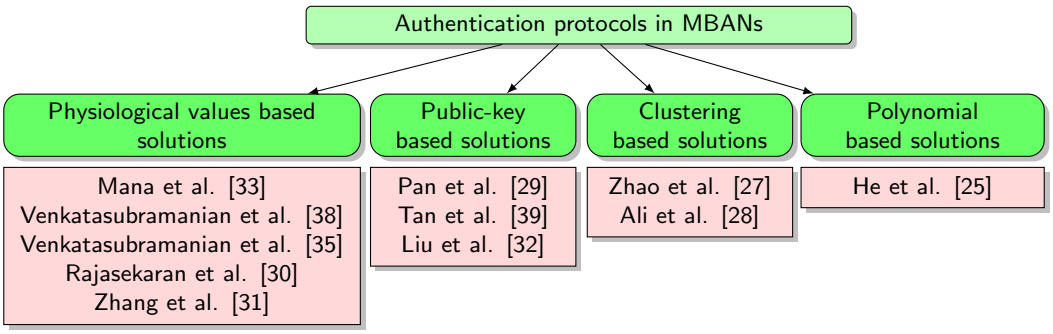

Figure 2: Classification of existing solutions

they are subject of novel attack risks [13, 15]. Securing MBAN is a serious challenge, which should be rigorously addressed in the healthcare applications, where the managed data is highly sensitive and associated directly to the patient health. Authentication is one of the important security services. In fact, there are several devices in charge to collect physiological parameters about a particular patient and transmit them to a remote server. In order to ensure a reliable gathering of the patient data, it is primordial to authenticate first the legitimacy of the data source devices. Several authentication solutions have been proposed in the literature. Most of the existing solutions are based on cryptographic mechanisms that consume an important part of sensor resources which are more limited in the framework of MBANs. For more information about the research effort of the energy-aware security schemes in such networks, kindly refer to [16].

The rest of the paper is organized as follows. In Section 2, we review some relevant authentication solutions in the framework of MBANs. In Section 3, we present the detailed description of the proposed solution. In Section 4, we analyze the security of the proposed solution. In Section 5 and 6, we evaluate its efficiency through modeling, simulations and practical experiments. Finally, we conclude the paper in Section 7.

2. Related work

In the literature, various solutions have been proposed to meet the security requirements in MBANs. In this section, we review some relevant solutions which we classify them as illustrated in Figure 2.

Venkatasubramanian et al. [38] have proposed a key agreement solution which allows two sensor nodes in a MBAN to agree upon a common key generated using electrocardiogram (ECG). Rajasekaran et al. [30] have proposed to use the physiological values to generate a symmetric shared cryptographic key between two neighboring nodes in a MBAN, and then converts it into frequency domains and generates features. The generated features are transformed into a cubic spline curve and the coefficients are concatenated to form the key. The latter key is then transmitted to the receiver by a fuzzy vault cryptographic method, where the receiver unlocks the vault (using cubic spline interpolation) and finds the key. Venkatasubramanian et al. [35] have proposed a PVS (Physiological Values based Security) for securing inter-sensor communication in MBANs. The PVS solution distributes the key used for securing a particular message along with the message itself hiding it using the physiological values. Zhang et al.

[31] have proposed to use the ECG signal, and the Improved Jules Sudan (IJS) algorithm (an improved fuzzy vault algorithm proposed in [40]) to secure the inter-sensor communication and to setup the key agreement for the message authentication. In the ECG-IJS solution, the sensor nodes need to store the polynomial coefficients and a subset of polynomial coefficients is required to be sent to the receiver. The use of physiological values has demonstrated the potential to eliminate the need for explicit key distribution, allowing the sensor nodes to agree upon a key, as needed, and ensuring their mutual authentication in a plug-and-play manner. However, it requires that each sensor node can measure the same physiological value type. This assumption is rather restrictive and makes this approach not suitable for many MBAN applications. Zhao et al. [27] have proposed to use a hybrid multi-hop network structure, organized in clusters, for two MBAN based applications: "the health monitoring" and "the drug delivery". Based on this, the authors have proposed a key management protocol to secure inter-sensor communication. This solution requires a high number of keys to be stored. Ali et al. [28] have proposed a cluster based secure key agreement protocol for MBANs. The authors have considered the MBAN as a single cluster and the personal server is considered as the cluster-head. To achieve the key agreement, HMAC-MD5 is applied to electrocardiography blocks. Pan et al. [29] have proposed a hybrid key management based on Elliptic Curve Cryptography (ECC) to protect sensitive data in stringent resource-constrained MBAN devices. This mechanism uses a modified Feistel algorithm to encrypt and decrypt sensitive physiological value, and then uses ECC to manage the key distribution, update and revocation. He et al. [25] have proposed a polynomial based authentication protocol to develop a secure network admission and transmission subsystem in MBANs to provide sensor node authentication and the establishment of pairwise shared keys. Although the proposed solution resists to many attacks, it requires a considerable storage space for the polynomials used for the key generation, the one-hop neighbor tables and the shared keys. Mana et al. [33] have proposed a scheme to secure the communication links between the sensor nodes using biometric data. Their approach generates symmetric cryptographic keys from the ECG and distributes them between the sensor nodes over the MBAN to secure end-to-end transmission. Tan et al. [39] have proposed a lightweight Identity-Based Encryption method named IBE-Lite. This solution is an enhancement of the conventional identity based encryption, which shares with it two properties, namely the ability to use an arbitrary string to generate a public key and the ability to generate a public key separately from the corresponding secret key. Liu et al. [32] have proposed a certificate-less authentication scheme allowing remote MBAN users to access securely various medical application services. In Table 1, we summarize per authentication session, the cost of each solution regarding the storage, computation and the communication. For more information about the protocol details of a particular solution, kindly refer to its corresponding reference presented in the first column of the table.

The proposed solution aims to ensure the authentication in the framework of MBANs, unlike the solutions proposed in [38, 28]. The proposed solution is a distributed protocol without cryptographic operations. The authentication is related to the patient body motion, in which we project the sensor authentication process to a movement model, unlike the solutions based on cryptographic mechanisms or physiological values [33, 35, 30, 31, 29, 39, 32, 27, 25]. Moreover, we have incorporated a new technique

of data communication based on the mobility estimation by taking in charge the energy aspect, which ensures a stable routing paths between the patients and the medical remote server. We have developed a generic analytical model for the authentication process with which we have evaluated the impact of attacks on all the reviewed solutions. We have implemented intensive simulations by comparing all the reviewed solutions, in which the proposed solution demonstrates the best results in terms of transmission overhead, response time and energy consumption. Finally, we have implemented a prototype of the proposed solution, which we have tested and validated through practical scenarios.

3. The proposed solution

The advancement of the medical body area networks can be related to the development of two aspects namely: the wearable medical devices and wireless communication networks. Wearable devices are developed with the aim to monitor and to record real-time individuals medical data unobtrusively and ubiquitously around the clock without disrupting their normal daily lives, when previously only intermittent data could be collected during their irregular visits to clinics or hospitals. Wearable sensor-based medical systems may comprise different types of flexible sensors that can be integrated into textile fiber, clothes, and elastic bands or directly attached to the human body. The wearable sensors are capable of measuring physiological signs such as electrocardiogram (ECG), electromyogram (EMG), heart rate (HR), body temperature, electrodermal activity (EDA), arterial oxygen saturation (SpO2), blood pressure (BP) and respiration rate (RR). On the other hand, advances in wireless communications technology have overcome most of the geographical, temporal, and even organizational barriers to facilitate a completely roaming way of transferring medical data and records [3, 4, 5, 6, 10].

In the scope of this work, we consider a MBAN, where a set of η wearable sensor nodes are deployed on a patient body to monitor physiological value. The sensor nodes have the capability of measuring continuously the physiological values and to sense multiple types of stimuli. They are deployed in such a way do not hamper the daily routine of the patient. The sensor nodes transmit the sensed data to one stationary sink device placed in the chest of the patient body. The sink device is responsible for collecting and forwarding the patient data to a remote medical server. We illustrate in Figure 3, the model of deployment adopted in this paper. We assume that the sink device has more computation, energy supply, and storage capabilities than a regular sensor node. We assume that the physical capture attack of sensor nodes is not possible because the latter are under the patient control. However, an external attacker may try to disrupt the inter-sensor communication by jamming the channels or may try to impersonate legitimate sensor nodes or claim multiple identities. In this case, how the sink device authenticates the legitimate sensor nodes and how it identifies if the received data is transmitted by a deployed sensor node from the patient body. This challenge has been formalized in [36] as "the one-body authentication problem". The proposed solution addresses directly this issue and operates in two separated phases: (1) the learning phase and (2) the authentication phase. The first phase consists of modeling the patient postures through the different distances separating the sensor nodes to the

Protocol	Storage	Computation	Transmission
[38]	01× Node identity 20× Block of 64 bits 04× Key of 128 bits 20 × 20 Matrix 20× Hashed block using SHA-256	01× Feature extraction 20× Hash operation 02× Key generation 04× MAC operation 02× XOR operation 01× Hamming distance of 2 matrix 01× Data sensing	04× Round
[30]	01× Node identity 01× Key for each knot 01× Vault (knots and chaff points)	01× Feature extraction 01× Cubic spline interpolation 01× Vault, CRC computation 02× MAC operation 01× Data sensing	03× Round
[35]	01× Node identity 01× Physiological value of 128 bits 01× Key for encryption and decryption	01× MAC operation 01× XOR operation 01× CRC operation 01× Encryption 01× Decryption 01× Data sensing	02× Round
[31]	01× Node identity 01× ECG Feature 01× Key for each polynomial coefficient	01× Feature extraction 01× Encryption 01× Decryption 02× MAC operation 01× Data sensing	02× Round
[25]	01× Node identity 01× Polynomial of degree t 01× Key shared with PWH 01× Table of the neighbor keys 01× Hashed value of the key	01× Encryption 02× Hash operation 01× XOR operation 01× Data sensing	04× Round
[27]	04× key of 128 bits	06× Hash operation 03× Encryption 03× Decryption 01× Data sensing	06× Round
[28]	01× Node identity 20× Block of 64 bits 01× Pairwise key of 128 bits 01× Key of 128 bits	01× Feature extraction 02× Key generation 06× HMAC operations 01× Encryption 01× Data sensing	03× Round
[29]	01× Node identity 01× Key of 128 bits 02× Key of 160 bits 01× Derived key	04× XOR operation 01× Encryption 01× XOR operation 01× HMAC operation 01× Data sensing	03× Round
[33]	01× Node identity 04× Key for each Node	01× Hash operation 01× MAC operation	07× Round
[32]	01× Key for each node 05× Node parameters	06× Arithmetic operation 01× Hash operation	02× Round
[39]	01× Node identity 01× Node parameters	02× Encryption 04× Arithmetic operation	02× Round
This paper	01× Node identity	01× Data sensing	01× Round

Table 1: Overall comparison of the reviewed solutions

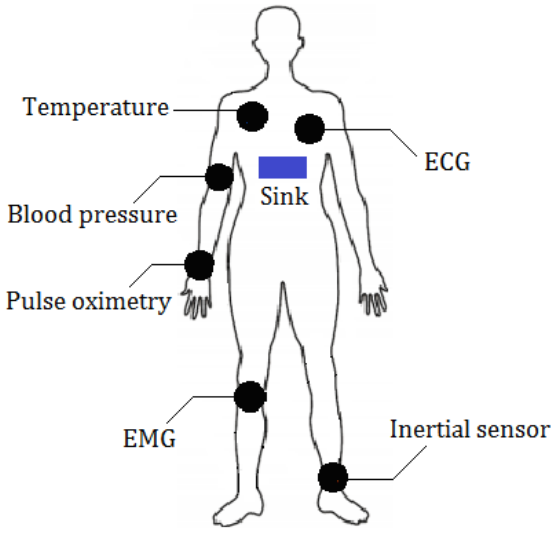

Figure 3: Sensor nodes deployment

sink device over the time. The second phase consists of the sensor node authentication under the developed model. In what follows, we give the description of each phase.

