Apuntes de la Revisión del Estado del Arte de Ciberataques Neuronales

Índice

1. Resumen

El paper en cuestión aborda la seguridad en las BCI, enfocándose sobre todo al punto de vista tecnológico, más que en las consecuencias biológicas. El artículo se divide en cuatro apartados:

1. El primer apartado trata sobre las vulnerabilidades en el ciclo BCI.
2. EL segundo apartado se centra en los posibles ataques a las BCI, los impactos y las contramedidas.
3. El tercer apartado es una revisión sobre las tendencias de evolución de las BCI y los retos de seguridad que conlleva.
4. Finalmente, el último apartado son las conclusiones y futuros trabajos.

El paper, además, propone un nuevo ciclo BCI de adquisición de señales y de estimulación, intentando así homogeinizar los ciclos propuestos en la literatura. El resumen del ciclo BCI propuesta se muestra en la siguiente figura:

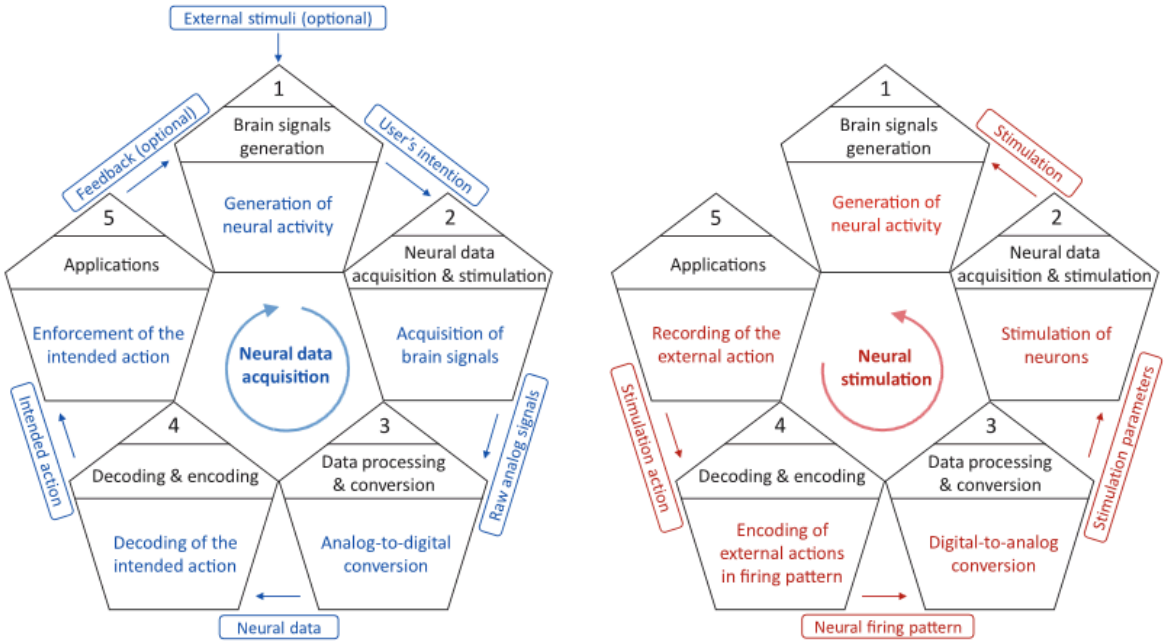

Figura 1: Ciclos BCI de adquisición y estimulación. A la izquierda, podemos ver en el sentido de las agujas del reloj un ciclo de adquisición de señales neuronales en un BCI. A la derecha, vemos un ciclo de estimulación de señales neuronales en un BCI.

2. vulnerabilidades en el ciclo BCI

Como se puede ver en la Figura 1, el ciclo BCI se divide en cinco partes, que pueden recorrerse en sentido horario o antihorario dependiendo de si se está realizando una adquisición o una estimulación de señales neuronales.

2.1. Fase de generación de señales neuronales

Para evaluar el impacto en seguridad de los ataques a las BCI, se usan las métricas de integridad, confidencialidad, disponibilidad y seguridad. Las definiciones más comunes de estas métricas son:

- **Integridad:** Protección contra la modificación o destrucción de información no autorizada.
- **Confidencialidad:** Preservación de las restricciones de autorización y de divulgación.
- **Disponibilidad:** Accesibilidad de los datos e información bajo la demanda de la persona autorizada.
- **Seguridad:** Ausencia de conficiones que puedan causar muerte, lesiones, enfermedades... En este trabajo se considera la seguridad desde las perspecivas física, psicológica y psiquiátrica.

Hay dos tipos diferentes de ataques a las BCI:

- El primer tipo de ataques se centran en coger el control de la simulación y dañar el tejido neuronal. Estos ataques pueden producir efectos secundarios presentes en los tratamientos de enfermedades neurológicas, además de prevenir la aplicación de los tratamientos.
- El segundo tipo de ataques se centran en inducir efectos y percepciones al usuario. Este tipo de neuroestimulación se centra en daños psicológicos y psiquiátricos, causando sensaciones como depresión, ansiedad, etc.

2.2. Fase de adquisición y estimulación

Esta fase se centra en la integración de los dispositivos BCI en el cerebro para la adquisición de datos o realizar estimulaciones. En la literatura se han identificado ataques spoofing y jamming. Con los ataques spoofing se suplantan estímulos neuronales para engañar al sistema. Por otr lado, los ataques jamming inhiben la estimulación neuronal.

Los ataques spoofing suplantan el comportamiento de las señales neuronales reales, pudiendo hacer que el BCI haga un diagnóstico erróneo de la enfermedad, desembocando así en tratamientos erróneos o innecesarios. Los ataques jamming, por su parte, producen una inhibición por generación de ruido en el proceso de adquisición, lo que afecta a la disponibilidad y seguridad.