Cluster Computing (2022) 25:33–48
https://doi.org/10.1007/s10586-021-03326-z

Noise-based cyberattacks generating fake P300 waves in brain–computer interfaces

Enrique Tomás Martínez Beltrán[1] · Mario Quiles Pérez[1] · Sergio López Bernal[1] · Alberto Huertas Celdrán[2] · Gregorio Martínez Pérez[1]

Received: 5 March 2021 / Revised: 14 April 2021 / Accepted: 31 May 2021 / Published online: 10 July 2021

Abstract
Most of the current Brain–Computer Interfaces (BCIs) application scenarios use electroencephalographic signals (EEG) containing the subject's information. It means that if EEG were maliciously manipulated, the proper functioning of BCI frameworks could be at risk. Unfortunately, it happens in frameworks sensitive to noise-based cyberattacks, and more efforts are needed to measure the impact of these attacks. This work presents and analyzes the impact of four noise-based cyberattacks attempting to generate fake P300 waves in two different phases of a BCI framework. A set of experiments show that the greater the attacker's knowledge regarding the P300 waves, processes, and data of the BCI framework, the higher the attack impact. In this sense, the attacker with less knowledge impacts 1% in the acquisition phase and 4% in the processing phase, while the attacker with the most knowledge impacts 22% and 74%, respectively.

Keywords Brain–Computer Interfaces · Cybersecurity · Noise-based cyberattacks · Data Integrity · Electroencephalographic signal · P300

1 Introduction

Brain–Computer Interfaces (BCIs) present a bidirectional communication channel between the brain and external devices. The BCI life cycle is bidirectional since it can acquire neural activity produced by a subject and stimulate or inhibit neurons. Figure 1 depicts a reduced view of the full BCI cycle presented in our previous work [15] with the processes and communications performed in both directions. Since this work focuses on neural data acquisition (represented by the darker flow in Fig. 1), we will pay more attention in that direction. In this sense, the brain signals produced by the brain activity are acquired and processed by the BCI. Finally, it is transformed into a command that BCI applications can execute. Sometimes this command generates visual, auditory, or somatosensory feedback to the user, closing the loop. In the opposite direction, in gray in Fig. 1, neural stimulation is also possible to stimulate specific areas of the brain.

In the medical field, BCIs provide an alternative communication system that helps rehabilitation, improvement of motor skills, and control of robotic prostheses [3]. BCIs are also used to treat cognitive dysfunction [20], neurological disorders such as Amyotrophic Lateral Sclerosis, ALS [4], or even to identify and alleviate pain triggered by phantom limb syndrome [21]. Alternatively, these systems also permit the prediction of a seizure before it occurs, allowing patients to receive the necessary care [12]. In driving scenarios, there has also been increasing use of

✉ Enrique Tomás Martínez Beltrán
enriquetomas.martinezb@um.es

Mario Quiles Pérez
mario.quilesp@um.es

Sergio López Bernal
slopez@um.es

Alberto Huertas Celdrán
huertas@ifi.uzh.ch

Gregorio Martínez Pérez
gregorio@um.es

[1] Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, 30100 Murcia, Spain

[2] Communication Systems Group (CSG), Department of Informatics (IfI), University of Zürich UZH, 8050 Zurich, Switzerland

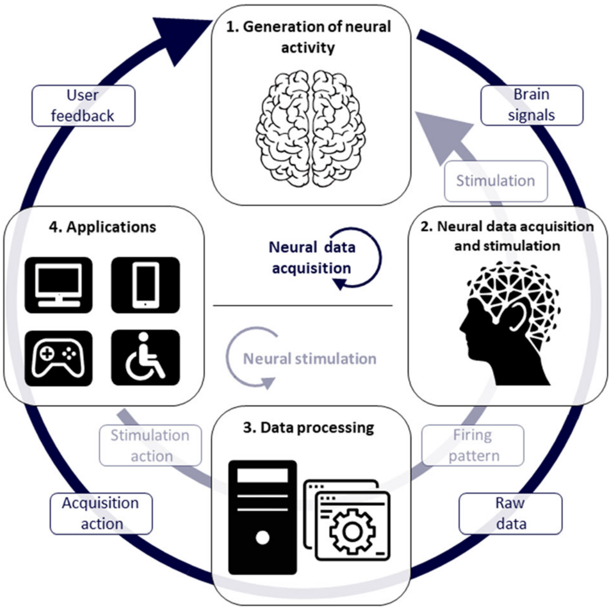


Fig. 1 Overview of the phases of the BCI cycle. Darker clockwise flow shows neural signal monitoring. Lighter counterclockwise flow indicates neural stimulation

these devices to detect drunkenness [28] or drowsiness [11] on the road. Both perspectives complement each other to promote optimal driving, reducing possible accidents. In other sectors such as entertainment, BCIs improve the interaction, immersion, and, in short, the gameplay experience of gamers [1]. BCIs have even reached the military sector, where BCIs are used in mental control of remote drones [2] or exoskeletons [5].

Most of the previous application scenarios use the electroencephalographic signal, EEG [18] and evoked potentials [7] as a means of obtaining neuronal information. Evoked potentials are signal patterns automatically generated by the brain when stimuli are presented to the individual. Depending on the kind of stimulus, there are different types of potentials: visual, auditory, somatosensory, or cognitive. The evoked potential P300 (or P3) [22] is one of the most studied and well-known for brain recording. This response originated by the brain carries an appreciable positive signal peak in the EEG signal at 250–500 ms after a stimulus is presented to the individual [22]. Different procedures can allow the P300 to appear in the EEG signal, like the Oddball Paradigm [8]. This paradigm consists of presenting a series of known stimuli, randomly shuffled, to a subject of which 10–20% are known or familiar. Visual and auditory stimuli can trigger the P300, but this work focuses on visual ones.

Among the existing evoked potentials, the P300 is one of the most widely used in end-use applications. This potential has the ability to represent sizeable neural information of the subject, making it a promising data source of information for the end device. For this reason, it is currently used for numerous applications such as controlling wheelchairs, military exoskeletons, and spellers. Despite the many benefits provided by the P300, the relevance and value of the neural data obtained increases the criticality in BCI devices. In recent years, numerous articles in the literature have focused on the lack of security measures in both BCI software and hardware. In this regard, some research has been published offering a cybersecurity perspective on BCI devices and the acquired EEG signal. More specifically, some authors detailed various cyberattacks targeting data confidentiality and user privacy [13, 17], while others focused on affecting the integrity of the EEG signal by attenuating evoked potentials [30].

In this context, despite the number of papers dealing with evoked potentials, more efforts are needed to measure the impact that cyberattacks have on them. More specifically, there is a lack of literature on how the integrity of data managed by BCI frameworks can be compromised. This weakness is complemented by a limited analysis of cyberattacks impact on the different phases of the BCI cycle. In this sense, this paper proposes a study of the impact of cyberattacks focused on maliciously generating P300 in the EEG signal to determine the impact on BCI devices and, consequently, on end applications. The research aims to show the real impact of cyberattacks that affect the integrity and the real concern for keeping devices secure in a world where BCIs are taking a relevant role in the way subjects communicate with the environment.

To improve some of the previous limitations, this work presents the following main contributions:

- The selection of four noise-based attack profiles with incremental knowledge to artificially generate P300 potentials within EEG signals. Therefore, the variation between profiles depends on the existing knowledge about the BCI device, aspects of the EEG signal, and the framework. More in detail, the first attacker knows the presence of wireless communication between the BCI headset and the BCI framework; the second knows theoretical concepts of the EEG signal and the P300 potential, such as its amplitude or generation interval; the third knows the same as the second and the nature and processing of the data exchanged; while the fourth knows the same as the third, plus the classification models used to detect the P300 and their predictions.
- The definition and deployment of a realistic scenario to execute the previous attacks and demonstrate their feasibility over two phases or processes of a BCI framework: EEG acquisition and processing. The proposed scenario considers a video containing images known and unknown to the subject. These visual stimuli generate a reaction in the subject's brain waves based

on the Oddball paradigm, whereby familiar visual stimuli (target) are presented within a set of unfamiliar ones (non-target). The scenario also considers a BCI headset to acquire the EEG and a framework that implements the BCI cycle (see Fig. 1) to obtain the EEG signals, process them, and detect the P300.

