Simulation and Analysis of Cyber Attacks on Power and Energy Systems

Zachary Andrew Ruttle

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
In
Electrical Engineering

Chen-Ching Liu
Ming Jin
Virgilio A. Centeno
Ali Mehrizi-Sani

Electrical Engineering
May 3, 2023

Blacksburg, VA

Keywords: Cyber-Physical System Security, Power Systems, Fuzzy Inference System, Criminology

Simulation and Analysis of Cyber Attacks on Power and Energy Systems

Zachary Ruttle

ABSTRACT

The power grid has evolved over the course of many decades with the usage of cyber systems and communications such as Supervisory Control And Data Acquisition (SCADA); however, due to their connectivity to the internet, the cyber-power system can be infiltrated by malicious attackers. Encryption is not a singular solution. Currently, there are several cyber security measures in development, including those based on artificial intelligence. However, there is a need for a varying but consistent attack algorithm to serve as a testbed for these AI or other practices to be trained and tested. This is important because in the event of a real attacker, it is not possible to know exactly where they will attack and in what order. Therefore, the proposed method in this thesis is to use criminology concepts and fuzzy logic inference to create this algorithm and determine its effectiveness in making decisions on a cyber-physical system model. The method takes various characteristics of the attacker as an input, builds their ideal target node, and then compares the nodes to the high-impact target and chooses one as the goal. Based on that target and their knowledge, the attackers will attack nodes if they have resources. The results show that the proposed method can be used to create a variety of attacks with varying damaging effects, and one other set of tests shows the possibility for multiple attacks, such as denial of service and false data injection. The proposed method has been validated using an extended cyber-physical IEEE 13-node distribution system and sensitivity tests to ensure that the ruleset created would take each of the inputs well.

Simulation and Analysis of Cyber Attacks on Power and Energy Systems

Zachary Ruttle

GENERAL AUDIENCE ABSTRACT

For the last decades, information and communications technology has become more commonplace for electric power and energy systems around the world. As a result, it has attracted hackers to take advantage of the cyber vulnerabilities to attack critical systems and cause damage, e.g., the critical infrastructure for electric energy. The power grid is a wide-area, distributed infrastructure with numerous power plants, substations, transmission and distribution lines as well as customer facilities. For operation and control, the power grid needs to acquire measurements from substations and send control commands from the control center to substations. The cyber-physical system has its vulnerabilities that can be deployed by hackers to launch falsified measurements or commands. Much research is concerned with how to detect and mitigate cyber threats. These methods are used to determine if an attack is occurring, and, if so, what to do about it. However, for these techniques to work properly, there must be a way to test how the defense will understand the purpose and target of an actual attack, which is where the proposed modeling and simulation method for an attacker comes in. Using a set of values for their resources, motivation and other characteristics, the defense algorithm determines what the attacker's best target would be, and then finds the closest point on the power grid that they can attack. While there are still resources remaining based on the initial value, the attacker will keep choosing places and then execute the attack. From the results, these input characteristic values for the attacker can affect the decisions the attacker makes, and the damage to the system is reflected by the values too. This is tested by looking at the results for the high-impact nodes for each input value, and seeing what came out of it. This shows that it is possible to model an attacker for testing purposes on a simulation.

DEDICATION

The author dedicates this work to several people. My mother and father have supported me throughout and ensured that I would not be worried about finances through my research work, and for emotional support in times of need. My brother, for always being someone I can rely upon, to talk with and to help each other as best we can. My academic advisor and committee chair, Dr. Liu, for guiding me through these times and to help me find my calling in pursuing this research. The author will also thank Mr. Chensen Qi for his universal support at the start of my thesis and for any advice when available. I would also like to thank my friends, both online and on-campus, for any other support in any other issues of personal matters and stresses with assignments, to make my work on this project manageable. Finally, I would like to thank my professors and teachers, both through college and in high school for their continued faith in my work, and the guidance to reach this point in my life. I hope that through this report, I can show how far I have come, and show my preparation to join the workforce.

ACKNOWLEDGEMENTS

The author would like to acknowledge everyone who has helped me through my academic accomplishments, struggles and successes. My committee chair and co-chair have helped me shape this work to the best possible form, checking through my research and methodology until it is satisfactory, as well as making a valid test for the work. I would also like to thank everyone in the Power and Energy Center (PEC) for providing questions and discussion, as well as giving their help for the first semester with how to draft a paper and give presentations. The author would also like to acknowledge the graduate school, that the author may be able to present this paper and that the author was accepted here to begin with to help advance research with creative ideas and innovative solutions. Finally, the author would like to acknowledge the support from C3.ai DTI and the University of California, Berkeley, through the project, "Physics-aware AI-based Approach for Cyber Intrusion Detection in Substation Automation Systems."

The author will thank the PEC for their support, and the author wishes everyone well in the years to come.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1: INTRODUCTION

Section 1.1: Overview

Today's world is highly dependent on the continued supply of electric energy for life and to support the economy. Much of the food has a requirement of being kept fresh with refrigerators or heated with other appliances for consumption. People can stay in moderate conditions indoors with heaters and air conditioning. Furthermore, most of our products for goods and services rely on electric energy for industrial work. Due to the massive expansion of the power grid over the century since its creation in the United States, many advancements have been implanted to improve its reliability and reduce power outages. These massive blackouts can be caused by abnormal conditions arising from weather-based events or equipment failures. The most recent example is the 2003 Northeastern blackout in the U.S., which was caused by a cascading sequence of events starting from the failure of one line. The results of this are billions of dollars in damage and 50 million people without power [1]. Due to the threat this poses, many upgrades have been completed to make sure that issues are identified and addressed and the power grid weaknesses are removed. However, due to the requirement for incredibly low latency and immediate actions in case of emergencies, these systems must be trusted and kept around the clock with as minimal processing as possible. This is helped by Supervisory Control And Data Acquisition systems, as well as Intelligent Electronic Devices (IEDs) that enable substation automation [2]. Figure 1 shows the main elements of the cyber-physical system environment through Information and Communications Technology (ICT). The figure shows a control center that talks to each substation, and how each component of the cyber layer connects. However, these systems are based on the condition that data would be reliable, and some errors can be tolerated for operation and control. As an infrastructure that evolves over decades, cyber-attacks had not been considered until the recent massive increase in connectivity among various components and facilities as well as customers in the power grid.

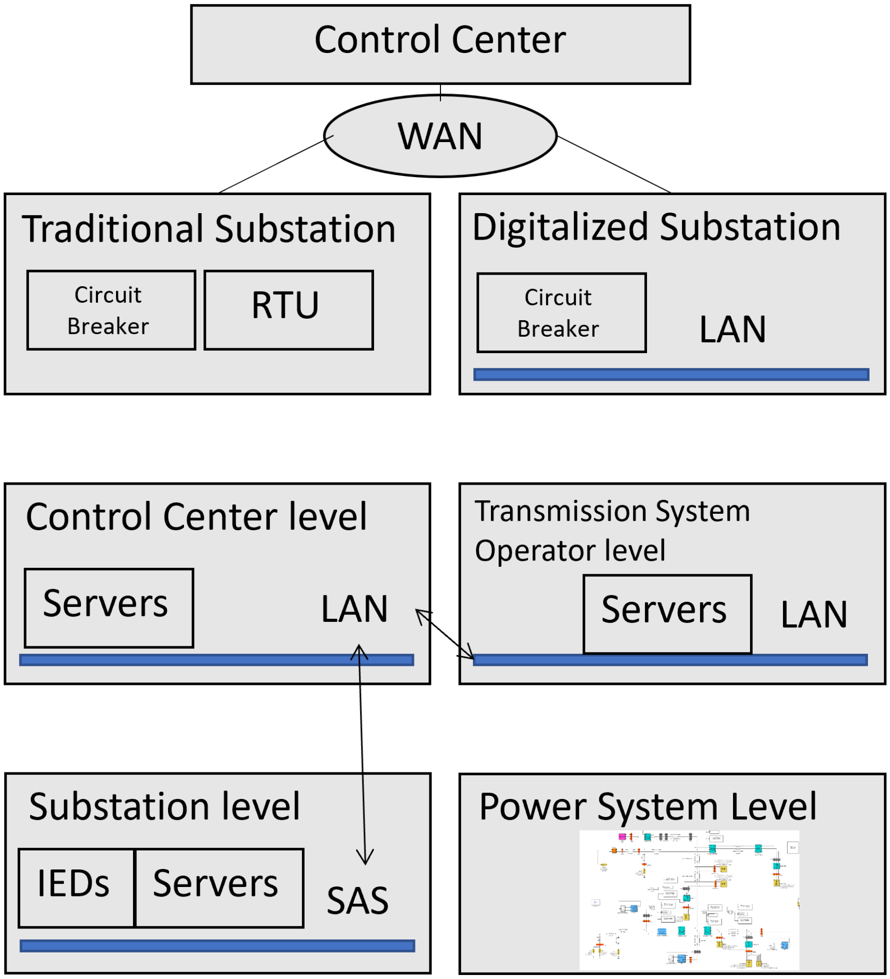


Fig. 1. The ICT model that is used typically for power systems is based on [2].

Section 1.2: Problem

A major feature of the power grid today that, due to its scale, to incorporate a cyber layer with the physical layer of the grid. The cyber layer reads information from the substations and other components and communicates with the control center for that area of the grid, as well as makes automated decisions in emergency cases. In recent times, hackers have had much more access to resources, both mechanically and in the knowledge base, over the course of this decade than ever before. Their computers now can remotely connect to and launch cyber-attacks on the power grid, due to the ability to acquire information through the internet as well as access the cyber systems on the grid. One well-known example of this is an attack on Ukrainian Kyvioblenergo, occurring on December 23, 2015 [3]. The attackers had set up a spear-phishing technique to implement their malware into the computers of the substation. Over the course of several months, their malware would crawl through the system, acquiring data to make an attack pattern and to acquire data. After a period of incubation, the attack occurred with the additional support of a telecommunications attack, opening circuit breakers, and altering systems, then finally deleting itself as well as the firmware to run the system. This effectively left the Ukrainian substation powerless, save for the manual breakers that existed there already. More importantly, it was a show of how dangerous cyber-criminals can become with the right motivations. A hacker with the right background in computer science and scripting, as well as sufficient resources, could become a threat to the power grids.

The method to defend against these attackers is more complex than the attacks themselves. The power grid, being a complex cyber-physical system, has a massive amount of information flowing through it that is time sensitive. If a cyber intrusion occurs on the system, the system must detect the anomaly and determine a solution within milliseconds. That is what the cyber layer’s job is; connecting the remote terminal units (RTUs) to a system to determine the status of the grid, and if there is a problem that will affect it, it will send commands to the physical layer via the cyber layer. The communication system that handles the real time function needs to be very quick to solve situations in milliseconds, and therefore typical encryption will not be efficient enough for the on-line environment. The time it takes to encrypt the data and then decrypt the data would not work for this case, since by the time it is transferred it is likely to be obsolete.

Section 1.3: State-of-the-art

There are, however, some implementations in the state-of-the-art that are already in place and are starting to be used to handle cyber-attacks. They are both proactive and reactive in nature, as a means of preparing and responding to anomalies. One method is simply an improvement of company policies to prevent malware from entering the system to cause the worst kinds of attacks, including how to deal with phishing frauds and social engineering [4]. Another method of protection is the Intrusion Detection System (IDS), which can detect malicious packets and inform operators of suspicious activities. However, while there are different configurations, they can have a faulty false positive flag or false negative pass in certain situations [2]. Also included in this set are Substation Automation Systems (SASs), which can handle sudden changes in topology, and make decisions that humans could not in a short time. Though, these are targets of attacks regarding false data injections. Regarding the determination of potential vulnerabilities, attack graphs are also created to determine issues in the cyber-physical system, regarding the criticality of the parts and the security measures in place [5]. Finally, there are also state estimators that use bad data detection (BDD) to determine if an Energy Management System is given the right analog and status measurements and determine that it has been tampered with. This is something that can be spoofed with masking effects if the attacker is knowledgeable on the limitations of BDD [6].

In the current situation regarding defending power grids from attacks, however, attackers can perform many kinds of attacks. Due to the nature of the power system, they can enter vulnerable locations and cause massive damages if vulnerabilities are not eliminated. The defenders must consider as many potential avenues of infiltration as possible, and some holes will always pop up. However, while people might miss information, defensive algorithms created through machine learning have a good chance of detecting and reacting to an attacker. However, the basis of machine learning must come from a comprehensive set of training and testing data, effectively serving as a background for what the defensive AI should expect. Research here should allow for a defensive algorithm to have a large testbed of information to go up against, to determine what is an attack and what to look for. However, such a simulation needs to be made to tie together energy and power systems with criminology to create a testbed of data to be utilized. Effectively, there needs to be an attacking algorithm that can work on a variety of power grid simulations, which provides a variety of attack types, so the attacks share specific characteristics but can attack many separate places.

After a review of the relevant literature, this thesis will go through the problem that needs to be solved in detail, followed by the methodology in the prototype and the main project. After that, the results will be shown, as well as their significance to the problem solution, with a discussion of the potential impacts and effectiveness of the model From there, the strengths and weaknesses of the attacking algorithm will be discussed in a conclusion section.

SECTION 2: LITERATURE REVIEW

Section 2.1: Criminology

One starts to know from research how it is easier to attack than to make a defense against an attack, from the perspective of the cyber-criminal. For instance, DoS attacks have been easily simulated, though with specific architecture and knowledge of it, they can be detected or mitigated [7]. The same can be said with more straightforward attacks that can inflict false injection or malicious control attacks. To best simulate the effects however, testbeds are implemented to figure out the impacts of an attack, using simulation tools such as OpenDSS and MATLAB [8]. For instance, they would use an ICT model with extensive programming to create a physical layer and a cyber layer, collecting data from the physical layer, making decisions with it in the cyber layer, and using an interface module to communicate between the two. This is the most effective method as it provides data in a real time environment, an active means to starting and stopping, and an ability for the malicious programs to be played alongside it to interact with the testbed and simulate the damage as in a real attack scenario. Testing can be performed by activating specific attacks in the layer upon the testbed, allowing for a realistic simulation. It is through means such as these that people will perform risk assessments and analyses of given physical systems to expose vulnerabilities that may otherwise be overlooked. These can range in their overall scope, such as testing the SCADA system's weaknesses to determine the efficiency of attacks, or with security implemented in the testbeds to determine their usefulness and further advance the technology in response to cyber threats [9] [10]. This methodology can be applied to power systems in general, from distribution to transmission levels. Due to the widespread usage of power flow tools, the results can provide details of what happens in each attack. Finally, due to the importance of cybersecurity for these critical electricity infrastructures there is a drive to use these attack models to develop defensive technology and standards for control systems. Papers also have been published concerning methods for anomaly detection, monitoring, analysis, and mitigation of attacks as well as prevention of damage [11]. So far, many of these models use these testbeds to develop new defensive mechanisms that look at the special components in the substations; in particular, the cyber layer which serves as entry points to cause damages. They look at the possible situations regarding cybersecurity that can arise, but not all the probable ones.

