Frequency Interception and Manipulation Vulnerabilities in Myoelectric-Computer Interface Signal Transmission

Emma V. Szczesniak

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Master of Science

In

Biomedical Engineering

Aaron F. Brantly, Chair

Sara L. Arena

Stephen M. LaConte

May 2nd, 2025

Blacksburg, Virginia

Keywords: Myoelectric-Computer Interface, Biomedical Device Security, Adversarial Attack, Signal Transmission Vulnerabilities

Frequency Interception and Manipulation Vulnerabilities in Myoelectric-Computer Interface Signal Transmission

Emma Szczesniak

ABSTRACT

Neural interface systems such as myoelectric-computer interfaces (MCIs) and brain-computer interfaces (BCIs) assist patients with motor impairments due to injury or neurodegenerative conditions. Neural interface research has focused on device accuracy and usability while neglecting to comprehensively assess security risks. These devices store substantial personal data that can lead to exploitation if compromised. Attacks can override user intent, having major implications on a user's physical safety and psychological well-being. As neural interfaces become more prevalent, understanding and addressing their vulnerabilities is imperative to ensure user safety and data privacy. This study aimed to identify distinct frequency characteristics between upper limb motor tasks and examine data transmission frequencies to assess potential vulnerabilities in MCI systems. The HackRF One identified three distinct frequencies involved in the frequency hopping pattern during signal transmission, which allows attackers to intercept EMG data. Surface electromyography (sEMG) data produced by wrist flexion and extension motor tasks were analyzed in the frequency domain and showed statistically significant differences in frequency metrics. Distinguishing frequency metrics enable manipulation of motor commands in MCI systems by sending false signals at specific frequencies. This work provides insight into vulnerabilities in the signal transmission stage of neural interfaces to encourage developers to safeguard against potential attacks and to inform consumers of the security risks associated with these devices and their impact on user safety and protection of neural data.

Frequency Interception and Manipulation Vulnerabilities in Myoelectric-Computer Interface Signal Transmission

Emma Szczesniak

GENERAL AUDIENCE ABSTRACT

Neural interfaces are devices that connect technology with the nervous system for use in medical and non-medical applications. Within the realm of neural interfaces are myoelectric-computer interfaces (MCIs) and brain-computer interfaces (BCIs) which use neural signals from the muscles and brain, respectively, to control an external device such as prostheses. This study aimed to assess weaknesses in the transmission stage of an MCI device, the step in a neural interface that involves transferring neural data obtained from electrodes on the body to a computer for processing. Two attack components were considered. The first involved studying the frequencies used for data transmission to assess the potential for signal interference and the second involved analyzing frequency characteristics of motor movement data to assess the potential for signal manipulation. Distinctions in frequency characteristics between motor tasks and an understanding of signal transmission patterns indicate that there are vulnerable aspects of MCI systems. As most neural interfaces function through the same series of stages, the results obtained from this study are applicable to a broad range of neural interface devices. Evaluating the ability to hack into these types of devices informs industry workers on security risk areas and notifies the public of potential privacy risks from neural interfaces.

Acknowledgements

I would like to thank my chair, Dr. Aaron Brantly, for encouraging me to pursue my research interests and providing me with the necessary resources to be successful. Through his help obtaining a research grant to fund experimentation to his time spent reviewing my thesis writing, this project would not have been possible without his support and valuable insight. Dr. Brantly has opened doors for me by providing opportunities to present at conferences, a chance to lead a podcast discussion, and feedback to improve my scientific writing. He has been an incredible mentor, and I look forward to applying the skills I have learned while a part of the Tech4Humanity Lab to my future endeavors.

I would also like to thank my committee members, Dr. Stephen LaConte and Dr. Sara Arena, for working with me throughout this process.

Finally, I would like to thank my family for their unwavering support and for being a sounding board throughout this process. Their thoughts and suggestions helped me dive deeper into my research investigation. I truly appreciated their positivity and consistent cheerleading for my success.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Introduction to Neural Interfaces

The persistent integration of technology into society engenders change in human interactions and poses challenges with protecting the safety and security of personal data. Neural interfaces streamline communication between humans and technological equipment, improving productivity and enhancing workforce capabilities. A subsect of neural interfaces used in the medical field are myoelectric-computer interfaces (MCIs) and brain-computer interfaces (BCIs), which are used to augment, restore, or rehabilitate features of the human condition that are dysfunctional due to injury, disease, or an alternative circumstance.

Research into MCIs and BCIs garnered interest in the 1970s when Vidal probed the potential for human electrical signals to be used for controlling prosthetic devices [1]. Despite Vidal's intrigue into this area of biomedical research, an incomplete understanding of brain physiology and slow technological development limited research progression [2]. However, throughout the following three decades, researchers continued to study and assess the potential for communication between the brain and machines. By the 2000s, it was possible for a person to control a computer cursor and open/close a robotic hand using signals acquired invasively from the motor cortex of the brain [3]. An interest in BCIs and MCIs has gained traction in recent decades, leading to research and development expanding beyond academia to industry. Industry participation in neural interface research has led to the commercialization of MCI and BCI products. In the realm of BCIs, NeuroSky and Emotiv have created electroencephalography (EEG)-based headsets for consumers [4]. NeuroSky offers MindScribe, a system that allows users to communicate in complete sentences [5]. This product is effective for disabled individuals with functional minds to restore communication capabilities. Emotiv is currently marketing their EPOC product that has been applied by users for hands-free gaming [5]. These examples represent only two of the many companies that have delved into neurotechnology development to meet the interests and needs of consumers. MCIs have used surface electromyography (sEMG) in rehabilitation and prosthetic products as well as for neural-driven gesture control for entertainment and daily living [6]. As researchers improve their understanding of the physiological connections between the nervous system and other biological processes and where technology might augment these

systems, continued research in this field will uncover new applications for neurotechnology and incorporate them into humanity's social structure.

1.2 Privacy and Security of Neural Interfaces

As neural interfaces are further integrated into society, it is essential to focus on how to secure these devices and ensure users' data privacy. Prior to protecting users from a privacy breach or security violation, it is important to define these terms. Privacy refers to control over access to and use of personal information and security is the means of ensuring the privacy and accessibility of information by preventing its unauthorized access, use, or manipulation [7]. Thus, the privacy and security of neural data covers who has access to an individual's neural information when using a neural interface device and how unauthorized access can be prevented. This applies to all forms of wearable technology that collect biosignal data; however, this exploration focuses on neural data obtained via EMG and EEG as these are the most common biosignals used in MCI and BCI systems, respectively.

Computers and smart phones are classes of technology widely used by individuals to assist with many aspects of everyday life including banking, scheduling, and communicating. Initially people were encouraged to add password protection to their devices; however, in recent years this has not been sufficient to minimize the risk of attacks. Two-factor identification is becoming a more widely used means for adding additional protection to personal technological devices [4]. As adversarial attacks have become more prevalent, the general public has begun to understand the impact of an attack on their device and what it means for their personal data.

The rising use of neural interface systems means increased personal data being passed through the digital ecosystem. Similar to traditional personal information stored on computers, biological data can cause serious harm to a person if obtained by an adversary [4]. This is particularly relevant to medical devices that manage vitals, authorize access to a user's health system, or control neuroprostheses as physical harm or data exploitation could occur if these systems are compromised. Therefore, it is important that the same attention put towards computers and smart phones also be placed on neural interfaces. Similar to computers and smart phones, these devices hold substantial amounts of personal data [4]. Without proper security, attackers can infiltrate a neural system and gain access to this data.

Adversarial attacks on neural interfaces not only affect the functionality of a device but also alter a user's intent by overriding the device to change the output command, which can negatively impact a person's self-identity as they no longer have control over their behavior [4]. To determine whether an output command while using a neural interface is representative of an individual's intended action, the concept of personal autonomy must be considered. Personal autonomy is an individual's ability to act on their own volition without influence from external manipulation [4]. When "brain-hacking" occurs, a user's decision-making or behavior may become compromised, leading to a loss of personal autonomy. This situation can cause fear and distress in users during the time of attack, while also negatively impacting their feeling of free agency long-term [4]. Although "brain-hacking" is limited to BCI systems, the psychological bearing of manipulating output commands of a device is applicable to any neural interface system. Thus, the psychological effect on users is a critical consideration when assessing the need to secure neural interface devices.

1.3 Testing Methods

An MCI system for classification of upper-limb movements was developed for this study as a framework to assess adversarial attacks on the signal transmission phase of MCI systems. Surface electrodes were used to acquire EMG signals from the forearm of the flexor and extensor muscle groups. The electrodes were connected via wires to the Cyton biosensing board which functions as an analog-to-digital converter that amplifies and digitizes EMG data. The digital EMG data was sent from the Cyton board to a computer via a Nordic Gazell transmission protocol for preprocessing, feature extraction, and classification. The data was analyzed in the frequency domain to evaluate distinct frequency characteristics between wrist flexion and extension motor tasks amongst the participants. Frequency characteristics between motor tasks were analyzed to explore their potential use in Man-in-the-Middle (MITM) attacks aimed at sending false signals to prompt data misclassification. The HackRF One assessed frequency hopping patterns during the Cyton board's signal transmission, capturing changes in frequency patterns during different Cyton board states including pairing and data streaming. Potential implications of the observed frequency characteristics and transmission patterns in the context of executing adversarial attacks were addressed.

1.4 Specific Aims

This study aimed to investigate whether distinguishing frequency characteristics of sEMG data between motor movements and identified transmission frequency hopping patterns could be used to successfully perform an adversarial attack on the signal transmission stage of an MCI system. To achieve this goal, the following objectives were addressed.

Objective 1: Identify frequency hopping patterns during Cyton board signal transmission.

Objective 2: Evaluate differences in frequency characteristics of wrist flexion and extension motor movements and determine trends among study participants.

Objective 3: Examine how distinguishing frequency characteristics and understanding signal transmission patterns could be exploited for use in adversarial attacks.

A security risk assessment of signal transmission in an MCI system provides insight into where measures need to be taken to reduce adversarial attacks that can be performed on MCI devices. As the Cyton biosensing board has been used in a variety of studies that developed upper- and lower-limb prosthetics controlled by MCI and BCI systems, this study can reveal the potential vulnerabilities in multiple proposed devices. In addition to informing researchers on the stages of neural interface systems that need further security measures, this study will serve to educate the public on the safety and security of commercial BCI and MCI products, allowing individuals to make informed decisions about purchasing neural interface devices.

2 Literature Review

2.1 Neural Interfaces for Movement Rehabilitation

Neural interfaces represent a nervous system to technology connection aimed at augmenting or restoring an aspect of the human condition. The signaling processes involved in motor movement initiation and execution have been well-established through a variety of in vitro, in vivo, and human subject models as well as a few computational approaches [8-11]. Within the realm of neural interfaces are MCIs and BCIs which rely on peripheral (PNS) or central nervous system (CNS) signals, respectively, to control an external system. Both neural interfaces are composed of four main stages which include signal acquisition, feature extraction, classification, and device output [4]. MCIs and BCIs can be differentiated by their signal acquisition methods. MCI systems utilize functional peripheral neurons to record electrical potentials whereas BCI systems record neuronal activity in the brain [2]. Neural interfaces have numerous potential applications with motor movement rehabilitation as a heavily studied research area. Despite differences in the locations used for signal acquisition, researchers employ similar motor tasks when assessing the function and precision of MCI and BCI devices. Commonly studied motor movements when developing and testing these systems include elbow extension and flexion, forearm pronation and supination, palmer and lateral grasp, and fist clenching and unclenching [12]. These motor tasks constitute fundamental movements applicable to many daily tasks and are thus important movements to restore in individuals with reduced motor capabilities. Neural interfaces can function as either a linear process in which there is no feedback to modify earlier stages of the system pipeline, or as a closed-loop system that allows for a continuous exchange of information between a user's nervous system and an external device [13]. A closed-loop system improves control and allows for adaptation that enhances the performance of the neural interface; however, it requires greater complexity [13]. Thus, neural interfaces can be separated based on their signal acquisition techniques and by the basis of their control paradigms. Regardless of potential differences in system architecture, both MCIs and BCIs exist with a large focus on aiding patients with motor impairment.

2.1.1 Myoelectric-Computer Interfaces

Despite extensive research into MCI systems, there exists a dichotomy between research in academia and limited clinical or commercial impact. Myoelectric devices deemed effective through research lack usability in practice. Ning et al. published a review on the state of myoelectric devices nearly thirteen years ago emphasizing insufficient sensory feedback, inadequate algorithm robustness for natural background movement in daily activities, nonintuitive pattern-based recognition systems, and single-sensor modality as the main drivers for the disconnect between research and practical application [14]. A follow-up review published a decade later acknowledged that advancements in the past decade had improved both the accuracy and usability of sEMG-based prostheses through the use of deep learning for signal classification as well as the implementation of sensory feedback for an enhanced user-device interaction [15]. However, persisting limitations of single-modality devices indicate that further research on neuroprostheses should examine multimodal options to achieve a more applicable prosthetic device for intended users. Sensory feedback strengthens the connection between patient and prosthetic, improving the control, safety, and performance of the device [15]. Mechanotactile, electrotactile, and proprioceptive feedback are noninvasive sensory feedback techniques used for prosthetic control [15]. Complete sensory restoration is unlikely due to limits on the number of signaling channels that can be actively operating to generate a sensory feedback response in an MCI device user [15]. Therefore, implementing sensory feedback or a closed-loop system focuses on supporting user agency of their neuroprosthesis.

There are mixed findings regarding biosignal modalities for MCI devices. Based on past and present studies, it is evident that EMG is the agreed upon primary biosignal for MCI devices. EMG signals represent the electrical potential produced by the depolarization of muscle fibers after an action potential propagates from a motor neuron to the muscle fibers it innervates [16]. As such, these signals provide valuable insight into the process of muscle contraction and relaxation. In-depth studies on these processes allow for the development of rehabilitative technology that directly focuses on the neuron to muscle fiber interaction. However, continued limitations in the degrees of freedom and compound movement capabilities of myoelectric prostheses have led researchers to seek alternative modalities for neuroprosthetic devices. Some researchers persist with single modality systems [16-27], while others are working to combine biosignals using varying signal acquisition techniques to create a multimodal system. EMG has been combined with EEG [28-31], electrooculography (EOG) [28], electrocardiography [32],

gestures [33], and functional near-infrared spectroscopy (fNIRS) [34] in an effort to improve the capabilities of MCI devices. Continued research is needed to determine the most effective multimodal system for an MCI device to function as a prosthesis.

The two main methods for acquiring EMG data are needle and surface electrodes. Needle electrodes are invasively inserted into the muscle to record the electrical potential when the muscle contracts [35]. Surface electrodes are placed on the surface of the skin over the muscle of interest and are a noninvasive technique for EMG signal acquisition [19, 35]. sEMG is the widely used method for signal acquisition in MCI systems and records the electrical potential produced by motor unit action potentials. A motor unit is the muscle fibers activated by a single neuron with the number and type of motor unit varying based on the muscle [16]. Since sEMG electrodes are placed on the skin over the muscle region of interest, sEMG data consists of the summation of simultaneously activated motor units [15]. Silver/silver chloride gel electrodes are the preferred electrode type when recording sEMG data [16-18, 20]. Mahboob et al. selected silver/silver chloride electrodes for their minimal polarizability that allows for a higher signal-to-noise (SNR) ratio than other electrodes [20]. A higher SNR reduces the effects of signal interference and artifacts when acquiring data.