3.1. Learning phase

Body mobility plays an important role in the performance of the protocols in MBANs due to the patient body movement, where the sensor nodes would move along with patient being. During daily activities, the patient body exhibits different postures, like standing, walking, sitting, running, etc. In MBANs, these postures change affects the position of the sensor nodes, and hence, the distances separating them to the sink device. To determine the different positions of the sensor nodes, the system should first identify the posture and then the related movement. The patient body motion, when taking a particular posture can be determined from real patient mobility traces. To model the sensor node movement, the patient will be asked to go through a learning phase once the sensor nodes are deployed by the medical assistant. The learning phase is executed in offline by the system administrator. The posture should be defined and the patient will be invited to exercise the movement, during which the sink device analyzes the different cartesian distances estimated through the signal strength. For instance, we present in the general case three types of postures:

(1) Standing: the patient is standing at rest, the arms at the sides, the palms facing forward, and the feet tight and parallel. It is the standard anatomical position. As illustrated in Figure 3, the distances between the sensor nodes and the sink device are constant as the patient body is in a static position.
(2) Walking: during walking, the arms and the legs move in a defined trajectory repeatedly. The limbs move in forward and backward directions. Therefore, the sensor nodes placed on the limbs also move in these directions. In addition, as the torso is less mobile, the sensor nodes placed on this area show a few variation in their positions relating to the sink device. Figure 4 illustrates the patient body

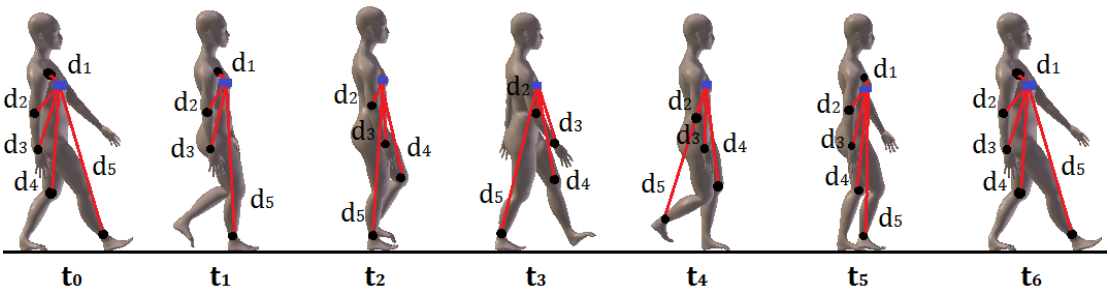

Figure 4: Patient body motion during walking

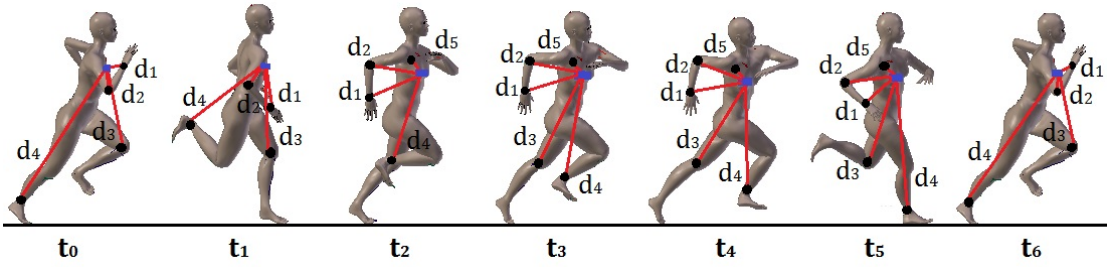

Figure 5: Patient body motion during running

motion during walking. At each instant, the patient body is characterized by specific cartesian distances separating the sink device to the sensor nodes.

(3) Running: similar to walking, the arms and the legs perform a repetitive movement in forward and backward directions. In addition, when running, the left arm and the right leg are synchronized and move in these directions at the same time. Therefore, the sensor nodes placed on the limbs of the patient body move in the same trajectory. Figure 5 illustrates the patient body motion during running. At each instant, the patient body is characterized by specific cartesian distances separating the sink device to the sensor nodes.

In the learning phase, the sink device initiates the system by diffusing a request $Req = \langle t_0, \Delta t, T \rangle$ to the sensor nodes. The request asks each sensor node to start upon t_0 time-unite transmitting the sensor node identity, continuously, every Δt time-unite during a period of T time-unite. At each instant t_i, each sensor node S_j transmits its identity to the sink device. Upon receiving, the sink device estimates for each time t_i, the cartesian distance d_{j_i} which separates it to the transmitter sensor node S_j through the signal strength using for instance RSSI (Received Signal Strength Indication) or LQI (Link Quality Indication) [14]. For each sensor node, the sink device collects a number $\frac{T}{\Delta t}$ of cartesian distances stored as points. Let's consider $n+1$ points $\{(t_0, y_0), (t_1, y_1), ..., (t_n, y_n)\}$ such as:

$$y_i = d_{j_i}, \ \forall \ i = 0..n \tag{1}$$

Afterwards, the sink device interpolates a polynomial $\mathcal{F}_j$ of degree n for each sensor

node S_j, such as:

$$\mathcal{F}_j(t_i) = d_{j_i},\ \forall\ i = 0..n \tag{2}$$

The polynomial $\mathcal{F}_j$ characterizes the movement pattern of the sensor node S_j. This polynomial is computed using the Newton interpolation method, such as:

$$\mathcal{F}_j(t) = D_{0,0} + (t-t_0)\cdot D_{0,1} + (t-t_0)\cdot(t-t_1)\cdot D_{0,2} + ... + (t-t_0)\cdots(t-t_{n-1})\cdot D_{0,n} \tag{3}$$

where the coefficients $D_{i,k}$ are computed by:

$$D_{i,k} = \frac{D_{i+1,k} - D_{i,k-1}}{t_k - t_i},\ \forall\ i = 0..n,\ \forall\ k = 1..n,\ k > i \tag{4}$$

where $D_{i,i} = y_i,\ \forall\ i = 0..n$. We note that three of conventional interpolation methods are equivalent, namely Lagrange, Neville and Newton-Aitken. They result to same polynomial but differ in operating cost. We have opted for the Newton method because additional points can be added to create a new interpolation polynomial without the recalculation of coefficients [43].

The body movement is a biometric feature which is unique and related only to one patient at a given time. Therefore, the set of $\mathcal{F}_j,\ \forall\ j = 0..\eta$ of all the possible postures of a patient characterizes in a unique manner its feature. Thus, this set of parameters represents the credential of the patient when considering external authentication. These parameters are stored in both sides, namely in the patient sink device and the remote medical server. If an external authentication is required, the latter parameters can be used as a common key ensuring the key security services through the conventional methods. However, in this paper, the scope is limited in the sensor node authentication, due to their challenging characteristics of the sensor resources. The next phase describes the authentication process on the patient body.

3.2. Authentication phase

The proposed solution aims to verify the legitimacy of the sensor nodes wishing to communicate with the sink device. Upon receiving the sensed data from the sensor nodes, the sink device estimates for each S_j, the distance d'_j using the transmission signal strength. Then, it computes t_i using the reverse polynomial function $\mathcal{F}_j^{-1}(d'_j)$ corresponding to each sensor node S_j. The sink device can authenticate the legitimacy of all the sensor nodes $\{S_1, S_2, ..., S_\eta\}$ being at the respective distances $\{d'_1, d'_2, ..., d'_\eta\}$, only if:

$$\mathcal{F}_1^{-1}(d'_1) \approx \mathcal{F}_2^{-1}(d'_2) \approx ... \approx \mathcal{F}_\eta^{-1}(d'_\eta) \tag{5}$$

Afterwards, the sink device can identify individually each sensor node S_j through d'_j. In this manner, is not possible for an external equipment in the vicinity to impersonate a valid sensor node. We denote P_S the probability of successful authentication of the patient body sensor nodes. The probability P_S represents the probability that the actual cartesian distances of all the sensor nodes coincide with the same value of the reverse

polynomial output. This probability depends on the estimated cartesian distances and is measured by:

$$P_S = \prod_{j=1}^{\eta-1} \frac{1 - |\mathcal{F}_j^{-1}(d_j) - \mathcal{F}_{j+1}^{-1}(d_{j+1})|}{\mathcal{F}_j^{-1}(d_j) + \mathcal{F}_{j+1}^{-1}(d_{j+1})} \tag{6}$$

The proposed solution aims also to authenticate individually in a direct way a given sensor node S_j. Upon receiving the sensed data from the latter at the instant t_i, the sink device estimates d'_j and resolves the equation $\mathcal{F}(t) = d'_j$. The sensor node S_j will be correctly authenticated if and only if it exists t' among all the possible solutions, such as:

$$t' \approx \frac{t_i}{\Delta t} \bmod n \tag{7}$$

3.3. Data communication

An important requirement in MBANs is the energy efficiency. To guarantee a reliable gathering of medical data, the communication process should be efficient against the frequency of movement and in energy-consumption. Several data communication protocols with mobility support are proposed in the literature for both ad-hoc and sensor networks. However, they are not suitable for MBANs due to the different movement pattern. To address this issue, several research works highly depend on the existing mobility models [24, 17, 18]. The drawback of such solutions is that they may work well with a specific model, but perform poorly with another. Other works have been based on their developed mobility models as the solutions proposed in [34, 20, 21] and few solutions have focused on the mobility parameters integration in the data communication process [23, 26]. The majority of these solutions has shown weaknesses to face the mobility and energy constraints. For this purpose, we incorporate a data communication technique to overcome the frequent changes on the network topology due to the posture changes and variation of the wireless link. We consider the architecture illustrated in Figure 6. This architecture is composed of a set of MBANs supervised by a single base station, which is in charge to transmit the medical data to the remote medical server via the Internet. The collected data of a patient are delivered to the base station through a set of intermediate sink devices of different other patients using a multiple-hop communication. The proposed technique is based on the patient mobility index and the sensor nodes energy states. The mobility estimation is performed in the neighboring topology change in function of the link availability. We introduce two metrics denoted by IL and OL representing, respectively, the number of in-links and out-links. These links could be or not available during an interval $[t, t+\delta]$ between the patients at each round. We use the same estimation approach given in [37]. At each round, each sink device S_i computes the mobility index $MI_i(t)$ at the instant t such as:

$$MI_i(t) = \alpha \cdot \frac{OL_i(t)}{L_i(t-\delta)} + (1-\alpha) \cdot \frac{IL_i(t)}{L_i(t)} \tag{8}$$

where L_i is the available link number and α represents the mobility coefficient, which can be adjusted according to the application requirements. Afterwards, the sink

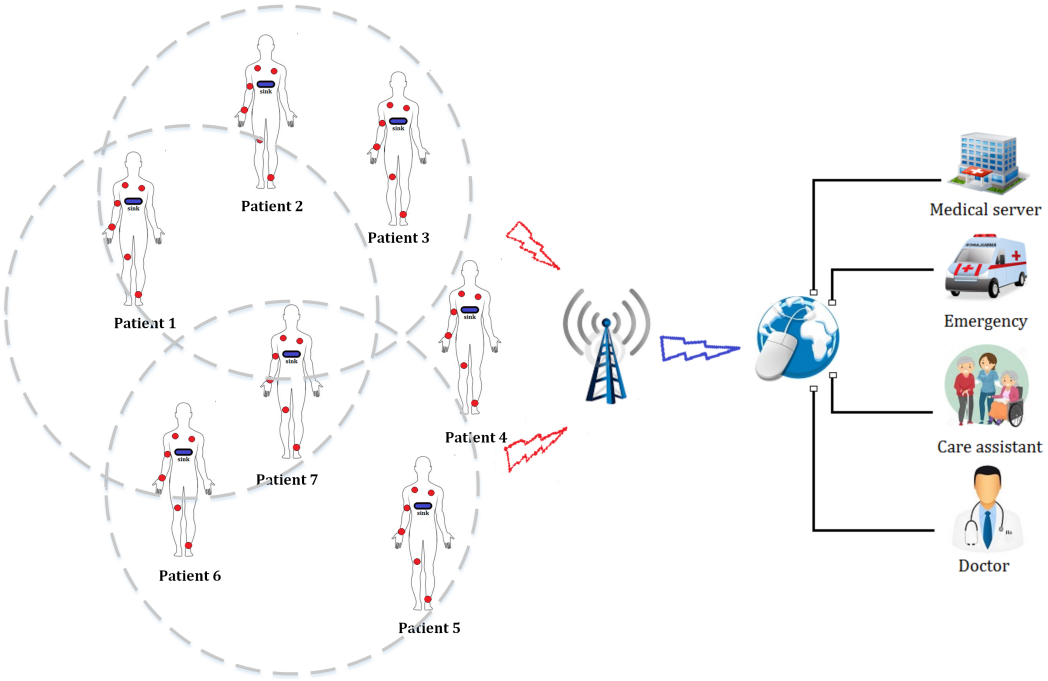

Figure 6: Data communication

device S_i sends the computed index to the neighbors in order to be used in the stable neighboring selection process. Based on this concept, our aim is to select the most stable neighbor to forward the medical data. Furthermore, to balance the energy consumption, the residual energy $E_j(t)$ at the instant t of the neighbor is also considered by selecting the best patient neighbor in terms of residual energy state. When forwarding, the sink device S_i computes $C(t)$ for all the reachable sink devices, such as:

$$C(t) = \frac{MI_j(t)}{E_j(t)} \tag{9}$$

Finally, the sink device selects the patient neighbor with the minimum value of $C(t)$. This process is repeated hop-by-hop until the data reaches the base station.

4. Security analysis

In this section, we analyze the security of the proposed solution. First, we give an overall analysis of its robustness against conventional attacks, namely the impersonation, Sybil, man in the middle, replay and denial of service attacks. Next, we analyze the impact of the attacks on the network. In order to support this part of analysis, we have developed an analytical model which compares the proposed solution with the solutions presented in Section 2.

4.1. The robustness of the authentication mechanism

The impersonation attack happens when the identity information is used to carry out a non-authorized action. Unlike the existing approaches, the proposed solution does not use cryptographic parameters in the authentication process. The unique parameter used is the signal strength at the right instant following the right node mobility model. Therefore, a non-authorized equipment has no way to impersonate a legitimate sensor node. Sybil attack happens when a node is diverted to claim multiple identities. The proposed solution resists well against this type of attack, because the attacker must generate several signals with different power at a given instant.

All the sensor nodes of the MBAN are within the sink device range. The authentication process is, then, performed directly between the sink device and the sensor node without intermediate nodes. An attacker trying to stand between the two latter nodes will have no way to impersonate neither of them. It is hard to launch a man in the middle attack in such case, because both the nodes receive the messages transmitted by the attacker. An attacker cannot reuse messages from a session in another one since the signal strength is different from an instant to another due to the mobility, i.e., the actual position of the interlocutor.

The denial of service attack is not considered by the proposed solution in the sense that we cannot prevent this attack from occurring. However, the proposed solution provides authentication even when this attack occurs or is combined with another attack. For example, if an attacker flood a sensor node with unnecessary requests in order to conduct an impersonation attack, neither the authentication, nor an attempt to retrieve the patient data can be successful, because it cannot be able to transmit the data with a specific signal strength.

4.2. Impact of attacks

In order to analyze the impact of attacks, we propose a generic analytical model of the process of internal node authentication in MBAN. The main aim of this model is to measure the probability of attacks. In this context, we classify the possible attacks into two categories, namely physical and logical attacks. The physical attack represents the interruption of communication, such as packet dropping attack or buffering attack to harm the network operation. The logical attack represents the failure when verifying the cryptographic parameters, such as signatures, hash values, etc. We consider a successful of the authentication process if the authentication session does not undergo both physical and logical attacks. The sensor nodes execute the authentication process either between them or with the sink device. This process is initiated in all the cases by an authentication request. Then, a certain number of communication rounds are performed in order to authenticate the data source node. The exchanged messages include in the most cases of the protocols a set of encrypted parameters supported by a set of operations, such as encryption, key generation, hash operation, etc., performed on both sides. We denote by v the communication round number, which varies from a solution to another.

We model the authentication process using the Markov chain [42]. The Markov chain is a technique for statistical modeling of a random process, in which the system state changes through progression. It is composed by a set of states $A = \{A_1, A_2, ..., A_N\}$ and transition probabilities among the system states. The process starts with one of

these states and moves successively from one state to another. If the system is currently in the state A_i, then it moves to A_j in the next step with a probability, denoted by P_{ij}. This probability does not depend upon which states the system was in before the current state. A Markov chain has the property that the probability of transition between any two states depends entirely on circumstances in the state from which the transition originates and not on the previous history of the process. Given a sequence of states $A_1, A_2, ..., A_N$, the Markov property is given as:

$$P = (A_{N+1} = x | A_N = x_N, ..., A_1 = x_1) = P(A_{N+1} = x | A_N = x_N) \tag{10}$$

We model as states the different transmissions and receptions between the two nodes in an authentication session. The proposed model characterizes the authentication process in order to estimate the probability of authentication success and failure. We introduce two metrics r and s which denotes, respectively, the probability of physical attack for an individual message transmission and the probability of logical attack for an individual message verification. The state transition model represents the manner how the node is authenticated according to the generated data packet in the network. Before the authentication is achieved, the process may pass through other transient states. Note that the latter represent the possible transmissions and receptions states until the authentication process becomes absorbed. We illustrate in Figure 7 the proposed model and we present in Table 2 the corresponding notations. The system starts from the initial state W denoting the waiting state, where a source node generates an authentication request. Hence, the system may pass to the state T_1 with a probability q or pass again to the state W with a probability $1 - q$. The probability q depends mainly on the application context, which is different from an application to another. The system may pass to the failure state PA with a probability r if a physical attack is launched, otherwise, it passes to the state R_1 with a probability $1 - r$. Upon the verification of the received parameters, the system passes to the state LA with a probability s if a logical attack is detected, otherwise, it passes to the state E_2 with a probability $1 - s$. The process is repeated as the indicated communication round number υ. From the state R_υ, the system may pass to the successful state S with probability $1 - s$ if the $\upsilon - 1^{th}$ received parameters are correctly verified.

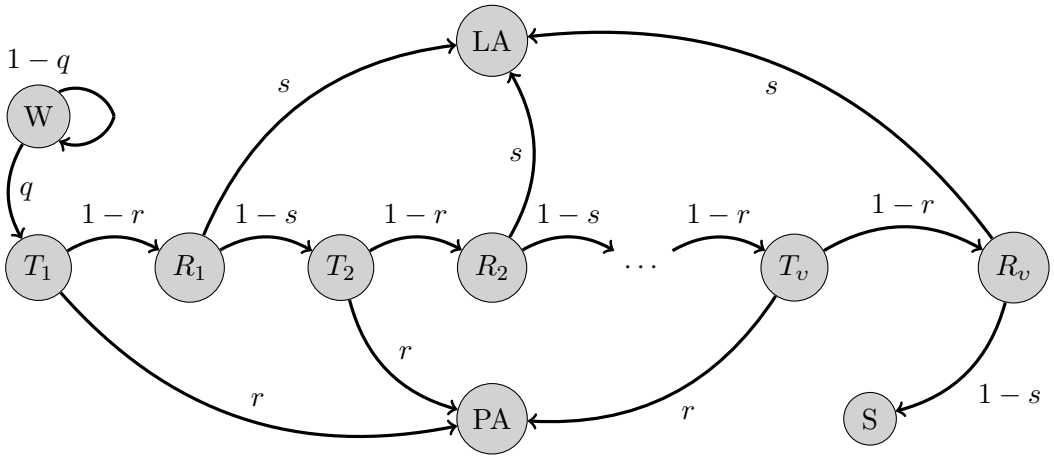

Figure 7: Transition graph

Notations	Description
W	Waiting state
T_i	Transmission state
R_i	Reception state
PA	Physical attack state
LA	Logical attack state
S	Successful authentication state
q	Probability of request authentication reception
r	Probability of packet dropping
s	Probability of verification failure
P_S	Probability of successful authentication
P_{PA}	Probability of physical attack
P_{LA}	Probability of logical attack

Table 2: Notations

From the proposed model is computed the probability of successful authentication, physical and logical attacks, denoted by P_S, P_{PA} and P_{LA}, respectively. The probability of successful authentication represents the probability $P\{W \longrightarrow S\}$, which is calculated as:

$$P_S = q \cdot \Big((1-r)\cdot(1-s)\Big)^{v} \cdot \Big((1-q)^{\mu}+1\Big) \tag{11}$$

where μ denotes the number of iterations the system remains in the waiting state. The parameter μ is expected to be high in case of specific types of medical applications, such as real-time medical motoring, military medical applications, etc. The probability of physical attack P_{PA} represents the probability $P\{W \longrightarrow PA\}$, which is calculated

as:

$$P_{PA} = q \cdot r \cdot \frac{\left(1 - (1-r)^{\upsilon} \cdot (1-s)^{\upsilon}\right) \cdot \left((1-q)^{\mu} + 1\right)}{1 - (1-r) \cdot (1-s)} \tag{12}$$

The probability of logical attack P_{LA} represents the probability $P\{W \longrightarrow LA\}$, which is calculated as:

$$P_{LA} = q \cdot (1-r) \cdot s \cdot \frac{\left(1 - (1-r)^{\upsilon} \cdot (1-s)^{\upsilon}\right) \cdot \left((1-q)^{\mu} + 1\right)}{1 - (1-r) \cdot (1-s)} \tag{13}$$

In what follows, we quantify the impact of attacks on the proposed solution with comparison to the reviewed solutions under the analytical model. Depending on the solution design, the parameter υ takes different values. This allows classifying the solutions into six classes as presented in Table 3.

