A Novel Deep Learning Strategy for Classifying Different Attack Patterns for Deep Brain Implants

Sent
19-Jun-2018
From
hadi.heidari@glasgow.ac.uk
To
amrm@qu.edu.qa
CC
r.hytowitz@ieee.org, hadi.heidari@glasgow.ac.uk, heena7sept@gmail.com, abdulla.alali@qu.edu.qa, amrm@qu.edu.qa, xjdu@temple.edu, mguizani@ieee.org
Subject
IEEE Access - Decision on Manuscript ID Access-2018-05366
Body
19-Jun-2018

Dear Dr. Mohamed:

I am writing to you in regards to manuscript # Access-2018-05366 entitled "A Novel Deep Learning Strategy for Classifying Different Attack Patterns for Deep Brain Implants" which you submitted to IEEE Access.

In view of the criticisms of the reviewer(s) found at the bottom of this letter, your manuscript has not been recommended for publication in IEEE Access. Unfortunately, we will not accept resubmissions of this article.

Thank you for considering IEEE Access for the publication of your research.

Sincerely,

Dr. Hadi Heidari
Associate Editor, IEEE Access
hadi.heidari@glasgow.ac.uk

Reviewer(s)' Comments to Author:

Reviewer: 1

Recommendation: Reject (do not encourage resubmit)

Comments:
The goal of this manuscript is to describe how an adversary can inhibit the function of stimulation systems by introducing fake stimulation, and to present predictions of attack patterns. The predictions involve recurrent networks for forecasting rest tremor velocity, and DBS was tested on tremor patients.
In the introduction there is a brief of review of Benabid's initial tremor and Parkinson's work, FDA approval of DBS for sinemet-induced Parkinson' symptoms (ie, dyskinesia, fluctuations, etc) in 2002, though there FDA approval for tremor in 1997. The estimate of DBS implants reaching 1,593 million by 2020 (ie, 1.59 billion) is wildly off course, with the more likely estimate optimistically as ~ 200,000 total, far less than the world number of cardiac pacemakers and defibrillators, which are much more crucial for life. The rough numbers worldwide show > 1.15 million total cardiac pacemakers implanted by 2016, nearly 10 times the number of DBS implants. The IPG is a "implantable pulse generator" not a "heartbeat generator" (p1, line 14). The number of implants for depression in the USA is < 200, mainly from the failed trials, and this is not clinically

performed except in research studies at this time. Thus, there is a misleading introduction which could be improved by conversation with a DBS clinician.

Since the authors do not seem to be very familiar with DBS implants there is no such problem in clinical practice as envisioned “unpredictable security issues in such gadgets” (p1, line 35). There are multiple layers of security, not the least being the use of very short field wireless control (ie, < 1 inch in proximity to the IPG) by non-standard wireless protocols (ie, proprietary technology which is not published). Second, there is a paucity of controller devices which can set parameters (ie, programmers) and even fewer clinicians who know how to use one with any knowledge. These devices (unlike cardiac pacemakers) are not any form of critical or lifesaving device, hence can easily be turned on and off by the patient. Thus, an attack by an adversary most likely would simply turn the device off, which happens occasionally in adverse environments. In turning the device off the effect or tremor or Parkinson’s rigidity/bradykinesia would slowly be lost, sometimes over 2-3 days. Thus, the authors are envisioning a problem (and a potential solution) that simply does not exist regarding attacks and security.

In contrast, there have been real plots to turn of cardiac pacemakers from a wireless distance, and the large numbers of these in current use, the critical nature of pacemakers for life sustenance, and the ease with which they could be re-programmed should be the focus of this type of report, rather than DBS.

The problem statement relates to introduction of different types of stimulation patterns. As studied extensively, most alternative stimulation patterns have less neurological effect, as shown by Warren Grill and Collaborators in multiple papers. But, of course, this is simply less tremor control, which is minimally disabling. The authors propose a recurrent neural network, a standard approach, to predict DBS patterns. What is not clear is why not just read what was put into the device (ie, how it was programmed)? Theoretically, what the authors envision is hacking into a device somehow (no specifics given) and recreating the stimulation parameters.