Differing opinions on the best approach to sEMG electrode arrangement has resulted in a variety of experimental setup designs. The two setups widely used for recording sEMG data are based on either unipolar or bipolar electrode placement. Bipolar electrode signal acquisition records the voltage difference between two active electrodes on the same muscle [18]. This technique allows for electrical potentials at motor units for individual muscles to be measured. Myoelectric devices can then target specific muscles to maximize signal detection, in turn enabling more accurate classification of intended movements. However, consistent and precise electrode placement to ensure data acquisition solely for the muscle of interest has its challenges [21]. A bipolar setup typically exhibits a higher SNR due to common-mode rejection between the two electrodes on the muscle, though this requires that the electrodes be placed along the fiber length of the muscle [36]. In unipolar signal acquisition, the reference electrode used for reducing common-mode noise is further away from the active electrodes, leading to more discrepancy in the noise detected by the reference and active electrodes. Chen et al. applied a unipolar electrode setup for a proposed soft exoskeleton glove because it does not require precise placement,

allowing for easier repetition of experiments and potentially greater ease of use for clinical applications [17]. Researchers have utilized a unipolar setup to create an armband-based neuroprosthetic device since it can be placed anywhere along the forearm or bicep, making it adaptable to patients with differing upper-limb loss [17, 19-20]. Based on current literature, both electrode arrangements can be effective for an sEMG-based prosthetic device. Therefore, the patient of interest and device application are important considerations when developing an initial experimental design protocol.

Machine learning (ML) is used for the classification stage of MCI systems, with support vector machines and neural networks as the most frequently adopted models. Cao et al. and Abougarair et al. used a support vector machine (SVM) in upper limb neuroprostheses to classify hand and arm movements [21]. Li et al. applied an SVM for an EMG-based biometrics study due to its frequent adoption as a supervised learning model and applicability to situations requiring multi-class classification [37], demonstrating the versatility of SVMs for decoding EMG data. Neural networks were the other widely implemented method for classification in neuroprosthetic studies [17, 24, 31, 38]. Feature extraction is performed to acquire characteristics of the filtered EMG data to improve signal classification [39]. As feature data is the direct input to the ML classifier, selected features play a significant role in MCI device accuracy [39]. Based on the literature, both time and frequency domain features were applied to MCI systems, but time domain features were preferred for their ease of calculation and therefore lower computational complexity [39]. Time domain features are extracted to analyze muscle force whereas frequency domain features are extracted to study muscle fatigue [39]. As muscle force variation detection provides a means to distinguish between tasks for a prosthetic device, time domain feature extraction is more suitable to improve classification accuracy in MCI systems. Time-frequency domain features can also be extracted from EMG signals for data classification but are less commonly used in real-time signal processing due to their high computational complexity [39]. Root mean square (RMS) [16-17, 21, 26, 32, 40] was predominantly utilized regardless of the ML model. RMS is a commonly extracted feature for gesture classification as it can estimate force during grasping tasks and hand-lifting with varying loads [39]. Additional features used in EMG prosthetic studies included mean absolute value [21, 26], variance [21], mean frequency [16], waveform length [26-27, 34], and zero crossing [16, 26]. Variance and WL are indicators of signal variation and MAV represents muscle activation [39]. Zero crossing is a time domain feature that provides

insight into the frequency content of the EMG signal and mean frequency is a frequency domain feature that indicates muscle fatigue [39]. Despite system pipeline changes for application specificity, the four stages of neural interfaces remained consistent across the myoelectric devices found in the literature.

2.1.2 Brain-Computer Interfaces

A BCI is a computer-based system that acquires, processes, and classifies data to initiate a command in a peripheral device. BCIs only encompass systems that acquire signals from the CNS [2]. A BCI must contain two main components, a device for signal acquisition and a device that produces an output command, as together they form a system that applies a user's biosignal data to act upon that user's environment [2]. Compared with myoelectric interfaces, BCIs are less dependent on amputation conditions since they enable motor intention, initiation, and execution to be monitored and controlled via sensors either on or in the brain [12]. Thus, BCIs allow motor tasks to be completed without the user performing traditional neuromuscular processes.

There are a variety of signal acquisition techniques used in BCI systems and can be invasive, semi-invasive, or noninvasive. Invasive methods involve implanted electrodes within the cortex of the brain, requiring an intense surgical procedure [41]. Although invasive signal acquisition can lead to better temporal and spatial resolution of electrical signals, there remain practical and health-based downsides towards these types of BCIs such as surgical risk and tissue scarring. Similarly, semi-invasive BCIs such as those that utilize electrocorticography for signal acquisition still require a surgical procedure to implant electrodes on the surface of the brain below the skull [41]. Noninvasive techniques used to record brain activity include EEG, functional magnetic resonance imaging (fMRI), fNIRS, and magnetoencephalography (MEG) [13]. With current biomedical technology, noninvasive recording techniques are optimal for BCI applications.

EEG is the most established and widely used method for signal acquisition in BCIs as it is noninvasive, inexpensive, and generally user-friendly. Furthermore, EEG has been standard practice in the medical field for decades for diagnostic testing of sleep disorders, cranial injuries, epilepsy, psychiatric disorders, as well as numerous other medical conditions [42-43]. The extensive application and thus understanding of EEG data makes it an easier biosignal to

incorporate into a BCI system. Many commercial and research-grade devices have been developed to record EEG data. The most widely used commercial-grade EEG headsets include those produced by companies such as Emotiv, OpenBCI, NeuroSky, interaXon, and MyndPlay [44]. Researchers have found that noise and artifacts pose a significant disturbance to EEG data regardless of the device used for signal acquisition. To reduce the effect of noise on classification output, researchers have collectively implemented filtering into their signal processing pipelines. The techniques used for signal processing varies, but the consensus in the field is that the removal of artifacts, powerline noise, and frequencies outside the expected range for a given application are required for accurate task classification.

Individual brain capacity and cognition also impact the quality of data obtained and thus the efficacy of a BCI device. Cognitive states related to user fatigue and emotion can cause fluctuations in brain activity during EEG testing [12]. Data variability between users occurs due to differences in learning ability, cognitive power, and brain disease [12]. As a result, researchers have found the most success in creating patient-specific BCI systems and have experienced challenges developing a generalized system that offers comparable performance metrics.

The 10-20 electrode system has been adopted as the primary electrode placement design. Most EEG-based BCI studies use a derivation of the 10-20 system, regardless of the number of electrodes included in the study. Variations of the 10-20 system include the 10-10 and 10-5 systems which use additional electrodes as compared to the traditional 21, providing researchers with higher spatial resolution [43]. In addition to the consensus on electrode placement, most studies reviewed on motor BCIs have used visual cues to indicate to patients when to perform certain movement tasks. Pairing visual cues with marker placement in the data during real-time recording simplifies segmentation procedures during signal processing by allowing for easy identification of the start and end points of performed tasks.

For EEG-based motor BCIs, steady-state evoked potentials (SSVEPs) and motor-based electrical potentials are the main electrical signals acquired and translated into commands. Both SSVEPs and motor-based signals produce event-related potentials (ERPs). An ERP is an increase in electrical activity in the brain in response to an internal or external event [42]. Although SSVEPs are easier to study due to the rhythmic response produced in the visual cortex in relation to stimuli [45], their application in motor movement settings is not as intuitive for patients as BCIs

based on motor movement tasks. Therefore, research has turned toward brain activity produced by motor imagery and motor execution tasks as the primary electrical activity studied in relation to motor BCIs. Motor execution and motor imagery tasks represent physically performing or imagining performing a movement task, respectively [46]. Mustile et al. found that motor execution and motor imagery of walking have similar neural features, but that motor imagery has a higher cognitive demand and results in a wider distribution of brain activity [46]. Conclusions from a meta-analysis of motor imagery, observation, and execution by Hardwick et al. were consistent with the findings of Mustile et al [47]. The divergence in motor imagery and motor execution studies are in part due to their application objective. Motor imagery is more applicable for BCIs where patients require a neuroprosthetic device, whereas BCIs involving motor execution might be more beneficial for stroke rehabilitation. As such, the intended application of a BCI device is a significant factor in designing a research study.

2.1.3 Applications of Neural Interfaces in the Medical Field

Improved understanding of the neural processes in the brain that underly cognitive functions related to motor control has driven an increase in MCI and BCI research for clinical applications. Conditions that lead to decreased motor movement capabilities include stroke, amyotrophic lateral sclerosis, spinal cord injury, Parkinson's disease, and multiple sclerosis [12]. Despite having limited control over peripheral nerves, the cerebral cortex of many of these patients remains either semi or fully functional. BCIs provide a way for these individuals to regain motor control despite their medical condition, restoring the ability to perform daily tasks that had become challenging or impossible prior to implementing a BCI device into these patients' lives. BCIs can also be used in neurorehabilitation situations to assist with motor relearning in stroke patients using assistive robotics [2]. Nann et al. assessed the feasibility of an EEG and EOG controlled whole-arm exoskeleton for patients suffering the residual effects of a hemiplegic stroke [48]. Furthermore, motor imagery-based tasks can aid in improving motor function of patients with spinal cord injuries [2]. For patients with partial upper or lower limb loss or patients with some retained peripheral nerve function, MCI devices provide a more simplified and straightforward way to restore the motor capabilities of peripheral limbs through neuroprosthetics. Reaching and grasping motor movements are integral for daily living; therefore, the development of biomedical devices that assist with motor control and rehabilitation

will persist [12]. As research on these devices continues, it is imperative to assess vulnerabilities in their development framework.

2.2 Privacy and Security of Neural Interface Systems

2.2.1 Current Landscape of Neural Data Security

Privacy and security of neural data is an understudied area of research. Focus primarily revolves around reliability, usability, and performance of neural interfaces, rather than the systems in place for data protection [49]. According to Bernal et al., insufficient testing has been conducted on neural interfaces to determine their vulnerabilities [7]. In the most recent decade, there has been a surge in research and publicity of neural interfaces, leading to questions regarding device security and privacy rights for neural data. Terms that have emerged in reference to neural interface cybersecurity include neuroethics, neurosecurity, and neuroprivacy [7]. The General Data Protection Regulation (GDPR) came into effect in 2018 and represents the framework for data protection in Europe [50]. The law does not contain a section specifically for neural data but does confirm that neural data is a form of personal data, thereby falling within the terms of the GDPR [50]. Companies are more likely to put effort into security during the research and development stage of neural interface product development knowing the fines the company would accrue from an unsecured product that violates the GDPR [42]. Although the GDPR includes neural information as personal data, supplementary policy is needed to proactively mitigate potential data breaches specifically within neural interfaces. The United States does not have a law equivalent to Europe's GDPR, thereby further lacking protections for neural data. Researchers are in agreement that neurotechnology is progressing at a faster rate than regulations can be made to ensure data confidentiality [7]. The private and information-rich nature of biosignal data makes it an ideal target for adversaries. Studies that address security risks in neural interfaces ensure a more detailed and accurate description of a device and its vulnerabilities, which would help potential users make informed decisions, and in the case of medical devices, provide informed consent.

One topic of conversation in the field revolves around the dual-use of neural interfaces. Ienca et al. describes dual-use and its applicability to BCI devices [4]. Similar to how other forms of technology can be used by adversaries for criminal purposes, there is potential for BCI systems

to be used with criminal intent [4]. Although Ienca et al. discussed dual-use specifically with regard to BCI technology, the concept and relevant concern is applicable to many neural interface devices. Enrique et al. took a different approach towards describing neurohacking. The authors perceived neurohacking as any manipulation to the brain, whether it be with a positive or negative intention [51]. Using this definition, neurohacking encompasses positive aspects of brain manipulation such as those performed to enhance human capabilities. Despite the broader definition of brainhacking discussed by Enrique et al., researchers can agree that all forms of brainhacking are considered to involve the use of technology to alter the natural functions of the brain.

2.2.2 The Hackability of Neural Interfaces

The ability for an adversary to infiltrate, manipulate, and control a neural interface is dependent on the structure of the device and its mode of data transfer. Conventional myoelectric control utilizes a simple algorithm in which an output command can be activated based on set EMG amplitude thresholds [14]. Elementary myoelectric control systems follow a simplistic model that allows for easier infiltration. System complexity provides elements of security since adversaries have a lesser understanding of the innerworkings of the device, thereby making the system more challenging to override or manipulate. Cybersecurity risks of neural interfaces can occur at the data, permission, or model level [13]. Data anonymization and pseudonymization remove or replace personally identifiable information, respectively, and have been applied to reduce the data leaked from a security breach [13]. Identity verification has been used in some devices to reduce the ability for a neural interface device to be hacked at the permission level [13]. At the model level, developing robust model architecture diminishes susceptibility to attack of a neural interface [13]. Minor protections might exist for each level depending on the device and its use case, but vulnerabilities remain present at all three levels.

Neural interfaces have been found to be vulnerable to adversarial attacks that inject perturbations into neural data, though there exists controversy regarding the effectiveness of perturbation-based attacks on neural interfaces. Comparing the vulnerability of neural interfaces to other technological systems, a perturbation-based attack technique is easier to conduct on neural systems that use EMG or EEG than on visual-based systems due to the brain's limited understanding of neural data as compared to visual representations as seen in the computer vision

field [13]. Users are less likely to notice changes in neural data as it is processed through a neural interface system than images found in visual-based systems that are detectable by the human eye. Bian et al. found that the success of the same perturbation-based attack performed on different subjects varied due to differences in the subjects' EEG data [52]. Meng et al. and Zhang et al. proposed two additional limitations that reduce the infiltration potential of a perturbation-based attack on neural interfaces. Partial understanding of the model is needed to create a perturbation template, and the signal streaming start time is needed prior to performing the attack [49, 53]. Based on these limitations, Meng et al. claimed that based on the proposed requirements, perturbation-based attacks on the model of a neural interface are limited, especially in real-world settings [53]. Conversely, Zhang et al. argued that transferability minimizes the first limitation by allowing an adversarial perturbation template to be created using a model that mimics the target model [49]. The second limitation can also be alleviated if success of the adversarial attack is independent of the time synchronization between the perturbation template and the neural data [49]. Thus, a neural interface's susceptibility to attack differs based on the model parameters and between-subject variability.

Advancements in wireless technology in recent decades have encouraged the development of wireless medical devices, including those used for motor rehabilitation. Wireless MCIs and BCIs allow for increased mobility and reduced restrictions for patients [54]. This technology is especially beneficial for ease-of-use outside the clinical space, such as for using a neuroprosthesis for daily tasks. Signal transmission protocols typically used for MCI and BCI systems include Wi-Fi, Bluetooth, and Gazell [55, 56]. These methods of data transmission can be distinguished by their range of transmission, rate of transmission, and the frequency range in which they transmit data [55]. Transmission range is an important factor when considering the application of a wireless device. Wi-Fi has a greater transmission range than Bluetooth and Gazell [55, 56]. Most wireless EEG and EMG devices use a 2.4 GHz frequency band, which is the range commonly used for handheld devices such as laptops, smartphones, and smart watches [55]. Gazell is a signal transmission modality developed by Nordic Semiconductor that uses frequency hopping in the 2.4 GHz frequency band to minimize interference from nearby 2.4 GHz wireless systems [56]. Furthermore, Wi-Fi protocols are more resistant to signal interference than Bluetooth due to their higher transmission power [55]. The additional capabilities of wireless

technology provide many benefits for neural interfaces; however, wireless data transmission creates an additional layer to neural interfaces that can be exploited by attackers [57].