At the current moment, there is a daunting amount of information to look through regarding cyber-security as well as the criminology that stems from it. The main importance of cybersecurity is to protect three parts of information: availability, integrity, and confidentiality. Availability is concerned with the customer having access to data. Integrity means the data or information will not be changed. Confidentiality is to ensure that it will not be shown to anyone unauthorized. Cyber attackers violate these rules, and it is the focus of cyber security technology and procedures to keep them in check. To do this, there are several parts to look at concerning cyber security. The behavior of the attacker is one of looking at the target, the attacker, and the goals that they make. It is one of the basic concepts for cyber security that the behavior of the attackers will be based on their motivation and goals, such as whether they will destroy data without caring for covering their tracks or quietly steal it for black market purposes [12]. In every system, some vulnerabilities are caused by both human error and machine error; social engineering is an example of the former, while any system will have some weak points due to how they are built, and because someone will always find an area, they can enter. These represent human factors that can be taken advantage of. Finally, cyber security also requires extensive simulation and testing, to determine when anomalies occur or how hackers could get in. These three concepts represent the Venn diagram in Figure 2. Looking more at behavior too, Figure 3 also visualizes the basis of the intentions and actions of attackers, where each of their beliefs affects their attitude and worldview, enough that each attacker has their individualized touch. Normative beliefs affect their subjective norms, and control beliefs also affect their controlled behavior, leading to the creation of intentions and then actions. This is a part of psychology, that can also be applied to this concept of cybersecurity.

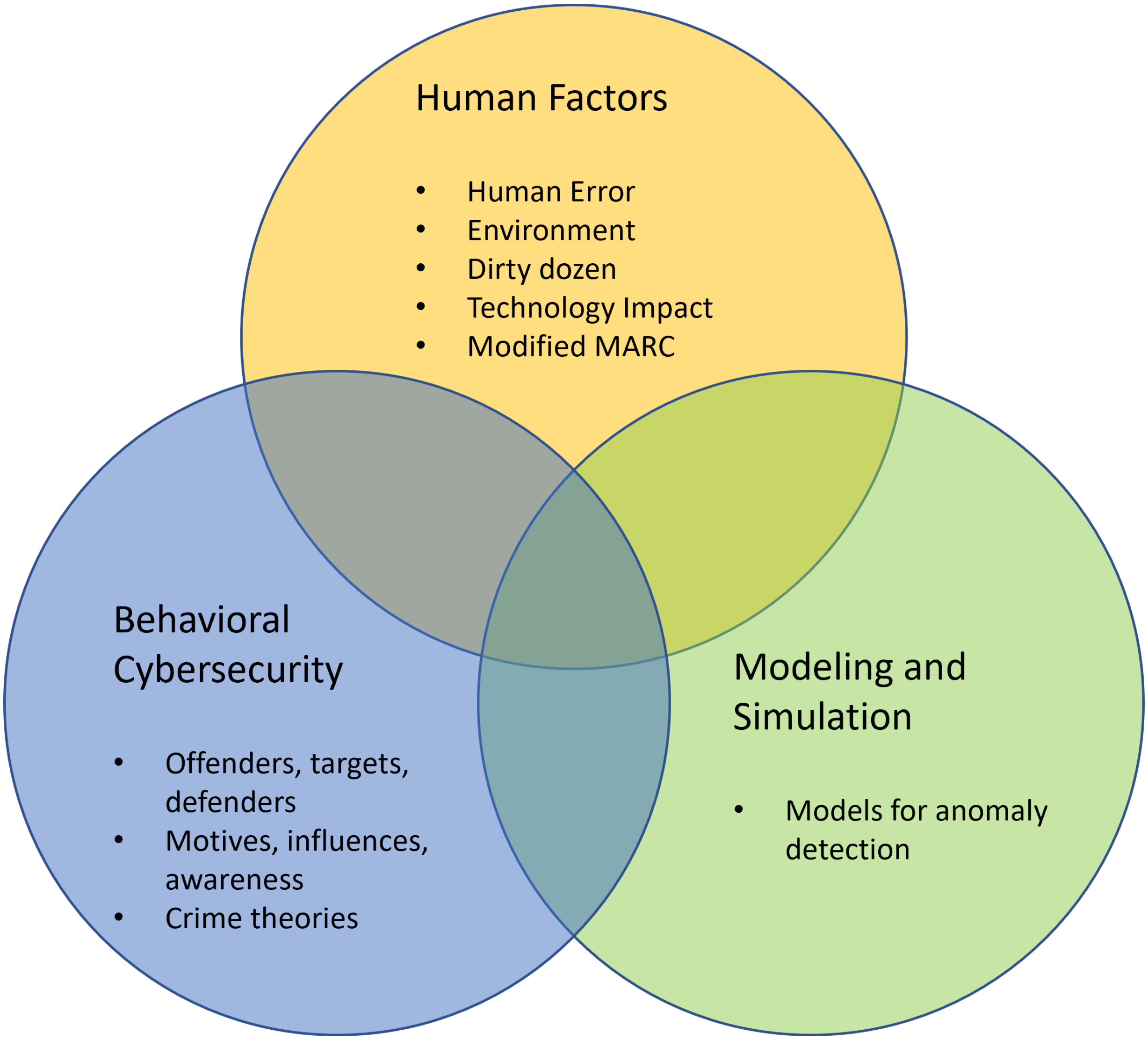


Fig. 2. The interdisciplinary framework of cyber-attacks based on [12].

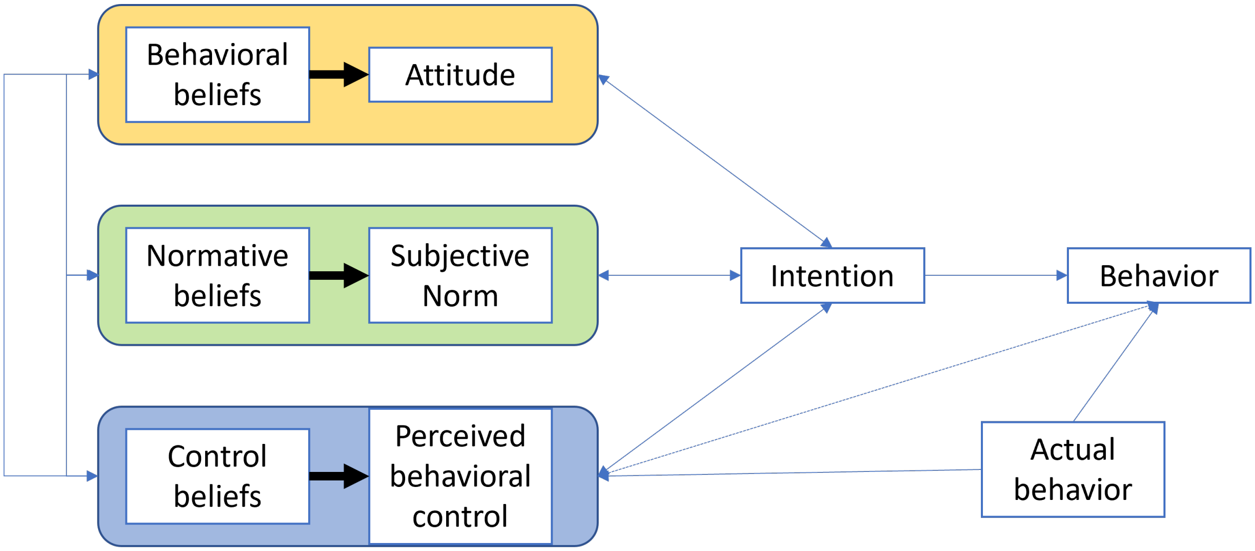


Fig. 3. The behavioral chart regarding cyber-attacks based on [12].

With this consideration of what an attacker may do based on their beliefs and goals, it is possible to create an attacker-centric model for a defense mechanism, and it has been considered in recent papers [13]. It will serve as a basis for connecting the literature on cyber criminology and power systems. One more important look is at a model for cybercriminals: The DSK-RAMG model developed off the online offender's SKRAM model [14]. This model is a way to look at the distinctive characteristics of an attacker to determine the attacker's identity and by extension their actions. This includes skills, knowledge, resources, authority, motivation, demographic (or disposition), and goals. This will serve as the basis for the methodology.

Section 2.2: Cyber-Physical Layer Interaction

An important background concerns the way of detecting vulnerabilities. Using the identification of attackers can create a risk assessment for several types of attackers over a grid, a subject covered in accompanying papers [15]. The power grid is connected on both cyber and physical layers, as shown in Figure 4; vulnerabilities in the cyber layer can affect the power grid's overall integrity, as there is an important distinction between how much protection a substation has in terms of cybersecurity and how integral it is to the overall grid. There will also be important implications regarding the importance of the location that is being attacked, such as a critical node connected to a hospital. Different attackers will want to target those places or avoid them for varying reasons, that is regarding their motivation and reasoning. This is the kind of information that can be taken advantage of in determining an attacker's identity.

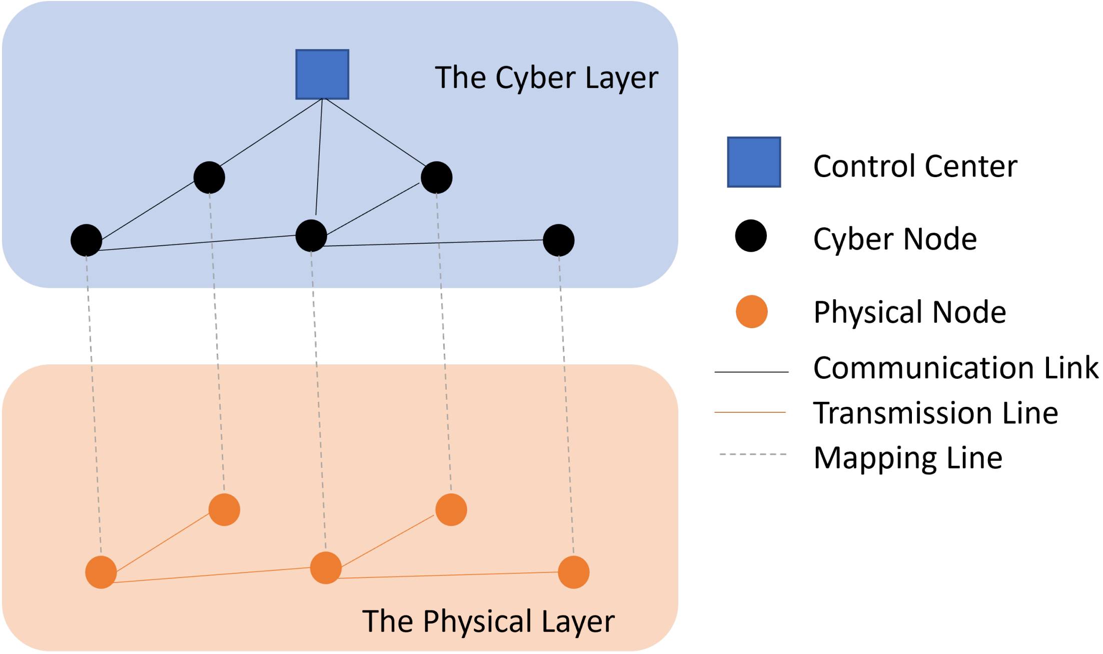


Fig. 4. Connections of the power grid to the cyber layer put two planes connected by mapping based on [15].

Overall, a large amount of research has already been done on the defense side of power systems, as well as cyber criminology in general due to it being a new advent. However, the connection between the two can help to solve the overall problem with the advantage attackers have over the defense systems.

SECTION 3: PROBLEM STATEMENT

The problem stems from the lack of a connection to the cybersecurity of power systems as well as the criminology on-base testing. The goal is to build a bridge between them and to make a varying simulated attack. At the current moment, most of the background for looking into defense mechanisms for power systems investigate viable solutions and incorporate an attack that investigates the vulnerabilities of the system. However, none of them specifically investigate the development of an algorithm that can simulate an attacker and the variations of attacks to allow for these defense mechanisms to be fully tested. The goal is to create an algorithm that can be tested on any given cyber-physical grid that can accurately represent a human attacker. This can vary such that attacker's capabilities, methods, and goals will affect how they will attack, but there is no guarantee that they will attack the same way again. However, they should know how to exploit vulnerabilities and perform their attacks their goals. The intentions can be modeled and decided at launch and an efficient and dynamic code can be used to output the results into a readable format. This results in defense mechanisms that are able to investigate the data and determine when the attack has commenced based on suspicious activity. This algorithm will be developed and validated on the IEEE 123-node system, then on the IEEE 13-node cyber-physical system model.

SECTION 4: METHODOLOGY

Section 4.1: Initial Implementation

The basis of this project starts with the concept of creating a test case and an accurate attacker for a defense mechanism, illustrated in Figure 5. The attacker will follow an algorithm that determines the attack strategy, initially using SoftMax but being updated fully later. Much of the process for entering the node, such as sniffing for ports and developing malware for entry, is assumed to be completed or automatically done during the process. Therefore, the main assumption for these attackers is that they are prepared for this and have a certain knowledge base about what they are doing. From there, they will follow an attacking process to reach their goals, going from node to node until they have run their course of the attack. During this, values can be sent out from the test grid regarding the state of voltages, currents, or circuit breakers, which can be analyzed for a potential defender.

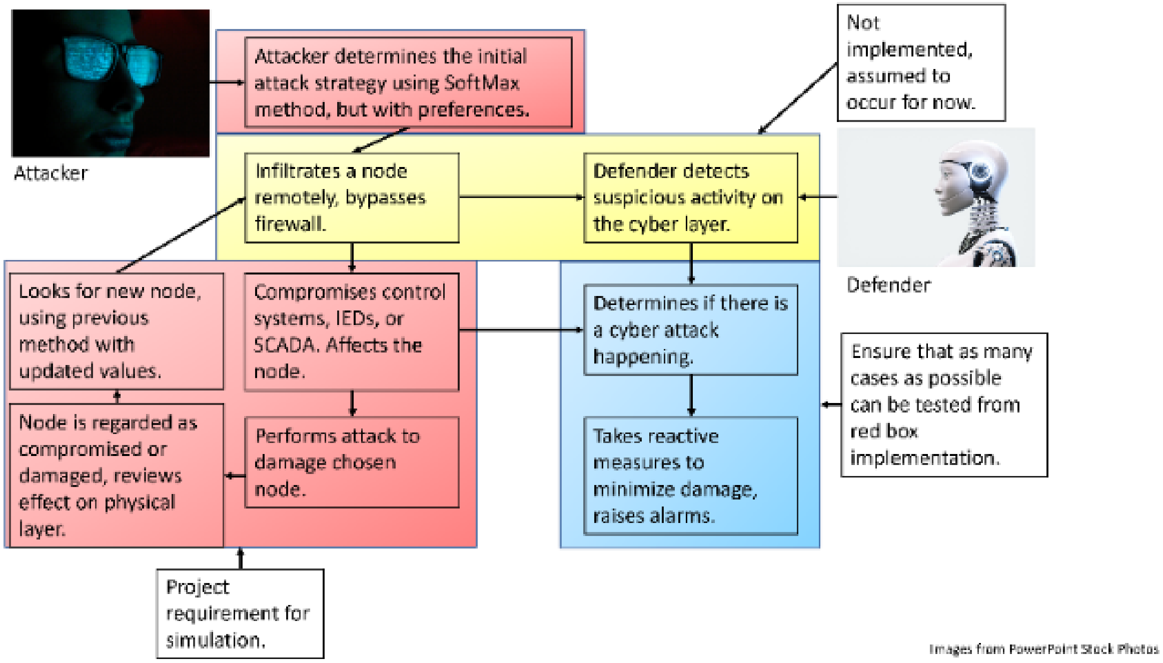

Attacker
Attacker determines the initial attack strategy using SoftMax method, but with preferences.
Not implemented, assumed to occur for now.
Infiltrates a node remotely, bypasses firewall.
Defender detects suspicious activity on the cyber layer.
Defender
Looks for new node, using previous method with updated values.
Compromises control systems, IEDs, or SCADA. Affects the node.
Determines if there is a cyber attack happening.
Ensure that as many cases as possible can be tested from red box implementation.
Node is regarded as compromised or damaged, reviews effect on physical layer.
Performs attack to damage chosen node.
Takes reactive measures to minimize damage, raises alarms.
Project requirement for simulation.
Images from PowerPoint Stock Photos

Fig. 5. Basis for the overall first part of experimentation and methodology.

