IARIA CONGRESS 2022

Hybridized Machine Learning Implementation for a Complex Network Cyber-Physical Supply Chain Analysis

Steve Chan, IARIA Fellow
& Decision Engineering Analysis Laboratory, VTIRL, VT
schan@dengineering.org

DECISION engineering Analysis Laboratory

IARIA CONGRESS | July 24-28, 2022 Nice, France

SPEAKER BIO

Dr. Steve Chan is an International Academy, Research and Industry Association (IARIA) Fellow. He is an inventor with international and U.S. patents and serves as a reviewer for 24 peer-reviewed journals/conference proceedings. He serves on the Advisory/Steering Committee for the IARIA Cyber-Technologies and Cyber-Systems venue and has been active in the Cyber, Artificial Intelligence, and Machine Learning arenas. He served as an invited Keynote Speaker for the Advances on Societal Digital Transformation (DIGITAL 2021) from 14-18 November 2021 in Athens, Greece for the talk, "AI-Centric Cyber Laboratory Services: Operationalizing White Box Architectures." His keynote for the Fifth International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2020) from 25-29 October 2020 in Nice, France was "Leveraging Sidecars for a More Probabilistic Cyber Convergence." His keynote for the Fourth International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2019) from 22-26 September 2019 in Porto, Portugal was "A Cyber Key to Log Analysis." His keynote for the Third International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2018) from 18-22 November 2018 in Athens, Greece was "Leveraging Artificial Intelligence/Cognitive Computing to Meet the Increasing Cycles of Adaptation within the Cyber Domain." His keynote for the Second International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2017) from 12-16 November 2017 in Barcelona, Spain was "Energy/Cyber Security Assessment: Data Analytics for Cyber Resilience of Strategic / Critical Electrical Grid Infrastructure." His prepared keynote for the First International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2016) from 9-13 October 2016 in Venice, Italy was "Enhancing Cyber Infrastructural Resilience for Cyber Cities." He has also served as an invited Panelist and Presenter at other IARIA venues, such as the Fourth International Conference on Data Analytics from 19-24 July 2015 in Nice, France.

DECISION engineering
Analysis Laboratory

TABLE OF CONTENTS

DECISION engineering Analysis Laboratory

IARIA

I. INTRODUCTION

DECISION engineering
Analysis Laboratory
IARIA

I. INTRODUCTION

There seems to be a dilemma in the realm of power system protection. On the one hand, the requisite reliability dictates that there are no missing operations (e.g., missed trippings). On the other hand, the requisite security dictates that there are no false operations (e.g., false trippings). Generally speaking, the more secure things are, the slower the involved systems tend to operate/mis-operate. Conversely, the more efficient things are, the faster the involved systems tend to operate (but also, potentially, in a specious fashion). The trade-off seems to be between speed and accuracy/precision (there is indeed a distinction between accuracy and precision). There is also a distinction between ambiguity and uncertainty. To accommodate and successfully harmonize among these various trade-offs, a particular hybridized machine learning implementation shows some promise.

II. BACKGROUND

DECISION engineering Analysis Laboratory

IARIA

II. BACKGROUND

According to the Pacific Northwest National Laboratory (PNNL), the power grid (a.k.a., electrical grid) is considered the world's largest machine.

Scientific American has stated that the electrical grid (a.k.a., "the grid") is the largest interconnected machine on Earth.

Suffice it to say, the grid is a Large Complex Networked System (LCNS).

According to the U.S. Department of Energy (DOE), the grid is the largest and most critical LCNS of the 16 Critical Infrastructure (CI) LCNS, since the grid provides the energy to run the other CIs.

As the largest LCNS, the grid has a large attack surface; according to the U.S. General Accountability Office (GAO), the sheer size and dispersed nature gives it a very large attack surface.

The U.S. National Academy of Engineering (NAE) has cited the grid as the greatest achievement of the 20th century. However, in a 21st century context, about five years ago, the American Society of Civil Engineers (ASCE) gave the grid a D+ on its Infrastructure Report Card.

II. BACKGROUND cont'd

The National Research Council (NRC) stated that the U.S. power grid is "vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale."

By way of background information, according to the U.S. Energy Information Administration (EIA), the grid is divided into three parts: generation, transmission, and distribution.