Class	υ	**Solutions**
A	1	The proposed solution
B	2	[32], [35], [31] and [39]
C	3	[30], [28] and [29]
D	4	[38] and [25]
E	6	[27]
F	7	[33]

Table 3: Classification of the solutions regarding υ

Indeed, we note a close relationship between the probability q to receive an authentication request and the waiting iteration number μ. More the value of μ is high more the probability to receive an authentication request is decreased, in which μ is inversely proportional to q. In order to maintain the coherence of the implied parameters we represents q in function μ, such as $q = \frac{1}{\mu}$.

First, we were interested to study the impact of the metrics r and s. In function of the latter metrics, we compare the different classes of solutions regarding the impact of both physical and logical attacks, which are illustrated in Figures 8 and 9, respectively. We set $\mu = 1$ in order to absorb the impact of this parameter in contrast of r and s. The probability P_{PA} increases when the probability r increases, and in the same way, the probability P_{LA} increases when the probability s increases. Beside the parameters r and s, the impact of physical and logical attacks depends strongly on υ. In the class A belongs the proposed solution, which gives the most optimal results and outperforms the other classes, where their value range of P_{PA} and P_{LA} are higher. This is due to the communication round number, which increases the risk of attack at each exchange between the communicating nodes. For instance, the class F provides the worst results due to the high value of υ which equals to 7. Second, we were interested to study the impact of the metric μ. In function of the latter, we compare the different classes of solutions regarding the impact of both physical and logical attacks, which are illustrated in Figures 10 and 11, respectively. As we can note, there is an inverse relationship

between the probabilities of attacks and μ. When the waiting time is reduced, the network will be a subject of attacks, like in real-time sensitive applications. The class A, in which belongs the proposed solution, gives the best result and outperforms the other classes, where their value range of P_{PA} and P_{LA} are lower.

5. Efficiency analysis

In this section, we analyze the efficiency of the proposed solution. We have conducted intensive simulations to evaluate the performances of the proposed solution, which we have compared with all the solutions reviewed in Section 2. In what follows, we present the simulation environment, the performance metrics, and finally we discuss the obtained results.

5.1. Simulation parameters

We have developed the simulations using the programming language Java. The aim of this evaluation is to position the efficiency the proposed solution in contrast to the others. The simulation duration is of 150 second with 6 sensor nodes deployed on the patient body supervised by a single sink device placed at the center. We consider a deployment area of 10m×10m, where the sensor nodes are deployed in a deterministic manner at fixed positions. Each sensor node has a radio range of 1m and an initial energy source of 0.5 Joule. To measure the energy consumed by the sensor nodes during transmission, we have used the radio model proposed by Heinzelman et al. [41]. The energy consumption cost for the transmission of a k-bit data packet over a distance d meter is computed in joule by:

$$E = k \cdot (E_{elec} + E_{amp} \cdot d^2) \tag{14}$$

where E_{elec} denotes the electronic energy and E_{amp} the transmitter amplifier. When receiving a k-bit packet, it consumes in joule:

$$E = k \cdot E_{elec} \tag{15}$$

In the simulation scenario, the sensor nodes measure continuously the physiological values, which are managed with different sizes regarding the nature of the sensed data. The simulator identifies the data size following the identity of the sensor node generator. The simulation starts with the learning phase, where the sink device recovers at each slot of time Δt of 1 second, the distances separating it to the other sensor nodes. The learning phase is executed during a time period T of 10 second for three types of posture, namely standing, walking and running. The network topology changes due to the patient body movement. In this context, we have implemented the body mobility model MoBan (Mobility BAN) [34]. This model considers the global movement of MBAN by introducing the different patient body posture and permits individual mobility of the deployed sensor nodes on the patient body. In Table 4, we summarize the main simulation parameters.

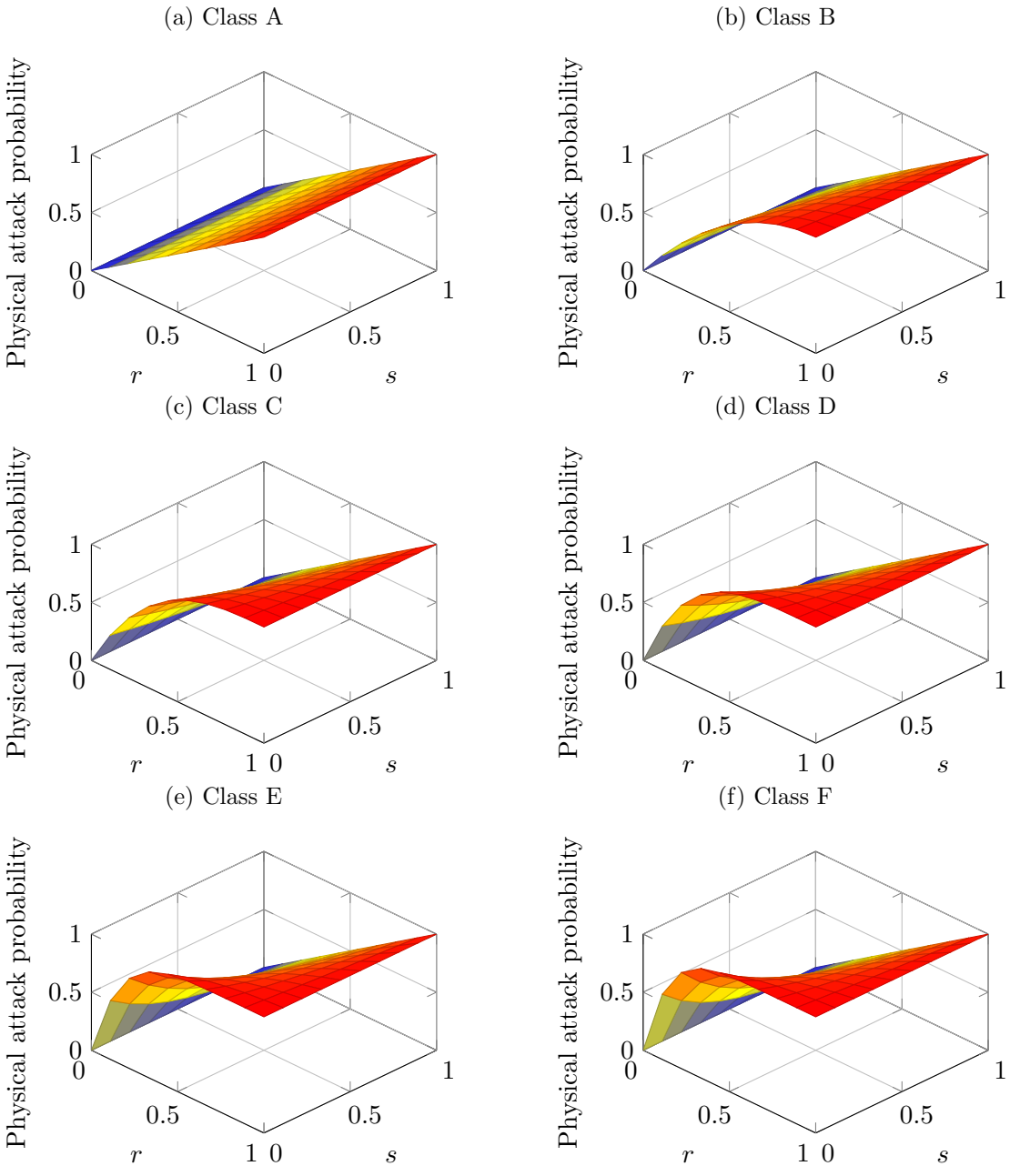

Figure 8: Physical attack probability in function of r and s for the different classes of solutions

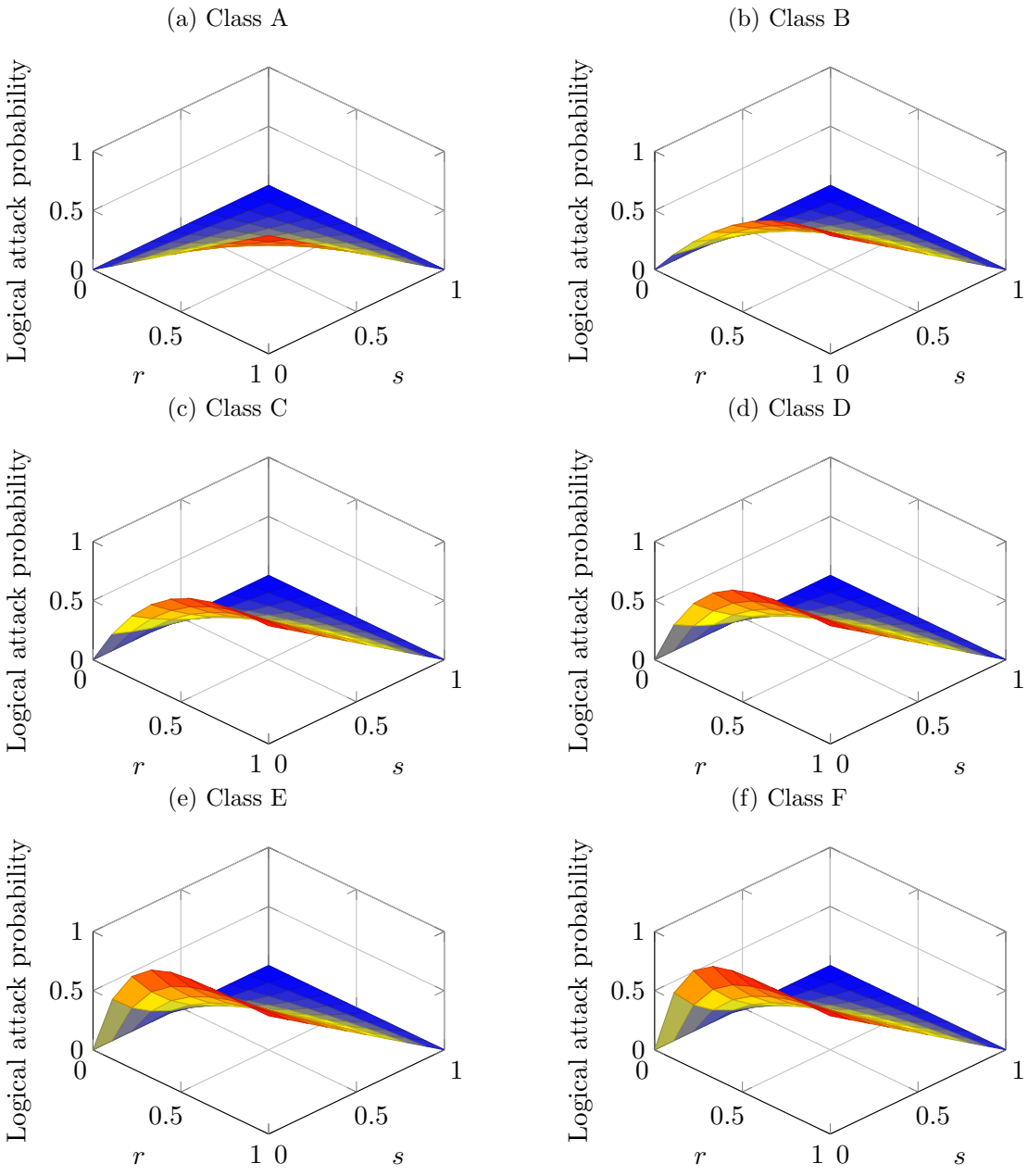

Figure 9: Logical attack probability in function of r and s for the different classes of solutions

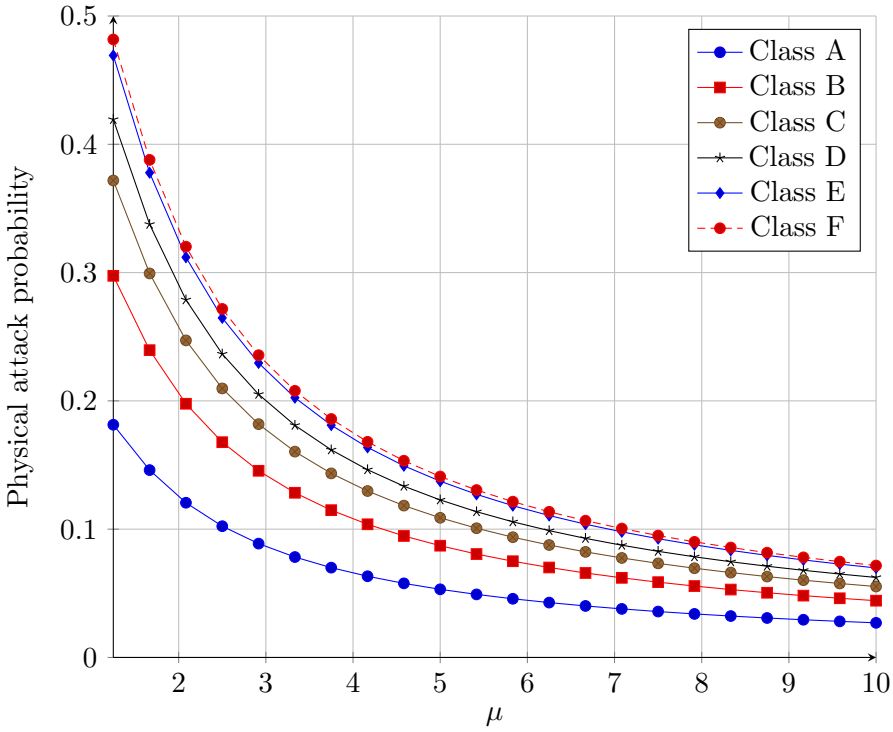

Figure 10: Physical attack probability in function of μ for $r = 0.2$ and $s = 0.2$

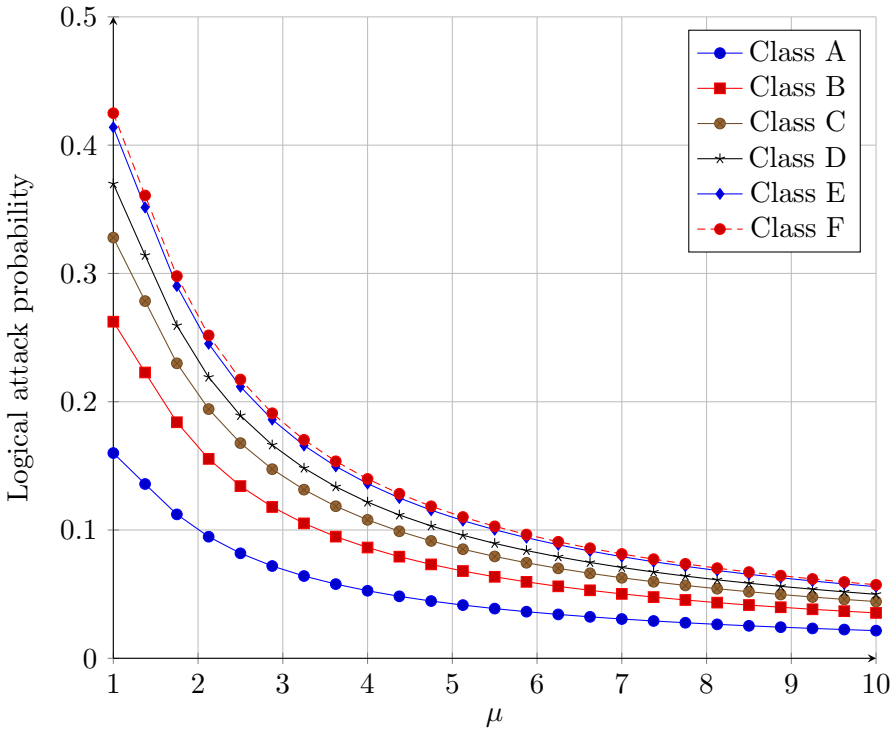

Figure 11: Logical attack probability in function of μ for $r = 0.2$ and $s = 0.2$

Parameter	Value
Number of sensor nodes (η)	6
Number of sink devices	1
Sink device position	Patient body center
Simulation area	10m×10m
Simulation time	150 second
Learning phase period by posture (T)	10 second
Maximal transmission range	1m
Data generation rate	1 Mbit/second
Initial energy per sensor node	0.5 Joule
Energy consumed by the electronic circuit (E_{elec})	16.7 nJoule
Amplification energy (E_{amp})	1.97 nJoule

Table 4: Simulation parameters

5.2. Performance metrics

We were interested on three important performance metrics, namely the transmission load, the response time and the energy consumption. Unlike the other solutions, which require to store at least one key, the proposed solution does not prevent any extra parameter to store on the sensor nodes apart their proper identifiers. For this reason, the metric of the storage load is not considered in the performance evaluation. Through the transmission load, we quantify how well the proposed solution optimizes the communication. Reducing the transmission load allows to decrease considerably the negative impact of the generated radio signals by the sensor nodes on the patient health. Through the response time, we analyze the reactivity in order to promote the real-time criterion, which is highly required in emergency healthcare applications. Through the energy consumption, we evaluate the endurance of the MBAN in terms of lifetime. Prolonging the network lifetime decreases considerably the frequency of sensor node relocation on the patient body. The energy consumption is computed from the total amount of energy consumed in the MBAN over all the sensor nodes.

5.3. Transmission channel reliability impact

Figure 12 illustrates the transmission load in function of the transmission channel reliability rate. We note that the proposed solution achieves the best results compared to other protocols with a considerable transmission load performance when the reliability is about 20%. However, for the other solutions the transmission load is high. The proposed solution uses only the collected medical data by the sensor nodes unlike the other solutions. In the latter, further to the measured data, they require to exchange several cryptographic parameters (encryption key, identifiers, MAC, etc.) to perform the authentication process. Figure 13 illustrates the response time in function of the transmission channel reliability rate. Regarding the obtained results, the proposed solution achieves again better results compared to other solutions with a basic response time of 65 millisecond in the case of reliable channels. For instance, in [27], the data packets are transmitted through several paths to reach their destination, thus leading higher response time that continues to grow with the retransmissions number. In the