The method and algorithm used for this portion can be summarized quickly, as the attack itself is simple. First, it determines the power flow on each of the breakers and randomly chooses which one to start on, with a bias towards ones that have more power flow through them. To determine the attack, there is a preset set of attacks available that will cause distinct types of damage, allowing for modular attacking methods. The bias towards higher power flow is also modeled after a linear equation, $\alpha*P + \beta$, which is put on the top of an exponent and made as a ratio to determine where to strike. When a node has been compromised, it is removed from the list, power flow is recalculated, and the attacker continues until they have finished their attack or run out of resources. While this all happens, information on the grid is recorded in a table, resulting in an easy-to-read set of numbers for both humans and machines to determine when attacks happen.

Section 4.2: Modeling the Attacker

However, this first part of the problem only accounts for a few of the actual inputs, so it is important to go back and look at a previous model used, the DSK-RAMG model for the attacker [14]. Each attacker will have a unique set of values associated with them that can be an important indicator of what they are going to do: attackers with more resources have a higher potential to break through more protected cyber nodes but may only want to disrupt one area. Or, they have fewer resources and want to perform a more efficient attack to cause damage with this in mind. Here is the full list of the items from the model and how they are used in this context:

- Knowledge: The amount of information that the attacker has on the power grid. Some grids are exceptionally large, and they may only have information to attack a small subset of it. This will determine the range in which they can perform attacks. If it is outside of their knowledge range, an attacker will not be able to effectively attack an area. Represented with ψ.

- Skills: Computational power and efficiency in programming, used to determine the time it will take to compromise one node. Important to determine how quickly a system will fail. Represented with λ.
- Resources: This represents labor, computer power, and prior development to perform an attack. There would be a vast difference in capabilities between a person with one computer in their basement and borrowed code and a team of experts with a whole number of powerful computers and a budget. More resources mean they can attack more nodes, as well as more defended nodes, determined by linear growth.
- Authority: This will stand for the already existing presence that an attacker has in a grid. Will be an indication of an insider attack, that can be performed much more quickly than an outside attack. The difference will typically be the speed of attack, so the authority will be the number of nodes that will either be already taken or quickly taken. Represented with Φ.
- Motivation: The general reason that they are attacking. This can be divided into three subsections. Low, for no real intention to cause damage, more just trying to test if they can do it. Disruptive, for wanting to cause a minor area disruption, such as causing a blackout at an area to do another job. Destructive, where the target is the power grid's integrity itself and the goal is purely to damage it.
- Disposition: Some attackers will wish to cover their tracks and identities, while some groups will not care if they are known and wish to cause heavy damage no matter the cost. This will vary between careful plans, and just straightforward attacking with no underhanded regards.
- Goals: The culmination of the previous resources and the reason why they are doing this, to begin with. This is the node that the attacker will intend to take that best achieves their goals and will be more determined from the rest of the previous inputs.

Motivation, Resources, and Disposition will be input in values between 0 and 10. The rest, however, are going to be varied in how they are measured, such as authority is a small number that represents the number of free nodes that they influence. Knowledge will be applied based on Figure 16, where the connections of the nodes to the goal will influence how likely they are to attack it. The further that the candidate targets are away from the primary target, the less likely they are to be targeted, with knowledge being the basis of how far it will drop. This primary target, as well, is the goal, which will be determined using fuzzy logic.

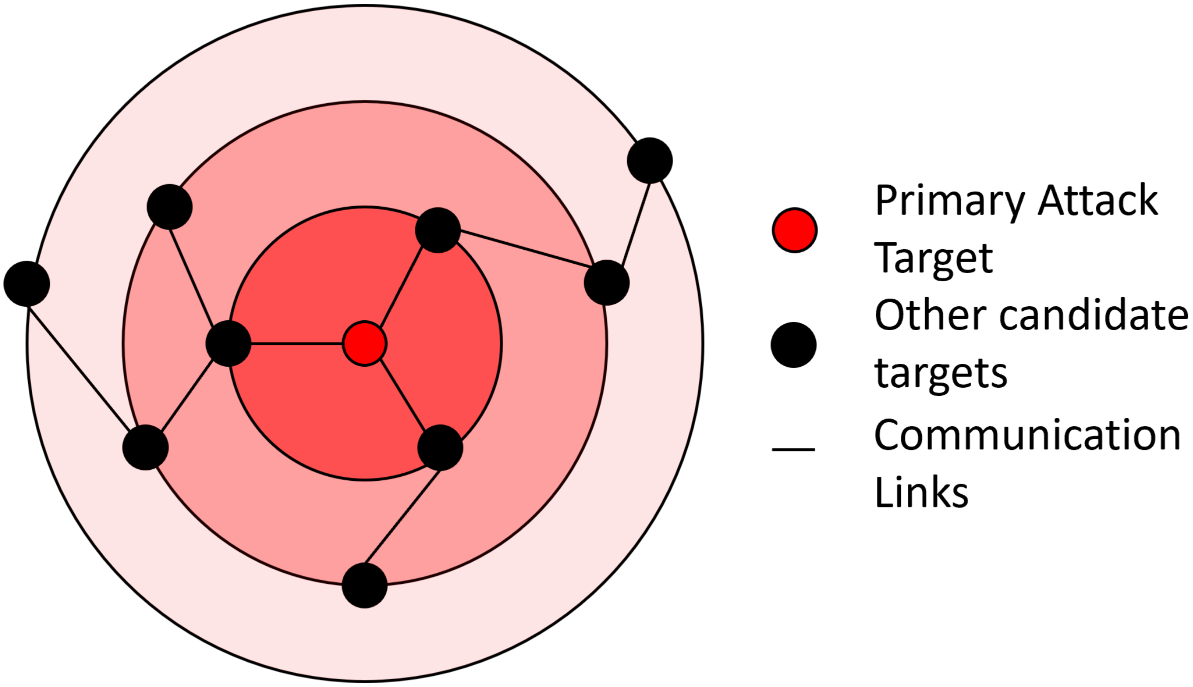


Fig. 6. Topological chart for candidates based on distance based on [15]. The closer they are in terms of links, the more likely the target is.

Section 4.3: Modeling the Targets

Before moving onto the logical portion of this, there also needs to be a determination of what these inputs will amount to. Each node, like attackers, has its properties to look at, here are the three main ones from the previously mentioned paper [15]:

- Cybersecurity level: The amount of cyber defense technology that is put into this, whether it is simply unprotected or with state-of-the-art security.
- Topological relationship: How connected the node is to the rest of the grid in terms of the topology.
- Criticality: Whether the node is critical, such as an airport or a hospital.

These are the Node Properties (NP). Each of these is going to be the characteristics of the nodes in the system put into 3 distinct numbers. The 3 numbers will be related to the inputs of the qualities of the attackers based on a given set of rules, such that if the rules determine that an attacker has outputs close to the properties of a node, they are more likely to attack said node due to the similarities. Determining these in nodes will be attributed to the properties of the grid itself. It is feasible to assume that higher load areas will be seen as more critical, and thus there will be a higher security level in those critical areas. There will be some variance (a Gaussian random distribution), however, they can be determined by the power flow. This power flow is normalized between 1 and 10 and given a Gaussian random distribution to it.

$$AC = norm(V * I) + N(0,1)$$

Note, the resources that the attacker will have regarding this security level will be a linear relationship. The attacker has attack points that are determined by resources by the following relationship:

$$ATK = 2 * RE$$

Topological relationships are also simple, as they only deal with how many connections are at each end of the breaker. The maximum is assumed to be 4 connections for both ends, so they will be similar in value to each other, but still normalized to fit in the correct range.

When considering what an attacker will do, however, there is also an important consideration in risk assessment regarding the importance of the nodes themselves. A substation could be connected to a critical load, such as a hospital or water treatment plant, that being knocked down will have a larger impact on the public area. Some attackers are aware of this and wish to cause more disturbance for varying reasons, so these areas would be better targets for them. The value of μ_t to be combined with load for special buses will range from 1 to 2.0 in increments of 0.2. These will account for different values of critical loads that will be distributed throughout the grid.

Section 4.4: Fuzzy Inference System

The fuzzy logic decision-making process uses a set of input ranges to output ranges, for instance, one can define each of the inputs on a scale of 0 to 10, and for each number, it has a certain degree of certainty to an area, such as “low,” “medium,” or “high.” The three inputs will be the resources, motivation, and disposition in these values, and the outputs will be the above preferences for attack complexity, topological relationship, and criticality. Using these inputs to these degrees, it can follow certain rules, such as “if low resources, output low attack complexity” to create the output values that will be used for comparing to nodes. For determining the fuzzy logic rules to attribute input to output, there is also a need for tuning to make the method more efficient. There are methods such as pattern search, KFold, and particle swarm to create these separate possibilities, though the goal is for fewer rules and accurate surfaces to represent the cases.

The system that is used for actual testing however, due to the cyber layer built with it allowing for much better validation, will be the IEEE 13-node system. This is detailed in Figure 7 each of the parts and how it is set up. The attacker will need to determine which nodes to choose from, though, so a slightly larger system that can be looked at for trends is needed before applying to this. Plus, the algorithm should have proof it can work in multiple areas. However, after the tests for the Fuzzy Inference System, tests will return to this.

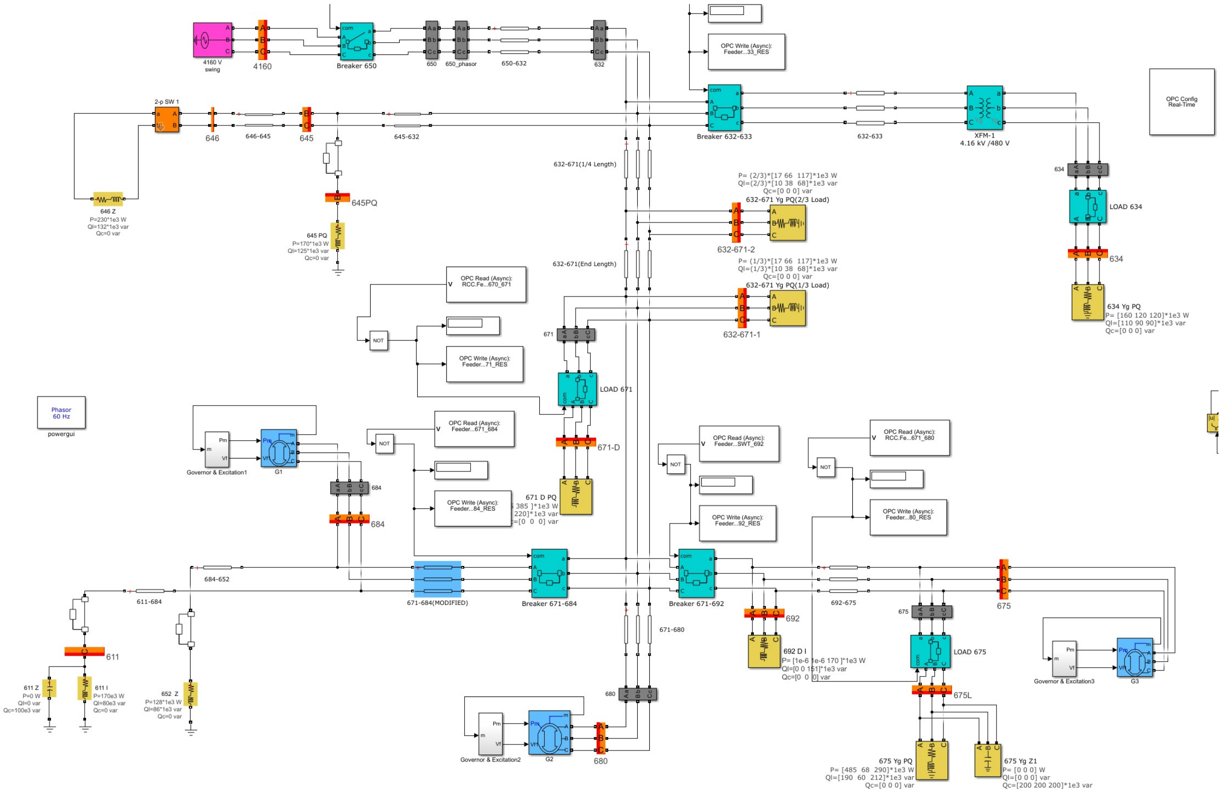


Fig. 7. Visualization of IEEE 13-node bus system for part 1 and final tests.

For the testing of the fuzzy inference system, the IEEE 123-node system is made on MATLAB [18], detailed in Figure 8 to show all the connections, loads, and breakers. Since it can be visualized, it would be easy to determine distances between breakers for decision-making.

However, compared to the 13-node system, it is a static model, so it is not as robust. To acquire the information, an initial benchmark test is performed to show it in nominal cases. This data is analyzed at each of the breakers to determine the load and create the characteristics for each of them, acquired from both the benchmark values, as well as the data that is already in the code regarding breakers and lines. Also on the breakers are the status of being open or closed, and these are the values that decisions will be made to manipulate.