- The analysis of the impact of the four noise-based attack profiles affecting the proposed scenario. In this context, the obtained results demonstrated that higher knowledge about the BCI and the scenario increases the impact of noise-based cyberattacks. Likewise, it is shown that the AUC score of the best classifier detecting P300 is reduced the 1%, 3%, 12% and 22% attacking the acquisition phase and the 4%, 10%, 41%, and 74% when the data processing phase is affected by each one of the four profiles, respectively.

The remainder of the paper is structured as follows. Section 2 analyzes security issues in BCI devices and the most relevant works of the literature. It also reviews manuscripts focused on noise-based cyberattacks and their impacts. After that, Sect. 3 focuses on noise-based cyberattacks affecting BCI frameworks, describing the details of the proposed four attack profiles. Section 4 presents the design and implementation of a realistic scenario composed of a use case and a BCI framework. Subsequently, Sect. 5 details the experiments and impacts of the four noise-based attacks affecting the acquisition and processing phases of the BCI framework. Finally, Sect. 6 presents some conclusions and future work.

2 Related work

This section reviews the state-of-the-art concerning common cybersecurity issues in BCIs. After that, it analyzes works that use noise-based cyberattacks with the purpose of affecting the acquired EEG signal.

2.1 Cybersecurity issues in BCIs

Over the last years, different works have studied the cybersecurity implications of BCIs. However, these studies only focus on partial aspects, missing the whole range of cybersecurity issues. To address these limitations, López Bernal et al. [15] analyzed the current state of cybersecurity in BCI from the perspective of confidentiality, integrity, and availability of the exchanged information. Finally, the study included possible countermeasures for the reviewed attacks.

Further studies have classified cyberattacks according to the type of application scenario: medical applications, entertainment, authentication, and smartphone-based applications. In this sense, Li and Conti [14] detailed that attackers can generate illicit commands and achieve malfunctioning of prostheses or create incorrect actions. On the other hand, they highlight the generation of patterns in the EEG signal to breach authentication systems. Rushanan et al. [25] focused on cybersecurity issues in the first and last phases of the BCI cycle (see Fig. 1). The authors demonstrated that communication with the BCI and with end applications can be captured or eavesdropped on, in some cases even modifying the transmitted data.

BCI devices based on EEG have gained popularity in recent years due to their versatility and low cost, making them an attractive target for potential cyberattacks. One of the uses of these technologies is to acquire neural information from stimuli. In this context, Martinovic et al. [17] performed some experiments to steal critical information from the subject, such as the 4-digit PIN code, banking information, and even the person’s place of residence. The authors used a commercial BCI, the Emotiv EPOC headset, and sampled visual stimuli for 250 ms with a 2-s interval between images. Lange et al. [13] expanded Martinovic’s research with the total or partial recovery of the proposed PIN code, adding different scenarios that vulnerate the individual’s privacy. Similarly, Rosenfeld [24] reaffirmed the concern with information extraction and presented applications in forensic and counter-terrorism scenarios. Other attacks, performed by Frank et al. [6], reduce the intervals between visual stimuli by making them subliminal.

The literature has also studied the impact of cyberattacks on the processing phase of the BCI cycle. Most BCI devices have a classification module that is responsible for interpreting the acquired signal. Therefore, these attacks corrupt the models with adversarial samples, causing a significant impact on BCI and actions intended by the user. In this sense, Zhang and Wu [29] defined an unsupervised fast gradient sign method (UFGSM) to attack three popular convolutional neural networks (CNN) in BCI, demonstrating its effectiveness. In other cases, the density and high frequency of the EEG signal make it challenging to process the signal locally. Juhasz [10] discussed the possibility of migrating local clusters to a cloud infrastructure, significantly reducing execution time and ensuring data security.

2.2 Noise-based cyberattacks

Other works in the literature study cyberattacks affecting the integrity and availability of transmitted data. More specifically, cyberattacks have been designed to directly affect the signal captured in the acquisition or processing phases of the BCI cycle. These threats aim to hide segments of neural signal, primarily associated with Event-

Related Potentials (ERPs). In other cases, they are intended to encourage the attacker to generate them deliberately. These data alterations constitute a significant problem in many application scenarios.

In EEG devices, the problems are increased by acquiring a signal that is very susceptible to noise. Therefore, cyberattacks use the technique of noise generation to impact the acquired data. In this context, Zhang et al. [30] deployed an EEG-based speller system using P300. The authors generate adversarial perturbations that are too small to be perceived when added to EEG signals but can induce the system to spell anything the attacker wants. Likewise, they only consider a white-box scenario where the attacker knows everything about the model used, adjusting the parameters to the scenario deployed. Despite being the first work demonstrating the impact of noise on decision making, these attacks are limited only to affecting the P300 and not enabling its generation in specific EEG segments. Other studies, such as the one performed by Jiang et al. [9], considered transferability-based black-box attacks. To achieve this purpose, the attacker trained a model to replicate the legitimate model. Subsequently, it generated adversarial examples by employing dynamic noise mechanisms with the trained model, using them to attack the legitimate model. On the contrary, Meng et al. [19] considered white-box attacks for regression problems where all information about the learning algorithm is known. This assumption makes it possible to generate perturbations to the input EEG signal to vary the result by a specific amount. Also, the authors considered the transferability of the procedure to black-box scenarios where the models are unknown.

3 Noise-based cyberattacks to generate fake P300 in BCI frameworks

This section presents four different attack profiles that use noise-based cyberattacks to affect the detection of P300 waves by BCI framework detecting P300. The selection of four profiles is determined by the number of phases of the implemented BCI cycle: neural activity generation, EEG signal acquisition, processing, and P300 detection. The proposed cyberattacks aim to generate false P300 in EEG signals that were previously absent. This procedure is performed in two phases of the BCI cycle: acquisition and processing. However, these are not the only types of threats focused on breaching data integrity. There are other modalities of noise-based cyberattacks in the literature, where instead of artificially generating signals, the threat causes an attenuation or removal of P300 in the EEG signal [30]. These attacks are beyond the scope of this article, although it is a good starting point for future work.

The profiles of the study are incrementally ordered based on the knowledge that the attacker has about the BCI framework and the application scenario. This incremental knowledge implies that a particular profile presents the characteristics and functionalities of the previous ones, leading to more robust attack techniques to breach the BCI framework. Figure 2 summarizes the characteristics of each attacker profile graphically, showing in darker color the data, processes, and background that the attacker knows. Thus, the attacker profiles have knowledge associated with the four phases of the BCI cycle implemented in this work.