The authors describe “46” Hz (p5, line 3) but what they really mean is 4 to 6 Hz, a major type or misunderstanding. This continues with Fig. 5 where tremor frequency is shown on a 0-1Khz plot, far out of any physiologically observed range (ie, again, please see Warren Grill’s multiple reports on tremor control and frequency). The authors do not describe how an attack could practically occur or how to “break” into a system effectively. It is not at all clear what Fig. 9 and Table 1 show.

In summary, the authors propose some form of poorly-described solution to a problem that does not practically exist. They actually should explore more knowledge about DBS systems from various companies to become realistic about their goals, and to understand the clinical realities of the disease. Though it is possible to potentially “hack” into a DBS system, the system intentionally simply turns itself off with such interference, with only minor loss of symptom control, and the authors do not appear to have sufficient practical knowledge to inform the reader as to how this may happen.

Additionally, the references are old, the authors have not investigated most current knowledge in the last 10 years regarding stimulation protocols, and have insufficient manufacturer’s knowledge of the device to really understand critical security issues.

Additional Questions:

Does the paper contribute to the body of knowledge?: Minimally.

Is the paper technically sound?: No.

Is the subject matter presented in a comprehensive manner?: No. The authors have a very superficial idea and do not appear to have performed any extensive research on the topic.

Are the references provided applicable and sufficient?: No, old and not relevant.

Reviewer: 2

Recommendation: Accept (minor edits)

Comments:
1. Page 3, Heading, III. NETWORK AND ATTACK MODEL
Good if you can specify the network. This sounds generic.
2. Page 7, Fig. 7 arrangement of graphs. Can they be arranged in symmetrical columns.
3. Page 8, Fig 9. Good if graphs can be symmetric number. Easy to ready and compare.

Additional Questions:
Does the paper contribute to the body of knowledge?: Yes. The paper explores the importance of security in Deep brain stimulators which is important aspect of implementation.

As paper states, "Deep brain stimulators (DBS), a widely used and comprehensively acknowledged restorative methodology, is a type of implantable medical device which uses electrical stimulation to treat neurological disorders. These devices are widely used to treat diseases such as Parkinson, movement disorder, epilepsy, and psychiatric disorders. "

The paper highlights the importance of Security which is less explored but highly important and vulnerable area in implementation of DBS.

As researchers review on DBS Security, "Security in such devices plays a vital role since it can directly affect the mental, emotional, and physical state of human bodies."

Is the paper technically sound?: Yes. The sections and paragraphs well arranged. Easy to understand.

Is the subject matter presented in a comprehensive manner?: Yes. Prefer to use markers in Fig 6,8 & 9 to avoid dependence on colour.

Are the references provided applicable and sufficient?: Yes. Reference [2] does not have a year.
Reference of year is not consistent. Please see below.

E.g.,
[12] Rathore, H., 2016. Artificial Neural Network. In Mapping Biological Systems to Network Systems (pp. 79-96). Springer International Publishing.

and

[30] X. Hei, and X. Du, “Biometric-based Two-level Secure Access Control for Implantable Medical Devices during Emergency”, in Proc. of IEEE
INFOCOM, 2011.

Reviewer: 3

Recommendation: Accept (minor edits)

Comments:
A novel deep learning methodology to classify and predict different attack patterns in deep brain stimulators, which is based on the long short term memory, is proposed in this paper. The results show it can classify different attack patterns with smaller loss values and mininmal training time.

Additional Questions:

Does the paper contribute to the body of knowledge?: Yes

Is the paper technically sound?: Yes

Is the subject matter presented in a comprehensive manner?: Yes

Are the references provided applicable and sufficient?: Yes