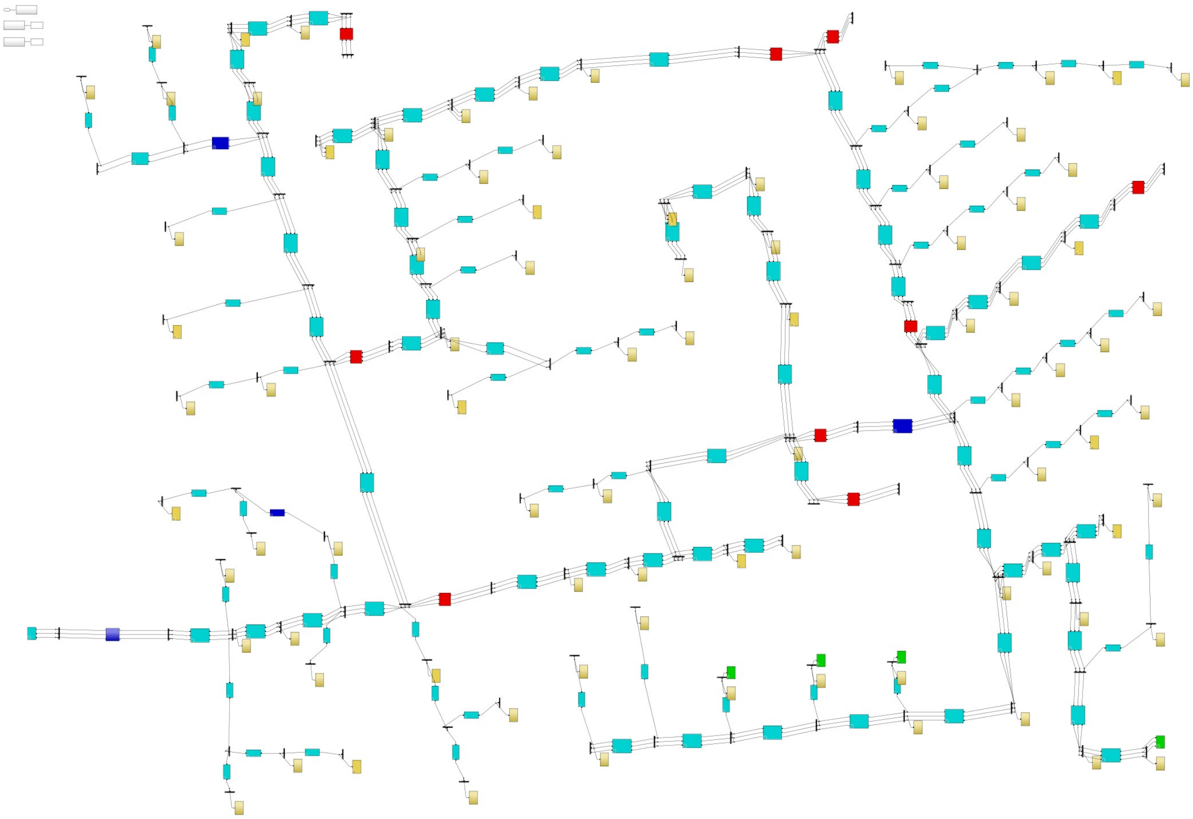


Fig. 8. The IEEE 123-node system. The breakers are red or blue in color [18].

With all the background put together for each part, the process goes as follows: The inputs from the DSK-RAMG model will first be entered into the code per their values. The 3 values that represent the inputs to the fuzzy inference system are from 1-10, while the others have their exclusive value. Once input, the fuzzy logic goes through the process of getting the outputs and creates the 3 values for the attacker's ideal target. Then, it will calculate these values for each of the important nodes where a breaker exists. All the data regarding power flow and topology will be normalized during this time to assign a value between 1 and 10. These will create 3 values for each node, and these are compared to the preferences to determine which has the lowest overall residue. Whichever is the most similar will be deemed as the target, and the last point in the attack, therefore the "goal". From here, based on the attacker's knowledge and the distance from this goal, the attack ratio, used to multiply the residue, and possibility will be determined for the rest of the nodes.

$$attack\ ratio = \frac{knowledge}{distance}$$

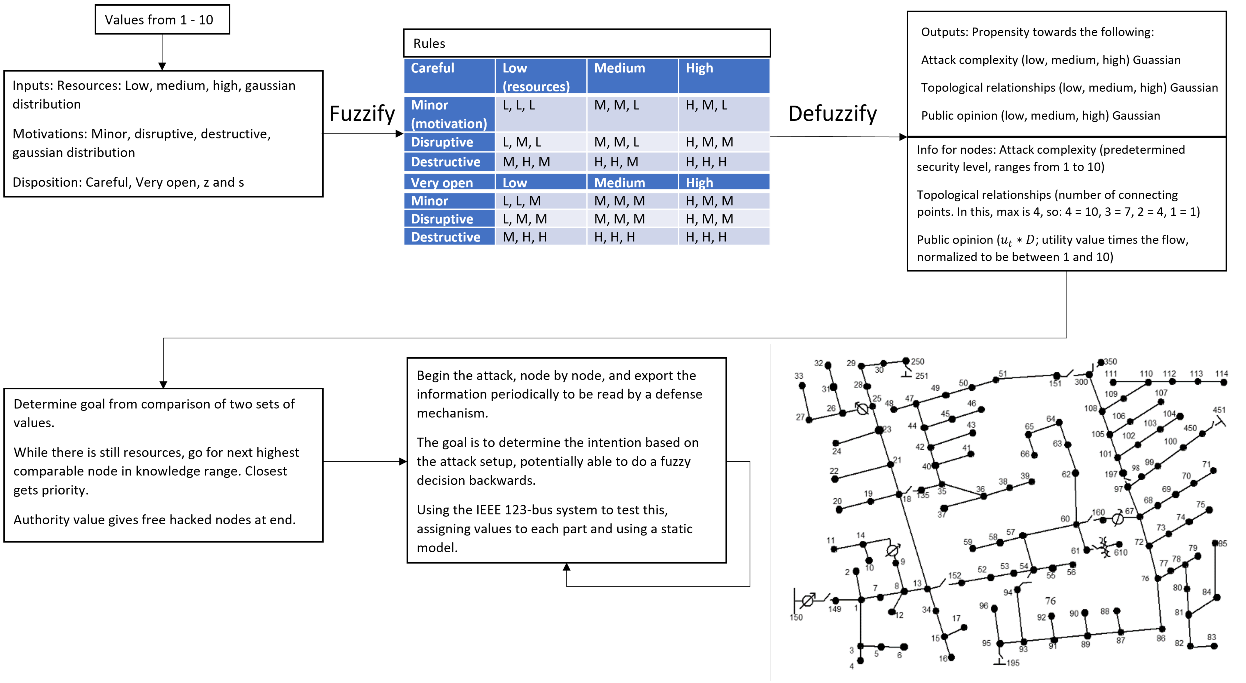
$$attack\ possibility = \frac{1}{ratio} * residue$$

This results in the following attack probability (AP) from point "i" as the goal to j as the secondary target, using previously established information.

$$AP[i][j] = \frac{D[i][j]}{\psi} * mean(AV - NP(j))$$

$$AV, NP(j) = [AC, TR, C]$$

Therefore, with all of this put together in mind, this leads to Figure 9 as the overall system that is used for this project. Each of the boxes represents a portion of the code, which loops at the end until the attack has been completed fully.



Inputs: Resources: Low, medium, high, gaussian distribution

Motivations: Minor, disruptive, destructive, gaussian distribution

Disposition: Careful, Very open, z and s

Rules

Careful	Low (resources)	Medium	High
Minor (motivation)	L, L, L	M, M, L	H, M, L
Disruptive	L, M, L	M, M, L	H, M, M
Destructive	M, H, M	H, H, M	H, H, H
Very open	Low	Medium	High
Minor	L, L, M	M, M, M	H, M, M
Disruptive	L, M, M	M, M, M	H, M, M
Destructive	M, H, H	H, H, H	H, H, H

Outputs: Propensity towards the following:

Attack complexity (low, medium, high) Guassian

Topological relationships (low, medium, high) Gaussian

Public opinion (low, medium, high) Gaussian

Info for nodes: Attack complexity (predetermined security level, ranges from 1 to 10)

Topological relationships (number of connecting points. In this, max is 4, so: 4 = 10, 3 = 7, 2 = 4, 1 = 1)

Public opinion ($u_t * D$; utility value times the flow, normalized to be between 1 and 10)

Determine goal from comparison of two sets of values.

While there is still resources, go for next highest comparable node in knowledge range. Closest gets priority.

Authority value gives free hacked nodes at end.

Begin the attack, node by node, and export the information periodically to be read by a defense mechanism.

The goal is to determine the intention based on the attack setup, potentially able to do a fuzzy decision backwards.

Using the IEEE 123-bus system to test this, assigning values to each part and using a static model.

Fig. 9. Algorithm using fuzzification and defuzzification for the IEEE 123-node system.

As the last part of this testing, due to the lack of a cyber layer for the IEEE 123-node system, the previous IEEE 13-node system will be used for the final test of the decision process. All the processes for the fuzzy inference system, the node inputs, and logic will be transferred and ensured to be properly cohesive with the new physical layer. This should be feasible because the process for attack decision-making is not tied directly to one power grid but is made so it can be implemented with any grid so long as the topology is known, which is to be expected by the attacker. This final test will ensure that the attacker can perform these decisions through a cyber layer, and obtain the results on how the cyber-physical layer will respond. As with the first part of this, an OPC will be used. The best way to perform this will be on the IEEE 13-node system again, which already has this, and is shown in the setup in Figure 7.

Overall, the methodology will focus on the determination of the attacker's path based on their properties, and from there will focus on what the effects of those actions are going to be. To connect the attacker’s preferences to a potential target, it is important to realize that the exact details of human preferences cannot be quantified. However, people tend to have preferences based on their experiences, backgrounds, and intentions, and fuzzy logic does well in these kinds of situations. This process will be key in connecting cyber criminology to actual algorithms for power systems, but for the time being the implementation will focus on just getting the order of nodes attacked. Once that is completed, it will be possible to see the effects that they have on the grid, and if it is comparable to the intention.

SECTION 5: RESULTS

Section 5.1: First Tests

For tests to be performed, there needed to be a cyber layer to interact with the physical layer. For this instance, one is already in place with the IEEE 13-node system, implemented in MATLAB as shown in Figure 10. It is an effective simulation that takes measurements from the physical layer passed through the OPC and put them through a First-In-First-Out (FIFO) queue to allow the system operator model to read them and figure out what to do with them and send out appropriate commands to the physical layer. Through the cyber system model, the attacker model is able to execute the malicious code.

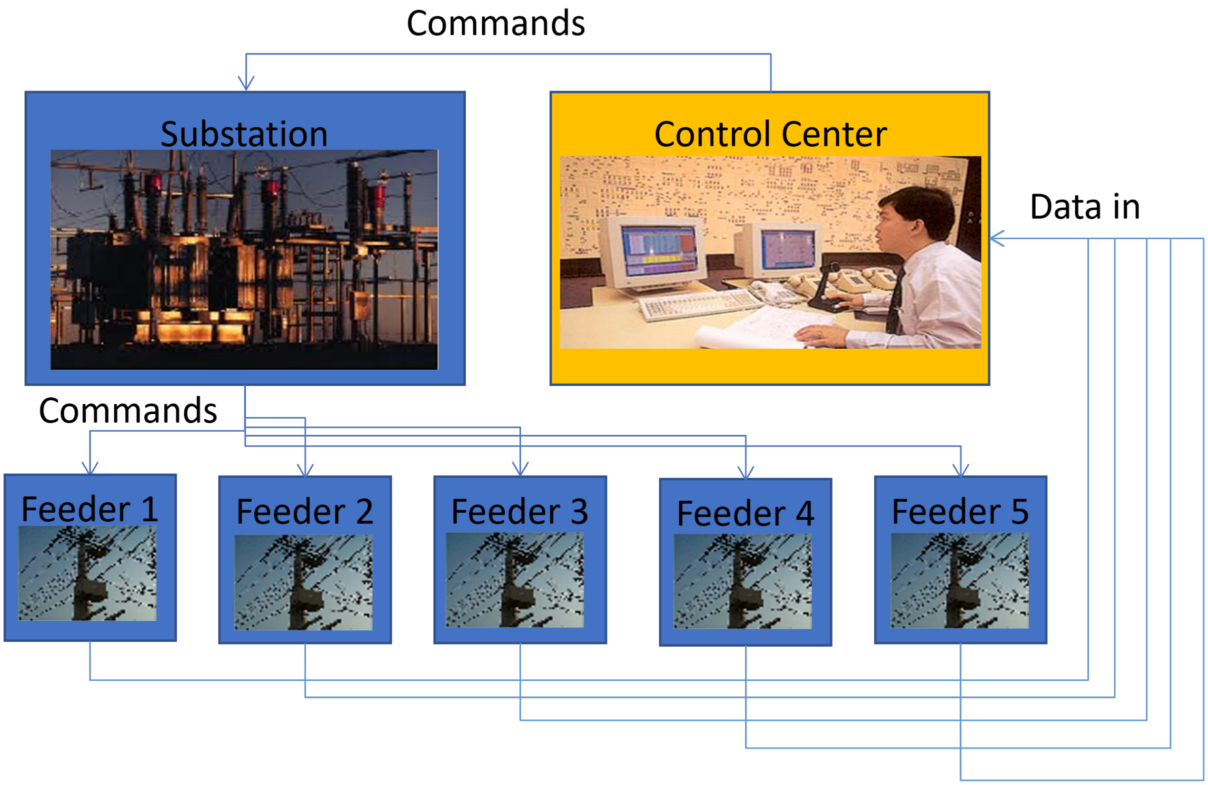
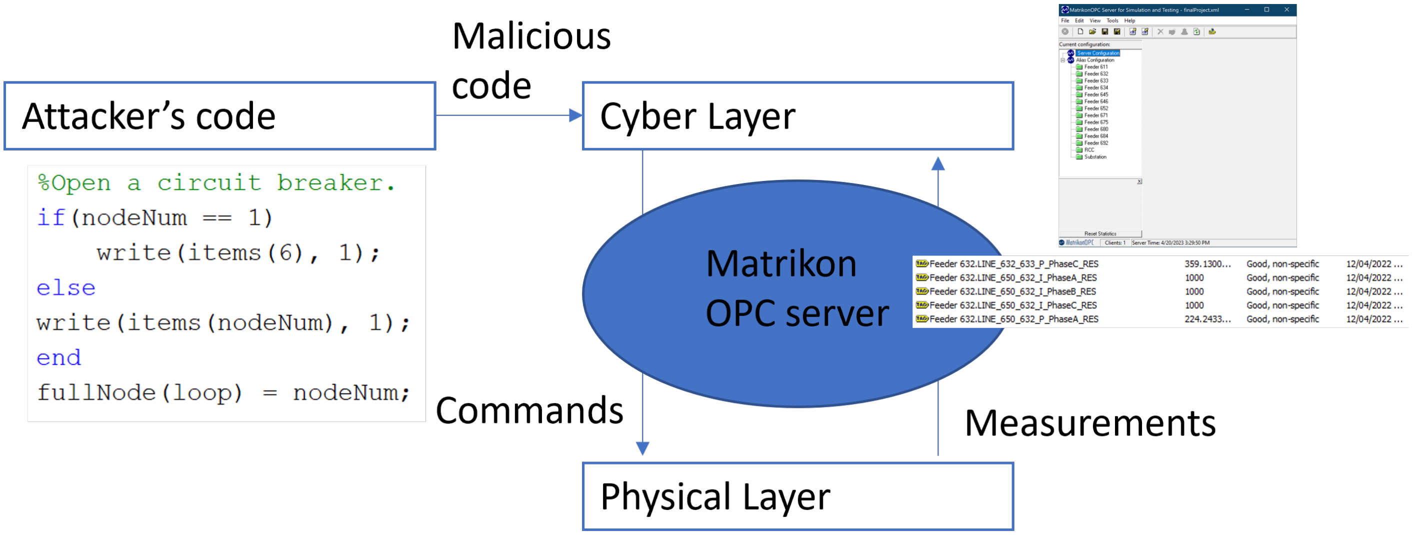


Fig. 10. Cyber layer used for simulation of the attacks.