2.2.3 Commonly Used Attack Techniques

Most studies on neural interface vulnerabilities have focused on SSVEP or P300 spellers since they are the easiest types of BCIs to use for assessing attack capabilities. Studies on security vulnerabilities in neural interfaces mainly focused on BCIs, with only one study by Xue et al. that addressed adversarial attacks on a myoelectric interface system. Of the BCI vulnerability studies reviewed, the main stage of attack was in the ML model of BCI systems. Adversarial attacks at the model level can be separated into two categories, evasion or poison, based on their technique [52-53]. An evasion attack involves small perturbations to a test sample to confuse an ML model [53]. A poisoning attack contaminates training set samples to produce a backdoor in an ML model [53]. Meng et al. assessed a poisoning attack mechanism on three publicly available EEG datasets by applying a narrow period pulse (NPP) to the EEG data which was used as a backdoor key [53]. The key was planted within the training set and opened a "backdoor" when the BCI system was active, allowing for the attacker to manipulate the EEG data [53]. NPPs are advantageous as they can include randomness that makes their role as a key to the ML model adaptable to different situations [53]. Szegedy et al. found that attackers can exploit the transferability of adversarial samples to train a model that mimics the behavior of the target model [58]. This substitute model allows an adversary to gain insight into the vulnerabilities of the mimicked target model, enabling a more effective attack. Furthermore, Zhang et al. examined an evasion attack using an adversarial patch to infiltrate a P300 BCI speller [49]. The singular study found on an MCI system employed universal adversarial perturbations (UAP) to perform an evasion attack on the convolutional neural network (CNN) used for classification of sEMG data [38]. Xue et al. found that DeepFool-based UAPs and Total Loss Minimization-based UAPs were able to successfully force the CNN to misclassify the data [38]. Both attack techniques at the classification stage of BCI systems allow an adversary to modify the results of a classifier to produce unintended output commands.

The second stage in MCI and BCI systems that is vulnerable to attacks is signal acquisition. In neural interfaces, signal acquisition encompasses the physical process of collecting neural data from the body to transmission of that data to a computer or robotic device. Common attack types

during signal acquisition include sniffing in which an attacker can view or listen to a data channel transmission and spoofing in which a false signal can impersonate a true signal to deceive a device [7]. Three BCI studies were found that tested an adversarial attack during the signal acquisition stage. Armengol-Urpi et al. used a BladeRF to inject false signals imitating brainwaves into an SSVEP-based BCI device [59]. One form of signal noise occurs from electrodes collecting signals in the environment that are not related to the EEG signals of interest. The attack technique proposed by Armengol-Urpi et al. used this natural noise occurrence to their advantage by injecting sufficient noise into the BCI system to cause data misclassification without alerting the system to a possible attack [59]. The BladeRF effectively tricked the device into recording the false signals as if they represented real EEG data [59]. The BladeRF could modify frequencies and signal characteristics in real-time, making the attack mechanism ideal for experimenting with RF interference on an EEG-based BCI [59]. Bian et al. also studied signal acquisition vulnerabilities in SSVEP-based BCIs by implementing a square waveform to alter the frequency characteristics of neural data [52]. The frequency domain plays an important role in discriminating between neural data caused by different stimuli [52], thus manipulating the frequency data in the EEG dataset affected the ML output. Hossen et al. used modulated electromagnetic interference signals to inject noise into EEG data from seizures to lower the performance accuracy of various ML models [60]. The three existing studies on signal acquisition vulnerabilities did not utilize motor imagery or execution EEG data nor did they evaluate vulnerabilities in MCIs. Therefore, studies assessing vulnerabilities in the signal acquisition stage of neural interfaces remain limited and present an area of neural interface research that requires further exploration.

2.2.4 Functionality Effects of Adversarial Attacks

Adversarial attacks harm a user's independence and control over their device. Functionality impacts of an attack involve a neural interface performing an unintended action that causes a user physical harm or inhibits them from using their device as directed. Whether intended or unintended in nature, disturbances in EMG data can occur without being recognizable to the naked eye [61]. Noise or other chance interference does not cause intentional harm to a user, but it can have the same adverse effects as an adversarial attack if the signal disturbance causes misclassification of the data that sends an unintended command output to a peripheral device

[61]. This is especially dangerous when considering devices that utilize EMG data for motor restoration or enhancement such as exoskeletons and upper and lower limb prosthetics [61]. Malfunction of a lower limb neuroprosthetic device could cause a user to trip or fall. In some situations, misclassification of an output command could even harm a nearby individual. Attacks that intentionally alter the functionality of a neural interface could be performed to gain complete control over the user's peripheral device, whereby the user is no longer able to autonomously manage their health and safety. More broadly, devices that utilize biosignals such as BCIs that acquire EEG data can also be detrimental to the user if not properly functioning.

Researchers have implemented feedback loops in MCI and BCI devices to create an adaptable system for enhanced functionality. With a feedback loop, the user receives sensory stimuli to learn and adjust their behavior to improve system performance [15]. Although this provides a valuable service to the user, in relation to adversarial attacks, a built-in stimulus system can have a harmful effect. Gaining control over a closed-loop MCI or BCI system would potentially allow the adversary to send unwanted and dangerous stimuli to the user, threatening the user's health and safety [4].

An attack can also involve unauthorized access to a person's neural data. Obtaining EMG or EEG data can have indirect effects on an individual in addition to causing a disruption or malfunction in a neural interface system [42]. For instance, information stolen during signal transmission can be used to identify an individual or as an access point to obtain their personal information [42]. This situation would become even more detrimental if the device user utilizes EMG or EEG biometrics for authentication, enabling the adversary to use the acquired neural data to gain access to the user's accounts or systems. A seemingly insignificant breach of a user's MCI or BCI system can escalate to severe consequences if not properly handled. As such, privacy protections are needed to reduce unauthorized access to users' neural data.

2.2.5 Psychological Impact of Adversarial Attacks

In addition to affecting the functionality of a neural interface, attacks on an MCI or BCI system can have a psychological impact. Escalation in the number of computer hacks has increased the general public's awareness of cyber-based adversaries. However, the potential detriment of an attack on a neural interface is even higher than that of an attack on a computer [58]. Attacks on a neural interface can directly affect the well-being and free will of the user whereas a computer-

based attack only directly affects the computer itself [58]. Loss of control can invoke feelings of frustration, fear, and distress [4, 53]. Users might lose trust in the safety of their neural interface and choose to live without their device. Understanding the potential for an MCI or BCI to be hacked brings into question the risk versus reward of using a neural interface. For someone with severe movement impairment, the potential loss of autonomy due to an attack or other means might be worth the risk given the gain in mobility achieved by using the neural interface [4].

Ethical questions have arisen from BCI research studies such as how to determine whether a BCI device output is truly produced by the user. This addresses the concept of user autonomy and who bears the responsibility if a negative consequence occurs in response to an unintended command sent to a peripheral device. User autonomy is a topic commonly brought up in the discussion of BCI studies [4, 41, 49], though the emphasis on maintaining autonomy is typically in reference to risk of dependency and impaired self-perception rather than cyber-attacks. Neurotechnology continues to embed itself within human routine and societal function, thus cybersecurity needs to be a forethought when developing neural interfaces and considering their applications.

2.2.6 Securing Neural Interfaces

Biometrics serve as a unique identifier that allows for secondary authentication. As such, they have been used in two-factor authentication for a multitude of technological systems. Li et al. applied sEMG as a biometric for two-factor authentication of a device that used pattern unlock and found that this technique strengthened the security of the device [37]. Yamaba et al. also used sEMG signals from motor tasks to unlock a mobile device [62]. EMG data is more optimal as a biometric than the traditional facial and optical biometrics because if compromised, a new motor task can be used to replace the compromised token whereas traditional biometrics do not have that capability [13]. Since sEMG can be used for authentication in pattern unlock scenarios, it has potential use in sEMG-based MCI devices as a self-authentication measure. According to Jiang et al., EEG, EMG, fMRI, and MEG are the optimal identity verification biometrics for neural interfaces [13]. One approach would involve using a patient's physiological signals as a biometric to create a secure key to access the network of a neural interface device [54]. Landau et al. expanded upon basic user authentication for neural interface security by proposing continuous user authentication during device use [42]. By utilizing neural data already being

acquired for device operation, the user can secure their device while maintaining the efficacy of the neural interface. A second approach would entail using sensors placed around the body to form a bubble network containing only the user's neural interface device [54]. This system would allow for mobility of both the user and device while maintaining a secure connection.

The emphasis placed on neural interface device performance limits potential security features to those that have a minimal effect on the execution speed of the device. Thus, it is important to consider the applicability of a user verification technique in a neural interface to limit computational time and requirements while maintaining functionality. Authors have proposed adversarial training as a means to combat adversarial attacks [49]. Landau et al. recommended implementing anomaly detection, which is a subsect of adversarial training that can be used to mitigate attacks in the signal acquisition stage of a neural interface [42]. One approach that has been widely applied to amplifiers used for signal acquisition is common-mode rejection. Common-mode rejection is a technique that can lower the risk of interference due to noise or adversarial attacks by removing signals common across all electrodes [59]. For an adversarial attack based on noise injection, common-mode rejection would eliminate the false signal during signal acquisition, allowing for processing and classification of the neural data to proceed as intended. Despite the techniques and justification provided by researchers, many of these proposed solutions remain theoretical in the context of neural interfaces. Researchers need to test these security approaches so that they can be implemented in neural interface devices prior to their mass commercialization.

2.3 Neural Interface Applications Beyond the Medical Sphere

Neural interfaces have gained public attention in the past decade now that industries have begun their own research and development on these devices and have marketed them to garner consumer interest in their applications. Neural interfaces are being studied for use in the commercial sphere as companies aim to create a more interactive virtual reality (VR) or augmented reality (AR) environment [63]. Haptic suits provide a computer-to-human interaction by integrating electro muscle stimulation and transcutaneous electrical nerve stimulation to produce an immersive virtual experience [64]. Predicted growth of commercial availability and use of VR and AR products will encourage research and development on myoelectric-based systems for enhanced experience within an extended reality environment. Researchers have also

investigated synthesizing BCI technology with VR. As VR already requires a head piece, implementing a BCI element to the system would require minimal alterations to the headset design [22]. Studies on neural interface use in gaming have existed for over a decade [65-66]. The potential for BCI devices is high within the gaming market since most of the current gamer population includes individuals that have spent most of their lives implementing or immersed in technology [42]. These individuals are likely to be more inclined to adopt BCI devices for entertainment.

In 2015, Li et al. claimed that there are four main categories of BCI applications: medical, user authentication, entertainment, and smartphone-based apps [67]. Although these categories might have been the initial marketable areas for BCI technology, the potential applications of BCIs have expanded to additional societal domains. Integration of MCIs and BCIs in the processes and procedures for managing well-being, education, and marketing have also been explored [41]. The US Defense Advanced Research Projects Agency has also invested money to find military applications for BCIs for performance enhancement and neuronal or motor function restoration in soldiers [4].

Studies on neural interface vulnerabilities have identified that there has been insufficient investigation into security risks of neural interfaces, and that security measures and protocols need to be implemented for data confidentiality and user safety [7, 57]. Authors are also in agreement that increasing public awareness of neural interface security risks is imperative, especially given that neural interfaces are becoming more applicable in the commercial sphere [4, 42]. Industry research centers on device comfort, accuracy, and usability, with limited focus on device vulnerabilities. As with any form of technology, device security poses a concern for digital privacy and user safety. As applications for neural interfaces expand beyond the clinical domain, security vulnerabilities within these devices will impact a broader range of individuals. To proactively prepare for future privacy and security threats, continued studies assessing neural interface vulnerabilities need to be conducted.

3 Methodology

3.1 Subject Information

Eight individuals between the ages of 19 and 25 were recruited from the Tech4Humanity Lab at Virginia Tech to participate in this study. The study was approved by the Virginia Tech IRB and assigned protocol #25-167. All individuals were healthy adults with full range of motion in their upper limbs. Each participant signed an informed consent form prior to beginning involvement in the study.

3.2 Testing Methods

3.2.1 Subject Preparation

The dominant arm was used for EMG signal acquisition. Subjects sat in a chair with their dominant arm extended in the air in front of them. The hand of their extended arm was positioned so that their thumb faced towards the ceiling and their pinky finger faced the floor. This orientation was selected to minimize the effect of gravity on the selected motor tasks by having the subjects move their wrist laterally rather than vertically.

3.2.2 Electrode Placement and Signal Acquisition

sEMG data acquisition was conducted using silver/silver chloride gel electrodes placed on the flexor and extensor muscles of the forearm. Novice user placement was used to position the electrodes, resulting in electrode placement on non-specific flexor and extensor muscles. Based

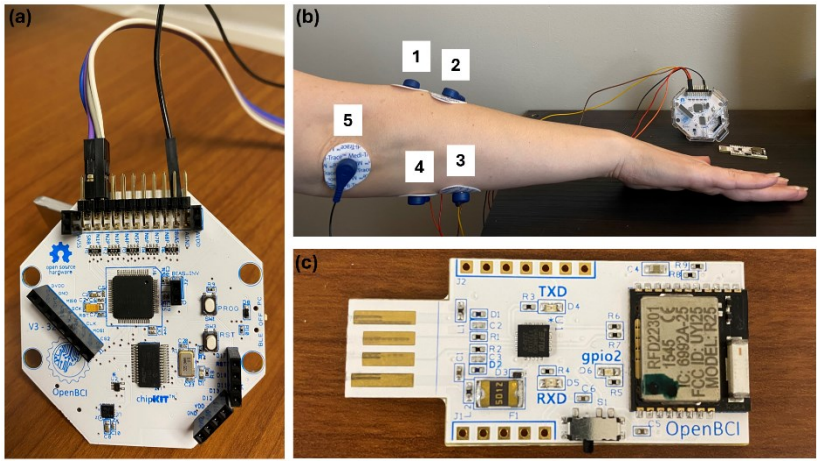

Figure 3.1: (a) OpenBCI Cyton biosensing board with cable setup. The purple and blue wires are connected to N1P top and bottom. The gray and white wires are connected to N2P top and bottom. The black wire is connected to the bottom of the BIAS terminal. (b) Electrode placement on forearm. Electrodes 1 and 2 are positioned over the extensor muscle group. Electrodes 3 and 4 are positioned over the flexor muscle group. Electrode 5 is positioned on the elbow and serves as the reference electrode. (c) OpenBCI USB dongle.

on known human anatomy, sEMG signals pertaining to the flexor muscles were most likely collected from the flexor digitorum and flexor carpi radialis [68]. The sEMG signals pertaining to the extensor muscle group were likely representative of extensor capri radialis brevis and extensor digitorum muscle contraction [68]. With novice electrode placement, crosstalk from surrounding muscles could occur due to less precise muscle targeting, leading to imprecise sEMG recordings during the movement tasks [69]. Crosstalk refers to sEMG signals collected from muscles adjacent to the electrode positioned on the target muscle, resulting in sEMG data that includes signals from multiple muscles [69]. This can lead to inaccurate sEMG recording of the target muscle, affecting target muscle analysis [69]. Advanced prosthetics would be set up for patients by clinicians, allowing for precise electrode placement on targeted muscles and minimizing crosstalk. The electrodes were arranged in a bipolar setup with one pair, electrodes 1 and 2, positioned over the extensor muscle group and a second pair, electrodes 3 and 4, positioned over the extensor muscle group. A fifth electrode was placed on the lateral epicondyle of the humerus to serve as a ground electrode to eliminate common noise detected by the electrodes on the two muscle groups. The ground electrode was positioned in proximity to the other electrodes to acquire similar noise signals but placed on an area of the body that minimized muscle activity [16]. The bipolar electrode setup can be observed in Fig 3.1b.

The electrodes were connected to an OpenBCI Cyton biosensing board using snap electrode cables (Fig 3.1a). The Cyton board is a commercially available eight-channel bio-amplifier containing a 32-bit processor powered by a rechargeable 3.7 V lithium-ion battery [18]. The Cyton board samples data at 250 Hz per channel and wirelessly transmits the data to a computer via the OpenBCI USB dongle using Gazell as the radio frequency transmission modality (Fig 3.1c) [18]. Given a sampling frequency of 250 Hz, the maximum frequency that can be accurately represented without aliasing is 125 Hz due to the Nyquist theorem which states that only frequency components less than half the sampling frequency can be properly reconstructed [70]. The majority of EMG signal power occurs within 20-200 Hz [16] and preliminary EMG recordings during flexion and extension motor tasks showed a drop in signal intensity after 100 Hz. Therefore, the low sampling rate of the Cyton board as compared to other recording devices with sampling rates at or above 1 kHz was not a concern for this study [71-72]. The first two channels, N1P and N2P, were used to record data from the extensor and flexor muscle groups, respectively.