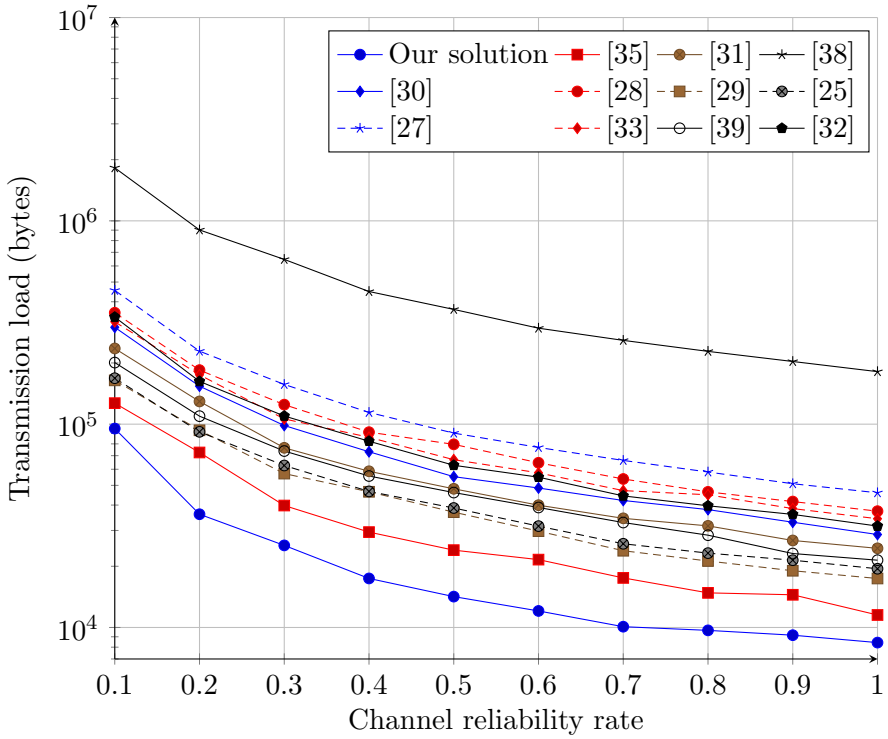

Figure 12: Transmission load in function of the transmission channel reliability

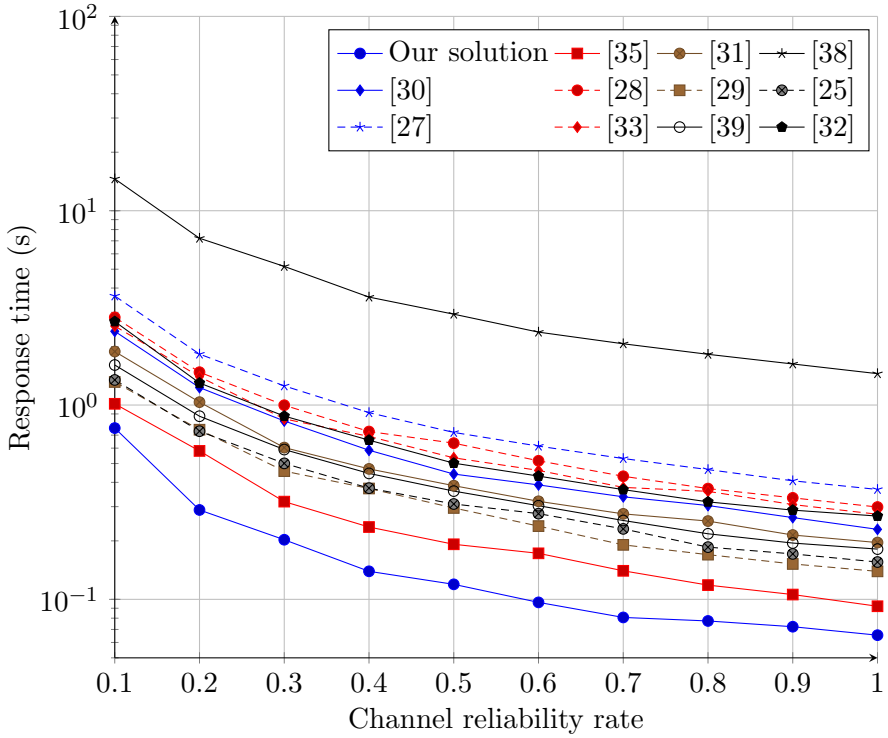

Figure 13: Response time in function of the transmission channel reliability

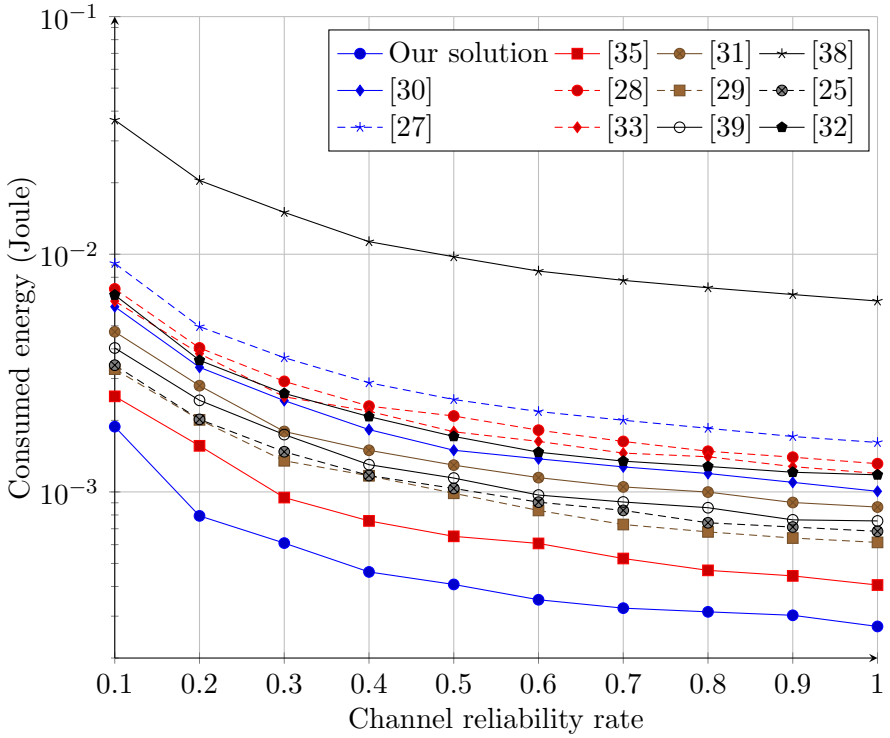

Figure 14: Energy consumption in function of the transmission channel reliability

proposed solution, the data are transmitted through a single-hop toward the sink device, and hence offering a good effect in terms of response time. Figure 14 illustrates the energy consumption in function of the transmission channel reliability rate. The obtained results show that the energy consumed in the proposed solution is lesser than the other protocols. In this way, it allows an effective management energy consumption, and hence prolonging the network lifetime. Although the transmission channel inherent characteristics and the nature of links, which is generally power limited in the case of MBANs, the proposed solution provides an effective results in terms of transmission load, response time and energy consumption.

5.4. Transmission frequency impact

Figure 15 illustrates the transmission load in function of the transmission frequency. The proposed solution demonstrates better results compared to the other protocols. The other solutions present a considerable increase in terms of load transmission due to the exchanged data amount among the sensor nodes in the authentication process. For instance, the solution [38] presents a high increase of transmission load due to the exchanged data which are of size to 640 bytes in order to establish a common key. Figure 16 illustrates the response time in function of the transmission frequency. The obtained results show that the proposed solution provides better performances compared to other protocols with a tolerable increase where the exchanged packet frequency becomes excessively high. We note a slight gap between the solutions [30] and [31]. Indeed, the latter solutions are based on fuzzy vault technique to exchange the shared key. In [30],