3.1 First profile: the attacker knows the existence of a wireless communication

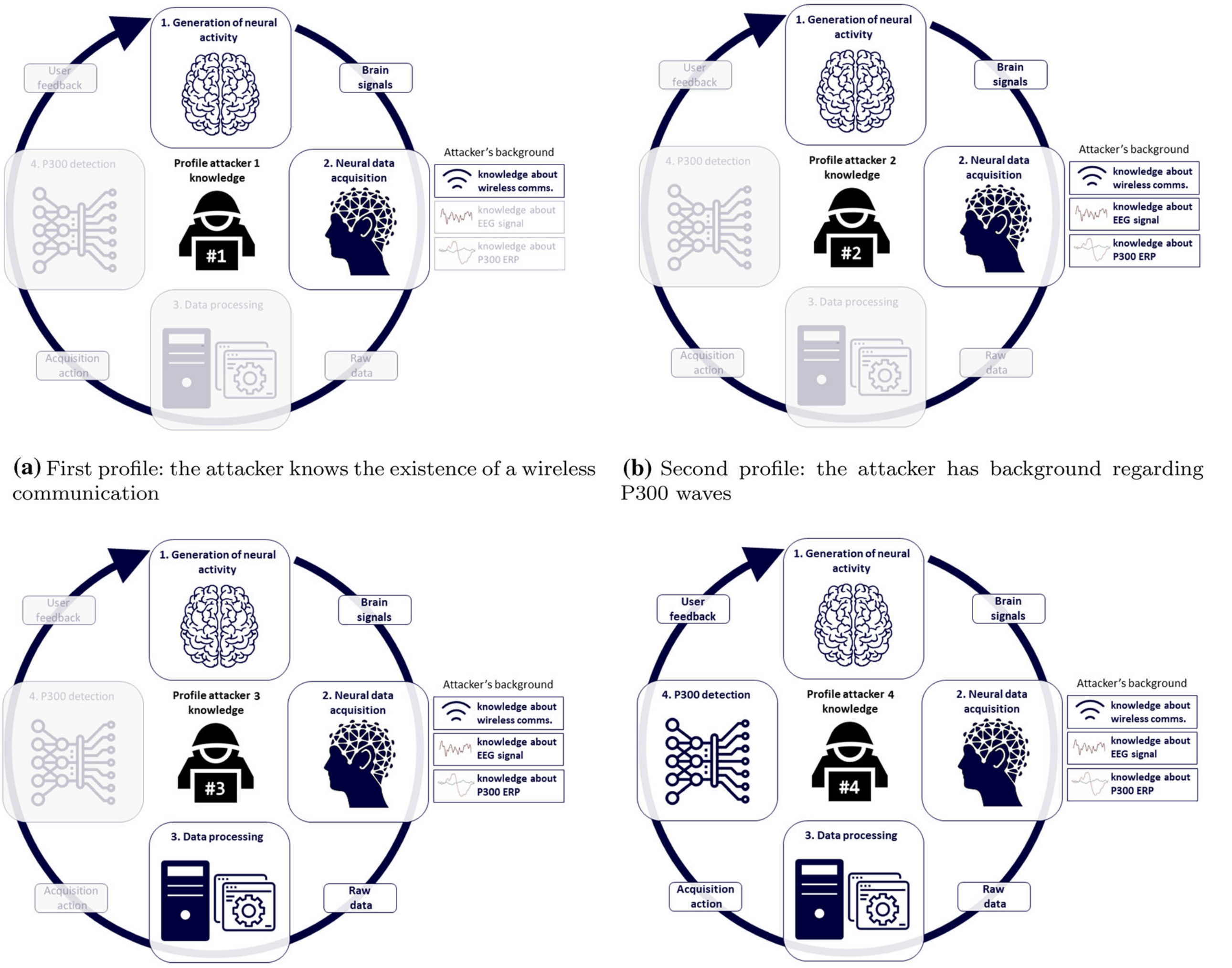
In this profile, the attacker is aware of the wireless communication between the BCI headset and the BCI framework. However, he/she does not know the data exchanged, the phases of the BCI cycle implemented by the BCI framework (detailed in Sect. 1), the format of the data transmitted by the BCI headset, nor the information storage structures implemented by the framework. Likewise, the attacker does not have the necessary knowledge to understand the EEG signals or P300 generation to make a precise attack. Figure 2a shows the attacker's knowledge regarding the BCI framework phases and exchanging data, as well as his/her background regarding EEG and P300.

Based on the previous assumption, the attacker generates a series of random noises. This noise belongs to a given range determined by the attacker, pseudo-randomly applied during the wireless data communication between the BCI headset and the BCI framework.

3.2 Second profile: the attacker has background regarding P300 waves

This attacker has some knowledge of the BCI framework used in the scenario. In particular, he/she knows the most common mechanisms for acquiring brain signals (phase 1 of Fig. 2b) and the weaknesses of each one. The EEG weakness is the high sensitivity to external noise and the need to process the data to obtain relevant information (see Sect. 2.2). Similarly, the attacker knows about P300 general information and the techniques to favor their generation or attenuation (latency, polarity, amplitude, or the stimuli that trigger it).

According to the previous information, the attacker generates a noise template with a shape similar to a P300 potential or pseudo-random noise to disrupt the detection of a P300 potential. The different noises are randomly applied to the EEG signal during the acquisition and processing phases of the BCI framework.


1. Generation of neural activity
Brain signals
2. Neural data acquisition
Raw data
3. Data processing
Acquisition action
4. P300 detection
User feedback
Profile attacker 1 knowledge
#1
Profile attacker 2 knowledge
#2
Profile attacker 3 knowledge
#3
Profile attacker 4 knowledge
#4
Attacker's background
knowledge about wireless comms.
knowledge about EEG signal
knowledge about P300 ERP

(a) First profile: the attacker knows the existence of a wireless communication

(b) Second profile: the attacker has background regarding P300 waves

(c) Third profile: the attacker has knowledge about the BCI framework and P300 waves

(d) Fourth profile: the attacker knows not only the same as the third, but also the P300 detection model details and outputs

Fig. 2 Attacker profiles. Each sub-figure represents a different attacker profile: the components in red describe the data, processes and background that the attacker knows

3.3 Third profile: the attacker has knowledge about the BCI framework and P300 wave

This attacker is aware of the details of the data acquisition and processing phases of the BCI framework. On the one hand, he/she knows the data transmitted between the BCI headset and the BCI framework. Specifically, the attacker has permanent access to the voltage measured by each electrode of the BCI headset. Thus, he/she is aware of the BCI sampling frequency and the positions of the scalp where the electrodes of the headset are located. On the other hand, this attacker knows the processing techniques applied to the signal data (more details in Sect. 4.2). It means that the noise-based cyberattack can target the frequencies not filtered by the band-pass filters (3–17 Hz in the case of P300 processing). He/she is also aware of the rejection parameters based on the peak-to-peak amplitude applied at each electrode. Therefore, the attacker can generate noise with dynamic amplitude adapted to the previous voltage value. Figure 2c shows the attacker's knowledge (in darker color), as well as the unknown aspects (in lighter color).

According to the previous assumptions, the attacker can generate dynamic noise, varying its characteristics according to the data acquired by the BCI. This attacker has greater control over the BCI operation, modifying exactly those data that he/she considers relevant to the attack. In the case of the P300, the modification is intended to affect the data of the different epochs to generate P300 waves, affecting external applications that use this ERP as a transmitter of neural information. In short, the attacker attempts to breach the BCI by adapting the cyberattack conditions to the acquisition and processing phases of the BCI framework.

3.4 Fourth profile: the attacker knows not only the same as the third, but also the P300 detection model details and outputs

The last attacker knows the whole BCI framework, including its implementation and data exchanged by each phase. The main difference compared to the previous attacker is the knowledge about the machine or deep learning-based classification module details able to detect P300 waves, detailed in Sect. 4.3. This attacker knows the models output, so he/she can adapt the cyberattack according to this value obtained during the evaluation. In other words, the attacker applies noise on the EEG signal and, depending on the model's output, adapts the attack for successive evaluations (see Fig. 2d).

In this case, noise generation is based on the automatic creation of templates depending on how well the model fits the data. The use of noise templates can address some issues: (1) adapting the noise to the deployed scenario, regardless of the functionality being performed and (2) adapting the noise to the external or physiological conditions of the user, e.g., a patient manifesting a higher latency on the P300 due to ALS.

4 Scenario setup

This section details the scenario deployed to obtain EEG signals and detect P300 potentials. The scenario is divided into three components: (1) a monitor where visual stimuli are presented to the subject following the Oddball paradigm, (2) a non-invasive BCI headset to acquire the EEG signal while the subject visualizes the stimuli, and (3) a BCI framework that obtains the EEG signal, synchronizes it with the visual stimuli displayed on the monitor and processes the data to detect P300 potentials.