3.2.3 Visual Cue Setup

Participants were shown a series of text-based visual cues on a monitor to direct motor task execution. The cues were displayed in black text on a light gray background and consisted of three sets of instructions presented in a cyclic manner. The first visual cue stated the upcoming motor task and displayed an arrow indicating the wrist motion direction relative to the stated task. The second cue signaled for the subject to begin the motor task and the third cue initiated a rest period. The task descriptor and rest cues were three seconds in duration and the begin task command cue was displayed for two seconds. Two motor tasks were chosen for the study: wrist extension and flexion. A single trial consisted of ten repetitions of each of the two motor tasks for a total of 20 movements per trial. Six trials were performed, with the first trial functioning as a practice run for the subjects and the subsequent five trials recorded and used for analysis. The amplitude of an individual's EMG signals is subject to minor changes as the person becomes more familiar with and adept at performing a particular task [73]; therefore, the motor tasks were randomized to minimize the influence of contextual inference on signal activity.

NeuroPype Suite is a platform for biosignal recording, processing, and analysis. The Experiment Recorder application within NeuroPype Suite was used to display the visual cues and insert data markers into the EMG signal stream. As visual cues were presented on the monitor, markers were added to the EMG signal data and saved as an XDF file for subsequent processing. The EMG data was streamed via the lab streaming layer from the OpenBCI GUI to the NeuroPype

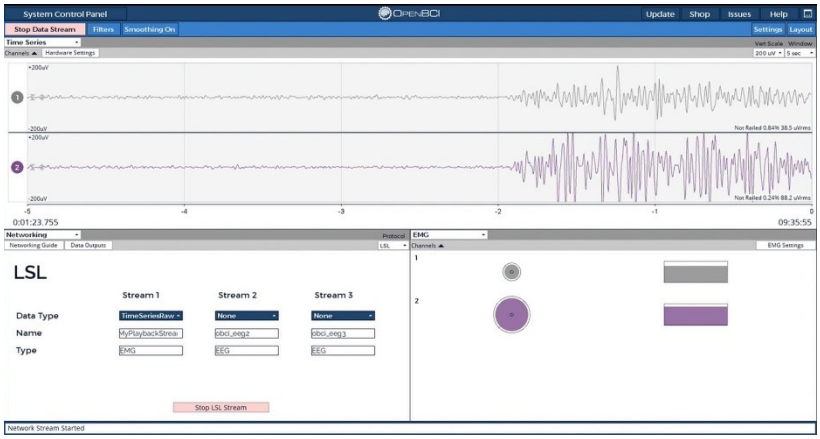

Figure 3.2: OpenBCI GUI displaying the Time Series, Networking, and EMG widgets for data visualization during streaming. The Networking widget allows the OpenBCI GUI to send data via the LSL for recording with NeuroPype Suite's Experiment Recorder.

Experiment Recorder. The OpenBCI GUI was configured to display the EMG signals in the time domain and the magnitude of signal strength, which allowed for the data to be monitored throughout the trials (Fig 3.2).

3.2.4 Processing and Classification Pipeline

Preprocessing and classification procedures for the XDF files containing the EMG data and markers were conducted in Python. Two channels were used to record data during testing and both channels underwent the same preprocessing procedure. EMG data is commonly filtered with a bandpass filter from 20-500 Hz [16, 24]. As the Cyton biosensing board has a sampling frequency of 250 Hz [18], which is within the 20-500 Hz frequency range, a band-pass filter was not needed to remove high frequency signals in addition to low frequency signals. Therefore, data preprocessing began with applying a fourth order Butterworth high-pass filter set at 20 Hz to remove low frequency noise (Fig 3.3) [16]. The filtfilt function was used to apply the filter with zero-phase distortion [74]. Subsequently, an infinite impulse response notch filter was applied to remove 60 Hz powerline noise (Fig 3.3).

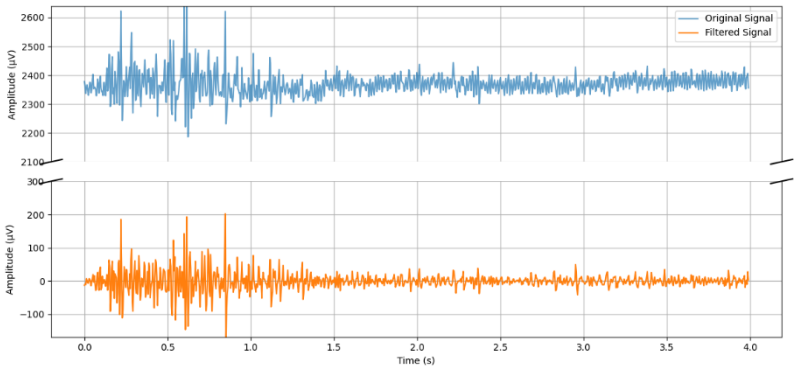

Figure 3.3: Channel 1 segment of raw EMG data (blue) and EMG data post notch and high-pass filtering (orange).

The filtered data was segmented into 2-second intervals based on marker data that was inserted into the EMG data during signal acquisition. The markers were added in real time to ensure that the timing of marker insertion aligned with subject wrist movements. The marker data was obtained via the marker stream present in the XDF file with a marker corresponding to each visual cue presented to the subjects during the testing session. There were three types of markers inserted in the EMG data. The first marker indicated whether the subsequent motor task was flexion or extension and was inserted into the EMG data when the upcoming task visual cue was presented to the subject. The second marker indicated the start time of the motor task and was inserted when the begin task cue was presented to the subject. The final marker indicated the end

of the motor task and was inserted when the subject was presented with the rest visual cue. The 2-second period between the start and end task markers was extracted from the filtered data to create motor task segments. The segments were labeled as flexion or extension based on the marker associated with the upcoming task visual cue. A set of 20 segments were created for each trial.

The RMS, mean absolute value (MAV), and waveform length (WL) were extracted from each segment as these are the commonly extracted features for classification based on the literature [39]. The RMS was computed by taking the square root of the average of the squared values of the signal [39]. The MAV was computed by finding the average of the absolute values of the signal [39]. The WL was calculated by summing the absolute differences between consecutive signal points [39]. Variable N represents the number of data points in the trial and variable x_i represents the signal values.

$$RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N} x_i^2} \qquad MAV = \frac{1}{N}\sum_{i=1}^{N} |x_i| \qquad WL = \sum_{i=1}^{N-1} |x_{i+1} - x_i|$$

The features were normalized to enhance the performance of an SVM classifier to distinguish between flexion and extension data segments. Although a classification system was not directly needed or utilized for this study, developing a functional MCI system with flexion versus extension classification provides a way to validate the theoretical adversarial attack frameworks presented in the discussion in future studies. An SVM classifier with a linear kernel was chosen for its broad use in neural interfaces. Ten-fold cross-validation was performed using StratifiedKFold from sklearn to evaluate model performance on a training dataset. The mean cross-validation accuracy for the model was 1.00. Pairwise feature plots were created to visually confirm that the model was not overfitting the data (Fig A1). The model was then fitted to the entire training dataset and used to make predictions on subject data. Averaging the classification accuracy across trials and subjects resulted in an overall accuracy of 97.6%, confirming that the myoelectric-computer interface system was performing as intended.

3.2.5 Signal Characterization in Frequency Domain

Fast Fourier Transform (FFT) converted each data segment into the frequency domain to conduct a frequency analysis. The FFT results were averaged across all segments in a single channel to obtain the mean FFT for each trial. Welch's method was used to find the Power Spectral Density

(PSD) of the averaged flexion and extension signals. The Welch periodogram approach was chosen for its smoothing feature that reduces signal variance to better detect major patterns in sEMG segment frequency content and it is a commonly used technique for sEMG frequency analyses [75]. The mean, median, and peak frequency metrics were calculated for each motor task and channel based on the PSD data. The mean frequency was computed by summing the product of frequency values and their corresponding PSD values and dividing by the total power [16]. The median frequency was found by calculating the cumulative sum of the PSD and identifying the first frequency (f_k) in which the cumulative power exceeded half the total power [69]. The peak frequency was determined by finding the index at which the PSD achieved its maximum value [62]. Variable N represents the number of frequency bins and variable $PSD(f_i)$ represents the PSD value at frequency f_i.

$$Mean\ Frequency = \frac{\sum_{i=1}^{N} f_i \cdot PSD(f_i)}{\sum_{i=1}^{N} PSD(f_i)}$$

$$Median\ Frequency = f_k\ where \sum_{i=1}^{k} PSD(f_i) \geq \frac{1}{2}\sum_{i=1}^{N} PSD(f_i)$$

The frequency metrics were analyzed to determine if they differed between flexion and extension motor tasks. Distinct differences would indicate that an adversarial attack could inject false signals at set frequencies to misdirect the MCI system's classifier into outputting an incorrect motor command. Therefore, assessing these metrics is relevant to understanding vulnerabilities in the transmission stage of MCI systems.

3.2.6 Adversarial Detection of Signal Transmission

The HackRF One was used to sniff data packets transmitted from the Cyton board to the USB dongle via Gazell to assess the ability for the developed MCI system to be hacked during frequency transmission. The adversarial attack technique schematic is shown in Fig 3.4. Gazell is a Bluetooth Low Energy (BLE)-like transmission modality as it uses the same 2.4-2.5 GHz frequency range to transmit information [76-77]. Gazell incorporates a frequency hopping functionality to minimize interference from nearby radio frequency sources [76, 78]. The frequency hopping mechanism prevents signals from being viewed or acquired by traditional Bluetooth sniffers [76, 78]. The HackRF One is a software defined radio peripheral capable of simultaneously sniffing and recording multiple channels worth of signals in the 2.4-2.5 GHz frequency range [79]. The device requires a USB connection to a computer downloaded with

HackRF software that enables interaction with the HackRF One device [80]. The maximum detection range of the HackRF One is not fixed, rather it depends on the signal strength and frequency from the target device, the HackRF One antenna type and quality, the specified HackRF One gain setting, and any interference due to walls or objects [80].

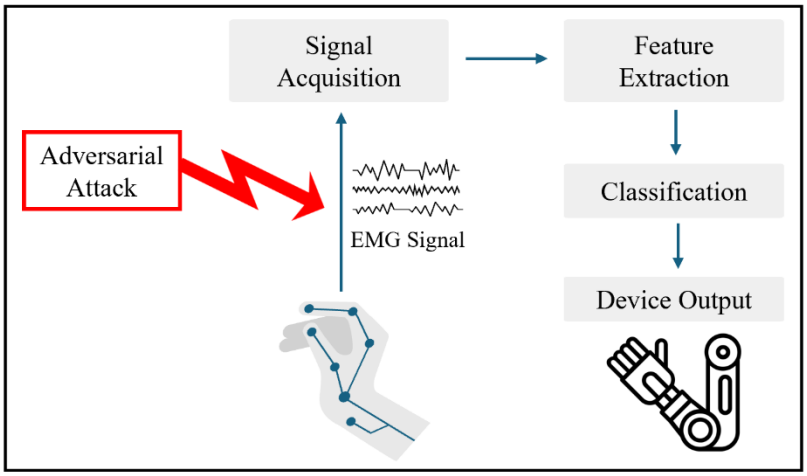

Figure 3.4: MCI system displaying the stage in which an adversarial attack will be performed.

The HackRF was connected via a secondary computer with the necessary HackRF tools installed within a Linux virtual machine. Gqrx, a software defined radio (SDR) receiver, was used to visualize data obtained by the HackRF One in real time [80-81]. EMG data streaming via the OpenBCI GUI was performed while the HackRF One actively swept the surrounding area for signals within the 2.4 GHz range. Data collected by the HackRF One was stored in CSV files for analysis. A single sweep consisted of obtaining a data point at each frequency across a set frequency band. Sweeps were performed consecutively for roughly 12 seconds to obtain and store sufficient data for analysis. The frequency bands chosen for data collection were 2.4-2.5 GHz, 2.416-2.420 GHz, 2.442-2.446 GHz, and 2.466-2.470 GHz. The 2.4-2.5 GHz band was chosen as it encompasses the whole range in which Gazell transmits signals [76]. After visualizing the full frequency spectrum, frequency bands displaying increased power activity were identified and narrowed readings were taken to see the specific frequency within each range that was used for hopping. Screen recordings of the Gqrx were taken to visualize changes in the Cyton board transmission data that were occurring in real time. The data was analyzed in Python. A spectrogram was created to determine whether the frequency hopping pattern of the Cyton board's signal transmission could be identified using the HackRF One.

Subsequent and alternative adversarial attack techniques within the signal transmission phase of MCIs were assessed theoretically. The first technique involved sending false EMG signals to the primary computer via the HackRF One to cause unintended classification and output commands to a peripheral device that is part of an MCI system. Additionally, a theoretical framework for an adversarial attack using a second OpenBCI USB dongle was considered for plausibility.

3.3 Statistics

Each frequency metric (mean, median, and peak frequency) was averaged across all five trials for each motor task. Paired T-tests were performed using SciPy.stats to calculate p-values for the comparison of frequency metrics between flexion and extension across subjects. A paired T-test was chosen because both the flexion and extension motor tasks were performed by each subject, allowing the data to be paired by subject and controlling for within-subject variability in the statistical analysis.

4 Results

4.1 Signal Transmission Attack

A 12 second sweep performed by the HackRF One captured signals transmitted in the 2.4-2.5 GHz frequency band. The HackRF One sampling frequency was 1 MHz. A spectrogram portraying the power for each frequency is displayed in Fig 4.1a. A -30 dB threshold was applied to the dataset and all data below the threshold was removed. The resulting spectrogram is shown in Fig 4.1b. The three frequency bands showing elevated power levels throughout the 12 second sweep were 2.416-2.420 GHz, 2.442-2.446 GHz, and 2.466-2.470 GHz. Distinct tick marks in the spectrogram demonstrate the presence and absence of signal transmission at a particular frequency and time. Of the identified frequency bands, it can be visualized in Fig 4.1 that when one of the three bands has an absence of tick marks, another band is experiencing peaks in power represented by the presence of tick marks in that frequency band. A HackRF One sweep for each of the identified bands was performed to identify the distinct frequencies with heightened power activity.

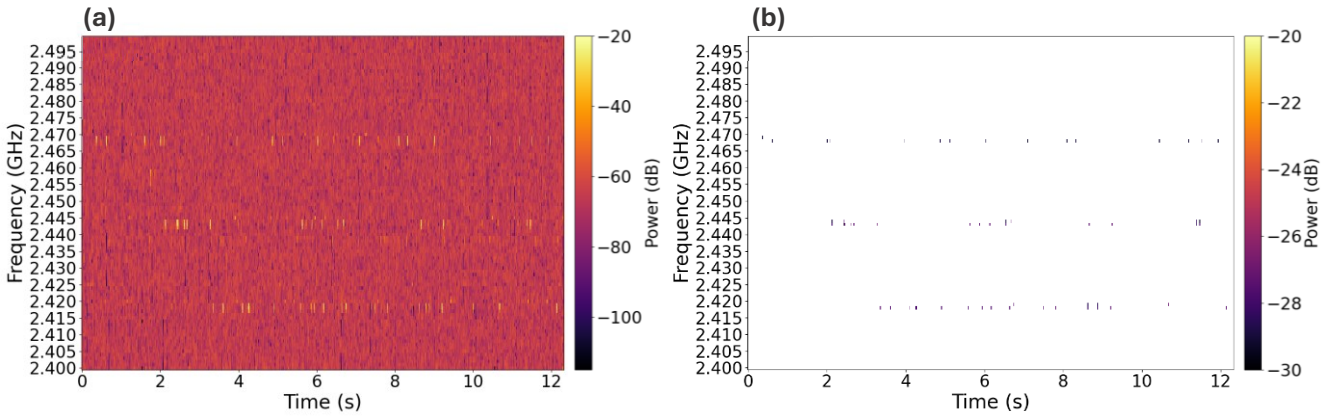

Figure 4.1: Spectrogram displaying HackRF One sweep from 2.4-2.5 GHz sampled at 1 MHz to collect Cyton board transmission signals. (a) All power data for each frequency in range. (b) Power data thresholded at -30 dB for each frequency in range.