Interestingly, according to various security experts, due to its architected resiliency, generation is least likely to be attacked by a sophisticated attacker; UtilityDive provides the example of the largest generation for the U.S. grid, the 6.8GW Grand Coulee Dam, and notes that its loss would not cause a blackout.

Also, although transmission lines and towers are highly visible and obvious of a target (and have experienced about 2,500 attacks in various parts of the world over the past 10 years, according to a National Academies Press [NAP] publication), according to various grid security experts, the sheer number of lines, ability to re-direct to other lines, and relative ease of repair/replacement makes it less likely to be attacked by a sophisticated attacker.

II. BACKGROUND cont'd

At the nexus of the Transmission and Distribution (T&D) systems, High Voltage (HV) Substations serve as interconnection points. For example, they help step down from HV to Medium Voltage (MV) for distribution.

A previous Federal Energy Regulatory Commission (FERC) director had commissioned a study to see if an attack on substation transformers could result in cascading failure and blackouts. It was found that a blackout could occur if 9 key substation transformers were compromised.

Executive Order 13920 had noted a supply chain risk in that Large Power Transformers (LPT) were among the most critical elements of the Bulk-Power System (BPS), but that there was a particularly heavy reliance upon the foreign supply of LPT or HV Transformers (HVT).

Unfortunately, HVT are expensive, so emergency inventories are not necessarily maintained, and the lead time for replacements can be more than a year.

According to the Congressional Research Service (CRS), HVT constitute less than 3% of the transformers at HV Substations; however, according to the DOE, 90% of consumed power pass through these HVT.

II. BACKGROUND cont'd

Although the previously referenced NAP publication cited only 500 attacks on substations with transformers (e.g., 17 of 21 transformers at the Metcalf Substation were taken out of commission by snipers in 2013), the GAO has found that the grid's distribution systems are particularly vulnerable, and the DOE agreed.

A prior President's Commission on Critical Infrastructure Protection (PCCIP) had found that the substation (e.g., distribution substation) was one of the most vulnerable parts of the power grid.

Among other components, apropos protection system devices have been found to have caused cascading failures and ensuing blackouts. In many cases, due to a loss of coordination (i.e., apropos localization of a fault event so as to constrain power outages), downstream affected upstream devices. For example, if the protective device does not respond quickly enough, upstream protective devices could trip.

The many and varied Distributed Generation (DG) sources are causing coordination problems, as DGs are variable. For this reason, the associated protection systems need to be dynamic and responsive at machine speed. This necessitates machine-based Decision Engineering (DE) for decision-making (e.g., to trip or not to trip).

III. THE PROTECTION CHALLENGE

DECISION engineering Analysis Laboratory

IARIA

III. THE PROTECTION CHALLENGE

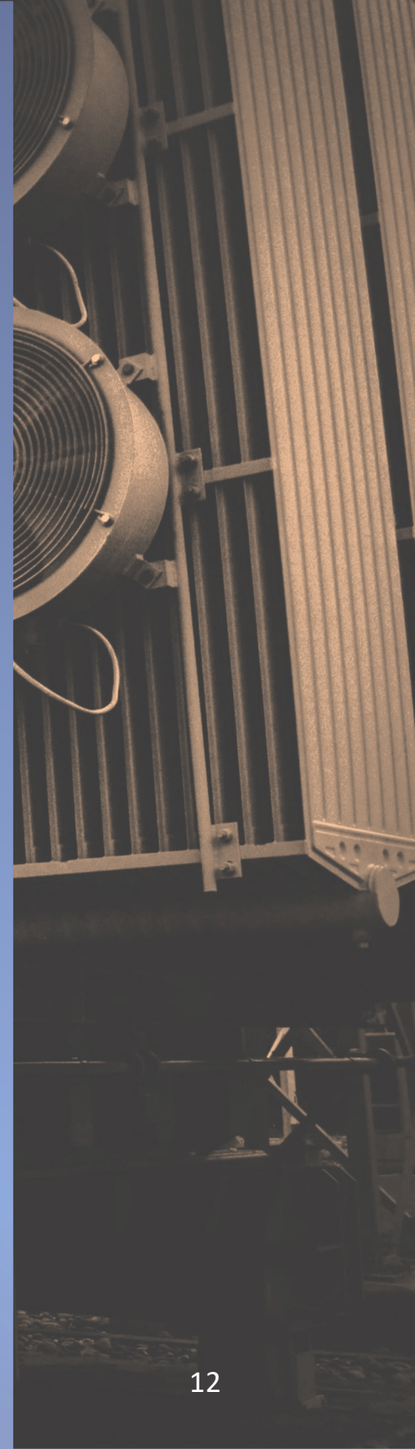
In an ideal situation, when protective devices are coordinated appropriately, a single event will not induce a cascading failure.

However, protection and coordination are often in conflict with each other, and proper counterpoising is essential. With the increasing DG Renewable Energy System (RES) utilization, existing protection and coordination schemas need to be revisited.

Consistent with the spirit of the National Electrical Code (NEC), by way of example and among others, a focus on selective coordination can be instrumental; in essence, for mission-critical operations, only the closest upstream device is tripped so that the parts of the grid that are taken offline are minimized.

NEC selective coordination is required for, among others: (1) Critical Operations Power Systems (NEC 708.54), (2) Standby Systems (NEC 701.18), (3) Emergency Systems (NEC 700.27), etc.

Central to selective coordination is robust DE and decision-making at machine speed. In this way, continuous operation of critical circuits can be maintained, thereby increasing the reliability and reducing the likelihood of cascading effects/failures/collapses leading to blackouts.



III. THE PROTECTION CHALLENGE cont'd

It has also been found the Protection System Hidden Failures (PSHF) have been a cause of power system disturbances (e.g., cascading upstream) and major cascading collapses.

Unfortunately, PSHF are, as implied by its name, hidden during the normal operating conditions and may only manifest during an abnormal event (e.g., fault, overload, etc.). The PSHF has various hidden failure modalities: covert failure, dormant failure, unrevealed failure, undetected failure, failure that may not be evident to the operations and/or maintenance teams when they occur, and any combination of the aforementioned.

In numerous instances, relying upon power system protection engineers and procedures to verify protection relay settings has segued to PSHF. In some cases, the use of Artificial Technology (AI) techniques, such as Rule-based Expert Systems (RBES), has been useful for checking the work of power system protection engineers; of note, these RBES need a robust knowledge base to operate from.

While Advanced Monitoring and Analysis (AMA) can assist in detecting some PSHF within protection relays, AMA has not been found to be effective for detecting PSHF at the Circuit Breaker (CB) Trip Mechanism (CBTM) level. PSHF in the CBTM typically remain undetected until the CBs fail to open during an event.

IV. POSITED APPROACH

DECISION engineering Analysis Laboratory

IARIA

IV. POSITED APPROACH

AI techniques, such as Artificial Neural Networks (ANNs) have been looked to as a promising potential mitigation approach for the treatment of the selective coordination and PSHF challenges, as ANNs do not need a robust knowledge base to work from and are quite good at pattern recognition and classification.

However, it has been noted, such as by an IEEE Spectrum publication, that ANN: (1) can be brittle (i.e., it can only recognize a pattern that it has seen before and will likely fail against new "black swan" patterns), (2) can exhibit amnesia (e.g., overwriting prior knowledge with more recent knowledge; rephrased, it can mis-contextualize due to prior training), (3) has inherent bias (i.e., can be skewed toward a particular position based upon its learning; restated, it may not live up to the spirit of intent of its assigned task), (4) has deficient explainability (i.e., it is more of a blackbox than a whitebox), (5) has questionable uncertainty quantification (very certain, albeit potentially very incorrect), and (6) can be deficient at mathematics (e.g. it has a highly parallelized approach versus sequential handling, and some AI engineers posit that this might be an issue).

The AI technique of Fuzzy Logic (FL) systems has been looked to as helping to treat the accuracy versus precision issue; criteria can be fuzzified to accommodate measurement errors (e.g., the lack of precision) and facilitate the consideration of multi-criteria before a tripping decision is made.

IV. POSITED APPROACH cont'd

Machine Learning (ML) algorithms endeavor to derive insights for decision-making from large amounts of data and engage in classification and clustering.

However, not all the data may be useful. There may be malformed data, dropped/missing data, false data, etc.

In this case, FL may help gauge the certainty/uncertainty of the involved problem.

RBES utilize prescribed knowledge-based rules to tackle the involved problem.