4.1 Use case

The proposed use case aims to present visual stimuli to a subject, which are part of a video, and generate P300 potentials. The Oddball paradigm has been employed to trigger the generation of this evoked potential. A set of images has been selected, where 20% of them were familiar to the user (target images), and the rest were unfamiliar (non-target images). The experiment begins with 30 s for baseline EEG activity. Then, visual stimuli are randomly displayed on the screen with a 0.250 s interval between them (see Fig. 3). The experiment ends when all images in the initial set are displayed to the user. Table 1 includes all the parameters used in the deployment of the framework and used during the experiments.

The experiments have been applied to two different subjects with similar physical characteristics. They were 22 and 23 years old, respectively, both approximately 1.80 m tall and with no cognitive or neurological problems. The posture maintained during the experiment was perpendicular to the floor, with the monitor in front of the subject's eyes, avoiding involuntary movements and, therefore, additional noise to the EEG signal. Besides, the project official repository [16] contains the necessary scripts for the deployment of the scenario and the guidelines for its customization.

4.2 EEG acquisition and processing

The acquisition phase is the process by which the BCI framework obtains the neural activity generated by the user's brain. This study performs EEG acquisition using a non-invasive BCI, OpenBCI Ultracortex Mark IV EEG Headset [27]. During monitoring, eight electrodes (Fp1, Fp2, C3, C4, P7, P8, O1, O2) are used. The electrodes are distributed according to the international 10-20 system [23], while the sampling frequency of the recording process is 250 Hz. Simultaneously, there is a synchronization of the visual stimuli displayed to the user and the monitored signal. This timing adjustment is essential to determine the generated waveform concerning the displayed target image.

Acquired EEG signals may be altered by noise caused by some artifacts such as blinking, muscle movements, eye movements, or breathing. Noise can have an impact on BCI performance by overloading it with extra data. For this reason, the data is processed before continuing in the BCI cycle. First of all, the signal is downsampled with ratio 5, modifying from having 250 samples every second (250 Hz) to 50 samples every second (50 Hz). Afterward, a Notch filter is applied using the FIR superposition-addition method with zero phase. This filter attenuates the frequency at 50 Hz and multiples thereof due to the noise caused by the electrical wiring of the BCI system in Europe. After removing the specific frequency, EEG data is band-pass filtered with the eighth-order Butterworth filter in the

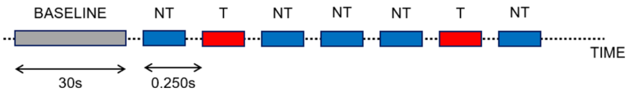


Fig. 3 Time distribution of the presentation of different visual stimuli. The symbol "T" denotes a target image, while "NT" denotes a non-target image

Table 1 Parameters used in the experiment

Experiment parameter	Value
External monitor size	1920 × 1080
Separation between individual and monitor	60 cm
Number of images	180
% Target images	20
% Non-target images	80
Interval time between images	0.250 s
Variable jitter time	0.2
Initial baseline	30 s

frequency range between 3 and 17 Hz to remove other high frequency noises. The objective is to keep frequencies within the specified frequency range and reject the rest. Finally, Independent Component Analysis (ICA) is employed in the processing, a powerful technique to reduce noise by separating independent linearly mixed sources on multiple electrodes. At the end of the processing phase, the EEG signal is divided into epochs, EEG segments classified according to the eventuality produced. Each epoch starts 0.1 s before the event occurs and 0.8 s after. The segments corresponding to target events are assigned a label with a value of "2", and non-target events are assigned a value of "1". Figure 4 shows a set of epochs of the scenario and the EEG signal segments corresponding to each electrode. The epochs are associated with an event identifier as previously discussed, "1" for target and "2" for non-target. The green vertical lines mark the beginning of the event.

4.3 P300 detection

The last phase of the implemented BCI framework aims to detect the P300 waves in the captured and processed EEG signal. For this purpose, the BCI framework implemented uses classifiers, which are elements belonging to supervised learning that attempt to predict the outcome based on trained models.

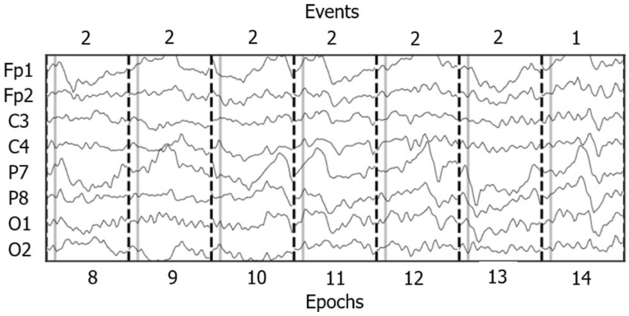


Fig. 4 Set of epochs of the labelled EEG signal

The framework uses the following classifiers for the detection of P300 potentials: *Classifier I*, employing scalar standardization algorithms and regressions; *Classifier II*, consisting in a model with a linear decision boundary, generated by fitting conditional class densities to the data and using Bayes' rule; *Classifier III*, the same operation as classifier II but adding xDAWN as spatial filter; *Classifier IV*, estimation of the covariance matrix of the possible potentials, spatial projection of the tangent and regressions; and *Classifier V*, with an estimation of the covariance matrix and classification by Minimum Distance to Mean.

Before training the classification models, EEG signal activity is analyzed to check the quality of the data obtained in the previous phase. Figure 5 shows the brain activity at six different instants, using the average of all the eventualities produced during target image visualization. During the first second, when the visual stimulus is displayed, brain activity is observed in the occipital area related to the processing of visual stimuli (first representation of Fig. 5). However, the brain activity increases considerably at around 217 ms, followed by a decrease in this activity to negative values in an interval of 90 ms. As the literature states, increased electrical activity occurs in the occipital area when the P300 is generated [26]. Likewise, it describes the P300 as a voltage decrease in the signal, which can reach negative values (second representation in Fig. 5), then increases the voltage to a peak of 20–40 µV (third representation) and finally, a slight decrease in voltage (fourth representation) [22]. Finally, in the fifth and sixth representations, the brain activity does not show characteristic patterns concerning neutral areas of the brain.

Once the brain activity is related to the possible P300, the classifiers are trained with each of the labeled segments obtained in the previous phase. The data is manually split into two different sets: training data and test data, with proportions of 75% and 25%, respectively. Cross-validation and stratified validation process (due to the unbalanced nature of the dataset) have been applied to the training dataset. The implemented strategy, *StratifiedShuffleSplit*, allows 10 partitions of the input data, generating ten different combinations. Each combination is split into two datasets again: training data and test data, with the same proportions as the previous subset. While the first ones are used to train the classifiers, the second ones are used to evaluate the accuracy of the given predictions. Using cross-

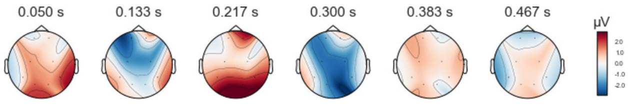


Fig. 5 Brain activity with the average of values captured during the display of the target

validation detects a situation of *overfitting* when the trained model does not generalize well with new test data.

4.4 Noise generation

This subsection presents the noise generation procedure used by attackers and the mathematical considerations of the concepts necessary to generate them.

The main objective of noise generation is to alter the original EEG signal. This technique must use noises of different signal-to-noise ratios to evaluate the P300 classifier performance under various noisy conditions. The signal-to-noise ratio (SNR) can be defined as follows:

$$SNR = 10\log_{10}\left(\frac{RMS^2_{signal}}{RMS^2_{noise}}\right), \quad (1)$$

where RMS_{signal} is the Root Mean Square (RMS) value of the signal and RMS_{noise} is the RMS value of the noise.

Noise generation, based on random signals, is created through a basic noise model called *Additive White Gaussian Noise* (*AWGN*). Firstly, it is additive, so the generated noise is added to the signal. Secondly, the noise has the same power distribution at each frequency, being the power spectral density constant. Finally, it is Gaussian in that it uses a mathematical model to calculate the probability of the generated events.

