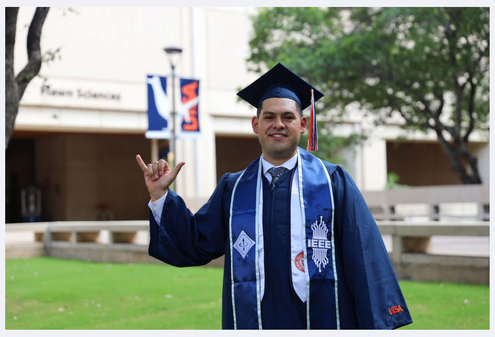
Artificial Neural Network Cyber Forensics Methodology For Identifying Internal Cyberattacks

Brandyn M. Campos, Miltos Alamaniotis PhD.

The University of Texas at San Antonio, San Antonio TX, 78249



Name: *Brandyn Marc Campos*
Status: *Graduating Senior*
Department: *Electrical and Computer*
Area of Study: *Computer Engineering*
USDA/UTSA Mentor(s):
Dr. Miltos Alamaniotis

WeARE Research Area

Nuclear Power Plants (NPP) were developed as a type of renewable and reliable energy source. NPPs have an increasing bulls-eye for any type of cyber-attack on grid stability. In order to further develop network security for NPP Control Networks, we have developed a comprehensive Artificial Intelligence (AI) model that is able to monitor all network activity and differentiate between an external and internal network attack. The development for this model includes research in neural networks, pattern recognition, and data forensics in cyber-security.

Motivation and Background

There has been a rise of cyber-attacks toward Power Generation Plants world-wide. This is partly due to the digitalization of classic analog systems. When transferring over analog systems to digital, there are surges of vulnerabilities within the new systems networks. Here are instances of major recent attacks:

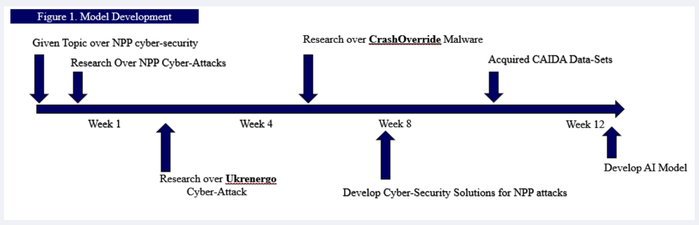
- **Ukrenergo** – Mass power outage Dec, 2017 that caused 20% power loss to Ukraine capitol. Malware used backdoor in 3rd party system software.
- **Stuxnet** – Malware that managed to manipulate Uranium enrichment control systems in over 17 different Nuclear Power Plants in Iran.
- **CrashOverride** – Quoted as the most destructive and complex malware the U.S. government has seen to date.

Objectives

1. The challenge exists to increase network defenses by developing a comprehensive Intelligence model that will read-in network activity data and differentiate an external cyber-attack from one that has been introduced internally.
2. The AI digital forensics system will analyze all data traffic on network data-sets by utilizing machine learning, data analytic techniques, and pattern recognition software.

Methodology

- Understand what systems and networks were effected by recent cyberattacks.
- Develop an efficient method of receiving and analyzing network traffic data-sets.
- Research over network security data forensics techniques allowed a verification of the ability for a machine learning system to monitor abnormalities in a control systems network.