Hopefully, the rules are still valid; after all, some rules persist for quite some time (i.e., might constitute brittleness) and may need to be altered/discarded.

Due to the inherent variability of DG RES, effective feature extraction and classification remains challenging. However, Deep Transfer Learning-Based Feature Extraction, via a mixture of bespoke Convolutional Adversarial Neural Networks (CANN) conjoined with an Adaptive Inertial Weighting (AIW)-Particle Swarm Optimization (PSO) implementation on a Deep Convolutional Generative Adversarial Network (DCGAN) has shown some promise as a framework for better harmonizing the certainty/uncertainty issue with FL and the precision/accuracy issue with an Enhanced Robust Convex Relaxation (ERCR) engine.

IV. POSITED APPROACH cont'd

The ERCR engine tends more toward being a whitebox paradigm with its improved bound tightening at each successive neural network layer.

ML can be impacted by the uncertainty within the data or its given tasks (thereby potentially leading to selection bias).

Some AI practitioners also link the uncertainty/ambiguity challenge with volatility and complexity. The acronym VUCA (Volatility, Uncertainty, Complexity, and Ambiguity) is often used.

In certain cases, uncertainty can be reduced by enhancing data labeling and annotation. This helps to mitigate against the Garbage In Garbage Out (GIGO) paradigm. Then, a variety of ML models can be leveraged. In addition, active learning algorithms, utilizing a variety of query strategies, can be leveraged. Researchers have found that Reinforcement Learning (RL) can be quite useful; However, prototypical instantiations of RL necessitate a reward function, and studies have found that it is difficult for a RL agent to avoid stagnation at local optima.

However, if the Enhanced RL Component (ERLC) is operationalized with the discussed AIW-PSO atop DCGAN-CANN1-CANN2- … CANNy, high efficacy for avoiding local optima and attaining a globally optimal solution can be more readily achieved.

IV. POSITED APPROACH cont'd

The utilization of a Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) can be useful in mitigating against the previously discussed amnesia challenge.

The LSTM can also be useful in mitigating against brittleness by informing new rules and altering/discarding invalid old rules.

This helps to better contextualize the current situation, which in turn, better mitigates against inherent biases.

The whitebox architecture of the ERCR engine, with its improved bound tightening at each successive neural network layer, lends toward enhanced explainability.

With regards to the ERCR engine, the utilization of a translation-invariant Continuous Wavelet Transform (CWT) PyWavelet schema, via cascading, smaller convolutional filters aboard an ERCR-based Convolutional LSTM Deep Neural Networks (a.k.a., CLSTMDNNs or CLNNs), improves the involved bound tightening, is likely to lead to better discernment, and will more closely approximate a whitebox paradigm.

V. CONCLUDING REMARKS

DECISION engineering Analysis Laboratory

IARIA

IV. CONCLUDING REMARKS

The overarching ERCR & AIW-PSO-ERLC with FL atop DCGAN-CANN1-CANN2- … CANNy-CLNN shows some promise as a hybridized ML implementation for LCNS, such as the power grid, and warrants further investigation.

Power grid reliability and resiliency is predicated upon, among other paradigms, an apropos counterpoising of protection and coordination. Often, these are in conflict, and the matter is aggravated by the increasing utilization of (and inherent variability of) DG RES.

Power grid reliability and resiliency is also predicated upon, among other paradigms, sufficient mitigation against PSHF, which have been a significant cause of power system disturbances (e.g., cascading upstream) and major cascading collapses segueing to blackouts.

Preliminary experimental findings have shown that a translation-invariant CWT PyWavelet schema, via cascading, smaller convolutional filters aboard an ERCR-based CLNN, more closely approximates a whitebox paradigm.

The insight/discernment provided by this whitebox paradigm improves the likelihood of repeatability, thereby potentially enhancing the provenance of the involved AI/ML paradigm.

IARIA CONGRESS 2022

Hybridized Machine Learning Implementation for a Complex Network Cyber-Physical Supply Chain Analysis

Thank you!

Steve Chan, IARIA Fellow
& Decision Engineering Analysis Laboratory, VTIRL, VT
schan@dengineering.org

DECISION engineering Analysis Laboratory

IARIA CONGRESS | July 24-28, 2022 Nice, France