The control center sees the cyber layer's information, which may be true measurements or falsified, it is susceptible to attacks through these means. The code will execute on the side in MATLAB and send falsified commands to the cyber layer, and from there it goes through the OPC to the physical layer. The process is shown in Figure 11, where the attacker uses code to artificially alter values in the cyber layer, which in turn will affect the physical layer of the grid.



```
%Open a circuit breaker.
if(nodeNum == 1)
    write(items(6), 1);
else
write(items(nodeNum), 1);
end
fullNode(loop) = nodeNum;
```

Feeder 632.LINE_632_633_P_PhaseC_RES	359.1300...	Good, non-specific	12/04/2022 ...
Feeder 632.LINE_650_632_I_PhaseA_RES	1000	Good, non-specific	12/04/2022 ...
Feeder 632.LINE_650_632_I_PhaseB_RES	1000	Good, non-specific	12/04/2022 ...
Feeder 632.LINE_650_632_I_PhaseC_RES	1000	Good, non-specific	12/04/2022 ...
Feeder 632.LINE_650_632_P_PhaseA_RES	224.2433...	Good, non-specific	12/04/2022 ...

Fig. 11. Cyber layer interaction with the attacker, using code to perform actions through the cyber layer manually.

From the first part of the project, the attack determination using the OPC, and the cyber layer is performed using reads from each of the breakers, which determined where in Figure 10 the attacker would send their attack to. In the case of α = 1, the attacker decides to attack node 1, or breaker 671-692 in Figure 12.

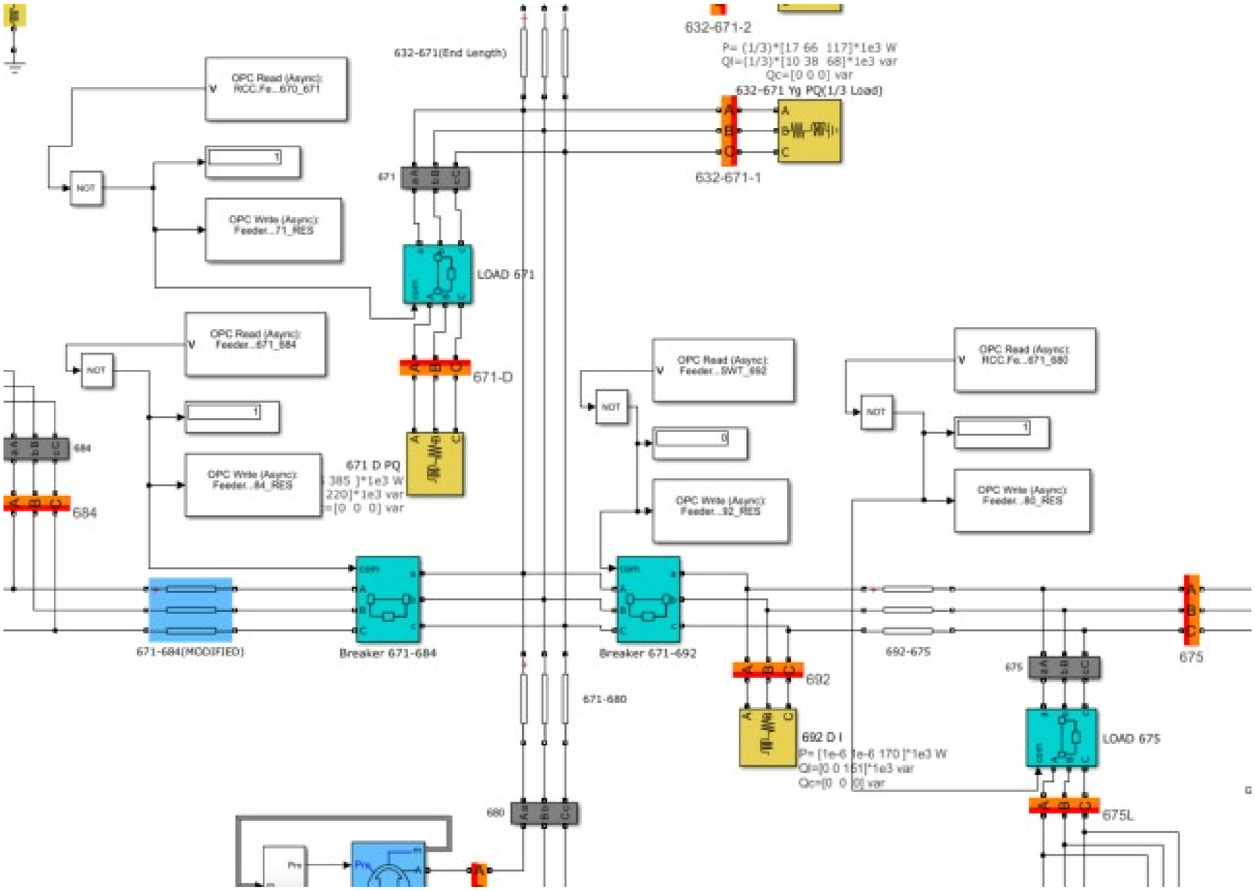

632-671-2
P= (1/3)*[17 66 117]*1e3 W
Ql=(1/3)*[10 38 68]*1e3 var
Qc=[0 0 0] var
632-671 Yg PQ(1/3 Load)
632-671(End Length)
OPC Read (Async): RCC.Fe...670_671
632-671-1
671
NOT
OPC Write (Async): Feeder...71_RES
LOAD 671
OPC Read (Async): Feeder...671_684
671-D
684
671 D PQ
385]*1e3 W
220]*1e3 var
=[0 0 0] var
OPC Write (Async): Feeder...84_RES
OPC Read (Async): Feeder...SWT_692
OPC Write (Async): Feeder...92_RES
OPC Read (Async): RCC.Fe...671_680
OPC Write (Async): Feeder...80_RES
671-684(MODIFIED)
Breaker 671-684
Breaker 671-692
692-675
675
692
671-680
692 D I
P=[1e-6 1e-6 170]*1e3 W
Ql=[0 0 151]*1e3 var
Qc=[0 0 0] var
LOAD 675
675L
680

Fig. 12. A part of the physical layer shows most of the writing to the circuit breakers, allowing for planned opening and closing.

The results of the malicious command attack have a few effects. The generator that is directly connected to this branch in the IEEE 13-node system, generator 3, the power output begins to oscillate heavily, as shown in Figure 13. Furthermore, the power flow through many areas are affected by this. These values are shown in Table 1. The attack happens approximately at the 4th timestamp.

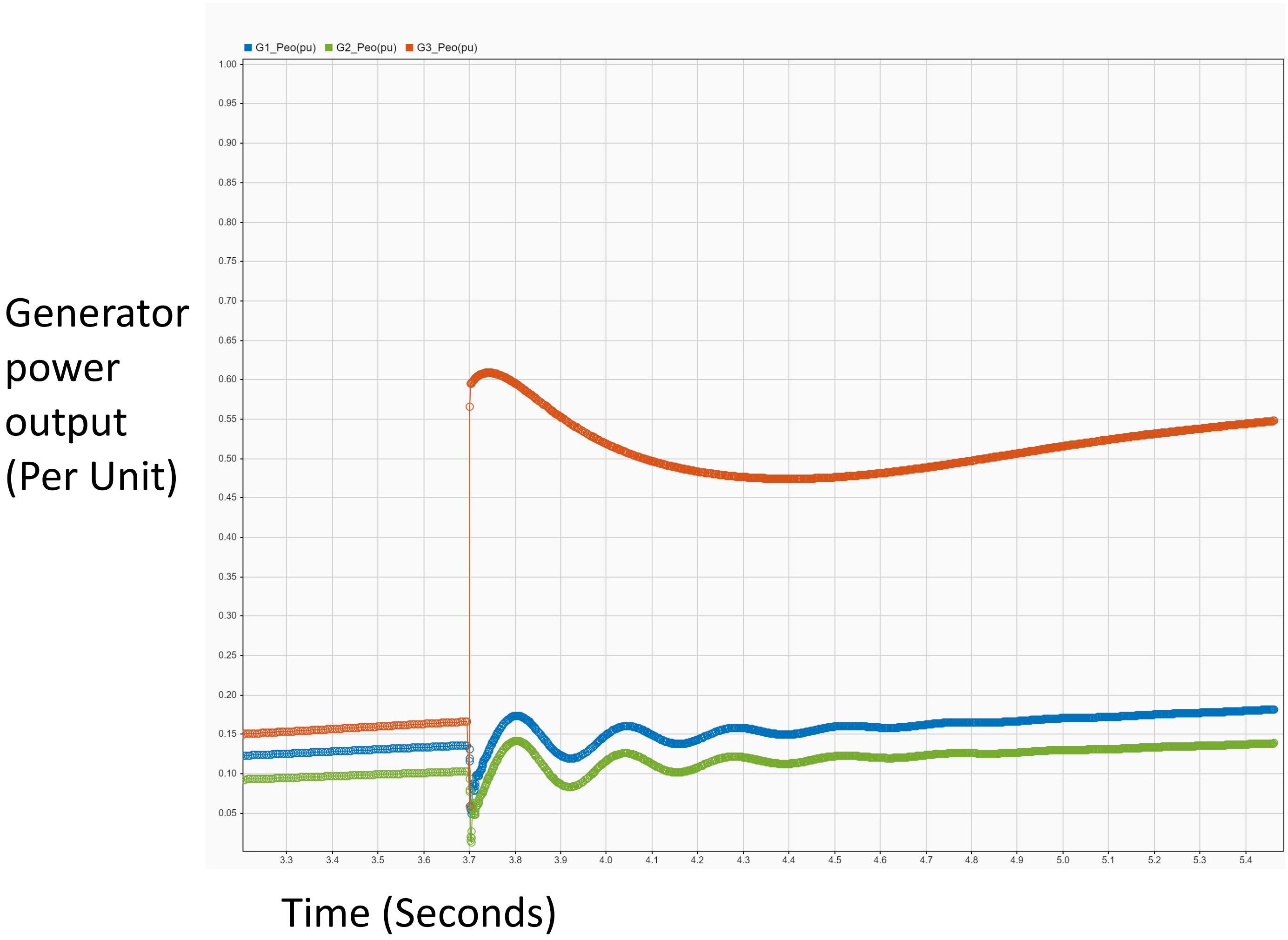


Fig. 13. G1, G2, G3 power waveforms following the malicious command attack.

Timestamp	P1	P2	P3	P4	P5
18	4.69*10^5	63.0	3.97*10^2	2.32*10^2	1.36*10^2
19	4.69*10^5	63.0	3.97*10^2	2.32*10^2	1.36*10^2
20	4.69*10^5	63.0	3.97*10^2	2.32*10^2	1.36*10^2
21	4.71*10^5	60.9	5.39*10^-7	2.10*10^2	1.37*10^2

Table 1. Data from malicious command attack for nodes 1-5 at each timestamp. P is power flow through node.

The other generators in this situation are able to recover after some oscillation, however. Another well-known of attack, particularly for less damaging attack methods, is the false data injection, which resulted in Figures 14 and Table 2 for the outputs. These false data injection attacks incite a drop in the load served, which can be seen here, and thus opens a breaker that is directly related to load. This creates some oscillation, but the goal would be to cause a certain area to lose power, or to make the grid run sub-optimally.

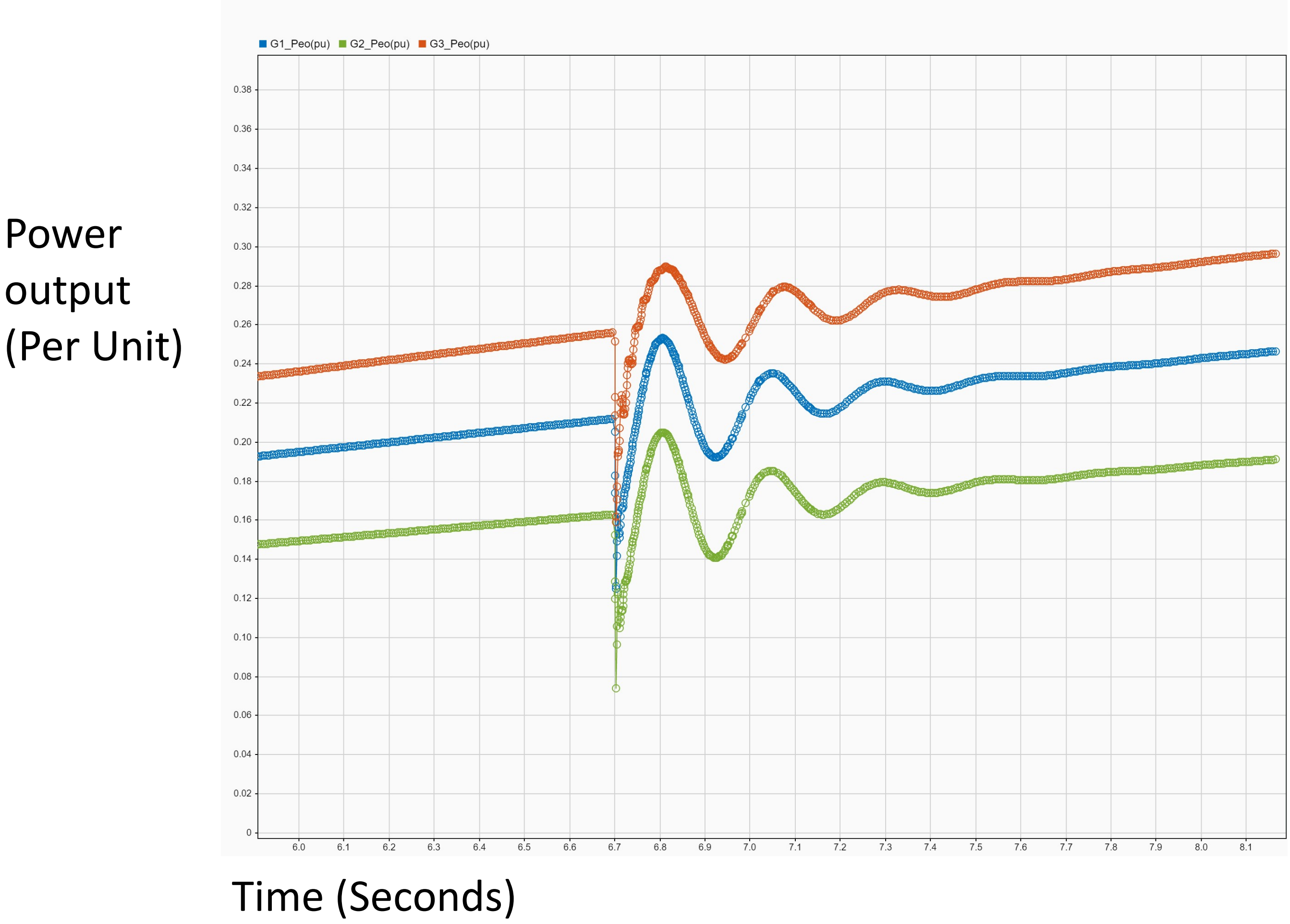


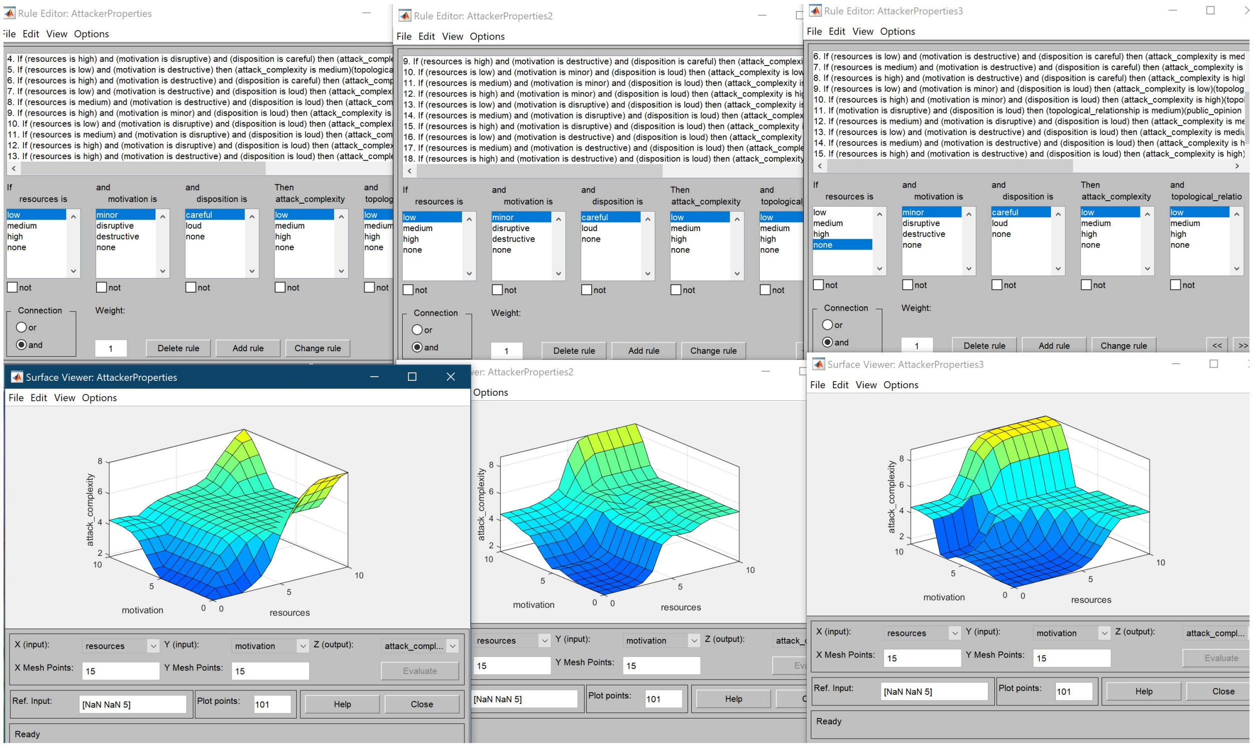
Fig. 14. Oscillation of power output from G1, G2, G3 following a FDI attack and subsequent load drop.

Timestamp	P1	P2	P3	P4	P5
11	4.67*10^5	60.4	3.97*10^2	2.41*10^2	1.36*10^2
12	4.67*10^5	60.5	3.97*10^2	2.40*10^2	1.36*10^2
13	4.67*10^5	60.7	3.97*10^2	2.40*10^2	1.36*10^2
14	4.67*10^5	60.7	3.97*10^2	2.40*10^2	1.36*10^2
Timestamp	I1	I2	I3	I4	I5
11	1.84*10^2	1.19*10^2	8.09*10^2	4.82*10^2	2.66*10^2
12	1000	1.19*10^2	8.09*10^2	4.81*10^2	2.66*10^2
13	1.85*10^2	1.19*10^2	8.09*10^2	4.80*10^2	2.66*10^2
14	1.85*10^2	1.19*10^2	8.09*10^2	4.80*10^2	2.66*10^2

Table 2. Data from a FDI attack for nodes 1-5 at each timestamp. P is power flow, I is current for node.

Section 5.2: Fuzzy Optimization and Testing

From the start of applying the methods, several different fuzzy inference systems (available in MATLAB) are made to simulate the relation of the attacker's properties to the properties of the nodes. Initially, it is based on the ruleset that is crafted by hand in Figure 9, but put through optimization algorithms, the various properties that make up Figure 15 are observed.



Rule Editor: AttackerProperties

```
4. If (resources is high) and (motivation is disruptive) and (disposition is careful) then (attack_comple
5. If (resources is low) and (motivation is destructive) then (attack_complexity is medium)(topologica
6. If (resources is high) and (motivation is destructive) and (disposition is careful) then (attack_comp
7. If (resources is low) and (motivation is destructive) and (disposition is loud) then (attack_complexi
8. If (resources is medium) and (motivation is destructive) and (disposition is loud) then (attack_com
9. If (resources is high) and (motivation is minor) and (disposition is loud) then (attack_complexity is
10. If (resources is low) and (motivation is disruptive) and (disposition is loud) then (attack_complexi
11. If (resources is medium) and (motivation is disruptive) and (disposition is loud) then (attack_com
12. If (resources is high) and (motivation is disruptive) and (disposition is loud) then (attack_complex
13. If (resources is high) and (motivation is destructive) and (disposition is loud) then (attack_comple
```

Rule Editor: AttackerProperties2

```
9. If (resources is high) and (motivation is destructive) and (disposition is careful) then (attack_complexi
10. If (resources is low) and (motivation is minor) and (disposition is loud) then (attack_complexity is low
11. If (resources is medium) and (motivation is minor) and (disposition is loud) then (attack_complexity is
12. If (resources is high) and (motivation is minor) and (disposition is loud) then (attack_complexity is hi
13. If (resources is low) and (motivation is disruptive) and (disposition is loud) then (attack_complexity is
14. If (resources is medium) and (motivation is disruptive) and (disposition is loud) then (attack_complex
15. If (resources is high) and (motivation is disruptive) and (disposition is loud) then (attack_complexity i
16. If (resources is low) and (motivation is destructive) and (disposition is loud) then (attack_complexity
17. If (resources is medium) and (motivation is destructive) and (disposition is loud) then (attack_comple
18. If (resources is high) and (motivation is destructive) and (disposition is loud) then (attack_complexity
```

Rule Editor: AttackerProperties3

```
6. If (resources is low) and (motivation is destructive) and (disposition is careful) then (attack_complexity is med
7. If (resources is medium) and (motivation is destructive) and (disposition is careful) then (attack_complexity is
8. If (resources is high) and (motivation is destructive) and (disposition is careful) then (attack_complexity is higl
9. If (resources is low) and (motivation is minor) and (disposition is loud) then (attack_complexity is low)(topolog
10. If (resources is high) and (motivation is minor) and (disposition is loud) then (attack_complexity is high)(topol
11. If (motivation is disruptive) and (disposition is loud) then (topological_relationship is medium)(public_opinion
12. If (resources is medium) and (motivation is disruptive) and (disposition is loud) then (attack_complexity is me
13. If (resources is low) and (motivation is destructive) and (disposition is loud) then (attack_complexity is mediu
14. If (resources is medium) and (motivation is destructive) and (disposition is loud) then (attack_complexity is h
15. If (resources is high) and (motivation is destructive) and (disposition is loud) then (attack_complexity is high)
```

Surface Viewer: AttackerProperties — X (input): resources; Y (input): motivation; Z (output): attack_compl...; X Mesh Points: 15; Y Mesh Points: 15; Ref. Input: [NaN NaN 5]; Plot points: 101; Ready

Surface Viewer: AttackerProperties3 — X (input): resources; Y (input): motivation; Z (output): attack_compl...; X Mesh Points: 15; Y Mesh Points: 15; Ref. Input: [NaN NaN 5]; Plot points: 101; Ready

Fig. 15. Three surfaces and rulesets for Pattern Search, KFold, and Particle Swarm methods for fuzzy inference system building respectively.

They are built with a general input-to-output in mind, and based on the prior fuzzy inference system's distribution, but more optimized. Pattern search creates fewer rules with less accuracy, KFold makes more rules and is more accurate, while particle swarm has a middle ground with the rulesets. From there, the decision is made to continue with the particle swarm, creating a more specific tuning with additional inputs and outputs and the resulting ruleset in Figure 16.

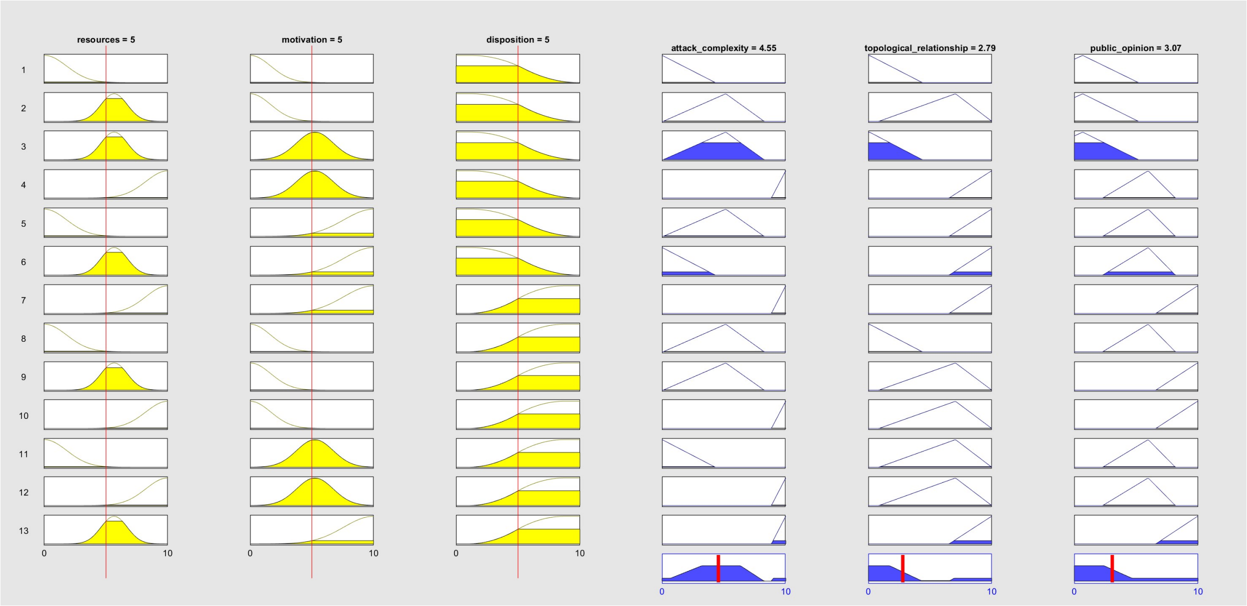


Fig. 16. Particle Swarm ruleset visualized with the new parameters. Used in the most up-to-date version of the code.

To better visualize the results of the fuzzy inference system, graphs are made that map the points from the various inputs of resources, motivation, and disposition to a 3d scatter plot for Security Level (or AC), TL, and C. This will show the distribution for a given fuzzy inference system for a set of inputs, which in this case will be the base ranges for each type of attacker. Since there are three distinct types of attackers, it is possible to put them through a KMeans clustering method and create three clusters for these to determine at which points the attacks can become more damaging. Figure 17 shows this for the base set, as there are three distinct groups that it accurately points out. The less impactful overall is the ordinary attacker group, one more to the topological relationship with less security is the efficient attacker group, and finally, the terror attacker group sits at the top of all three.

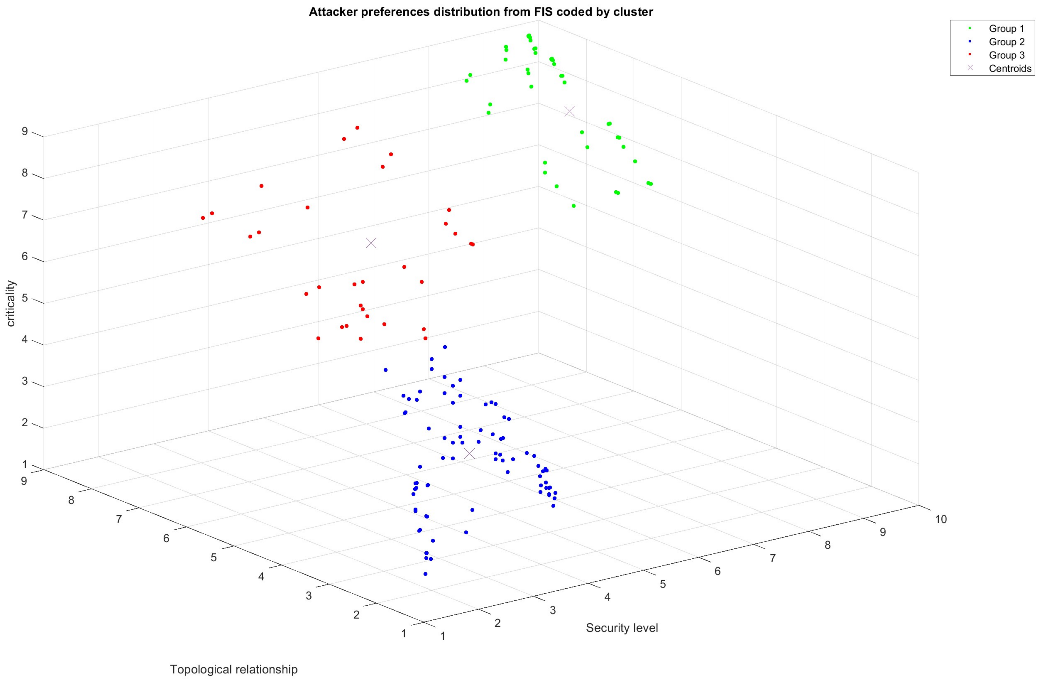


Fig. 17. Fuzzy inference system output visualization on 3d scatter plot. The three groups are colored differently, with an "x" for each centroid.