The data for each narrowed sweep was thresholded at -30 dB and plotted as a spectrogram (Fig 4.2). Each of the three subplots displayed periodic spiking at two frequencies within the frequency bands, with one frequency in each plot exhibiting a more consistent spiking pattern. The frequencies identified as having regular power peak intervals were 2.418 GHz (Fig 4.2a), 2.444 GHz (Fig 4.2b), and 2.468 GHz (Fig 4.2c). The regularity of power peaks at these frequencies reveals the frequency hopping pattern present during Cyton board signal transmission.

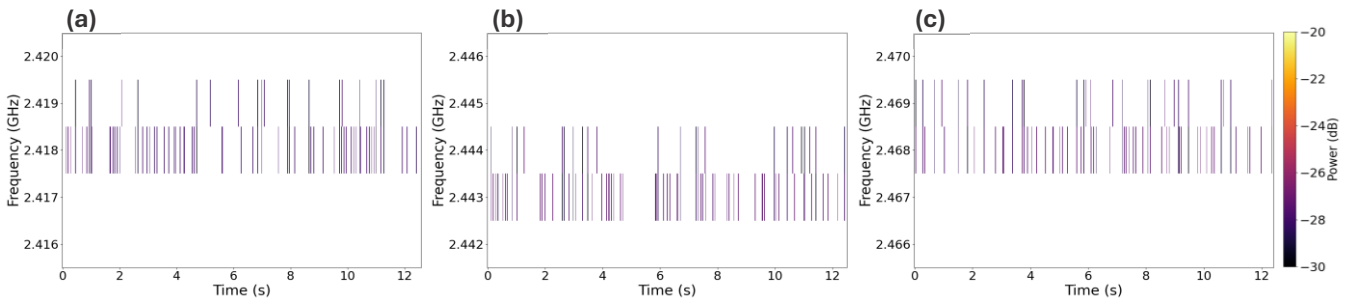

Figure 4.2: Spectrograms thresholded at -30 dB displaying HackRF One sweep sampled at 1 MHz for the identified frequency ranges. (a) 2.416-2.420 GHz. (b) 2.442-2.446 GHz. (c) 2.466-2.470 GHz.

Gqrx screenshots were taken during real time HackRF One sweeps. A screenshot during each of the eight phases in the complete Cyton board transmission process is displayed in Fig 4.3. As the Cyton board requires recharging, the board cannot stream data 24/7. Therefore, in addition to data streaming, pairing and initialization are part of the dynamic operation of the Cyton board. When the Cyton board was powered off (Fig 4.3a), there was no signal transmitted to the USB dongle as indicated by the absence of power spikes. Powering on the Cyton board caused almost immediate pairing with the USB dongle as reflected by nonuniform power spiking at 2.418 GHz, 2.443 GHz, and 2.468 GHz (Fig 4.3b). Cyton board initialization commences when a streaming session is started in the OpenBCI GUI and is characterized by a brief power spike at most frequencies across the 2.41-2.47 GHz range (Fig 4.3c). After a streaming session had been initiated but prior to starting the data stream, sporadic power spikes occurred at 2.418 GHz (Fig 4.3d). These power spikes dissipated following successful Cyton board pairing and initialization. During data streaming, there were repetitive power spikes at the three identified frequencies (Fig 4.3e). Stopping the data stream resulted in an immediate cease in power spikes at 2.443 GHz and 2.468 GHz (Fig 4.3f). The Cyton board then returned to its paired but idle state in which only power spikes at 2.418 GHz were present (fig 4.3g). Sporadic spiking at 2.418 GHz when the Cyton board is paired but not streaming data demonstrates that communication still occurs between the Cyton board and USB dongle despite the absence of EMG signal data. Powering off the Cyton board severed the connection with the USB dongle and terminated all signal transmission between the components.

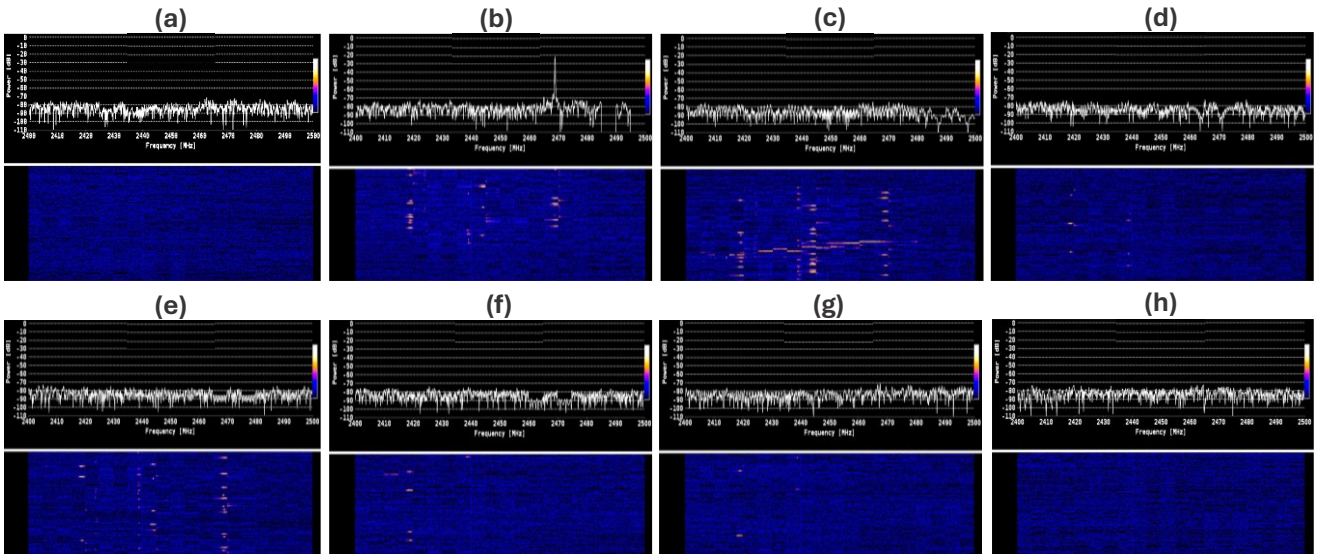

Figure 4.3: Gqrx visualization of the HackRF One stream showing the complete Cyton board transmission process. The frequency band was configured to 2.4-2.5 GHz and the HackRF One was set to a gain of 40 dB. (a) Cyton board powered off. (b) Cyton board pairing with USB dongle. (c) Cyton board initialization. (d) Cyton board paired and initialized, pre-data stream. (e) Cyton board transmitting during data stream. (f) Data stream stopped. (g) Cyton board paired, no active data steam. (h) Cyton board powered off.

4.2 Frequency Characteristics

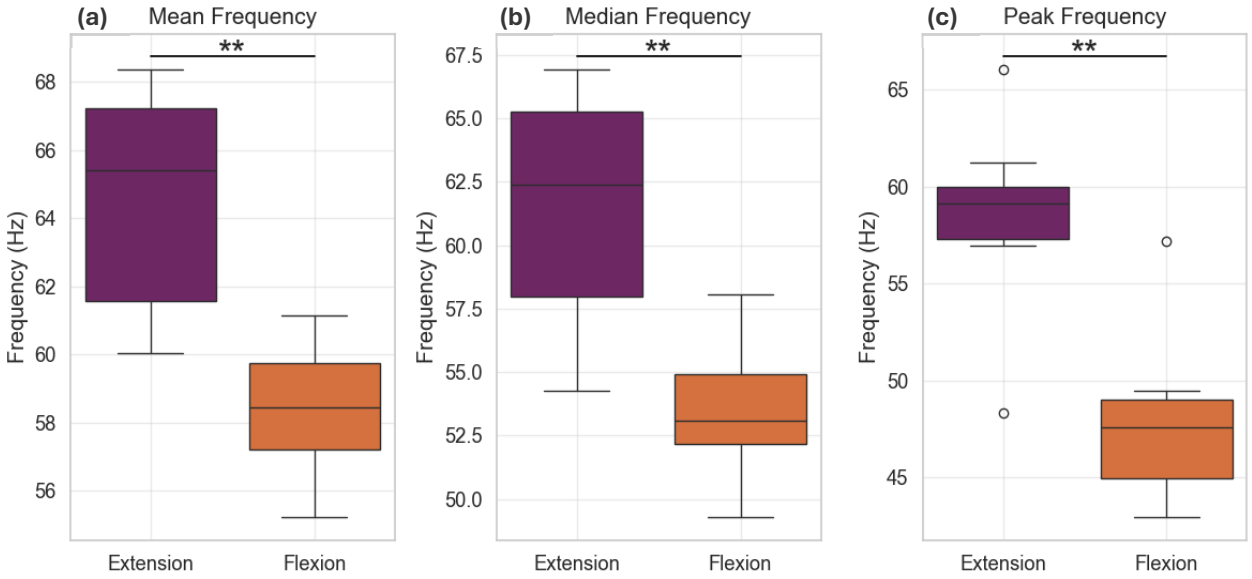

Figure 4.4: Comparison of frequency metrics between flexion and extension motor tasks averaged across channels and trials for each subject. Paired T-test results are indicated by asterisks where ** denotes $p < 0.01$. (a) Mean frequency. (b) Median frequency. (c) Peak frequency.

Box and whisker plots were created to compare frequency metrics for flexion and extension motor tasks (Fig 4.4). The average mean, median, and peak frequencies for the motor task segments were calculated for each channel and trial and averaged per subject, resulting in a

single flexion and extension value per subject for each frequency metric. Paired T-tests revealed the difference in values between flexion and extension motor tasks for all three metrics to be statistically significant ($p < 0.01$).

Fast Fourtier Transform (FFT) was used to convert the motor task segments into the frequency domain. The FFTs for channels 1 and 2 from a single subject and trial were displayed in Fig 4.5. Channel 1 and 2 electrodes were placed on the extensor and flexor muscle groups of the forearm, respectively. As expected, the strength of the sEMG signal for extension was greater for channel 1 as the electrodes were directly over the muscles responsible for enacting the extension movement. The same result was seen for flexion in channel 2. Despite experiencing decreased signal strength in channel 1, the peak FFT frequency for flexion was less than 50 Hz for both channels. Across the two channels, the peak FFT frequency for extension was greater than that for flexion, corroborating the results seen in Fig 4.4c.

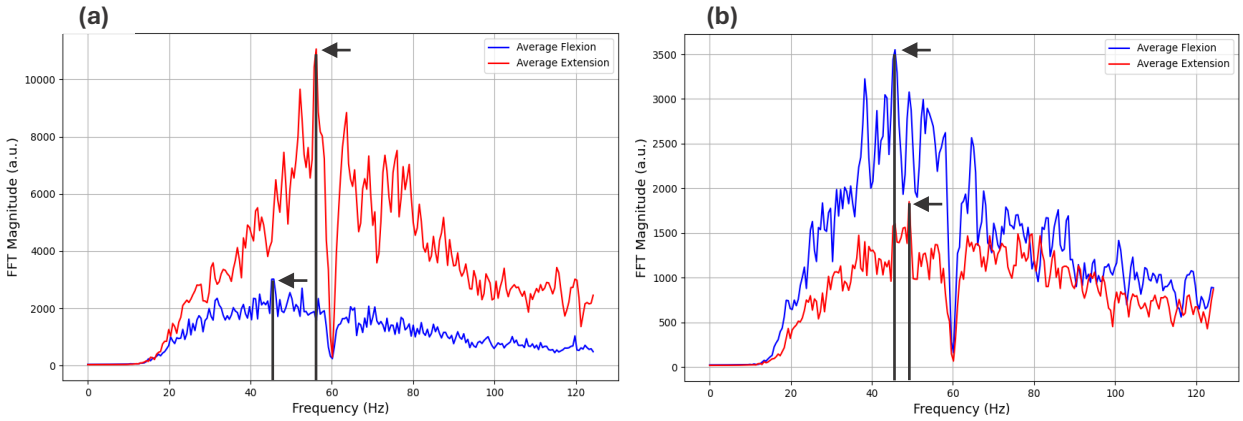

Figure 4.5: Fast Fourier Transform for averaged flexion (blue) and extension (red) motor tasks for a single subject trial. (a) Channel 1. (b) Channel 2.

A single flexion and extension segment in the time domain is shown for channels 1 and 2 in Fig 4.6. There was a distinct increase in sEMG amplitude during motor movement as compared to rest for both channels. Similar to the increase in magnitude of the extension frequency data during an extension motor task seen in the channel 1 FFT plot in Fig 4.5a, there was a corresponding increase in the amplitude of the extension sEMG signal for channel 1 in the time domain. The same pattern was observed for channel 2 during a flexion motor task. Despite the apparent difference in signal strength seen in Fig 4.6, the only instance in which the difference in frequency metrics between channels 1 and 2 was statistically significant was the mean frequency for flexion (Fig 4.7a) with $p < 0.05$. The absence of statistically significant differences in

frequency metrics between the two channels indicates that electrode placement might be independent of sEMG frequency characteristics for the motor tasks studied. A second explanation is the presence of crosstalk during signal acquisition in which the extension channel, channel 1, was picking up flexor activity during a flexion motor task and the flexion channel, channel 2, was picking up extensor activity during an extension motor task.

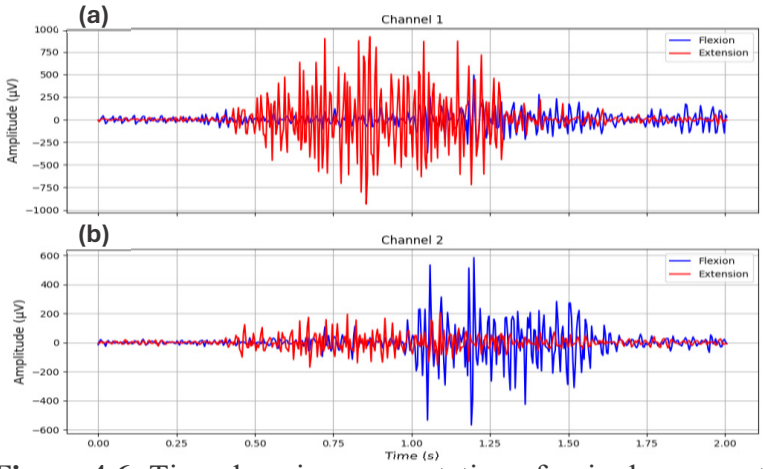

Figure 4.6: Time domain representation of a single segment for flexion (blue) and extension (red). (a) Channel 1. (b) Channel 2.