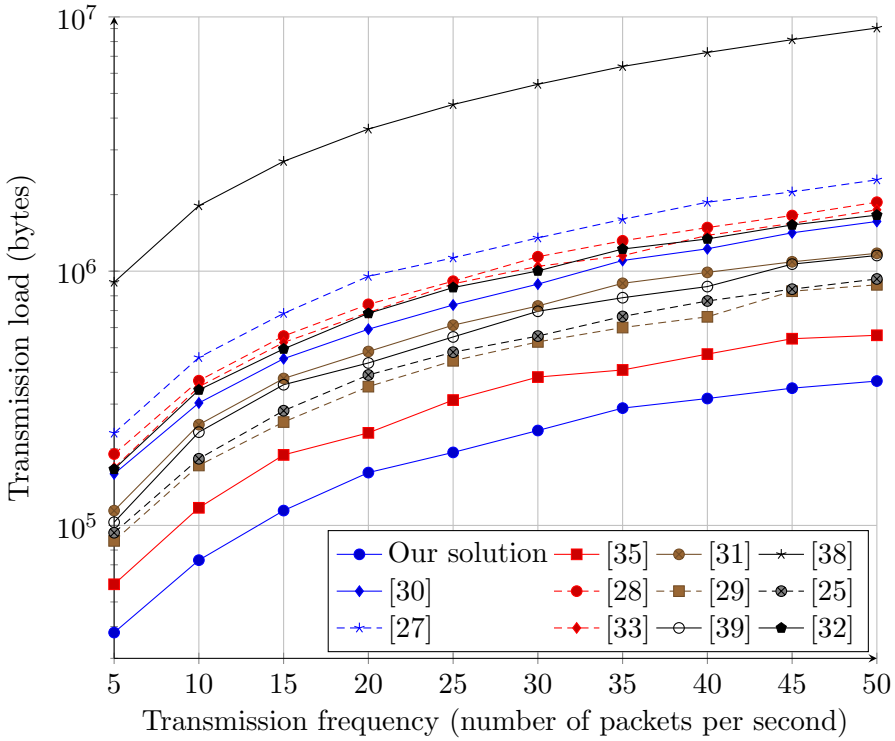

Figure 15: Transmission load in function of the transmission frequency

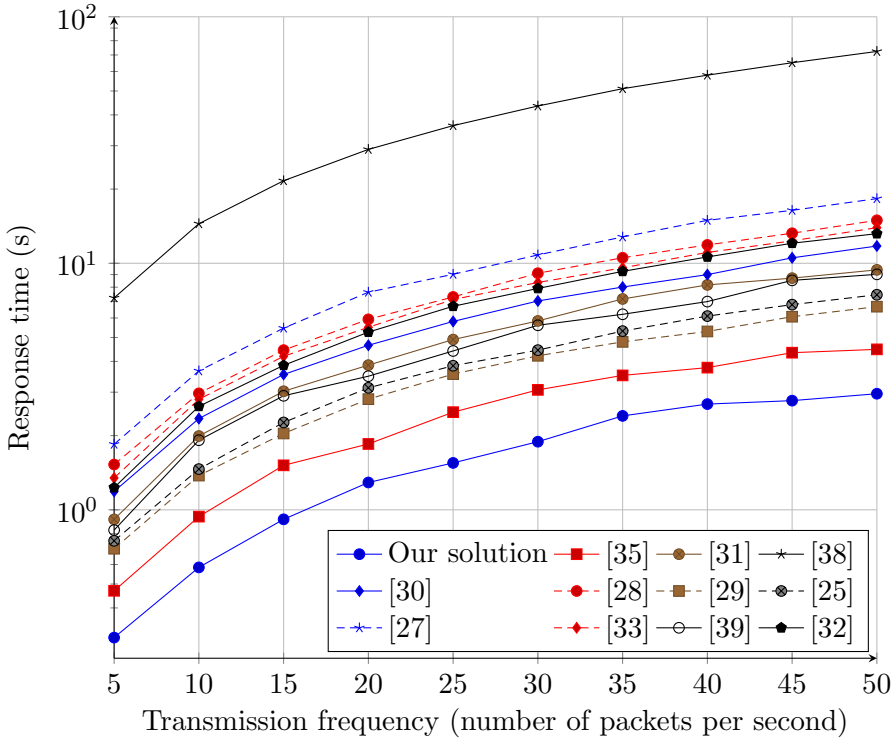

Figure 16: Response time in function of the transmission frequency

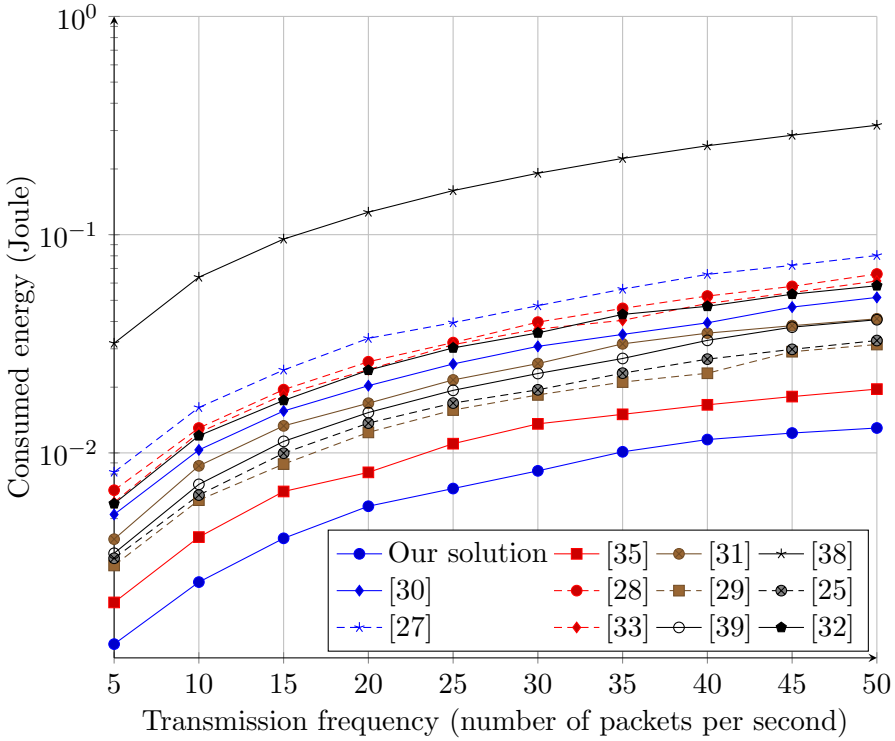

Figure 17: Energy consumption in function of the transmission frequency

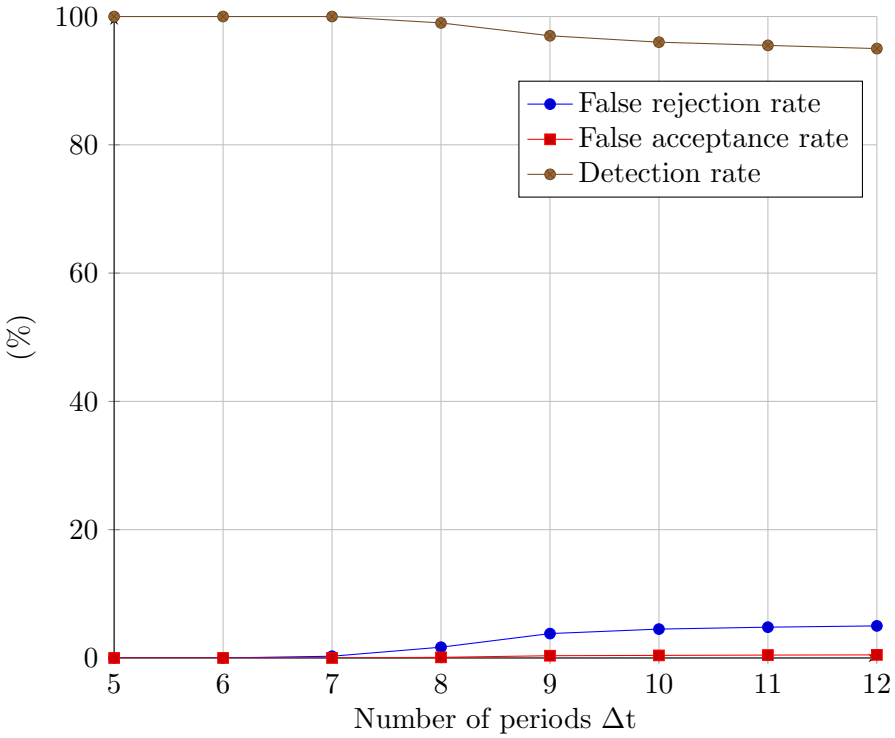

Figure 18: Detection, false rejection and false acceptation rates in function of the Δt period number

the secret key is concealed in the vault with distorted dots (chaff points), which will be also issued. In contrast, [31] uses a different technique, where the points are distorted, and hence, offering shorter response time. In [33], the response time is high because of the high number of packets transmitted through several intermediate sensor nodes before reaching the destination. Figure 17 illustrates the energy consumption in function of the transmission frequency. The energy consumed following the proposed solution is lesser than the other solutions. In the latter, the sensor nodes consume an important part of energy due to the transmission load. The obtained results show the effectiveness of the proposed solution for the medical applications requiring emergency in the treatment and communication.

5.5. Detection precision

We have evaluated the performances of the proposed solution in foreign equipment detection, which are located within the communication range of MBAN. In this context, we have measured the detection, false rejection and false acceptance rates based on the number of the selected periods during the learning phase. The detection rate denotes the ratio of the detected attack number to all the launched ones. The false rejection rate denotes the ratio of the number of non-authenticated legitimate sensor nodes to all the authentication requests. The false acceptance rate denotes the ratio of the number of authenticated non-legitimate sensor nodes to all the authentication requests. Figure 18 illustrates the obtained results with stranger equipments presence. We note that whatever the number of periods Δt, the detection rate is about 97%, which represents a an acceptable rate. Moreover, we note that the false rejection rate is relatively low and its growth in the number of periods Δt is very low. This result is quite understandable insofar as the number of periods Δt increases, the time interval becomes smaller. The distance between a sensor node and the sink device in two consecutive periods becomes very close and a slight difference may fail the authentication process. This slight increase in the false rejection rate is however acceptable as long as the false acceptance rate remains approximatively null.

6. Implementation

In this section, we present the description of the proposed solution implementation and the obtained results in terms of true acceptation and false rejection.

6.1. Description

The prototype which we have developed consists of a data generator device remotely connected to a smartphone which acts as the sink. We illustrate in Figure 19 the global view of the performed experiments. The data generator is prototyped by three units, namely a microcontroller, a wireless communicating module and an energy source. We have used an Arduino Nano, which is characterized by a weight of 7g, a microcontroller ATmega328, an architecture AVR, an operating voltage of 5V, a flash memory of 32KB of which 2KB is used by the bootloader, a SRAM of 2KB, a clock speed of 16MHz, an EEPROM of 1KB, a power consumption of 19mA, and a PCB size of 18mm×45mm [2]. The data generator device emulates the sensed data by the sensor of health monitoring, like ECG, temperature, blood pressure, blood oxygenation, etc. For the data

transmission, we have used a Bluetooth HC-05. The latter is a Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup. The module is compatible with Arduino Nano and can transfer data at the baud rate of 9600.

In the sink side, we have developed an Android program for transmission distance estimation, learning and authentication. Indeed, several characteristics make the smartphone more suitable in the MBAN applications such as the large capacity of storage, the high speed and precision of processing chip, the high capacity of the battery, and the powerful communication function. Especially, with an open operating system and the ability of installing and uninstalling new applications [22]. We have developed this part using Android Studio IDE 2.3. It is specifically designed for Android development based on the JetBrains and IntelliJ IDEA software and is a successor to Eclipse Android Development Tools (ADT) as Google's primary IDE for Android application development [1]. We have developed the sink program part on a Samsung Galaxy S5 mini characterized by a 1400 MHz CPU frequency, Android OS 4.4, a 1.5GB of RAM, and a Bluetooth 2.0 EDR.

After receiving the data via the socket connection between the smartphone and the Bluetooth module from the data generator, it processes the received data to extract the signal strength (RSSI). Based on the latter, the program computes the transmission distance at each time during the activity period, generates the polynomial function and stores it in its locally. Afterwards, the authentication process uses this polynomial function to determine if the received data at a particular instant is generated or not by the legitimated device.

6.2. Obtained results

A user has been equipped with a data generator placed on its left arm. During the test, the data generator device is connected to the sink program. In the experiment, the user has performed a walking activity for a period of time $T = 1$ minute, where the data are transmitted at each $\Delta t = 6$s by the data generator. This step allowed to learn the user behavior, and afterwards, the user was invited to the authentication phase, in which the sink tries to identify the data generator through its RSSI. This experiment is repeated 10 times by measuring for each one the true acceptation and the false rejection. The obtained results are illustrated in Figure 20. The results show that whatever the number of periods Δt, the true acceptation rate varies between $91,66\%$ and 100%, which is an acceptable interval. This result is quite understandable insofar as the user is walking, the distance between the data generator device and the sink device in two consecutive periods becomes close or away, and a slight difference may fail the authentication process. However, this slight increase in the false rejection rate is acceptable.

7. Conclusion

The area of MBANs is attractive in the research community due to its applications in the medical fields improving the service quality and allowing remote patient monitoring. The authentication is a challenging issue in MBANs due to the use of computational and resource limited sensor nodes. Any security protocol designed for use in MBANs should

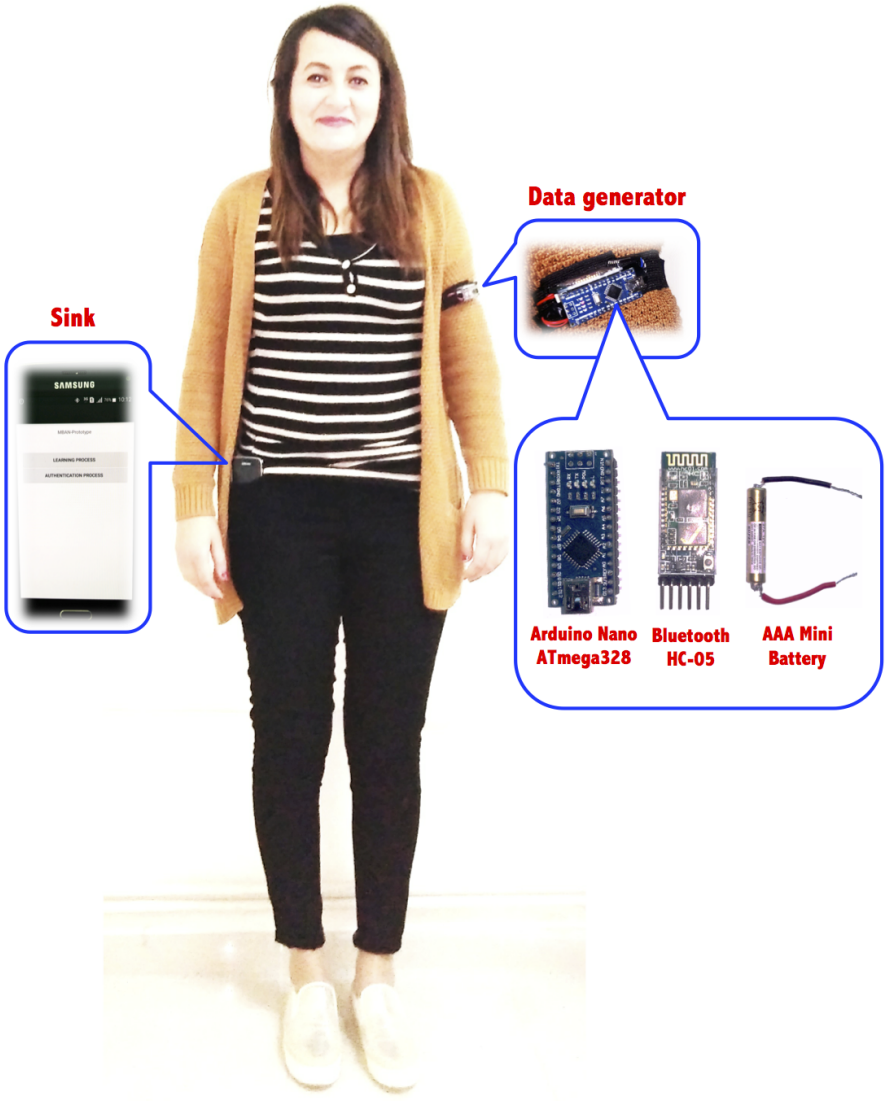

Figure 19: The prototype components.

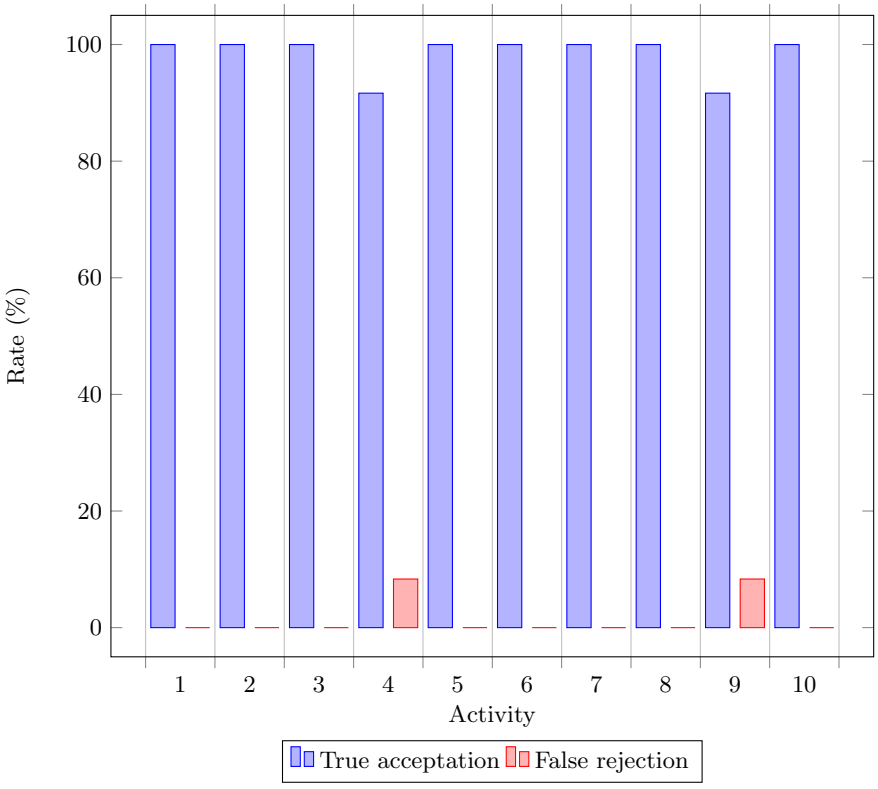

Figure 20: Accuracy of the proposed solution.

be robust against attacks, energy-efficient and should have a low impact on the network lifetime. In this paper, we have proposed a patient body motion based authentication solution which is very practical for mobile healthcare environments. The proposed solution provides a tradeoff between the efficiency and security. We have demonstrated its robustness against impersonation, Sybil, man in the middle and replay attacks. In order to evaluate the impact of physical and logical attacks on the proposed solution, we have developed an analytical model using Markov chain, where it demonstrates the best results compared to the other solutions. Again, in order to evaluate the efficiency of the proposed solution, we have developed simulations with comparison to all the reviewed solutions, followed by real experimentations. The results indicate better performance of the proposed solution in terms of transmission overhead, response time, energy consumption and accuracy.

Acknowledgment

This work was carried out in the framework of the research activities in the laboratory LIMED, which is affiliated to the Faculty of Exact Sciences of the University of Bejaia. The authors are very grateful and greatly thank the editors and anonymous reviewers for the time and effort they devote to the examination of the work. The authors thank also Mokhtari Walid and Ouzeggane Redouane for their technical assistance.

8. Bibliography

[1] Developer Android. Available online (27 April 2017): https://developer.android.com

[2] Arduino. Available online (27 April 2017): https://www.arduino.cc/en/Main/ArduinoBoardNano

[3] S. Majumder, T. Mondal, M.J. Deen, Wearable Sensors for Remote Health Monitoring, Sensors, 17(1) (2017) 130

[4] J. Gaskin, J. Jenkins, T. Meservy, J. Steffen, K. Payne, Using Wearable Devices for Non-invasive, Inexpensive Physiological Data Collection. In Proceedings of the 50th Hawaii International Conference on System Sciences (2017)

[5] Z. Taha, R.M. Musa, M.R. Abdullah, M.A.M. Razman, C.M. Lee, F.A. Adnan, M. Haque, The Application of Inertial Measurement Units and Wearable Sensors to Measure Selected Physiological Indicators in Archery. Asian Journal of Pharmaceutical Research and Healthcare, 9(2) (2017) 85–92

[6] V.A. Goodyear, Social media, apps and wearable technologies: navigating ethical dilemmas and procedures. Qualitative Research in Sport, Exercise and Health, 9(3) (2017) 285–302

[7] J. Qi, P. Yang, M. Hanneghan, S. Tang, Multiple density maps information fusion for effectively assessing intensity pattern of life logging physical activity, Neurocomputing, 220(2017) 199–209

[8] J. Qi, P. Yang, M. Hanneghan, D. Fan, Z. Deng, F. Dong, Ellipse fitting model for improving the effectiveness of life-logging physical activity measures in an Internet of Things environment, IET Networks, 5(5) (2016) 107–113

[9] P. Yang, D. Stankevicius, V. Marozas, Z. Deng, A. Lukosevicius, F. Dong, E. Liu, L. Xu, G. Min, Lifelogging Data Validation Model for Internet of Things enabled Personalized Healthcare, IEEE Transactions on Systems, Man and Cybernetics: Systems, (2016)

[10] E. Wartella, V. Rideout, H. Montague, L. Beaudoin-Ryan, A. Lauricella, Teens, health and technology: A national survey. Media and Communication, 4(3) (2016)

[11] V. Kumar, B. Gupta, S.K. Ramakuri, Wireless body area networks towards empowering real-time healthcare monitoring: a survey, International Journal of Sensor Networks, 22(3) (2016) 177–187

[12] S. Al-Janabia, I. Al-Shourbajib, M. Shojafarc, S.Shamshirbandd, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, Egyptian Informatics Journal, (2016)

[13] A. Tewari, P. Verma, Security and Privacy in E-Healthcare Monitoring with WBAN: A Critical Review, International Journal of Computer Applications 136(11) (2016)

[14] B. Mukhopadhyay, S. Sarangi, S. Kar, Performance Evaluation of Localization Techniques in Wireless Sensor Networks Using RSSI and LQI, National Conference on Communications (2016) 1–6

[15] V. Mainanwal, M. Gupta, S-K. Upadhayay, A Survey on Wireless Body Area Network: Security Technology and its Design Methodology issue, International Conference on Innovations in Information, Embedded and Communication systems (2015)

[16] A. Merlo, M. Migliardi, L. Caviglione, A survey on energy-aware security mechanisms, Pervasive and Mobile Computing, 24 (2015) 77–90

[17] R. Venkateswari, S. SubhaRani, V. Sudharshan, R. Umadharshini, A Cross-Layer Analysis for Providing Mobility in Wireless Body Area Networks, Artificial Intelligence and Evolutionary Algorithms in Engineering Systems 2 (2015) 625–632

[18] L. Yi, C. Mingyan, W. Yidan, Research on mobility module oriented to wireless body area network, Journal of Chemical and Pharmaceutical Research 7(3) (2015) 1546–1550

[19] F. Rezaei, M. Hempel, H. Sharif, A Survey of Recent Trends in Wireless Communication Standards, Routing Protocols, and Energy Harvesting Techniques in E-Health Applications, International Journal of E-Health and Medical Communications, 6(1) (2015) 1–21

[20] B. Alghamdi, H. Fouchal, A Mobile Wireless Body Area Network Platform, Journal of computational science 5(4) (2014) 664–674

[21] M-M. Sandhu, M. Akbar, M. Behzad, N. Javaid, Z-A. Khan, U. Qasim, Mobility Model for WBANs, Broadband and Wireless Computing, Communication and Applications (2014) 155–160

[22] D. Lou, X. Chen, Z. Zhao, Y. Xuan, Z. Xu, H. Jin, Z. Fang, A wireless health monitoring system based on android operating system, IERI Procedia 4 (2013) 208–215

[23] H. Su, Z. Wang, S. An, MAEB: Routing Protocol for IoT Healthcare, Advances in Internet of Things 3(2) (2013) 8–15

[24] S-H. Cheng, C-Y. Huang, Coloring-Based Inter-WBAN Scheduling for Mobile Wireless Body Area Networks, IEEE transactions on parallel and distributed systems 24(2) (2013) 250–259

[25] D. He, C. Chen, S. Chan, J. Bu, P. Zhang, Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks, In IEEE Journal of Biomedical and Health Informatics 17(3) (2013) 664–674

[26] J. Elias, A. Jarray, J. Salazar, A. Karmouch, A. Mehaoua, A Reliable Design of Wireless Body Area Networks, IEEE Global Communications Conference (2013) 2742–2748

[27] H. Zhao, J. Qin, J. Hu, An Energy Efficient Key Management Scheme for Body Sensor Networks, In IEEE Journal of Transactions on Parallel and Distributed Systems 24(11) (2013) 2202–2210

[28] A. Ali, S. Irum, F. Kausar, F-A. Khan, A Cluster-Based Key Agreement Scheme Using Keyed Hashing for Body Area Networks, In Springer Science+Business Media Multimedia Tools and Applications 66(2) (2013) 201–214

[29] J. Pan, S. Li, Z. Xu, Security Mechanism for a Wireless-Sensor-Network-Based Healthcare Monitoring System, In IEEE IET Communications 6(18) (2012) 3274–3280

[30] R-T. Rajasekaran, V. Manjula, V. Kishore, T-M. Sridhar, C. Jayakumar, An Efficient and Secure Key Agreement Scheme Using Physiological Signals in Body Area Networks. In proceedings of the ACM International Conference on Advances in Computing, Communications and Informatics (2012) 1143–1147

[31] Z. Zhang, H. Wang, A-V. Vasilakos, H. Fang, ECG-Cryptography and Authentication in Body Area Networks, IEEE Transactions on Information Technology in Biomedecine 16(6) (2012) 1070–1078

[32] J. Liu, Z. Zhang, K-S. Kwak, R. Sun, An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks, In Proceedings of IEEE International Conference on Communications (2012) 3404–3408

[33] M. Mana, M. Feham, B-A. Bensaber, Trust Key Management Scheme for Wireless Body Area Networks, In International Journal of Network Security 12(2) (2011) 75–83

[34] M. Nabi, M. Geilen, T. Basten, MoBAN : A Configurable Mobility Model for Wireless Body Area Networks, In Proceedings of the 4th International ICST Conference on Simulation Tools and Techniques (2011) 168–177

[35] K-K. Venkatasubramanian, S-K-S. Gupta, Physiological Value Based Efficient Usable Security Solutions for Body Sensor Networks, In Journal of ACM Transactions on Sensor Networks 6(4) (2010) 31–65

[36] C. Cornelius, D. Kotz, On Usable Authentication for Wireless Body Area Networks, In proceedings of the first USENIX Workshop on Health Security and Privacy (2010)

[37] M. Quwaider, S. Biswas, Probabilistic Routing in On-body Sensor Networks with Postural Disconnections, In Proceeding of the 7th ACM international symposium on Mobility management and wireless access (2009) 149–158

[38] K-K. Venkatasubramanian, A. Banerjee, S-K-S. Gupta, EKG-based Key Agreement in Body Sensor Networks, In proceedings of IEEE INFOCOM Workshops (2008) 1–6

[39] C-C. Tan, H. Wang, S. Zhong, Q. Li, Body Sensor Network Security : An Identity-Based Cryptography Approach, In Proceedings of the first ACM Conference on Wireless Network Security (2008) 148–153

[40] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, SIAM Journal on Computing 38(1) (2008) 79–139

[41] W-R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy Efficient Communication Protocol for Wireless Microsensor Networks, In Proceedings of IEEE 33rd Annual Hawaii International Conference on System Sciences (2000) 8020–8029

[42] N-M. Radford, Markov chain sampling methods for Dirichlet process mixture models, Journal of computational and graphical statistics 9(2) (2000) 249–265

[43] C-B. Liem, T-M. Shih, T. Lu, The Splitting Extrapolation Method : a New Technique in Numerical Solution of Multidimensional Problems, In Series on Applied Mathematics, World Scientific (1995)