Using this information, by looking at the nodes and attackers and comparing them to the centroids, one can determine which group a new attack can fit into. This can be applied not just in the base set, but for every combination of the three inputs as whole numbers, leading to a more cohesive graph that also shows the full breadth of the three groups, and not just relying on the three major designations. The best visualization of this is in Figure 18, which performs much of the same results as Figure 17, except with a larger sample size of inputs to outputs. This can be seen as the full mapping of the fuzzy inference system chosen.

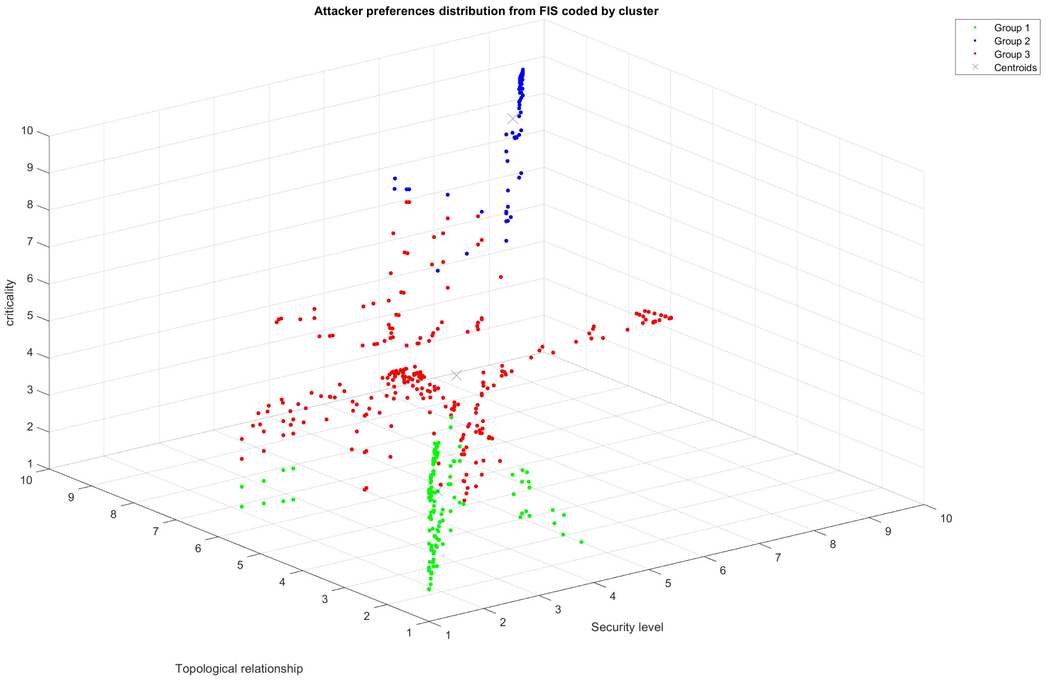


Fig. 18. Fuzzy inference system output of all whole values visualization on 3d scatter plot.

Tests that focus more on the sensitivity of the change in inputs are also performed. This is done by setting 2 of the 3 inputs to the value 5, and then iterating the third value between 1 and 10, creating a sensitivity test. The outputs show a mostly linear relationship for all outputs with a focus on criticality for disposition, while there are dips towards a higher topological relationship for the motivation and resources, as well as criticality. The latter two look more like exponential graphs in comparison. These graphs are included in the appendix. These changes, however, do show the dependence that these outputs have on a singular input, and are a way to ensure that the fuzzy inference system accurately changes the output for each of the inputs.

Next, the process of visualizing the results of the node data can be put into bar charts. This is done by putting Security Level, Topology Relationship, and Criticality on top of each other for each of the 6 smart switches on the grid, and the ratio of each of these regarding their importance, as well as their overall height. The higher the overall height, the more important the node is in the grid to its integrity, due to the previously discussed attributes. Figure 19 shows each of the nodes in their importance on the 3d bar graph, labeled 1-6 along the axis. This will represent the 3 values of the node to be calculated with the attacker preferences, shown in the scatter plot above.

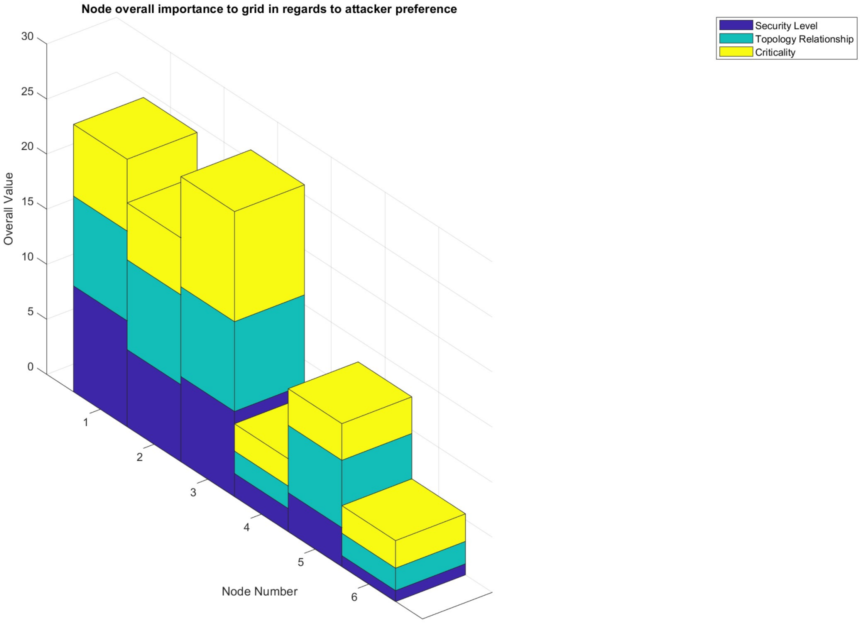


Fig. 19. Bar chart of the overall importance of node to attackers, used for determining residuals.

With these nodes now put together, the residuals can be calculated for different attackers. For example, the residual for a default attack of resource at 5, while motivation and disposition are at 1, is shown graphically in Figure 20. Here, the ideal target for them would be node number

4, as this is an attack with some resources but little motivation for damages, and node 6 would be right after it.

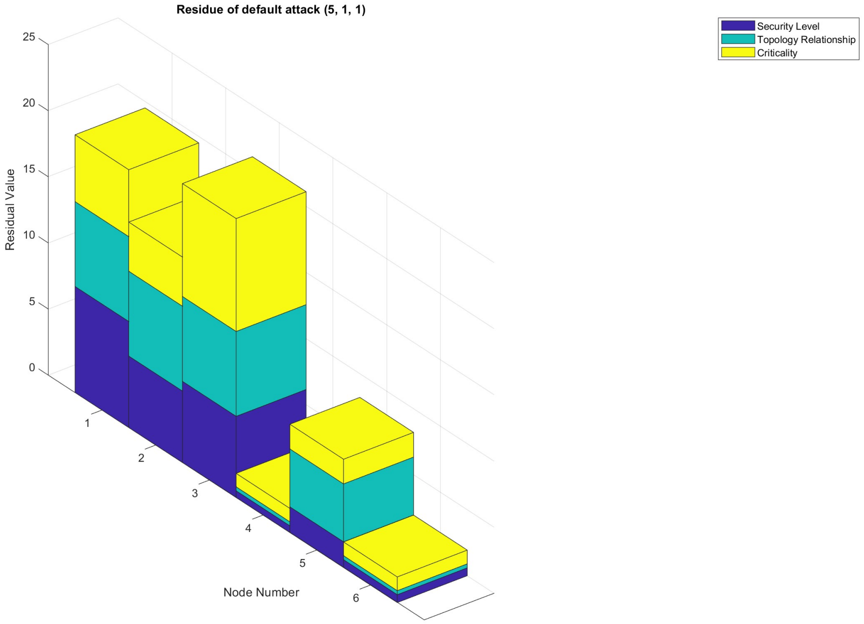


Fig. 20. Bar chart showing the residual values for the default attack, now having many different values for how far apart they are from the attacker’s preferences.

To properly determine if the calibration of target determination is on the right track too, a sensitivity test is done using the residuals. The resources, motivation, and disposition are set to 5, and one value at a time is changed from 1 to 10. They are put through the fuzzy inference system, and the results are the node number results for each of the attacks, shown in Table 3.

Sensitivity test value, all others set to 5	set to 1	Set to 2	Set to 3	Set to 4	Set to 5	Set to 6	Set to 7	Set to 8	Set to 9	Set to 10
Resources changing node target	5	5	5	5	4	4	5	2	1	1
Motivation changing node target	5	5	5	4	4	5	5	5	2	2
Disposition changing node target	4	4	4	4	4	5	5	5	2	2

Table 3. Node decisions for a sensitivity test.

What can be determined from these tests is that the choice in the node that would be attacked will vary depending on the inputs, which is based on the fuzzy inference system. So, the more accurate the fuzzy inference system is, the more accurate the determinations will be. The fuzzy inference system determines intentions from input to output and, in this case, simulates the attacker making their choices for targets.

Section 5.3: Final Test Application

For the final test with the cyber layer included now in the IEEE 13-node system, the attacks are revisited with the new algorithm put in place. With some adjustments, the code worked with it where the attacker would read the values from the OPC, and then write attacks based on it. Keeping with the idea of using malicious commands for these attacks, all of them would cause some degree of oscillation and damage, as shown in Figure 21. With low motivation on the attack, the generation is mostly fine after it, and the generators remain stable. These values are readily seen based on the outputs in Figure 22, describing the power flow, current flow, and status of breakers at each point. These are, as part of the code, exported to an Excel spreadsheet for viewing at consistent points in the code, resulting in lines of values that are easily readable. This will provide perfect training data, as it is simply data in its purest form. Finally, Table 4 also contains the residuals from the attack, having determined the goal node first and then which nodes to attack first based on distance and information. The residuals are calculated from the fuzzy inference system outputs from the attack, subtracted from the node's characteristics, and then multiplied by the distance over knowledge. The distance matrix is calculated here based on the difference of lines between each of the breakers, which is small in some cases. This is further compounded by the fact that the algorithm works on multiple kinds of systems as intended, meaning that the modular nature will be usable on any power grid, so long as enough information is known about it.

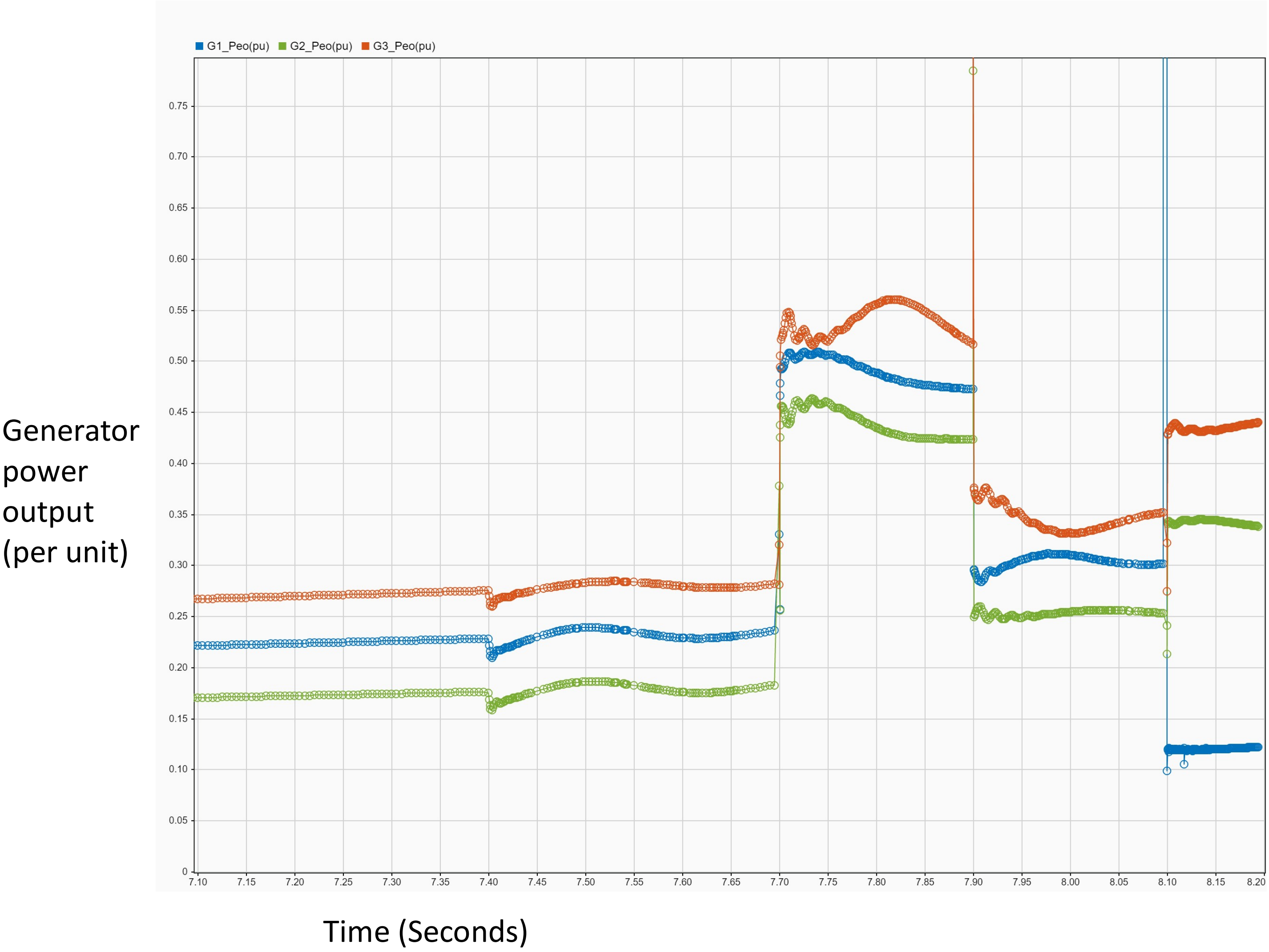
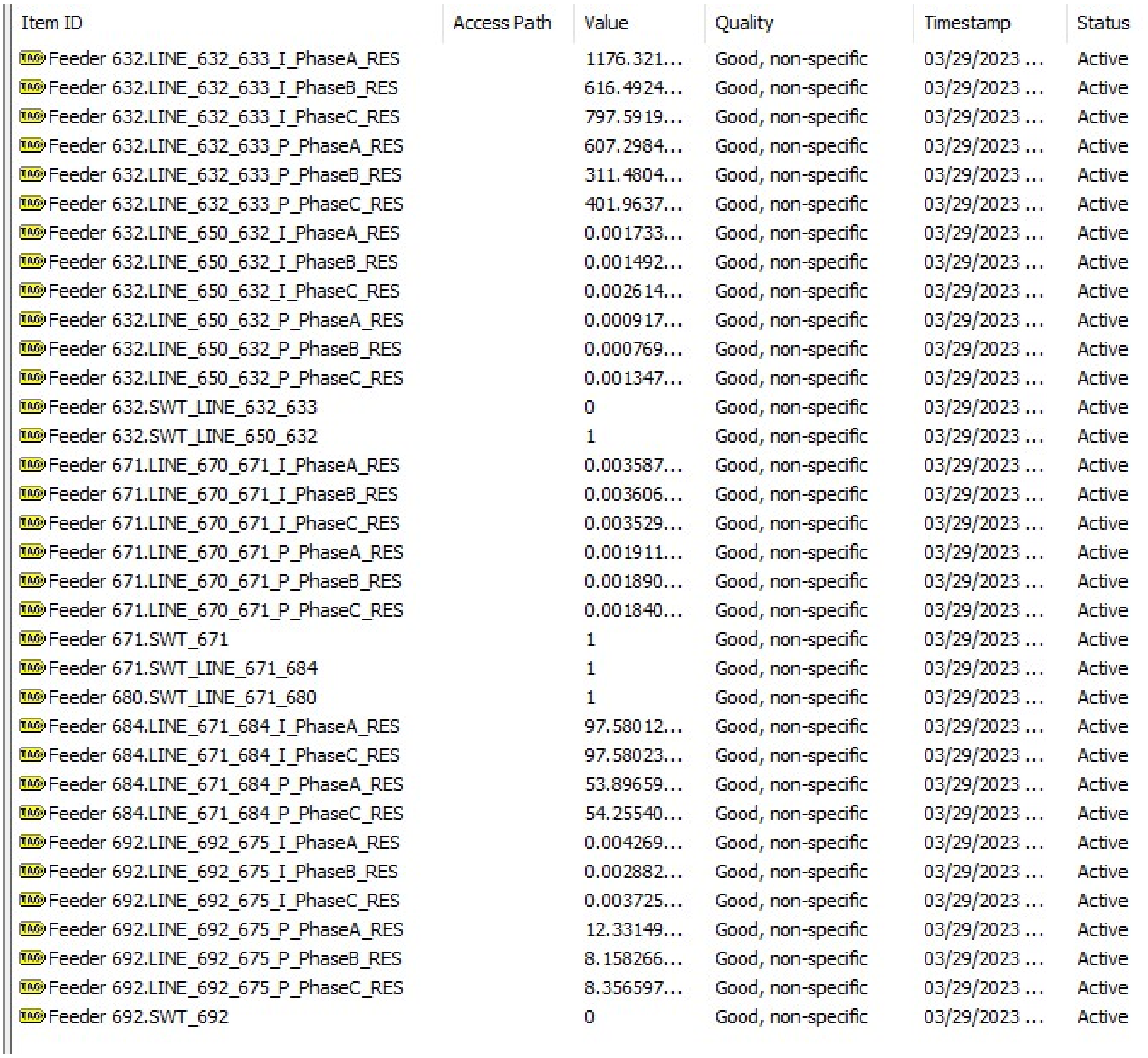