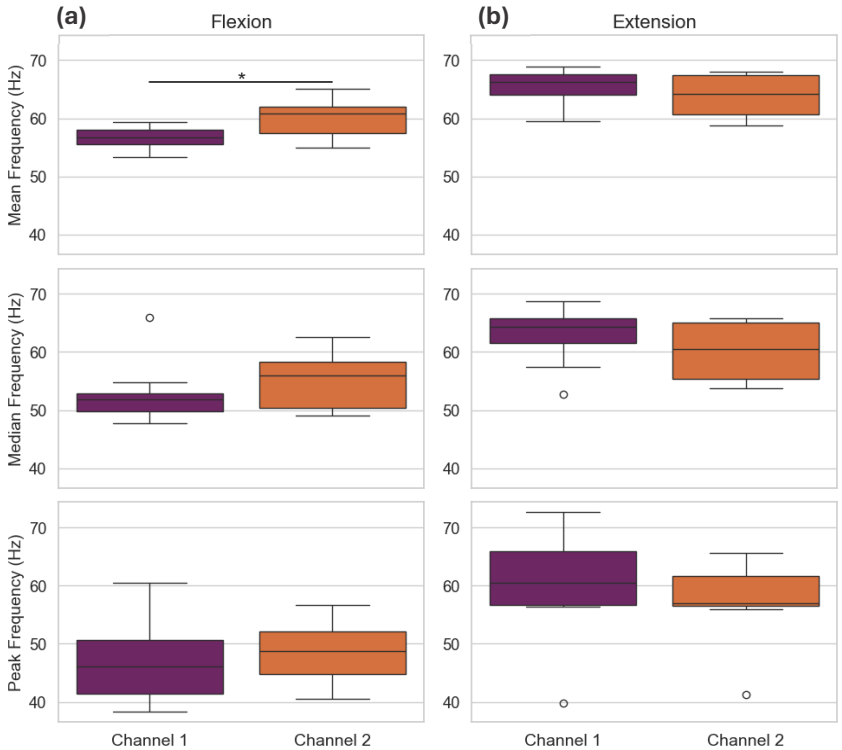

Figure 4.7: Comparison of frequency metrics between channels for flexion and extension motor tasks. Paired T-test results are indicated by asterisks where * denotes $p < 0.05$. (a) Flexion frequency metrics. (b) Extension frequency metrics.

The frequency metrics for each subject averaged across trials for flexion and extension are presented in Table 4.1 and Table 4.2. There was minimal between subject variability, indicating that the results from the earlier figures can be generalized to a broader range of individuals.

Table 4.1: Frequency metrics by subject for flexion

	Flexion		
Subject	**Mean Frequency (Hz)**	**Median Frequency (Hz)**	**Peak Frequency (Hz)**
1	59.395	54.48	47.73
2	61.135	58.065	57.195
3	56.39	49.26	42.93
4	57.465	52.465	45.53
5	58.38	58.165	43.13
6	60.815	56.195	47.46
7	58.515	53.465	49.46
8	55.205	51.195	48.865

Table 4.2: Frequency metrics by subject for extension

	Extension		
Subject	**Mean Frequency (Hz)**	**Median Frequency (Hz)**	**Peak Frequency (Hz)**
1	68.375	64.915	59.015
2	64.815	61.465	61.265
3	65.975	63.265	59.2
4	67.035	66.96	66.065
5	61.99	58.73	56.93
6	60.345	54.26	48.33
7	67.815	66.26	59.53
8	60.03	55.66	57.4

5 Discussion

Based on the reviewed literature, there have not been previous studies assessing signal transmission vulnerabilities in MCI systems and minimal studies focused on transmission security risks in BCI systems. Two stages of an adversarial attack were considered in this study. Investigating the frequency transmission patterns used by a biosensing board developed for neural interface use addressed the potential for sniffing and intercepting signal data during normal MCI system functioning. Evaluating sEMG data in the frequency domain considered whether frequency patterns provide a means for manipulating or sending false data to an MCI system to reduce device efficacy. Studying these potential attack points and techniques addressed a critical need in protecting neural data and user safety with regard to MCI devices and the broader neural interface domain.

5.1 Frequency Hopping Implications on Attack Potential

Detecting and collecting signal frequency data using the HackRF One accomplished the first study objective aimed at identifying frequency hopping patterns used by the Cyton board during signal transmission. Fig 4.1 findings visually indicated that there were three frequency bands utilized by the Cyton board in the 2.4-2.5 GHz range while transmitting data to the USB dongle. The narrowed HackRF One frequency sweeps performed within the three frequency bands and plotted in Fig 4.2 showed two frequencies with periodic power spikes for each of the frequency bands. For each band, one frequency experienced more frequent power spikes and thus was considered the main frequency used in Cyton signal transmission hopping. The secondary frequency for each band was thought to be spillover from the primary frequency caused by imperfect signal data collection via the HackRF One. Therefore, the three primary frequencies were established as the frequency hopping participants. Frequency hopping is a known characteristic of the Gazell protocol, but specific hopping frequencies vary according to the product type utilizing Gazell [76]. Therefore, biosensing boards other than the Cyton board developed by OpenBCI might use different hopping frequencies for transmission. However, as Cyton boards are developed with the same proprietary Gazell protocol and firmware, these boards would be expected to exhibit identical hopping frequencies. Understanding these hopping patterns allows for transmission detection by an adversary that can then sniff and collect signal

data. Furthermore, these patterns could be mapped and mimicked to spoof the USB dongle receiver and provide an adversary with access to the MCI system.

The Gazell frequency hopping functionality provides an innate layer of protection against attacks. This technique is implemented to reduce interference from other nearby signals in the 2.4 GHz frequency band as described by Karabacak et al. [78], which inadvertently makes it more challenging for an adversary to collect all data being transmitted and potentially send a false signal that is appropriately received by the USB dongle. Bluetooth is the second main transmission modality used by motor-based neural interfaces [55]. Similar to Gazell, Bluetooth uses frequency hopping. However, it incorporates an adaptive frequency hopping mechanism that allows for dynamic control over hopping frequencies [82], which is more advanced than Gazell's proprietary protocol. Thus, both transmission modalities provide neural interfaces with a fundamental structure for security protection.

The complete signal transmission process conducted by the Cyton board was presented in Fig 4.3 which showed changes in power activity across the 2.4-2.5 GHz band during different phases of the transmission process. The Cyton board is powered by a lithium ion battery that requires regular recharging. During experimental testing, it was found that operative EMG signal acquisition declined as the Cyton board's battery power depleted, highlighting the need for consistent charging. As charging requires disconnecting the battery from the Cyton board, the board must regularly undergo the pairing and initialization process. As shown by Fig 4.3d, there was only one frequency with active power spikes when the Cyton board was paired and initialized, but the data stream had not started. Therefore, there is a time period when signal transmission is occurring without frequency hopping, presenting an opportunity for signal interception without needing to know hopping patterns. An attack at this stage would not prevent sEMG data collection because there would be no data stream from the Cyton board. However, it would enable a Denial-of-Service attack, preventing neural interface functioning if the user attempted to initiate peripheral device commands via their MCI system since the sEMG signals would not be successfully transmitted. Though the timeframe for this attack is small and dependent on the adversary knowing when a user will pair and initialize their neural interface's biosensing board. The halt in frequency hopping also occurs when the board ends a streaming session as shown in Fig 4.3f and Fig 4.3g, providing an additional opportunity for an adversarial

attack that does not require matching frequency hopping patterns. Despite the increased opportunity for attack during these stages, an adversary must first identify the frequency used to maintain the Cyton board and USB dongle connection prior to being able to perform the attack. Therefore, the signal transmission attack potential on a device that uses a Gazell protocol is possible but limited by opportunistic timing and an understanding of transmission frequency hopping patterns.

5.2 Using Frequency Metrics for Adversarial Attacks

The mean, median, and peak frequency for each motor task was calculated to assess the potential for sEMG signal manipulation by an adversary, as outlined in the second study objective. The frequency domain was chosen for analysis instead of the time domain because manipulating signal transmission data would be expected to involve sending radio frequency signals. Therefore, frequency characteristics provide the optimal approach for performing an adversarial attack. These metrics were selected for their targeted approach capabilities and are considered important features in the frequency domain [83]. The mean frequency is calculated as the average frequency of power distribution and was predicted to differ between motor tasks. The median frequency is less impacted by outliers and was thus expected to be a more robust characteristic for distinguishing between motor movements. The peak frequency is the most visually distinct as it can be viewed in an FFT or PSD plot and was predicted to differ between motor tasks. This would allow an attacker to inject a false frequency with heightened power to manipulate data transmitted through the MCI system for classification.

Bian et al. identified that the attack success rate for a perturbation-based attack on an EEG-based BCI system differed by subject [52]. The attack proposed for this study focused on frequency domain characteristics to determine if false frequency signals could be used to spoof the MCI system's classifier. Given that frequency metrics are critical to assessing the plausibility of a spoofing attack, differences in the metrics between motor tasks provided insight into attack potential. Although novice electrode placement was used for signal acquisition in this study, there were still distinct frequency differences observed between the two motor tasks that an attacker could exploit to perform a targeted attack. The flexion and extension frequency domain findings by subject presented in Tables 4.1 and 4.2 showed that there was minimal between-subject variability. This indicated that although attack success could experience small variation

between subjects, the relative success would likely be comparable due to similarities in frequency metrics across the subjects tested. According to Muceli and Merletti, a subject's adipose tissue mass over the muscles of interest and the electrode position and size impact sEMG frequency content [75]. The findings contradict this claim as the subjects' muscle and adipose mass differed but resulted in minimal frequency content variability between subjects. Muceli and Merletti also proposed that electrode modality, a monopolar or bipolar setup, impacts sEMG bandwidth [75]. Although there might be variability in frequency bandwidth across device setups, bandwidth is less likely to be utilized by an adversary for a spoofing attack than the mean, median, or peak frequencies because it is a less targeted approach. An adversary can more easily send a false signal at a set frequency based on the mean, median, or peak frequency metrics of motor tasks rather than manipulating a broader set of signal frequency properties to mimic a certain bandwidth range. Furthermore, the frequency metrics comparison between channels was only significantly different for the mean frequency during flexion, indicating that electrode placement is not a major contributor to frequency domain characteristics. The structure, number, and style of electrode varies between MCI and BCI devices. Therefore, the absence of a significant difference between subjects and across channels suggests that distinguishing motor task sEMG frequency metrics are applicable to a wide range of neural interface devices, improving generalizability of the research.

The ability to send false signals broadens the scope of neural interface vulnerability because it enables an active attack. Eavesdropping and collecting signal transmission data, which was conducted using the HackRF One was a passive form of attack. Those techniques were performed without altering the transmitted signal or the MCI system and therefore did not pose immediate direct harm to a user. The attack mechanism becomes active when the adversary interferes with transmission by manipulating or sending false signals for classification. The distinguishing frequency characteristics observed in this study in addition to their similarity across subjects and between channels increases attack potential generalizability and augments security concerns.

5.3 Theoretical Attacks

While the following proposed attacks were not explicitly examined in this research, the findings offered insight into the mechanisms by which the proposed attacks could be executed, fulfilling

the third study objective. This section theoretically exemplifies how an understanding of frequency characteristics and frequency transmission hopping patterns provide access points to adversaries to intercept and manipulate data from neural interfaces during signal transmission. A thorough understanding of potential points of attack can facilitate instituting more effective security measures to minimize attack success rates.

5.3.1 False Signal Injection via HackRF One

A MITM attack is an active form of attack composed of two stages, data interception and data manipulation [42]. The HackRF One demonstrated its capacity for data interception by successfully eavesdropping on and collecting transmission data sent from the Cyton board to the USB dongle. The second stage of attack would involve data manipulation to spoof the USB dongle into accepting false signals, effectively executing a MITM attack. The HackRF One is an SDR that can both send and receive signals, enabling the device to perform both stages of attack [79]. Evidence of distinctions in frequency characteristics for motor tasks could be used in this context to send a signal at set frequency parameters to cause the neural interface's classification algorithm to output a particular command, effectively giving an attacker control over the actions of a neural interface's peripheral device. This attack technique requires both an understanding of the frequency transmission hopping pattern and sEMG frequency metrics to allow an adversary to perform a targeted attack that produces a particular unintended movement. Although not tested in this study, the findings suggest that implementation of this technique is plausible.

From a conceptual standpoint, the limitations of adversarial attacks during the machine learning stage of neural interfaces proposed by Meng et al. and Zhang et al. are in part applicable to signal transmission. These authors proposed that a partial understanding of the machine learning model is needed to perform a perturbation attack [49, 53]. In the realm of signal transmission, it would be ideal for an attacker to understand sEMG frequency characteristics for various motor tasks to most effectively create and transmit a false signal for a spoofing attack. Therefore, insufficient comprehension of sEMG frequency components could limit attack potential, though the attacker could still perform an untargeted attack by sending false signals at different frequencies to cause unintended classification. As such, current vulnerabilities in Cyton board security present an opportunity for MITM attacks to occur during signal transmission of the proposed MCI system.

5.3.2 Imposter USB Dongle

A second access point in the signal transmission stage of the proposed MCI system is through the use of a secondary OpenBCI USB dongle. The Gazell protocol's default settings use a star network topology in which one host, the USB dongle, can connect to up to eight Cyton boards [76]. The Cyton board will only pair to one USB dongle if two dongles are in proximity to the board [76]. Powering on the Cyton board initiates pairing with a nearby dongle in which a connection is established with the dongle that matches the board's expected host address [76]. The second USB dongle remains idle unless the first dongle is turned off or loses connection [76]. In the event of a break in connection, an adversary could initiate pairing with the Cyton board using their imposter USB dongle. Using an imposter USB dongle enables an attacker to intercept sEMG data transmitted by the Cyton board and analyze it in real time as the OpenBCI GUI could be run on the adversarial computer to monitor the incoming sEMG signals. This attack technique does not allow for sending false signals, rather it redirects the Cyton board into providing the adversary with the user's sEMG data by sending the data directly to the adversarial computer during signal transmission. Thus, this is a Denial-of-Service attack mechanism to impede communication between the user and neural interface's peripheral device while allowing an adversary to access a user's neural data. This inhibits a user's ability to interact with their neural interface and provides unauthorized access to personal data, thereby exposing potential security risks with current Cyton board transmission protocols.

5.4 Implications

Limited previous studies on MCI vulnerabilities and minimal neural interface studies on signal acquisition weaknesses presented a knowledge gap in neural interface functionality that needed to be addressed. Data privacy and physical safety of users is an important consideration in development of neural interfaces for both medical and commercial applications. The broad range of medical conditions and injuries that cause motor impairment provide a significant population of patients that would benefit from neural interfaces aimed at restoration or rehabilitation of motor function. The applicable population expands dramatically when neural interfaces are incorporated into daily life and entertainment. Though neural interfaces may augment human experiences either clinically or commercially, they pose harm to users and those they interact with if not properly secured. Adversarial attacks on these devices can affect the functionality of

neural interface systems by initiating unintended movements resulting in a loss of user control and autonomy and obtaining user's neural data [61]. Attacks also impact the psychological well-being of users by reducing user trust in their device and triggering emotional distress [4, 53]. To mitigate risks to users, it is essential to implement security and privacy protections during neural interface development.

This is not the first instance in which humanity was unprepared for the substantial implementation of technology into society. Initial creation of the internet did not include implementation of security as cyber threats did not exist when the internet was first established [57]. The system was then unprotected when cybercrime commenced. Retroactively attempting to secure a system to combat rising security threats has proved challenging given the numerous data breaches that continue to occur on the internet [57]. Learning from this situation, securing neural interfaces prior to their mass distribution would reduce the number of successful attacks on these devices in the future. Furthermore, early addition of security measures will initiate development of a framework for continuous security modifications as adversaries become more adept at hacking neurotechnology systems. Finally, informing potential consumers on the device vulnerabilities presented in this research enables them to make educated decisions on the use of neural interfaces.

5.5 Limitations and Future Research

The frequency characteristic analysis was limited in that it only tested sEMG frequency content for right-handed individuals. Angelova et al. concluded that natural differences exist between a person's left and right upper limbs that may result in sEMG signal variability, as determined by analyzing stroke impact on motor movement [84]. Whether differences in left and right upper limbs during motor tasks is applicable to motor-based neural interface systems would require further exploration. The use of novice electrode placement may have impacted the frequency domain analysis due to crosstalk arising from less-targeted electrode positioning. Crosstalk could explain the similarity in EMG frequency metrics across channels during each motor task. Physiologically, it would be expected that electrodes not positioned over the active muscles would have minimal EMG activity as those muscles were not involved in the motor task [69]. A future study applying more precise electrode placement is needed to determine whether the EMG activity observed in a non-targeted channel is due to crosstalk. Additionally, this study focused

on two upper limb motor tasks applicable to MCI systems. Testing the frequency characteristics of other commonly used motor tasks in neural interfaces should be considered for increased robustness. Applying findings from the study to develop proposed attack techniques were only considered theoretically. Future research could validate the attack mechanisms to more thoroughly assess their plausibility. Considering security techniques to mitigate attack potential would be an effective next step in studying neural interface security. Evaluating the security measures implemented for other neurotechnology devices would be a valuable basis for incorporating data and safety protections in MCI and BCI systems. Regular security risk assessments would enable security measures to remain current and ensure continuous protection against adversarial attacks.

6 Conclusion

Neural interfaces, including MCIs and BCIs, are part of an evolving field that has expanded beyond its initial product market in the medical domain to more widely used applications in gaming and entertainment. Continued progress in this field will yield a broader consumer base with the potential to impact an extensive population of people. Although neural interfaces promise numerous benefits to individuals and society to restore or rehabilitate motor impairment and augment the realm of entertainment, there is a potential for them to cause considerable harm. Adversarial attacks on neural interface systems could be performed to gain access to a user's data, take control over a device, or inhibit device functioning to negatively harm an individual and people in their vicinity. More than impacting device functionality, attacks could inflict psychological harm on users by taking away their autonomy, evoking fear and distress. Despite potential attack risk, minimal research has assessed vulnerabilities in motor-based neural interfaces and corresponding device safeguards. To minimize neural interface vulnerability to attack, measures must be taken to properly secure these devices. Effectively securing neural interfaces requires an understanding of the possible stages of attack and the mechanisms by which an adversary could attempt to infiltrate a neural interface device.

This research provided insight into potential vulnerabilities in the signal transmission stage of an MCI system that utilized the Gazell transmission protocol. The findings indicated that the frequency hopping patterns add an innate layer of protection during data transmission but still allow for eavesdropping and data interception. A frequency characteristic analysis determined that distinctions in frequency metrics between motor tasks could be exploited by an adversary to perform a MITM attack. Further analysis into frequency characteristics of additional motor tasks commonly used in neural interfaces designed for movement should be studied to more comprehensively explore vulnerable aspects of sEMG data. Two theoretical attack techniques were proposed based on the findings in this study to either deny service to the MCI device or intercept and manipulate signals to induce unintended motor commands. Future research should validate whether these attack methods are viable as well as introduce security measures to protect against attacks. As neural interfaces advance and their applications broaden, it is imperative that security be a forethought in designing these devices to ensure data privacy and security.

References

[1] J. J. Vidal, “Toward Direct Brain-Computer Communication,” *Annu. Rev. Biophys. Bioeng.*, vol. 2, no. 1, pp. 157–180, 1973, doi: 10.1146/annurev.bb.02.060173.001105.

[2] J. J. Shih, D. J. Krusienski, and J. R. Wolpaw, “Brain-Computer Interfaces in Medicine,” *Mayo Clin. Proc.*, vol. 87, no. 3, pp. 268–279, 2012, doi: 10.1016/j.mayocp.2011.12.008.

[3] L. R. Hochberg *et al.*, “Neuronal ensemble control of prosthetic devices by a human with tetraplegia,” *Nature*, vol. 442, no. 7099, pp. 164–171, 2006, doi: 10.1038/nature04970.

[4] M. Ienca and P. Haselager, “Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity,” *Ethics Inf. Technol.*, vol. 18, no. 2, pp. 117–129, 2016, doi: 10.1007/s10676-016-9398-9.

[5] S. Vashisht and B. Sharma, “A Comparative Analysis of NeuroSky and Emotiv EEG Systems for Brain-Computer Interface Applications,” *2024 Second Int. Conf. Intell. Cyber Phys. Syst. Internet Things (ICoICI)*, vol. 00, pp. 1113–1118, 2024, doi: 10.1109/icoici62503.2024.10696481.

[6] J. Yang, K. Shibata, D. Weber, and Z. Erickson, “High-density electromyography for effective gesture-based control of physically assistive mobile manipulators,” *npj Robot.*, vol. 3, no. 1, p. 2, 2025, doi: 10.1038/s44182-025-00018-3.

[7]S. L. Bernal, A. H. Celdrán, G. M. Pérez, M. T. Barros, and S. Balasubramaniam, “Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges,” *ACM Comput. Surv. (CSUR)*, vol. 54, no. 1, pp. 1–35, 2021, doi: 10.1145/3427376.

[8] K. Balasubramanian *et al.*, “Propagating Motor Cortical Dynamics Facilitate Movement Initiation,” *Neuron*, vol. 106, no. 3, pp. 526-536.e4, 2020, doi: 10.1016/j.neuron.2020.02.011.

[9] F. Hoffstaedter, C. Grefkes, K. Zilles, and S. B. Eickhoff, “The ‘What’ and ‘When’ of Self-Initiated Movements,” *Cereb. Cortex*, vol. 23, no. 3, pp. 520–530, 2013, doi: 10.1093/cercor/bhr391.

[10] N. Li, T.-W. Chen, Z. V. Guo, C. R. Gerfen, and K. Svoboda, “A motor cortex circuit for motor planning and movement,” *Nature*, vol. 519, no. 7541, pp. 51–56, 2015, doi: 10.1038/nature14178.

[11] S. S. James *et al.*, “Integrating Brain and Biomechanical Models—A New Paradigm for Understanding Neuro-muscular Control,” *Front. Neurosci.*, vol. 12, p. 39, 2018, doi: 10.3389/fnins.2018.00039.

[12] J. Wang, L. Bi, and W. Fei, “EEG-Based Motor BCIs for Upper Limb Movement: Current Techniques and Future Insights,” *IEEE Trans. Neural Syst. Rehabilitation Eng.*, vol. 31, pp. 4413–4427, 2023, doi: 10.1109/tnsre.2023.3330500.

[13] X. Jiang *et al.*, “Cybersecurity in neural interfaces: Survey and future trends,” *Comput. Biol. Med.*, vol. 167, p. 107604, 2023, doi: 10.1016/j.compbiomed.2023.107604.

[14] N. Jiang, S. Dosen, K.-R. Muller, and D. Farina, “Myoelectric Control of Artificial Limbs - Is There a Need to Change Focus?,” *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 152–150, 2012, doi: 10.1109/msp.2012.2203480.

[15] N. Jiang *et al.*, “Bio-robotics research for non-invasive myoelectric neural interfaces for upper-limb prosthetic control: a 10-year perspective review,” *Natl. Sci. Rev.*, vol. 10, no. 5, p. nwad048, 2023, doi: 10.1093/nsr/nwad048.

[16] A. J. Abougarair, N. A. A. Shashoa, A. M. Elmelhi, and H. M. Gnan, “Real Time Classification for Robotic Arm Control Based Electromyographic Signal,” *2022 IEEE 2nd Int. Maghreb Meet. Conf. Sci. Tech. Autom. Control Comput. Eng. (MI-STA)*, vol. 00, pp. 155–160, 2022, doi: 10.1109/mi-sta54861.2022.9837703.

[17] Y. Chen, Z. Yang, and Y. Wen, “A Soft Exoskeleton Glove for Hand Bilateral Training via Surface EMG,” *Sensors*, vol. 21, no. 2, p. 578, 2021, doi: 10.3390/s21020578.

[18] S. Juárez, A. González, M. Maya, A. Cardenas, E. J. Gonzalez-Galvan, and H. I. Medellin-Castillo, “A comprehensive system for the acquisition of EMG signals and muscle force in lower limb,” *2022 Int. Conf. Electr., Comput., Commun. Mechatron. Eng. (ICECCME)*, vol. 00, pp. 1–6, 2022, doi: 10.1109/iceccme55909.2022.9988114.

[19] M. Valderrama, E. González, and F. García, “Development of a low-cost surface EMG acquisition system device for wearable applications,” *2021 IEEE 2nd Int. Congr. Biomed. Eng. Bioeng. (CI-IBBI)*, vol. 00, pp. 1–4, 2021, doi: 10.1109/ci-ibbi54220.2021.9626100.

[20] T. Mahboob, M. Y. Chung, and K. W. Choi, “EMG-based 3D hand gesture prediction using transformer–encoder classification,” *ICT Express*, vol. 9, no. 6, pp. 1047–1052, 2023, doi: 10.1016/j.icte.2023.04.005.

[21] C. Junyi, T. Zhongming, and W. Zhengtao, “Hand Gestures Recognition Based on One-Channel Surface EMG Signal,” *J. Softw. Eng. Appl.*, vol. 12, no. 09, pp. 383–392, 2019, doi: 10.4236/jsea.2019.129023.

[22] A. Althekair, M. Odeh, M. AlBayaa, M. Sharawi, and I. A. Doush, “Mobile Gaming EMG-Based Brain Computer Interface,” *Commun. Comput. Inf. Sci.*, pp. 40–52, 2023, doi: 10.1007/978-3-031-49425-3_3.

[23] B. Núñez-Montoya, M. V. Añazco, A. Saravia-Avila, F. R. Loayza, E. V. Añazco, and E. Teran, “Supervised Machine Learning Applied to Non-Invasive EMG Signal Classification for an Anthropomorphic Robotic Hand,” *2022 IEEE ANDESCON*, vol. 00, pp. 1–6, 2022, doi: 10.1109/andescon56260.2022.9989874.

[24] D. Leonardis *et al.*, “An EMG-Controlled Robotic Hand Exoskeleton for Bilateral Rehabilitation,” *IEEE Trans. Haptics*, vol. 8, no. 2, pp. 140–151, 2015, doi: 10.1109/toh.2015.2417570.

[25] M. Nguyen, T. N. Gia, and T. Westerlund, “EMG-based IoT System using Hand Gestures for Remote Control Applications,” *2021 IEEE 7th World Forum Internet Things (WF-IoT)*, vol. 00, pp. 911–912, 2021, doi: 10.1109/wf-iot51360.2021.9595957.

[26] J. Huang, G. Li, H. Su, and Z. Li, “Development and Continuous Control of an Intelligent Upper-Limb Neuroprosthesis for Reach and Grasp Motions Using Biological Signals,” *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 52, no. 6, pp. 3431–3441, 2022, doi: 10.1109/tsmc.2021.3069084.

[27] A. Tigrini *et al.*, “Decoding transient sEMG data for intent motion recognition in transhumeral amputees,” *Biomed. Signal Process. Control*, vol. 85, p. 104936, 2023, doi: 10.1016/j.bspc.2023.104936.

[28] L. Minati, N. Yoshimura, and Y. Koike, “Hybrid Control of a Vision-Guided Robot Arm by EOG, EMG, EEG Biosignals and Head Movement Acquired via a Consumer-Grade Wearable Device,” *IEEE Access*, vol. 4, pp. 9528–9541, 2016, doi: 10.1109/access.2017.2647851.

[29] A. A. Cifuentes-Cuadros, E. Romero, S. Caballa, D. Vega-Centeno, and D. A. Elias, “The LIBRA NeuroLimb: Hybrid Real-Time Control and Mechatronic Design for Affordable Prosthetics in Developing Regions,” *Sensors*, vol. 24, no. 1, p. 70, 2023, doi: 10.3390/s24010070.

[30] X. Li, O. W. Samuel, X. Zhang, H. Wang, P. Fang, and G. Li, “A motion-classification strategy based on sEMG-EEG signal combination for upper-limb amputees,” *J. Neuroeng. Rehabilitation*, vol. 14, no. 1, p. 2, 2017, doi: 10.1186/s12984-016-0212-z.

[31] S. Kim, D. Y. Shin, T. Kim, S. Lee, J. K. Hyun, and S.-M. Park, “Enhanced Recognition of Amputated Wrist and Hand Movements by Deep Learning Method Using Multimodal Fusion of Electromyography and Electroencephalography,” *Sensors*, vol. 22, no. 2, p. 680, 2022, doi: 10.3390/s22020680.

[32] S. Zhao *et al.*, “Wearable Physiological Monitoring System Based on Electrocardiography and Electromyography for Upper Limb Rehabilitation Training,” *Sensors*, vol. 20, no. 17, p. 4861, 2020, doi: 10.3390/s20174861.

[33] I. Moon, M. Lee, J. Ryu, and M. Mun, “Intelligent Robotic Wheelchair with EMG-, Gesture-, and Voice-Based Interfaces,” *Proc. 2003 IEEERSJ Int. Conf. Intell. Robot. Syst. (IROS 2003) (Cat 03CH37453)*, vol. 4, pp. 3453–3458, 2003, doi: 10.1109/iros.2003.1249690.

[34] N. Y. Sattar *et al.*, “Enhancing Classification Accuracy of Transhumeral Prosthesis: A Hybrid sEMG and fNIRS Approach,” *IEEE Access*, vol. 9, pp. 113246–113257, 2021, doi: 10.1109/access.2021.3099973.

[35] M. Al-Ayyad, H. A. Owida, R. D. Fazio, B. Al-Naami, and P. Visconti, “Electromyography Monitoring Systems in Rehabilitation: A Review of Clinical Applications, Wearable Devices and Signal Acquisition Methodologies,” *Electronics*, vol. 12, no. 7, p. 1520, 2023, doi: 10.3390/electronics12071520.

[36] M. Mohr, T. Schön, V. von Tscharner, and B. M. Nigg, “Intermuscular Coherence Between Surface EMG Signals Is Higher for Monopolar Compared to Bipolar Electrode Configurations,” *Front. Physiol.*, vol. 9, p. 566, 2018, doi: 10.3389/fphys.2018.00566.

[37] Q. Li, P. Dong, and J. Zheng, “Enhancing the Security of Pattern Unlock with Surface EMG-Based Biometrics,” *Appl. Sci.*, vol. 10, no. 2, p. 541, 2020, doi: 10.3390/app10020541.

[38] B. Xue, L. Wu, A. Liu, X. Zhang, and X. Chen, “White-Box Attacks on the CNN-Based Myoelectric Control System,” *Lect. Notes Comput. Sci.*, pp. 149–157, 2022, doi: 10.1007/978-3-030-93046-2_13.

[39] S. M. Khan, A. A. Khan, and O. Farooq, “Selection of Features and Classifiers for EMG-EEG-Based Upper Limb Assistive DevicesA Review,” *IEEE Rev. Biomed. Eng.*, vol. 13, pp. 248–260, 2020, doi: 10.1109/rbme.2019.2950897.

[40] I. M. Rezazadeh, S. M. Firoozabadi, H. Hu, and S. M. R. H. Golpayegani, “A novel human–machine interface based on recognition of multi-channel facial bioelectric signals,” *Australas. Phys. Eng. Sci. Med.*, vol. 34, no. 4, pp. 497–513, 2011, doi: 10.1007/s13246-011-0113-1.

[41] R. Portillo-Lara, B. Tahirbegi, C. A. R. Chapman, J. A. Goding, and R. A. Green, “Mind the gap: State-of-the-art technologies and applications for EEG-based brain–computer interfaces,” *APL Bioeng.*, vol. 5, no. 3, p. 031507, 2021, doi: 10.1063/5.0047237.

[42] O. Landau, R. Puzis, and N. Nissim, “Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space,” *ACM Comput. Surv. (CSUR)*, vol. 53, no. 1, pp. 1–38, 2020, doi: 10.1145/3372043.

[43] M. Brienza and O. Mecarelli, “Neurophysiological Basis of EEG,” *Clinical Electroencephalography*, pp. 9–21, 2019, doi: 10.1007/978-3-030-04573-9_2.

[44] J. Sabio, N. S. Williams, G. M. McArthur, and N. A. Badcock, “A scoping review on the use of consumer-grade EEG devices for research,” *PLOS ONE*, vol. 19, no. 3, p. e0291186, 2024, doi: 10.1371/journal.pone.0291186.

[45] X. Chi, C. Wan, C. Wang, Y. Zhang, X. Chen, and H. Cui, “A Novel Hybrid Brain-Computer Interface Combining Motor Imagery and Intermodulation Steady-State Visual Evoked

Potential," *IEEE Trans. Neural Syst. Rehabilitation Eng.*, vol. 30, pp. 1525–1535, 2022, doi: 10.1109/tnsre.2022.3179971.

[46] M. Mustile, D. Kourtis, M. G. Edwards, D. I. Donaldson, and M. Ietswaart, "Neural correlates of motor imagery and execution in real-world dynamic behavior: evidence for similarities and differences," *Front. Hum. Neurosci.*, vol. 18, p. 1412307, 2024, doi: 10.3389/fnhum.2024.1412307.

[47] R. M. Hardwick, S. Caspers, S. B. Eickhoff, and S. P. Swinnen, "Neural correlates of action: Comparing meta-analyses of imagery, observation, and execution," *Neurosci. Biobehav. Rev.*, vol. 94, pp. 31–44, 2018, doi: 10.1016/j.neubiorev.2018.08.003.

[48] M. Nann *et al.*, "Restoring Activities of Daily Living Using an EEGEOG-Controlled Semiautonomous and Mobile Whole-Arm Exoskeleton in Chronic Stroke," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2314–2321, 2019, doi: 10.1109/jsyst.2020.3021485.

[49] X. Zhang *et al.*, "Tiny noise, big mistakes: adversarial perturbations induce errors in brain–computer interface spellers," *Natl. Sci. Rev.*, vol. 8, no. 4, p. nwaa233, 2020, doi: 10.1093/nsr/nwaa233.

[50] *Regulation (EU) 2016/679*. 2018. [Online]. Available: https://gdpr-info.eu/#:~:text=General%20Data%20Protection%20Regulation%20GDPR,as%20a%20neatly%20arranged%20website.

[51] C. E. Fernández-García, D. V. Marín, and H. S. Velásquez, "Neurohacking and Artificial Intelligence in the Vulnerability of the Human Brain: Are We Facing a Threat?," *Bridg. Hum. Mach.: Futur. Educ. Intell.*, pp. 117–128, 2023, doi: 10.1007/978-981-19-8641-3_9.

[52] R. Bian, L. Meng, and D. Wu, "SSVEP-based brain-computer interfaces are vulnerable to square wave attacks," *Sci. China Inf. Sci.*, vol. 65, no. 4, p. 140406, 2022, doi: 10.1007/s11432-022-3440-5.

[53] L. Meng *et al.*, "EEG-Based Brain–Computer Interfaces are Vulnerable to Backdoor Attacks," *IEEE Trans. Neural Syst. Rehabilitation Eng.*, vol. 31, pp. 2224–2234, 2023, doi: 10.1109/tnsre.2023.3273214.

[54] F. Badrouchi *et al.*, "Cybersecurity Vulnerabilities in Biomedical Devices: A Hierarchical Layered Framework," *Internet of Things Use Cases for the Healthcare Industry*, pp. 157–184, 2020, doi: 10.1007/978-3-030-37526-3_7.

[55] G. Niso, E. Romero, J. T. Moreau, A. Araujo, and L. R. Krol, "Wireless EEG: A survey of systems and studies," *NeuroImage*, vol. 269, p. 119774, 2023, doi: 10.1016/j.neuroimage.2022.119774.

[56] F. Karabacak, H. Koc, and A. Ceber, “A Low Power Electronic Sticker for Vehicle Identification System using Proprietary Active RFID Wireless Protocol,” *2013 Int. Conf. Connect. Veh. Expo (ICCVE)*, pp. 847–852, 2013, doi: 10.1109/iccve.2013.6799913.

[57] T. Denning, Y. Matsuoka, and T. Kohno, “Neurosecurity: security and privacy for neural devices,” *Neurosurg. Focus*, vol. 27, no. 1, p. E7, 2009, doi: 10.3171/2009.4.focus0985.

[58] C. Szegedy *et al.*, “Intriguing properties of neural networks,” *arXiv*, 2013, doi: 10.48550/arxiv.1312.6199.

[59] A. Armengol-Urpi, R. Kovacs, and S. E. Sarma, “Brain-Hack : Remotely Injecting False Brain-Waves with RF to Take Control of a Brain-Computer Interface,” *Proc. 5th Work. CPSIoT Secur. Priv.*, pp. 53–66, 2023, doi: 10.1145/3605758.3623497.

[60] M. I. Hossen, Y. Tu, and X. Hei, “A First Look at the Security of EEG-based Systems and Intelligent Algorithms under Physical Signal Injections,” *Proc. 2023 Secur. Trust. Deep Learn. Syst. Work.*, pp. 1–8, 2023, doi: 10.1145/3591197.3591304.

[61] M. Usman, M. Kamal, and M. Tariq, “Improved and Secured Electromyography in the Internet of Health Things,” *IEEE J. Biomed. Heal. Inform.*, vol. 26, no. 5, pp. 2032–2040, 2022, doi: 10.1109/jbhi.2021.3118810.

[62] H. Yamaba, A. Kurogi, S.-I. Kubota, T. Katayama, M. Park, and N. Okazaki, “Evaluation of feature values of surface electromyograms for user authentication on mobile devices,” *Artif. Life Robot.*, vol. 22, no. 1, pp. 108–112, 2017, doi: 10.1007/s10015-016-0323-4.

[63] Y. Shin and M. Lee, “Development of Sensory Virtual Reality Interface Using EMG Signal-Based Grip Strength Reflection System,” *Appl. Sci.*, vol. 14, no. 11, p. 4415, 2024, doi: 10.3390/app14114415.

[64] M. Pfeiffer and M. Rohs, “Haptic Feedback for Wearables and Textiles Based on Electrical Muscle Stimulation,” *Hum.Comput. Interact. Ser.*, pp. 103–137, 2017, doi: 10.1007/978-3-319-50124-6_6.

[65] C. Conati *et al.*, “Hand gesture recognition and virtual game control based on 3D accelerometer and EMG sensors,” *Proc. 14th Int. Conf. Intell. user interfaces*, pp. 401–406, 2009, doi: 10.1145/1502650.1502708.

[66] G. Pires, M. Torres, N. Casaleiro, U. Nunes, and M. Castelo-Branco, “Playing Tetris with Non-Invasive BCI,” *2011 IEEE 1st Int. Conf. Serious Games Appl. Heal. (SeGAH)*, pp. 1–6, 2011, doi: 10.1109/segah.2011.6165454.

[67] Q. Li, D. Ding, and M. Conti, “Brain-Computer Interface Applications: Security and Privacy Challenges,” *2015 IEEE Conf. Commun. Netw. Secur. (CNS)*, pp. 663–666, 2015, doi: 10.1109/cns.2015.7346884.

[68] J. G. Betts *et al.*, *Anatomy and Physiology*. Houston, Texas: OpenStax, 2013. [Online]. Available: https://openstax.org/books/anatomy-and-physiology/pages/1-introduction

[69] M. B. I. Reaz, M. S. Hussain, and F. Mohd-Yasin, "Techniques of EMG signal analysis: detection, processing, classification and applications," *Biol. Proced. Online*, vol. 8, no. 1, pp. 11–35, 2006, doi: 10.1251/bpo115.

[70] H. J. Landau, "Sampling, data transmission, and the Nyquist rate," *Proc. IEEE*, vol. 55, no. 10, pp. 1701–1706, 1967, doi: 10.1109/proc.1967.5962.

[71] M. A. Oskoei and H. Hu, "Adaptive myoelectric control applied to video game," *Biomed. Signal Process. Control*, vol. 18, pp. 153–160, 2015, doi: 10.1016/j.bspc.2014.11.002.

[72] R. Martinek *et al.*, "Advanced Bioelectrical Signal Processing Methods: Past, Present, and Future Approach—Part III: Other Biosignals," *Sensors*, vol. 21, no. 18, p. 6064, 2021, doi: 10.3390/s21186064.

[73] L. McManus, G. D. Vito, and M. M. Lowery, "Analysis and Biophysics of Surface EMG for Physiotherapists and Kinesiologists: Toward a Common Language With Rehabilitation Engineers," *Front. Neurol.*, vol. 11, p. 576729, 2020, doi: 10.3389/fneur.2020.576729.

[74] P. Virtanen *et al.*, "SciPy 1.0: fundamental algorithms for scientific computing in Python," *Nat. Methods*, vol. 17, no. 3, pp. 261–272, 2020, doi: 10.1038/s41592-019-0686-2.

[75] S. Muceli and R. Merletti, "Tutorial. Frequency analysis of the surface EMG signal: Best practices," *J. Electromyogr. Kinesiol.*, vol. 79, p. 102937, 2024, doi: 10.1016/j.jelekin.2024.102937.

[76] Nordic Semiconductor, "Gazell Link Layer." Accessed: Apr. 11, 2025. [Online]. Available: https://docs.nordicsemi.com/bundle/ncs-latest/page/nrf/protocols/gazell/gzll.html

[77] S. Bräuer, A. Zubow, S. Zehl, M. Roshandel, and S. Mashhadi-Sohi, "On Practical Selective Jamming of Bluetooth Low Energy Advertising," *2016 IEEE Conf. Stand. Commun. Netw. (CSCN)*, pp. 1–6, 2016, doi: 10.1109/cscn.2016.7785169.

[78] F. Karabacak, H. Koc, and A. Ceber, "A Low Power Electronic Sticker for Vehicle Identification System using Proprietary Active RFID Wireless Protocol," *2013 Int. Conf. Connect. Veh. Expo (ICCVE)*, pp. 847–852, 2013, doi: 10.1109/iccve.2013.6799913.

[79] X. Wang, J. Yang, M. Huang, and Z. Peng, "GNSS interference and spoofing dataset," *Data Brief*, vol. 54, p. 110302, 2024, doi: 10.1016/j.dib.2024.110302.

[80] G. S. Gadgets, "HackRF One Documentation," 2021. [Online]. Available: https://hackrf.readthedocs.io/en/latest/hackrf_one.html

[81] A. Csete, "Gqrx SDR," 2023. [Online]. Available: https://www.gqrx.dk/

[82] J. Marcel, “How Bluetooth Technology Uses Adaptive Frequency Hopping to Overcome Packet Interference.” Accessed: Apr. 11, 2025. [Online]. Available: https://www.bluetooth.com/blog/how-bluetooth-technology-uses-adaptive-frequency-hopping-to-overcome-packet-interference/

[83] M. del Olmo and R. Domingo, “EMG Characterization and Processing in Production Engineering,” *Materials*, vol. 13, no. 24, p. 5815, 2020, doi: 10.3390/ma13245815.

[84] S. Angelova, S. Ribagin, R. Raikova, and I. Veneva, “Power frequency spectrum analysis of surface EMG signals of upper limb muscles during elbow flexion – A comparison between healthy subjects and stroke survivors,” *J. Electromyogr. Kinesiol.*, vol. 38, pp. 7–16, 2018, doi: 10.1016/j.jelekin.2017.10.013.

Appendix A

Presented are the feature plots created to assess overfitting of the SVM model used in development of the classification stage of the MCI system.

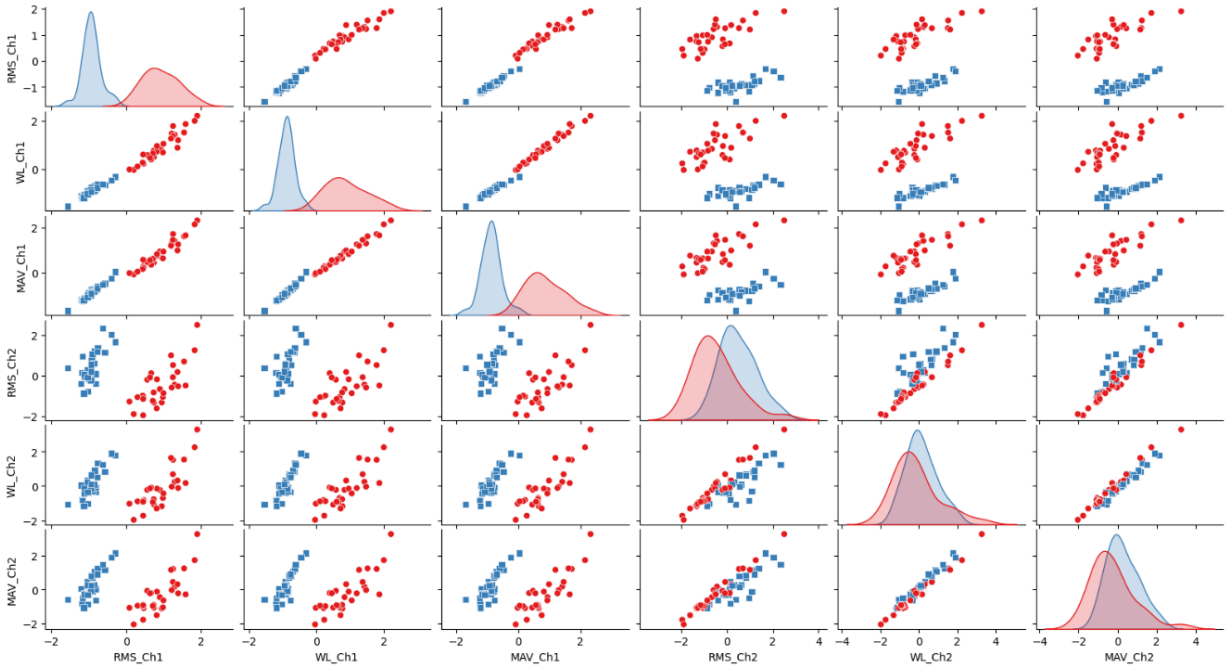

Figure A.1: Pairwise feature plots of the extracted features used to build the SVM for the MCI system. The extracted features were MAV, RMS, and WL. (red) Extension motor task. (blue) Flexion motor task.

The following table lists the acronyms and abbreviations used in this dissertation for reference and clarity.

Table A.1: Acronyms/Abbreviations used in the dissertation and their explanations

Acronym	Explanation
MCI	Myoelectric-Computer Interface
BCI	Brain-Computer Interface
EEG	Electroencephalography
sEMG	Surface Electromyography
PNS	Peripheral Nervous System
CNS	Central Nervous System
MITM	Man-in-the-Middle
EOG	Electrooculography
fNIRS	Functional Near-Infrared Spectroscopy
SNR	Signal to Noise Ratio
ML	Machine Learning
RMS	Root Mean Square
fMRI	Functional Magnetic Resonance Imaging
MEG	Magnetoencephalography

SSVEP	Steady-State Evoked Potential
ERP	Event-Related Potential
GDPR	General Data Protection Regulation
NPP	Narrow Period Pulse
UAP	Universal Adversarial Perturbations
CNN	Convolutional Neural Network
VR	Virtual Reality
AR	Augmented Reality
MAV	Mean Absolute Value
WL	Waveform Length
SVM	Support Vector Machine
FFT	Fast Fourier Transform
PSD	Power Spectral Density
BLE	Bluetooth Low Energy