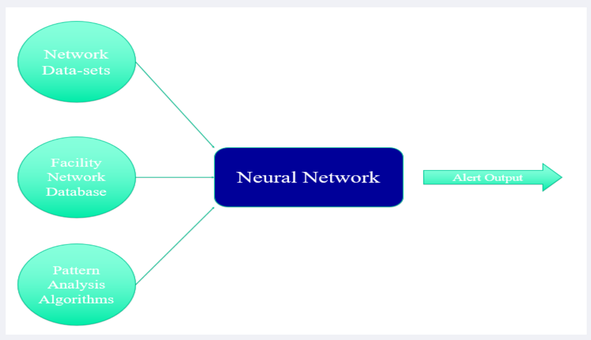


Fig. 1
Basic Model Configuration for network monitoring integration

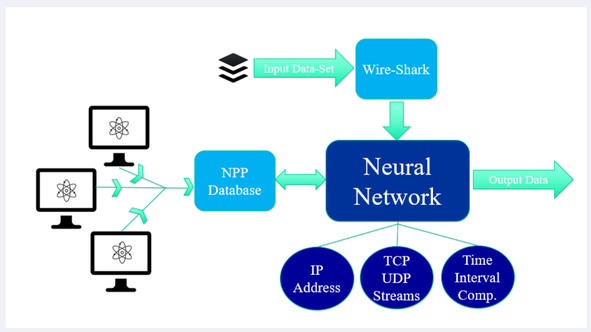
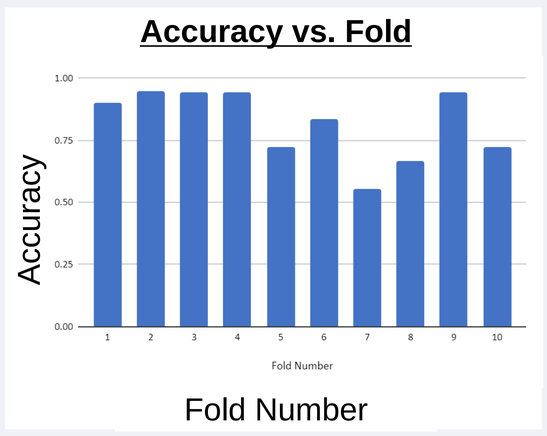
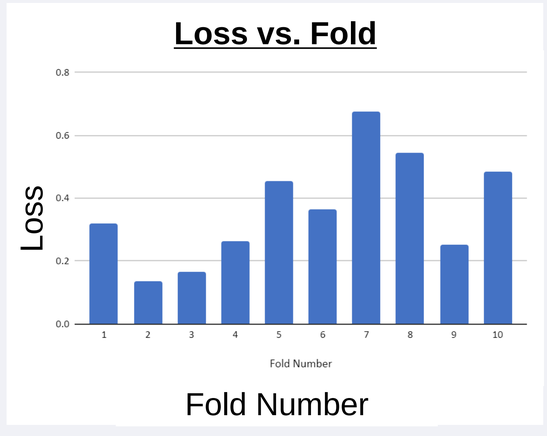
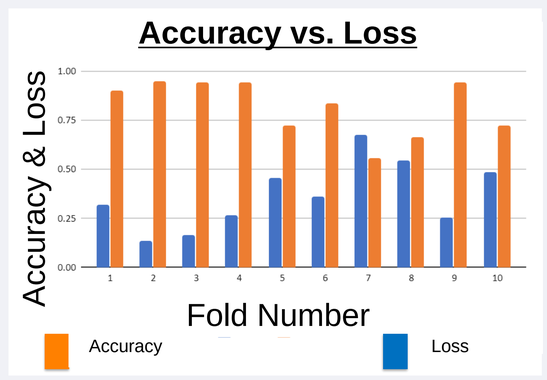


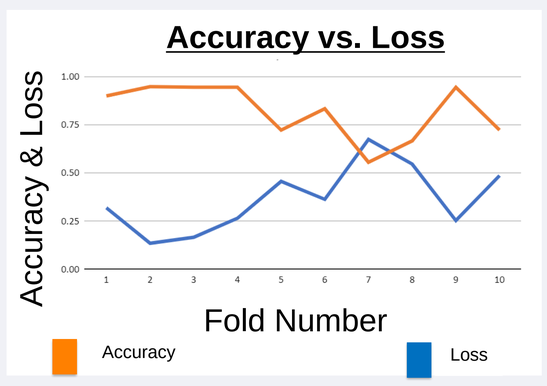
Fig. 2
Comprehensive model configuration for network monitoring integration

Results









Skills and Experience

- Computer Science and Electrical Engineering programming classes helped develop the coding skills necessary for developing a neural network system using Python Computer Language and TensorFlow Libraries
- Research team experience lead to the development of communication skills necessary for coordinating with my UTSA mentor Dr. Alamaniotis
- Researching skills allowed for efficient dataset acquisition and neural network model development

What I Learned

- Acquiring network traffic datasets that correlate with NPP network data is difficult considering the sensitivity of the data being processed
- Artificial Intelligence System Design
- Developing neural networks using TensorFlow
- Optimizing mathematical activation functions utilized within the neural network
- Training and Testing of neural network models

Future Plans

- Publishing my research paper, “Artificial Neural Network Cyber Forensics Methodology For Identifying Internal Cyberattacks in Nuclear Facilities.” with Dr. Alamaniotis as a co-author.
- Full-Time position as a cyber systems engineer for Northrop Grumman
- Enrolling in the graduate program in Electrical Engineering under Dr. Alamaniotis at The University of Texas at San Antonio

Acknowledgments

This work is supported by the USDA National Institute of Food and Agriculture, Interdisciplinary Hands-on Research Traineeship and Extension Experiential Learning in Bioenergy/Natural Resources/Economics/Rural project, U-GREAT (UnderGraduate Research, Education And Training) program (2016-67032-24984).

References

Center for Applied Internet Data Analysis. ***The CAIDA Anonymized Internet Traces Dataset 2008 - Ongoing***. 1 Dec. 2008, www.caida.org/data/passive/passive_dataset.xml. Accessed 12 Apr. 2019.

EISAC. “Modular ICS Malware .” *ICS SANS*, Industrial Control Systems Lab, 2 Aug. 2017, ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf.