IARIA CYBER 2022

An Emergent Cyber-Topology Attack Vector Assessment

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

DECISION engineering Analysis Laboratory

IARIA CYBER 2022

November 13-17, 2022
Valencia, Spain

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 IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications (IARIA Congress 2022) from 24-28 July 2022 in Nice, Saint-Laurent-du-Var, France for the talk, "Hybridized Machine Learning Implementation for a Complex Network Cyber-Physical Supply Chain Analysis." 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

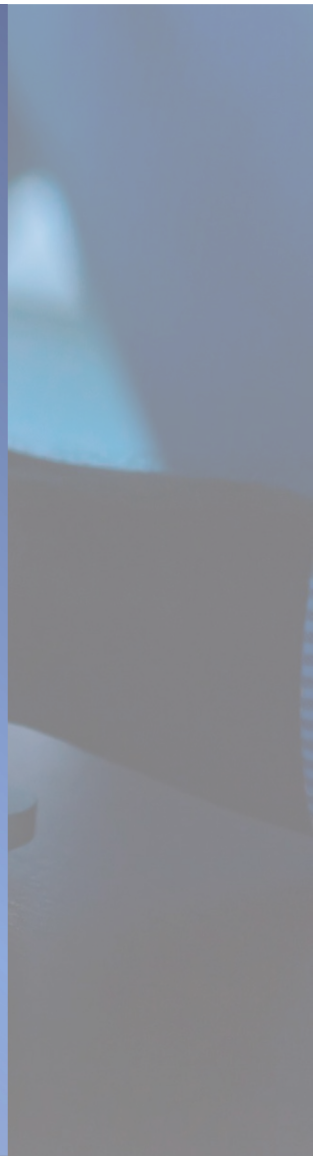
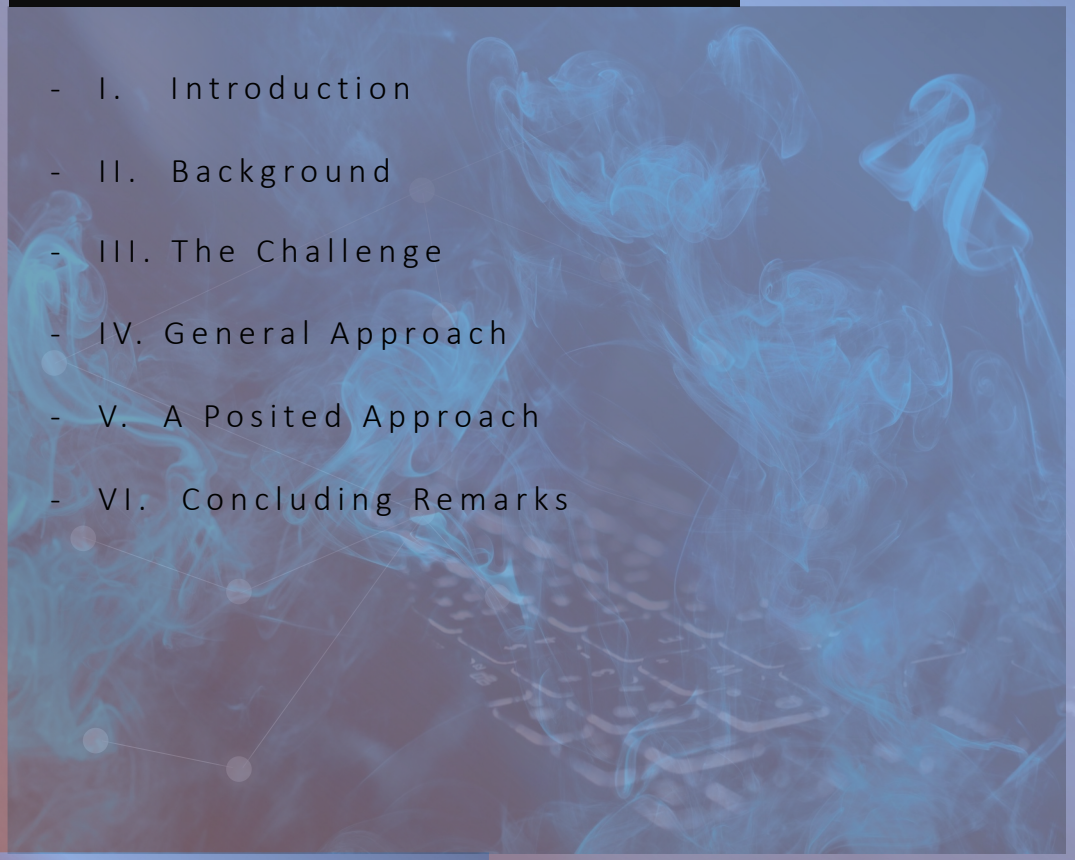
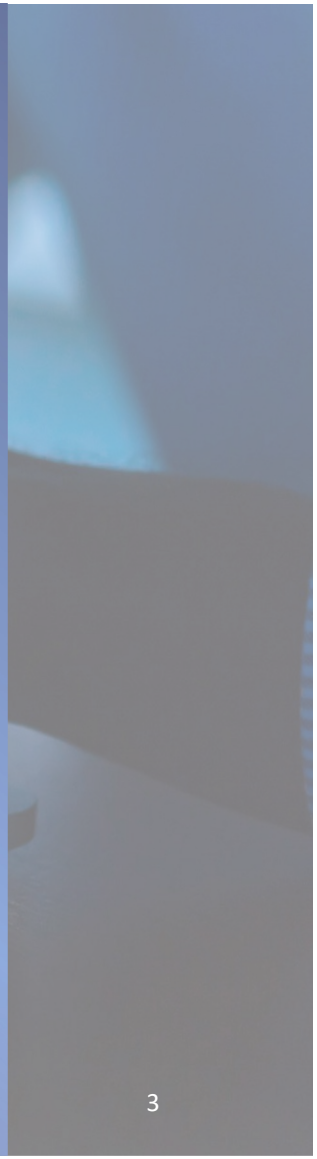


TABLE OF CONTENTS





DECISION engineering Analysis Laboratory

IARIA

I. INTRODUCTION

DECISION engineering Analysis Laboratory

IARIA

I. INTRODUCTION

Cyber-Physical Power Systems (CPPS)

The modern day CPPS, in the context of the energy sector, can consist of a physical system (e.g., equipment, hardware components, etc.) that is closely coupled with cyber-related systems (e.g., Information and Communications Technologies or ICT, software Command and Control or C2, etc.) for the enablement of the Smart Grid (SG). However, the more granular context and control is a double-edged sword, for it also makes the SG more vulnerable to cyber attacks.

I. INTRODUCTION cont'd

Information and Communications Technologies (ICT)

Modern ICT, in the context of the energy sector, is often used for measurement, monitoring, and control. With regards to measurement, ICT tends to leverage the Internet of Things (IOT) and Wireless Sensor Networks (WSN). With regards to monitoring, Power Line Communication (PLC) may come into play as well as a wide repertoire of other technologies. With regards to control, ICT is critical for coordination, synchronization, and optimization, among other responsibilities.

I. INTRODUCTION cont'd

DECISION engineering Analysis Laboratory

II. BACKGROUND

DECISION engineering Analysis Laboratory

IARIA

II. BACKGROUND

False Data Injection Attacks (FDIA)

A well-devised FDIA is a type of malicious data attack, which can target Critical Infrastructure (CI)/Strategic Infrastructure (SI) that are controlled by Cyber-Physical Information Systems (CPIS). In many FDIA cases, the attacker manipulates measurement readings so that incorrect data is utilized for mission-critical SG calculations – with ensuing potentially profound consequences (e.g., outage).

II. BACKGROUND cont'd

FDIA + False Command Injection Attack (FCIA) + Distributed Denial of Service (DDOS) Attack

The complexity of addressing FDIA (the falsification of measurement data) is often compounded, as FDIA is often also accompanied by a False Command Injection Attack (FCIA) (the forging of control instructions for breakers, etc.), and Distributed Denial of Service (DDOS) Attack (the flooding of the ICT network with traffic so as to block corrective actions). Hence, FDIA + FCIA + DDOS is a potent triumvirate.

II. BACKGROUND cont'd

III. THE CHALLENGE

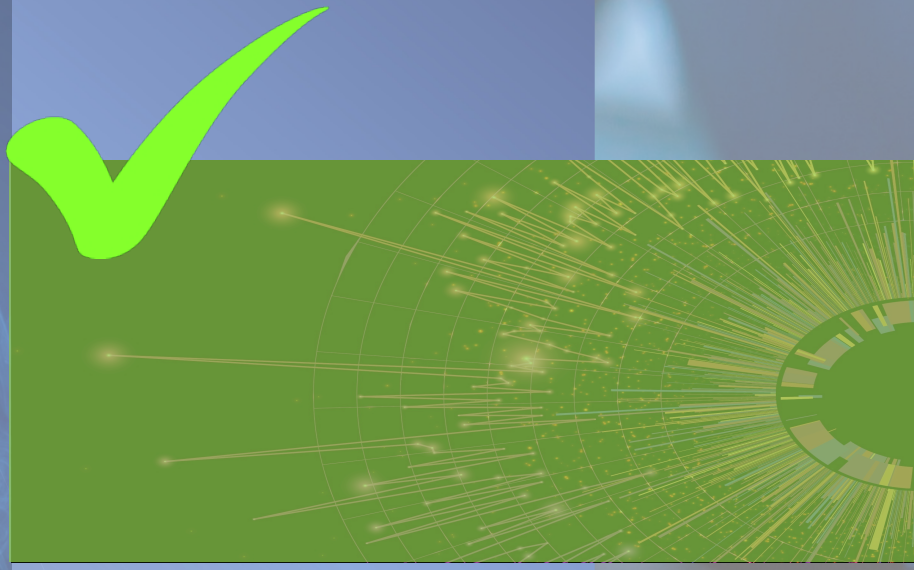
DECISION engineering Analysis Laboratory

IARIA

III. THE CHALLENGE

How Detect and Classify FDIA/FCIA?

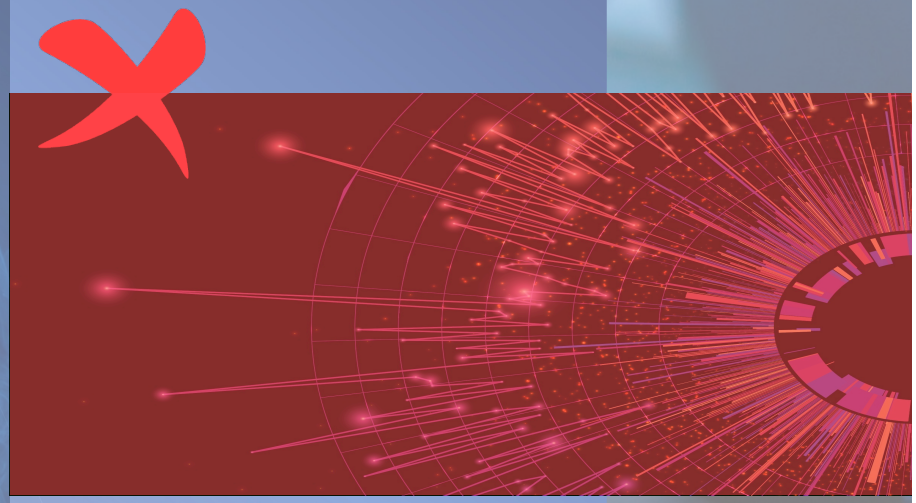
Detecting and Classifying FDIA/FCIA is non-trivial. Challenge problems include complex data features, which makes the task of Feature Extraction (FE) quite difficult. Other problems include the challenge of both false negatives and false positives (i.e., low detection accuracy), which makes the Dimensionality Reduction (DR) quite difficult as well. It should, therefore, be of no surprise that current Bad Data Detection and Identification (BDDI) for FDIA/FCIA are not yet robust.



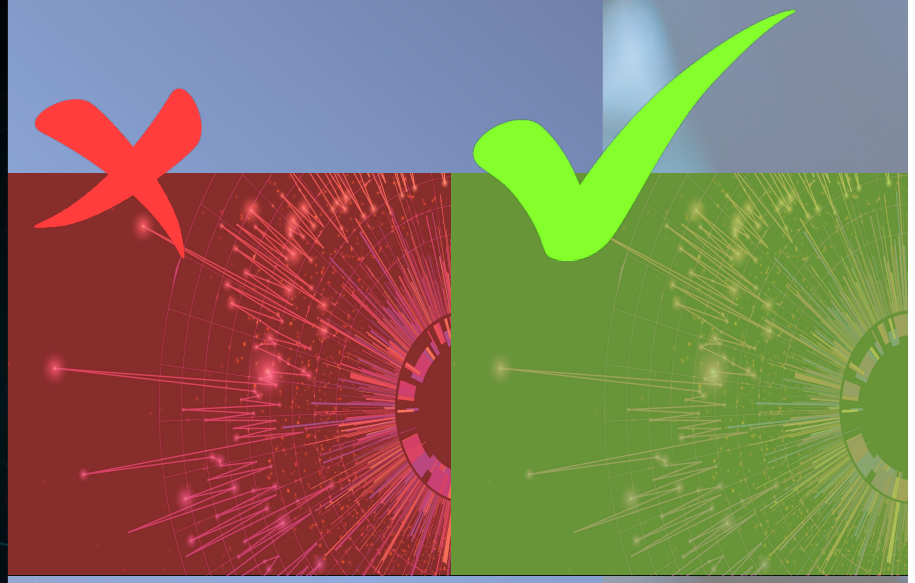
III. THE CHALLENGE cont'd

Data Integrity – What Data Should be Trusted?

Although Disturbance Monitoring Equipment (DME), such as Phasor Measurement Units (PMUs) and Phasor Data Concentrators (PDCs), can be utilized as part of a defensive strategy against FDIA, various studies have noted that compromised PMUs and PDCs can be enlisted as collaborators in a "Collusive False Data Injection (CFDI)" attack. In these cases, the PMUs and PDCs are no longer trusted defenders.



III. THE CHALLENGE cont'd



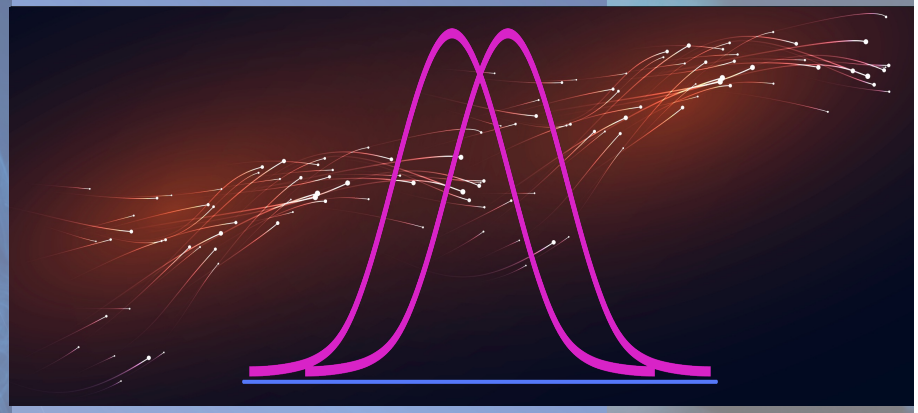
IV. POSITED APPROACH

DECISION engineering Analysis Laboratory

IV. GENERAL APPROACH

Kullback Leibler Divergence/Distance (KLD)?
Jensen-Shannon Divergence/Distance (JSD)? etc.

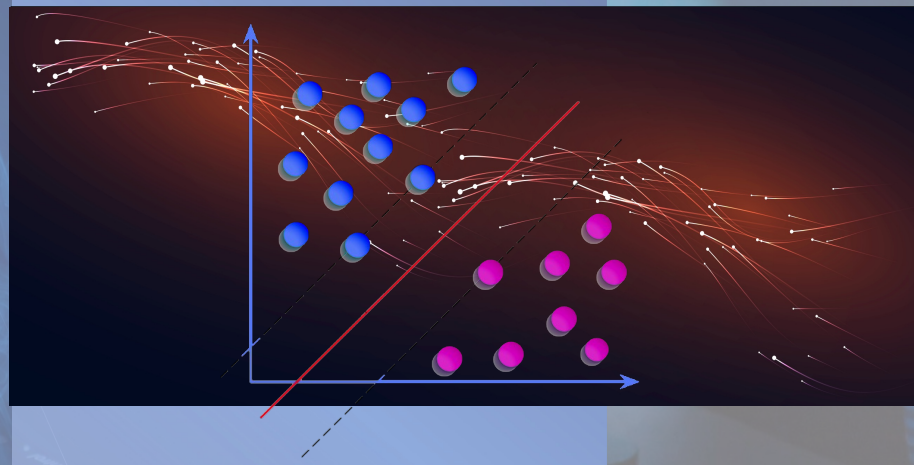
General approaches utilized to detect FDIA include Kullback-Leibler Divergence/Distance (KLD), which provides the distance between two Probability Distributions (PDs). For example, *m* could represent the *measured* PD (e.g., measurement deltas from historical data), and *p* could represent the *posit* PD regarding m (e.g., measurement deltas between current and historical data). The KLD can be construed as the average delta in the requisite number for bits for encoding *m* using optimized code for *p*.



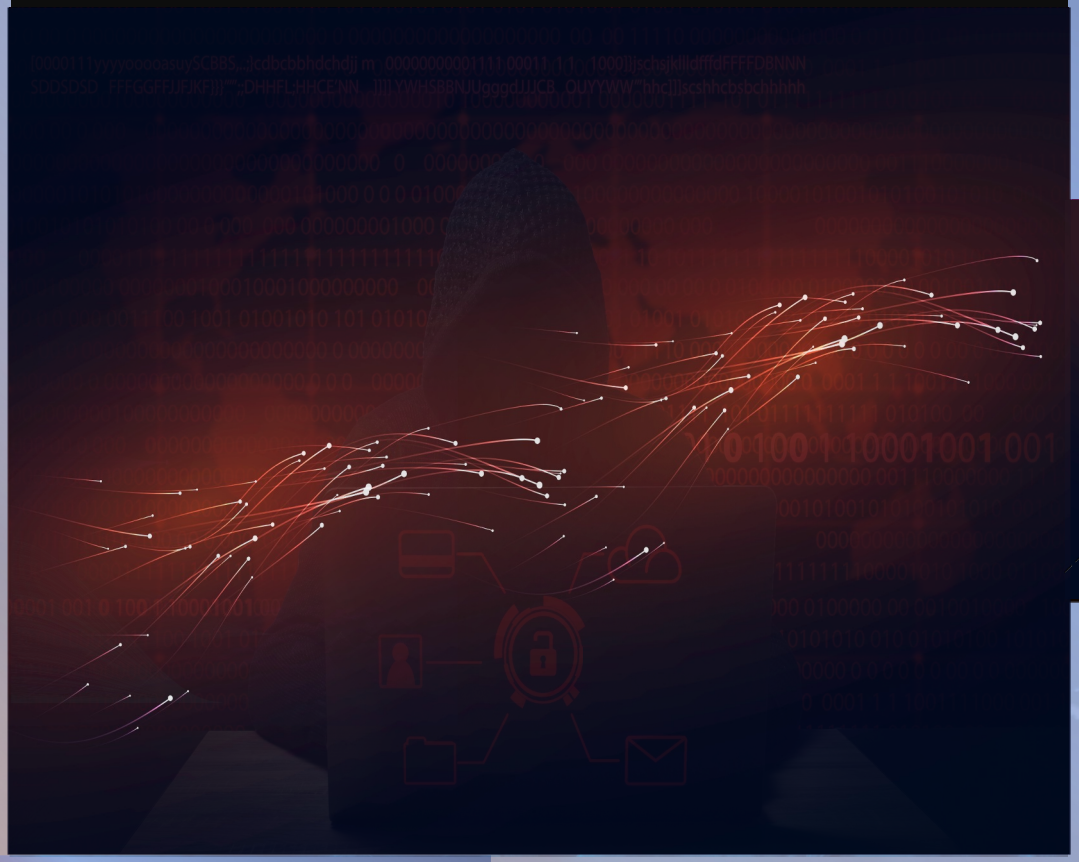
IV. GENERAL APPROACH cont'd

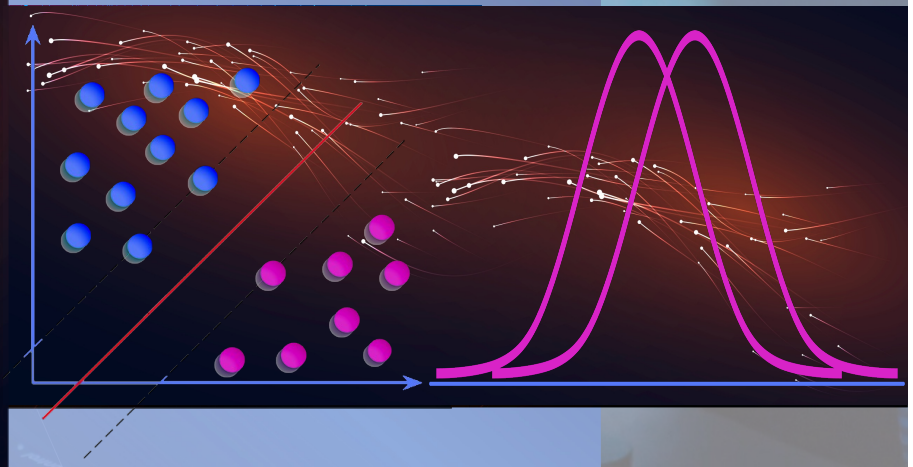
Support Vector Machine (SVM)? K-Nearest Neighbors (KNN)? Random Forest (RF)? etc.

Others prefer Machine Learning (ML) approaches, such as SVM to undertake effective Dimensionality Reduction (DR) and classification of the measurement data. Efforts have gone towards, among other pathways: (1) improving AutoEncoders (AE) for the DR as well as enhancing Feature Extraction (FE) with regards to the measurement data, and (2) improving the performance of the involved classification algorithm.



IV. GENERAL APPROACH cont'd





IV. POSITED APPROACH

DECISION engineering Analysis Laboratory

IARIA

IV. POSITED APPROACH

Metaheuristic Algorithm (MA)

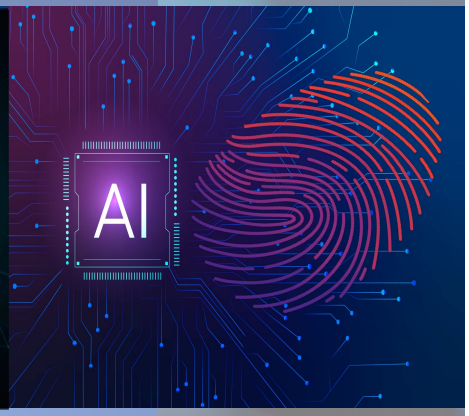
An MA can be construed as a Computational Intelligence (CI) paradigm, wherein the goal is to ascertain the optimal approach vector or most pragmatic solution set for the involved optimization problem. A heuristic is a specific technique for resolving the involved challenge problem more expeditiously when prototypical methods are not practical. The associated algorithms are typically designed for global optimization; otherwise, the algorithms might prematurely conclude at local optima.

IV. POSITED APPROACH cont'd

A Layered Defense-in-Depth Approach?

Perhaps, an MA might be useful to assess viable approaches and to handle the coordination thereof? For example, coordinated residual testing in various areas could be a viable approach. Other viable approaches include a variety of extensions for the CUmulative sUM (CUsUM) change detection test. Still other viable approaches include hop-by-hop authentication schemas. Yet other viable approaches include matrix separation schemas. These cited approaches have strengths and weaknesses depending upon context. Hence, if an MA could orchestrate the detection and classification, based upon the involved circumstances at the time, improved performance might be achieved.

IV. POSITED APPROACH cont'd



DECISION engineering Analysis Laboratory

IARIA

V. CONCLUDING REMARKS

DECISION engineering Analysis Laboratory

IARIA

IV. CONCLUDING REMARKS

For the realm of Cyber-Physical Systems (CPS), particularly CPPS, SG has a very large attack surface area, and it is highly susceptible to cyber attacks. Among these attacks, the triumvirate of FDIA/FCIA/DDOS has become a potent amalgam. Thus far, the efficacy of various FDIA detection and classification schemas varies greatly. The issue of false positives has been particularly nettlesome. Among other approaches, an MA for the mitigation of FDIA shows promise, and further research is warranted.

An Emergent Cyber-Topology Attack Vector Assessment

Thank you!

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