Chapter 10
SecBrain:
A Framework to Detect Cyberattacks Revealing Sensitive Data in Brain-Computer Interfaces

Enrique Tomás Martínez Beltrán
https://orcid.org/0000-0002-5169-2815
University of Murcia, Spain

Mario Quiles Pérez
University of Murcia, Spain

Sergio López Bernal
University of Murcia, Spain

Alberto Huertas Celdrán
University of Zürich, Switzerland

Gregorio Martínez Pérez
University of Murcia, Spain

ABSTRACT

In recent years, the growth of brain-computer interfaces (BCIs) has been remarkable in specific application fields, such as the medical sector or the entertainment industry. Most of these fields use evoked potentials, like P300, to obtain neural data able to handle prostheses or achieve greater immersion experience in videogames. The natural use of BCI involves the management of sensitive users' information as behaviors, emotions, or thoughts. In this context, new security breaches in BCI are offering cybercriminals the possibility of collecting sensitive data and affecting subjects' physical integrity, which are critical issues. For all these reasons, the fact of applying efficient cybersecurity mechanisms has become a main challenge. To improve this challenge, this chapter proposes a framework able to detect cyberattacks affecting one of the most typical scenarios of BCI, the generation of P300 through visual stimuli. A pool of experiments demonstrates the performance of the proposed framework.

DOI: 10.4018/978-1-7998-7789-9.ch010

INTRODUCTION

Brain-Computer Interfaces History

Brain-Computer Interfaces (BCIs) are devices that enable two-way communication between an individual's brain and external devices. This bidirectional connection allows two different functionalities in terms of BCI usage. The first one is focused on the acquisition of neuronal activity produced by an individual and its transmission to a computer for analysis and processing. The second is given by the stimulation and inhibition of brain activity to regulate abnormal impulses or improve motor actions at a neuronal level.

Traditionally, the usage of BCI has been aligned with the medical field. With this technology, many advances have been made in neuropsychology and neurophysiology. BCI has contributed to the treatment of neurodegenerative diseases by analyzing the brain state, such as epilepsy and the autonomic nervous system (Liberati et al., 2012; Simon et al., 2011). Over the years, BCI technology has undergone significant technological evolution. Thanks to numerous studies, BCI has increased its application fields and has started to be used in other scenarios than medicine. One of these scenarios is the entertainment and video game industry (Ahn et al., 2014; Finke et al., 2009). Another sector exploring the use of BCI is the military one, where studies are aiming to allow the telepathic handling of multiple drones at a distance (Al-Nuaimi et al., 2020) or even exoskeletons (Crea et al., 2018).

Most of the scenarios functionality is based on capturing and processing the electroencephalography (EEG) signal and evoked potentials. Event-related potentials (ERPs) are signal patterns automatically generated by the brain when stimuli are presented to the person. Different types of potentials depend on the trigger action performed: visual, auditory, somatosensory, or cognitive. The study of these potentials has made it possible to obtain information about the subject, such as his/her emotional state, neurological problems, dependencies, or even private information.

One of the most well-known and used ERPs in brain recording is P300 (or P3). P300 is related to the visualization of stimuli known by the person. It is produced between 250-500 ms after the visualization of each known-stimulus and has a positive signal peak. One of the most common ways of provoking this potential is through the Oddball paradigm. The Oddball paradigm shows a series of known stimuli belonging to a more extensive set of unknown stimuli. At this point, it is important to mention that the captured EEG and the labeling of the P300 are susceptible for the user. This problem is aggravated due to the lack of frameworks that consider security aspects such as authentication, confidentiality, and data integrity. In this context, attackers could turn their attention to the BCIs to carry out malicious actions.

Motivating Cybersecurity Issues

This work is motivated by the limitations of current frameworks, which do not provide security mechanisms to ensure the integrity of transmitted data or users' privacy (Ghoneim et al., 2018). Many times, this leads to a malfunction of the actions carried out by the BCI or to leak sensitive information of the individual. Similarly, current EEG-based BCI frameworks do not provide authentication mechanisms, so an attacker could impersonate the legitimate user to adapt the BCI functionality with malicious data. Besides, there is no standard or specific protocol for the secure development of BCI applications, causing a significant weakness in the software and its interaction with the hardware in many current alternatives.