The AWGN model adds a zero-mean Gaussian random variable to its original signal. The variance of that random variable will affect the average noise power. For a Gaussian random variable X, the average power is

$$E[X^2] = \mu^2 + \sigma^2. \quad (2)$$

In white noise generation $\mu = 0$, so the average power is then equal to the σ^2 variance. All in all, AWGN implementation can be performed in two different ways: (1) calculating the variance as a function of the signal-to-noise ratio (SNR) or (2) selecting a specific noise power and applying it to the EEG signal. In this work, the second way is implemented. Table 2 compares the different noise generations used in this work, being each noise type differentiated by the RMS noise level (dB) and by the dynamism in its application in the EEG signal.

5 Results and discussion

This section summarizes the results of applying noise-based cyberattacks on the EEG for each of the attacker profiles defined in Sect. 3. These cyberattacks affect two different phases of the BCI cycle: (1) acquisition phase, where the noise is applied during the acquisition of the brain waves by the electrodes placed on the scalp, and (2) processing phase, in which the noise is applied once the data is in the BCI framework and has been processed by the third phase. Figure 8 shows the cyberattacks performed by each profile for the same EEG signal segment and it provides a visual comparison between the attack techniques and the resulting impact on the signal.

In order to perform the attacks, several considerations have to be taken into account. On the one hand, the physical (analog) noise used to attack this phase is simulated digitally on the acquired signal. Therefore, a similar impact is obtained without using additional equipment for noise generation. On the other hand, the application of noise in the processing phase represents malware affecting the BCI framework, which generates an impact on the data exchanged between phases three and four of the BCI framework. The malware behaves similarly to the physical attack in order to establish a comparison between attacker profiles.

The attack profiles described in the following subsections share the same noise generation techniques described in Sect. 4.4. Despite generating both noise behaviors (physical and malware) with the same techniques, they vary in time and manner depending on the attacker's knowledge of the framework, adapting and focusing the noise generation target on provoking the appearance of the P300, thus increasing the overall impact to the proposed framework.

The impact generated by each attack profile is measured from the BCI framework. In particular, the framework uses the classifiers described in Sect. 4.3 to provide an aggregated metric of performance attack using the Area Under the Curve (AUC) metric. Since the attacks' goal is to generate P300 waves in the EEG signal that does not contain them, the AUC value is obtained by evaluating only non-target epochs of the EEG. Finally, a relationship is established between the metrics obtained by affecting the legitimate signal by noise and the attacker's knowledge.

Table 2 Features of the noise generated

Type of noise	Power level	RMS noise level (dB)
Gaussian with static range	Low	≈ 0.8
Gaussian with static range	High	≈ 5
Gaussian with dynamic range	Adaptive	Variation within the range 0.8 to 5

5.1 Legitimate EEG signal

This section describes the EEG signal acquired during the study without the disturbance caused by noise-based cyberattacks. Figure 6 shows a fragment of the legitimate EEG signal during the acquisition phase darker (in blue) and after the processing phase lighter (in orange). More specifically, the figure represents a 10-s segment of the EEG signal captured during the study. While the unprocessed EEG signal shows a usual noise caused by some artifacts, the processed signal provides more information by narrowing the frequency of brain waves and reducing noise with processing techniques. In addition, the figure presents the beginning of each epoch with its corresponding label according to the type of event produced (target or non-target image).

Subsequently, the processed EEG signal is fed into the trained classifiers of the P300 detection phase. Figure 7 shows the AUC values obtained by the five classifiers used in this work. As can be seen, the framework can classify approximately the 50–80% of non-target epochs. Among all the classifiers, classifiers I and V (with AUC values of 0.746 and 0.792, respectively) stand out as the most promising.

5.2 First attacker profile

The first attacker generates two different types of noise: (1) Gaussian noise with static range 0.8 dB and (2) Gaussian noise with static range 5 dB (see rectangular figure with grey color in Fig. 8a). The attacker only knows the wireless communication that occurs, so the objective is to alter the signal in the acquisition phase. The generation of the noises is prolonged during the whole acquisition phase, where both noises are interspersed with an interval of 2–3 s. Likewise, the attack is aimed at all BCI channels, applying the same amount and interval of noise to all of them. Besides, Fig. 8a includes cross and tick marks to indicate whether the applied noise is detected as P300 by the best performing classifier.

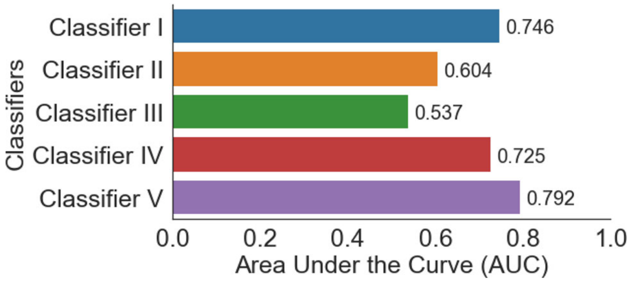


Fig. 7 AUC values obtained by classifier when evaluating non-target using a legitimate EEG signal

Table 3 shows the AUC values for each classifier and noise behavior. The results obtained in Table 3 and the following tables are the product of evaluating only the non-target epochs of the EEG signal, as previously discussed at the beginning of Sect. 5. Thus, the AUC values determine the impact of the attacks to generate P300 waves and, consequently, epochs labeled as target. From the results obtained, it can be concluded that both malware noise and physical noise obtain a similar reduction of AUC values concerning the legitimate EEG signal. These results are due to both noises are applied arbitrarily throughout the EEG signal. The noise application affects a set of random samples unknown to the attacker, spreading the attack over the entire acquired EEG signal without any adaptation. Therefore, the noise does not consider the EEG signal acquisition parameters, such as sampling frequency, epochs division, or the P300 wave characteristics. This procedure causes both non-target and target epochs to be affected by the noise, with the non-target epochs finally being evaluated by the classifiers. The AUC values obtained indicate

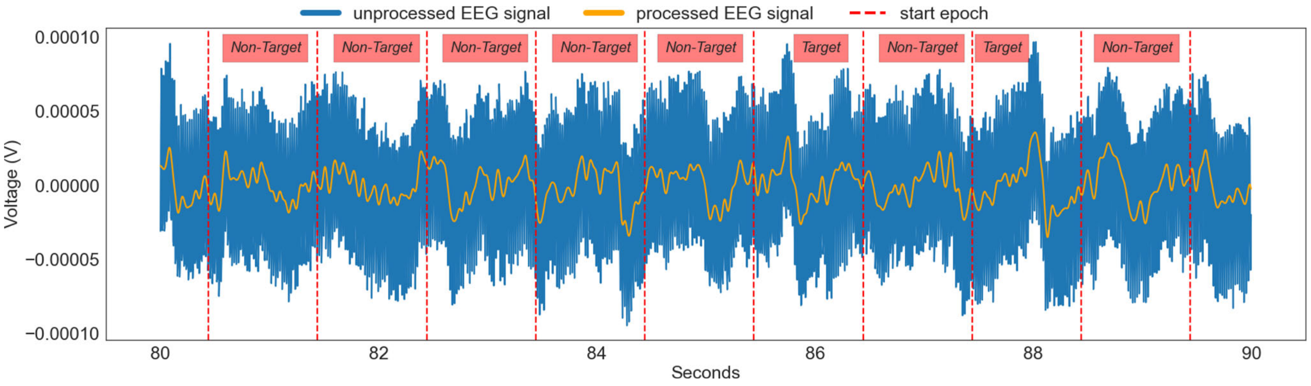
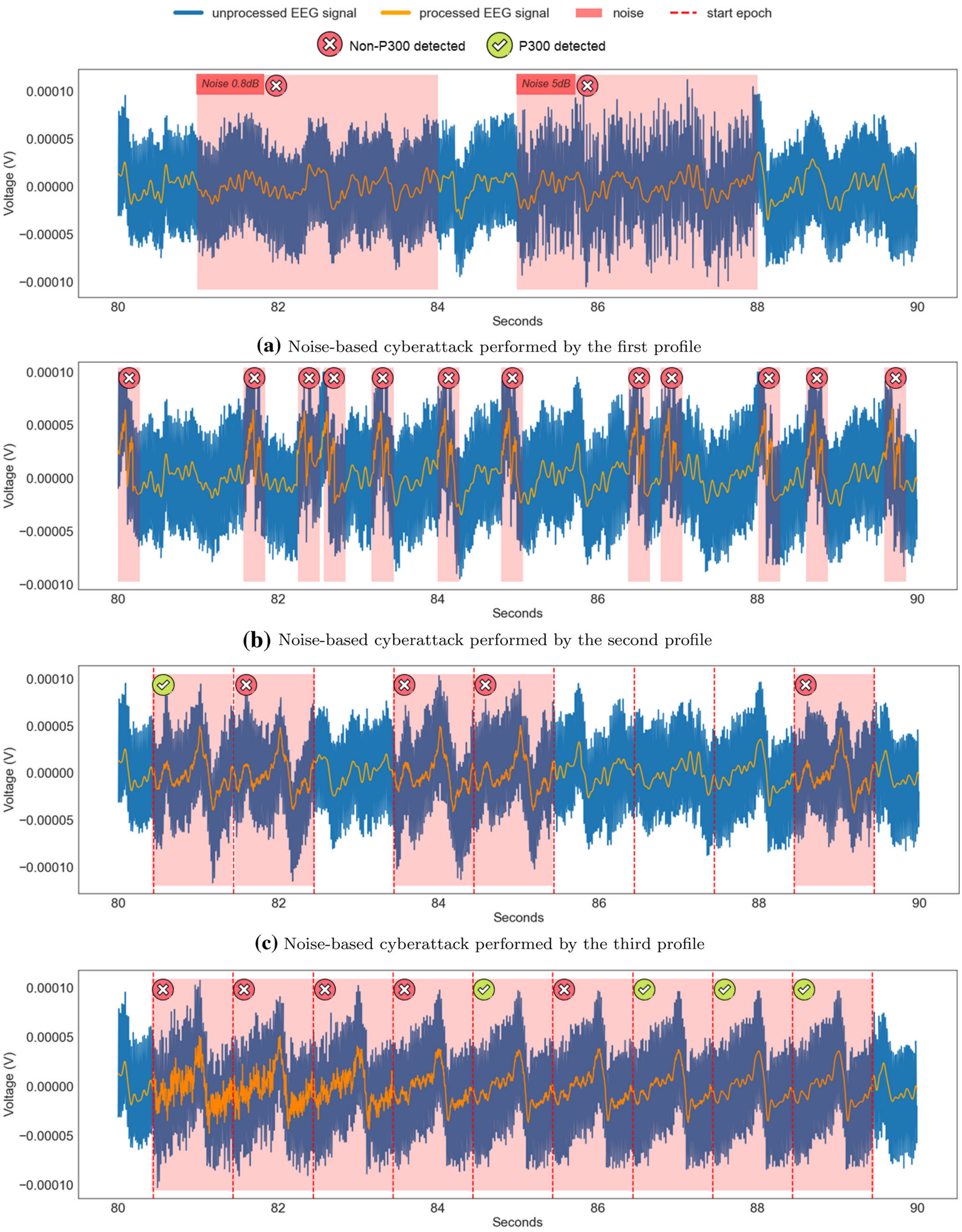


Fig. 6 Legitimate EEG signal (Color figure online)



(a) Noise-based cyberattack performed by the first profile

(b) Noise-based cyberattack performed by the second profile

(c) Noise-based cyberattack performed by the third profile

(d) Noise-based cyberattack performed by the fourth profile

◀**Fig. 8** Impact of noise-based cyberattacks on the EEG signal depending on the attacker profile

that the attack was not sufficient to trigger the generation of P300 in the EEG signal.

5.3 Second attacker profile

The second attacker generates specific noises based on the P300 wave. Therefore, it generates noises following the characteristics and behavior of the P300, consisting of (1) variable increment of the noise at the beginning of the attack in the first 100 to 300 ms, trying that the EEG signal is not in negative values, (2) a decrease of the noise, aiming that the signal can reach negative voltage values close to zero, (3) an increment of the noise pretending that the signal reaches 20–40 µV, and (4) a decrease of the variable noise between generations (see rectangular figure with grey color in Fig. 8b).

This attacker profile presents a slight decrease of the AUC values for all classifiers (see Table 4) compared to those obtained with the legitimate signal. This generalized decrease is due to not using long fragments with noise and accentuating them in specific areas of the EEG signal. Although the noise is generated by simulating the P300 wave, the attacker does not know the acquisition phase variables, such as the sampling frequency, the voltage range, or the synchronization with the stimuli.

5.4 Third attacker profile

The third attacker performs a process similar to the previous profile. The main difference is that now the attacker generates the noise in the EEG signal segments affecting different epochs individually (see Fig. 8c). It negatively impacts the classifiers by generating more specific noise in those EEG segments where a non-target event occurs. Figure 8c shows an example of that, where a classifier predicts the non-existence of P300 in the five epochs attacked, except for the first one. The goal of the attacker is to alter the EEG signal segment relative to the non-target event and generate a P300 wave. Noise generation involves monitoring the transmitted data and, more specifically, the voltage measured by each electrode. Once the information is known, the attacker generates noise similar to the P300 wave but with the frequency and amplitude adapted to the rest of the EEG signal. Besides, it limits the noise power

Table 3 AUC values by classifier and noise behavior in the first attacker profile

Noise behavior				
	#1	Physical noise	Malware noise	Legitimate signal
Classifiers	Classifier I	0.738	0.721	0.746
	Classifier II	0.587	0.583	0.604
	Classifier III	0.536	0.525	0.537
	Classifier IV	0.716	0.701	0.725
	Classifier V	0.783	0.759	0.792

Table 4 AUC values by classifier and noise behavior in the second attacker profile

Noise behavior				
	#2	Physical noise	Malware noise	Legitimate signal
Classifiers	Classifier I	0.737	0.701	0.746
	Classifier II	0.587	0.581	0.604
	Classifier III	0.521	0.517	0.537
	Classifier IV	0.718	0.689	0.725
	Classifier V	0.774	0.710	0.792

Table 5 AUC values by classifier and noise behavior in the third attacker profile

Noise behavior				
	#3	Physical noise	Malware noise	Legitimate signal
Classifier	Classifier I	0.678	0.445	0.746
	Classifier II	0.489	0.412	0.604
	Classifier III	0.501	0.313	0.537
	Classifier IV	0.679	0.389	0.725
	Classifier V	0.695	0.468	0.792

level, adapting the signal to the processing phase parameters. Likewise, both the physical noise and the malware noise are generated on the O1 and O2 electrodes (placed in the occipital region of the brain) since the attacker knows the voltages of each scalp electrode and which ones are involved in the generation of the P300 through visual stimuli.

Table 5 shows the AUC values obtained in each noise-based cyberattack. In this attacker profile, substantial changes are observed concerning the AUC values obtained in the legitimate signal, particularly malware noise. Contrary to the previous profiles, the knowledge of EEG signal processing and synchronization regarding the displayed stimuli generates a beneficial environment for the attacker. Similarly, the noise is generated without exceeding the artifact rejection of the framework, thus avoiding a voltage reduction in the generated P300 wave. This conclusion has its representation in (1) 6–12% decrease in AUC values with physical noise and (2) 35–40% decrease with malware noise, both concerning the legitimate signal.

5.5 Fourth attacker profile

The fourth profile focuses on attacking the acquisition and processing phases of the BCI cycle but having information about the classifier and its predictions. This type of attack has similarities with adversarial attacks on machines and deep learning in the literature, such as FGSM (Fast Gradient Signed Method). The difference concerning FGSM is that the latter needs to calculate the gradients using modifications to the epsilon, while the proposed attack uses the P300 features to apply it in the form of adaptive noise to the EEG signal. The objective is to modify the EEG signal, maximizing the probability that the classifiers predict P300. Figure 8d shows the noise adaptation along the EEG signal. While the classifiers initially predict the modification of the epochs as Non-P300, the continuous noise adaptation leads to the generation of the P300 in the EEG signal (fifth epoch in the figure). Noise adaptation is continuous until all epochs are classified as P300 (seventh epoch forward). In short, the attacker uses the feedback received by the classifiers to refine the generated noise, decreasing the impact of the attack and enhancing the generation of the P300.

Table 6 AUC values by classifier and noise behavior in the fourth attacker profile

Noise behavior				
	#4	Physical noise	Malware noise	Legitimate signal
Classifiers	Classifier I	0.603	0.201	0.746
	Classifier II	0.441	0.112	0.604
	Classifier III	0.467	0.104	0.537
	Classifier IV	0.621	0.155	0.725
	Classifier V	0.618	0.212	0.792

Table 7 AUC values of classifier V by attacker profile and noise behavior

Noise behavior			
		Physical noise	Malware noise
Attacker profiles	Profile I	0.783	0.759
	Profile II	0.774	0.710
	Profile III	0.695	0.468
	Profile IV	0.618	0.212

The AUC values obtained in this profile (see Table 6) are the lowest in the study, including those obtained by the previous profiles and the legitimate signal. These values comprise all the attack vectors performed, including the learning period to generate the ideal noise to favor the generation of the P300. This approach results in AUC values greater than zero. When the classifier detects mostly P300 with a specific noise template, it is applied in successive attacks. Therefore, the classifier is always fooled, which means that the attack can generate a P300 where there was not is most of the time. While the AUC values obtained with the physical noise have decreased by 20–28% concerning the legitimate signal, those of the malware noise have decreased by a more significant proportion, obtaining values between 0.104 and 0.212.

Finally, Table 7 compares the AUC values obtained by Classifier V, the one with the best prediction performance with the legitimate signal (see Fig. 7), according to the noise behavior and the attacker profile. On the one hand, the values demonstrate the slight progressive decrease of the AUC with physical noise in the different profile attacks. The decrease is between 1 and 22% concerning the legitimate signal, being 1% for the first profile and 22% for the fourth profile. On the other hand, the AUC values of the malware noise lead to a quantitative jump of decrease between the second and third profiles, being 34% less, and between third and fourth profiles, being 55% less. Similarly, the application of malware noise in the fourth profile has an impact of 74% in contrast with those obtained in the legitimate signal. Therefore, the application of malware noise in the processing phase by the fourth attacker profile has the most significant impact on the AUC, which translates into a high generation of P300 potentials in the EEG signal.

6 Conclusion

This work presents four incremental attacker profiles that generate noise-based cyberattacks affecting intelligent BCI frameworks that detect P300 waves. The first profile knows about wireless communication between the BCI headset and the BCI framework. The second has information about P300 waves. The third knows the BCI framework, and the fourth one also knows about P300 detection model details and outputs. For each profile, two types of noise are considered: (1) physical, affecting the EEG signal acquisition phase of BCI frameworks, and (2) malware-based, impacting the processing phase. To measure the impact of the attacks we have deployed a realistic scenario for EEG signal acquisition composed of (1) a video showing known and unknown visual stimuli, (2) a non-invasive BCI headset, and (3) a BCI framework implementing the acquisition, processing and P300 detection phases of the BCI life cycle. The performed experiments have demonstrated that increased knowledge about the BCI cycle allows an attacker to perform more sophisticated attacks to generate P300 waves. Likewise, we have observed attacks affecting the processing phase have a more significant impact on the generation of the P300. In particular, the AUC score of the best classifier detecting P300 is reduced the 1%, 3%, 12%, and 22% attacking the acquisition phase, and the 4%, 10%, 41%, and 74% when the data processing phase is affected by each one of the four profiles, respectively.

As future work, we plan to study the impact of new techniques and targets of noise application, creating new attack vectors. Likewise, the materialization of different attack vectors may give rise to new attacker profiles with a different impact than those described in this work. One of the future lines could delve into an attacker profile focused on the BCI hardware, at a lower level of abstraction or from the perspective of brain stimulation. It would be interesting to compare the profiles and determine the impact or criticality originated in future research. In the same way, we consider a study with a more significant number of labeled EEG signal samples for classifiers training, as well as more sophisticated algorithms to detect the P300. Finally, we propose to use a larger number of electrodes in EEG signal monitoring since interpolation could reduce the impact of these cyberattacks.

Author Contributions Conceptualization: ETMB and MQP; Methodology: ETMB; Software: ETMB; Validation: ETMB, SLB and AHC; Formal analysis: ETMB and SLB; Investigation: ETMB and MQP; Resources: AHC and GMP; Data curation: ETMB and MQP; Writing—original draft preparation: ETMB; Writing—review and editing: ETMB, MQP, AHC, SLB and GMP; Visualization: ETMB and MQP; Supervision: AHC and GMP; Project

administration: GMP. All authors have read and agreed to the published version of the manuscript.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. This work has been partially supported by (a) Bit and Brain Technologies S.L. under the Project CyberBrain: Cybersecurity in BCI for Advanced Driver Assistance, associated with the University of Murcia (Spain), (b) the Swiss Federal Office for Defense Procurement (armasuisse) with the CyberSpec (CYD-C-2020003) Project, and (c) the University of Zürich UZH.

Data availability Not applicable.

Code availability All code used in this work is publicly available at [16].

Declarations

Conflict of interest Not applicable.

Ethical approval Not applicable.

References

1. Ahn, M., Lee, M., Choi, J., Jun, S.: A review of brain–computer interface games and an opinion survey from researchers, developers and users. Sensors (Basel Switz.) **14**, 14601–14633 (2014). https://doi.org/10.3390/s140814601
2. Al-Nuaimi, F.A., Al-Nuaimi, R.J., Al-Dhaheri, S.S., Ouhbi, S., Belkacem, A.N.: Mind drone chasing using EEG-based brain computer interface. In: 2020 16th International Conference on Intelligent Environments (IE), pp. 74–79 (2020). https://doi.org/10.1109/IE49459.2020.9154926
3. Association of Academic Physiatrists: Controlling a Prosthesis with Your Brain. Association of Academic Physiatrists (2017). Retrieved January 27, 2021, from https://www.sciencedaily.com/releases/2017/02/170206084904.htm
4. Birbaumer, N., Hochberg, L.R.: A useful communication in brain–computer interfaces. Neurology **91**(3), 109–110 (2018). https://doi.org/10.1212/WNL.0000000000005804
5. Crea, S., Nann, M., Trigili, E., Cordella, F., Baldoni, A., Badesa, F., Catalán, J.M., Zollo, L., Vitiello, N., Aracil, N., Soekadar, S.: Feasibility and safety of shared EEG/EOG and vision-guided autonomous whole-arm exoskeleton control to perform activities of daily living. Sci. Rep. (2018). https://doi.org/10.1038/s41598-018-29091-5
6. Frank, M., Hwu, T., Jain, S., Knight, R.T., Martinovic, I., Mittal, P., Perito, D., Sluganovic, I., Song, D.: (2017) Using EEG-based BCI devices to subliminally probe for private information. In: Proceedings of the 2017 Workshop on Privacy in the Electronic Society, WPES '17, pp. 133–136. Association for Computing Machinery, New York (2017). https://doi.org/10.1145/3139550.3139559
7. Friganović, K., Medved, M., Cifrek, M.: Brain–computer interface based on steady-state visual evoked potentials. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 391–395 (2016). https://doi.org/10.1109/MIPRO.2016.7522174
8. Jang, Y.S., Ryu, S.A., Park, K.C.: Analysis of P300 related target choice in Oddball paradigm. J. Inf. Commun. Converg. Eng. (2011). https://doi.org/10.6109/jicce.2011.9.2.125
9. Jiang, X., Zhang, X., Wu, D.: Active learning for black-box adversarial attacks in EEG-based brain–computer interfaces. In: 2019 IEEE Symposium Series on Computational Intelligence (SSCI), pp. 361–368 (2019). https://doi.org/10.1109/SSCI44817.2019.9002719
10. Juhasz, Z.: Quantitative cost comparison of on-premise and cloud infrastructure based EEG data processing. Clust. Comput. (2020). https://doi.org/10.1007/s10586-020-03141-y
11. Kanna, R.K., Vasuki, R.: Advanced BCI applications for detection of drowsiness state using EEG waveforms. Mater. Today Proc. (2021). https://doi.org/10.1016/j.matpr.2021.01.784
12. Kumar, S.T.S., Kasthuri, N.: EEG seizure classification based on exploiting phase space reconstruction and extreme learning. Clust. Comput. **22**(5), 11477–11487 (2019). https://doi.org/10.1007/s10586-017-1409-z
13. Lange, J., Massart, C., Mouraux, A., Standaert, F.X.: Side-channel attacks against the human brain: the pin code case study (extended version). Brain Inform. **5**, 12 (2018). https://doi.org/10.1186/s40708-018-0090-1
14. Li, Q.Q., Ding, D., Conti, M.: Brain–computer interface applications: security and privacy challenges. In: 2015 IEEE Conference on Communications and Network Security (CNS), pp. 663–666 (2015). https://doi.org/10.1109/CNS.2015.7346884
15. López Bernal, S., Huertas Celdrán, A., Martínez Pérez, G., Barros, M.T., Balasubramaniam, S.: Security in brain–computer interfaces: state-of-the-art, opportunities, and future challenges. ACM Comput. Surv. (2021). https://doi.org/10.1145/3427376
16. Martínez Beltrán, E.T.: enriquetomasmb/bci (2021). Retrieved February 21, 2021, from https://github.com/enriquetomasmb/bci
17. Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., Song, D.: On the feasibility of side-channel attacks with brain–computer interfaces. In: 21st USENIX Security Symposium (USENIX Security 12), pp. 143–158. USENIX Association, Bellevue (2012). Retrieved January 15, 2021, from https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/martinovic
18. McFarland, D., Wolpaw, J.: EEG-based brain–computer interfaces. Curr. Opin. Biomed. Eng. **4**, 194–200 (2017). https://doi.org/10.1016/j.cobme.2017.11.004
19. Meng, L., Lin, C., Jung, T., Wu, D.: White-box target attack for EEG-based BCI regression problems. In: Gedeon, T., Wong, K.W., Lee, M. (eds) Neural Information Processing—26th International Conference, ICONIP 2019, Sydney, NSW, Australia, 12–15 December 2019, Proceedings, Part I, Lecture Notes in Computer Science, vol 11953, pp. 476–488. Springer (2019). https://doi.org/10.1007/978-3-030-36708-4_39
20. Monaco, A., Sforza, G., Amoroso, N., Antonacci, M., Bellotti, R., de Tommaso, M., Di Bitonto, P., Di Sciascio, E., Diacono, D., Gentile, E., Montemurno, A., Ruta, M., Ulloa, A., Tangaro, S.: The PERSON project: a serious brain–computer interface game for treatment in cognitive impairment. Health Technol. **9**(2), 123–133 (2019). https://doi.org/10.1007/s12553-018-0258-y

21. Peña, A., Arango, J., Mazo, J.: Sistema para rehabilitación del síndrome del miembro fantasma utilizando interfaz cerebro-computador y realidad aumentada. Rev. Ibér. Sist. Tecnol. Inf. (2013). https://doi.org/10.4304/risti.11.93-106
22. Picton, T.: The P300 wave of the human event-related potential. J. Clin. Neurophysiol. Off. Publ. Am. Electroencephalogr. Soc. **9**, 456–79 (1992). https://doi.org/10.1097/00004691-199210000-00002
23. Rojas, G., Alvarez, C., Montoya, C., de la Iglesia-Vaya, M., Cisternas, J., Gálvez, M.: Study of resting-state functional connectivity networks using EEG electrodes position as seed. Front. Neurosci. (2018). https://doi.org/10.3389/fnins.2018.00235
24. Rosenfeld, J.P.: P300 in detecting concealed information and deception: a review. Psychophysiology **57**(7), e13362 (2020). https://doi.org/10.1111/psyp.13362
25. Rushanan, M., Rubin, A.D., Kune, D.F., Swanson, C.M.: SoK: security and privacy in implantable medical devices and body area networks. In: 2014 IEEE Symposium on Security and Privacy, pp. 524–539 (2014). https://doi.org/10.1109/SP.2014.40
26. Takano, K., Ora, H., Sekihara, K., Iwaki, S., Kansaku, K.: Coherent activity in bilateral parieto-occipital cortices during P300-BCI operation. Front. Neurol. **5**, 74 (2014). https://doi.org/10.3389/fneur.2014.00074
27. The OpenBCI GUI: OpenBCI Documentation (2021). Retrieved February 19, 2021, from https://docs.openbci.com/docs/06Software/01-OpenBCISoftware/GUIDocs
28. Vinothraj, T., Alfred, D.D., Amarakeerthi, S., Ekanayake, J.: BCI-based alcohol patient detection. In: 2017 Joint 17th World Congress of International Fuzzy Systems Association and 9th International Conference on Soft Computing and Intelligent Systems (IFSA-SCIS), pp. 1–6 (2017). https://doi.org/10.1109/IFSA-SCIS.2017.8305564
29. Zhang, X., Wu, D.: On the vulnerability of CNN classifiers in EEG-based BCIs. IEEE Trans. Neural Syst. Rehabil. Eng. (2019). https://doi.org/10.1109/TNSRE.2019.2908955
30. Zhang, X., Wu, D., Ding, L., Luo, H., Lin, C.T., Jung, T.P., Chavarriaga, R.: Tiny noise, big mistakes: adversarial perturbations induce errors in brain–computer interface spellers. Natl Sci. Rev. (2020). https://doi.org/10.1093/nsr/nwaa233

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Enrique Tomás Martínez Beltrán is a M.Sc. Student in New Technologies at the University of Murcia, specialized in networking and telematics. He is currently working on his End of Master Project based on cybersecurity and Brain–Computer Interfaces. At the same time, he is researching the automation of attacks and defenses in different scenarios with the CyberDataLab team. His interests include cybersecurity and new technologies.

Mario Quiles Pérez B.Eng. Student in Computer Engineering at the University of Murcia (UMU). Mention in Information and Communication Technologies. Currently in his last academic year, he is investigating the possible attacks that could be carried out on brain–machine interfaces. Interested and initiated in cybersecurity, he develops training scenarios for the detection of adversarial attacks on internal networks. In the future, he hopes to dedicate himself fully to the world of cybersecurity.

Sergio López Bernal received the B.Sc. and M.Sc. Degrees in Computer Science from the University of Murcia, and the M.Sc. Degree in Architecture and Engineering for the IoT from IMT Atlantique, France. He is currently pursuing the Ph.D. Degree with the University of Murcia. His research interests include ICT security on brain–computer interfaces and network and information security.

Alberto Huertas Celdrán received the M.Sc. and Ph.D. Degrees in Computer Science from the University of Murcia, Spain. He is currently a Postdoctoral Fellow associated with the Communication Systems Group (CSG) at the University of Zurich UZH. His scientific interests include medical cyber–physical systems (MCPS), brain–computer interfaces (BCI), cybersecurity, data privacy, continuous authentication, semantic technology, context-aware systems, and computer networks.

Gregorio Martínez Pérez Full Professor in the Department of Information and Communications Engineering of the University of Murcia, Spain. His scientific activity is mainly devoted to cybersecurity and networking, also working on the design and autonomic monitoring of real-time and critical applications and systems. He is working on different national (14 in the last decade) and European IST research projects (11 in the last decade) related to these topics, being Principal Investigator in most of them. He has published 160+ papers in national and international conference proceedings, magazines and journals.