Fig. 21. Graphical result of a 5, 1, 1 default attack, where the new algorithm is used.



Item ID	Access Path	Value	Quality	Timestamp	Status
Feeder 632.LINE_632_633_I_PhaseA_RES		1176.321...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_632_633_I_PhaseB_RES		616.4924...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_632_633_I_PhaseC_RES		797.5919...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_632_633_P_PhaseA_RES		607.2984...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_632_633_P_PhaseB_RES		311.4804...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_632_633_P_PhaseC_RES		401.9637...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_650_632_I_PhaseA_RES		0.001733...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_650_632_I_PhaseB_RES		0.001492...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_650_632_I_PhaseC_RES		0.002614...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_650_632_P_PhaseA_RES		0.000917...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_650_632_P_PhaseB_RES		0.000769...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.LINE_650_632_P_PhaseC_RES		0.001347...	Good, non-specific	03/29/2023 ...	Active
Feeder 632.SWT_LINE_632_633		0	Good, non-specific	03/29/2023 ...	Active
Feeder 632.SWT_LINE_650_632		1	Good, non-specific	03/29/2023 ...	Active
Feeder 671.LINE_670_671_I_PhaseA_RES		0.003587...	Good, non-specific	03/29/2023 ...	Active
Feeder 671.LINE_670_671_I_PhaseB_RES		0.003606...	Good, non-specific	03/29/2023 ...	Active
Feeder 671.LINE_670_671_I_PhaseC_RES		0.003529...	Good, non-specific	03/29/2023 ...	Active
Feeder 671.LINE_670_671_P_PhaseA_RES		0.001911...	Good, non-specific	03/29/2023 ...	Active
Feeder 671.LINE_670_671_P_PhaseB_RES		0.001890...	Good, non-specific	03/29/2023 ...	Active
Feeder 671.LINE_670_671_P_PhaseC_RES		0.001840...	Good, non-specific	03/29/2023 ...	Active
Feeder 671.SWT_671		1	Good, non-specific	03/29/2023 ...	Active
Feeder 671.SWT_LINE_671_684		1	Good, non-specific	03/29/2023 ...	Active
Feeder 680.SWT_LINE_671_680		1	Good, non-specific	03/29/2023 ...	Active
Feeder 684.LINE_671_684_I_PhaseA_RES		97.58012...	Good, non-specific	03/29/2023 ...	Active
Feeder 684.LINE_671_684_I_PhaseC_RES		97.58023...	Good, non-specific	03/29/2023 ...	Active
Feeder 684.LINE_671_684_P_PhaseA_RES		53.89659...	Good, non-specific	03/29/2023 ...	Active
Feeder 684.LINE_671_684_P_PhaseC_RES		54.25540...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.LINE_692_675_I_PhaseA_RES		0.004269...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.LINE_692_675_I_PhaseB_RES		0.002882...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.LINE_692_675_I_PhaseC_RES		0.003725...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.LINE_692_675_P_PhaseA_RES		12.33149...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.LINE_692_675_P_PhaseB_RES		8.158266...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.LINE_692_675_P_PhaseC_RES		8.356597...	Good, non-specific	03/29/2023 ...	Active
Feeder 692.SWT_692		0	Good, non-specific	03/29/2023 ...	Active

Fig. 22. OPC layer values from the attack are applied.

Residual value	1.96	1.20	2.28	2.59	5.34
Node Number	3	4	5	2	1

Table 4. Residuals from the default attack with knowledge applied, sorted with node 1 as the target.

Additional tests are included in the appendix to cover the different situations regarding inputs, and adjustments to the other input values aside from the 3 for the fuzzy inference system. Regardless, however, there are plenty of tests to be performed for various given situations here, and there is the potential to understand the influences of numerous factors of the attacker on how the system will be attacked. The result is to verify that the attacker's characteristics will influence the attack that is performed.

SECTION 6: DISCUSSION

Section 6.1: Initial Thoughts

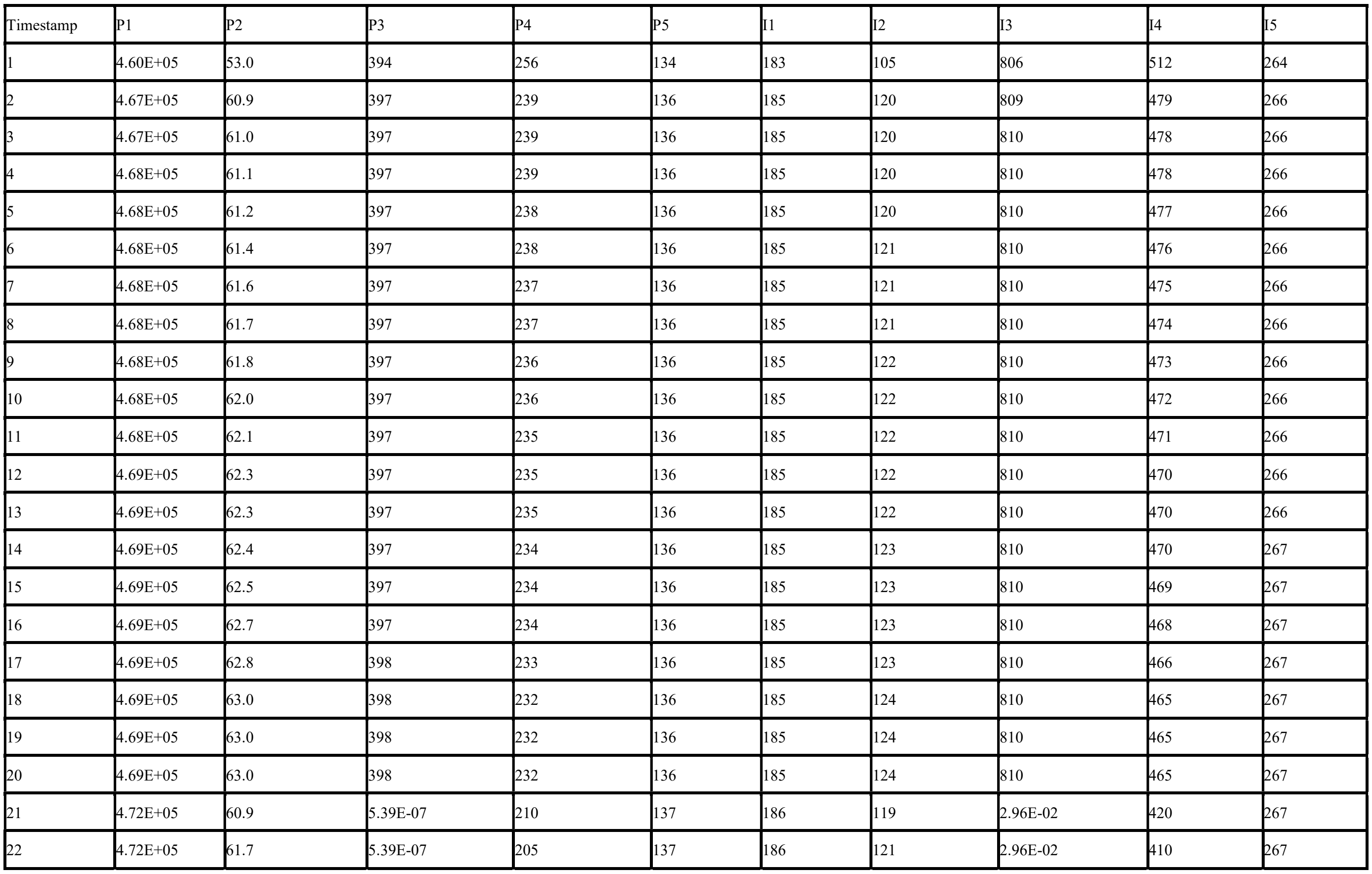
Regarding the first portion of the IEEE 13-node system, the linear system is not a very robust method for decision-making. It conveys the initial idea, but only using 2 vague values of α and β would not be helpful for reverse engineering the attacker and determining their intentions. Probability as a basis would also lead to similar issues of uncertainty regarding who is attacking and where they will strike next. The concepts from the initial tests remain that an algorithm can make decisions based on the cyber layer on the physical layer. Many kinds of attacks can be modeled and executed onto a range of systems, to serve as testing data for a real attacker. Of course, most of this can be seen via the output table for specific spots that can be read from, but if an attack can be seen based on the change in data and then reverse-engineered, it would be a great step up for AI to learn about this. This first portion's results serve as a basis to improve upon the attacker's decision model for higher accuracy.

Based on the results and how heavily they are altered in various iterations, the fuzzy inference system serves as the heart of the decision model. Since it is reasonable to model an attacker on a range for their various properties, with a proper fuzzy inference system one can accurately model which node would be attacked through the method of comparison. However, because of the nature of optimizing a fuzzy inference system, it can lead to inaccuracies. Without proper tuning, some of the variables will not do anything in a sensitivity test, leading to some cases of redundancy when each of the inputs is distinct and separate. As more data that would be accurate to the activities of attackers is input, the fuzzy inference system can be further tuned to be more accurate.

Section 6.2: Benefits of the System

As mentioned previously, this code is highly modular because most of it had to deal with the analysis of the nodes as individuals and their connections to each other, not relying on a specific part of the power grid that works as a point. Therefore, small or large grids can be considered as is done with the IEEE 123-node distribution system or the 13-node network. While one had much more distance and larger scope, able to handle several more switches to choose from for an attacker, the smaller grid is just as easily made with adjustments. However, the numbers for knowledge would have to be altered slightly to account for the smaller distances. Regardless, this system allows for most of the nodes to be chosen based on data used to create a node system to compare to the fuzzy inference system. While there are adjustments to be made for the fuzzy inference system based on the data, it will retain its ability to predict based on attacking characteristics. This variability can also be related to the attackers' actual attacks. Indeed, it is important to note that the original project's attacks have a variable type of attack. Also, if more types of attacks are added, it can further modulate the strategies that can be employed.

Of the major types of attacks that are used, there are clear differences. For the default attack, while it has resources but not as much motivation for causing damages, it attacked 3 breakers and caused some oscillations, but the power system is able to stabilize. However, when looking at attacks with higher motivations, the long-term effects became much more apparent as the generators are quickly becoming unstable from these attacks. In the appendix, it is shown that for the efficient attack and the worst-case scenarios (3, 7, 3, and 8, 8, 8) they had quickly destabilized the system, more obviously so for the latter but the former had a promising idea of where to hit. The implementation of authority also helped to make it much quicker as the attacks would be back to back, therefore increasing the overall effect on the system. Note that 1 authority means that the first attack will occur sooner, while 2 will allow for the first two targets to be compromised within seconds of each other. The skill also would be a determining factor for how long it takes. However, the actual change in time is hard to determine due to the calculations for the grid taking longer as the attacks occurred. This is more of an error in computing power compared to anything else in the code, however. Knowledge being increased also affects the residuals as expected, where closer nodes would become more susceptible. As a result, they end up becoming potentially better targets than the goal in terms of residuals because of this. Because the 13-node system is a smaller system overall with closer points to each other, it results in the knowledge basis having to be smaller as a result. Regardless, the attacks are distinct enough from each other in terms of the order of operations, as a result, the fuzzy inference system works well to make determinations and, most importantly, can model potential avenues for dangerous attacks or efficient attacks. Since each value has a different impact on the attack and each attack has a great variation of what will happen, it serves as a good testbed at this point. Note, that the values can be exported to a table for analysis or viewed on a graph, as shown in Table 5. However, the three major inputs for the DSK-RAMG model, those being resources motivation and disposition, are the main point to use for this. They determine the target and the corresponding attack path.



Timestamp	P1	P2	P3	P4	P5	I1	I2	I3	I4	I5
1	4.60E+05	53.0	394	256	134	183	105	806	512	264
2	4.67E+05	60.9	397	239	136	185	120	809	479	266
3	4.67E+05	61.0	397	239	136	185	120	810	478	266
4	4.68E+05	61.1	397	239	136	185	120	810	478	266
5	4.68E+05	61.2	397	238	136	185	120	810	477	266
6	4.68E+05	61.4	397	238	136	185	121	810	476	266
7	4.68E+05	61.6	397	237	136	185	121	810	475	266
8	4.68E+05	61.7	397	237	136	185	121	810	474	266
9	4.68E+05	61.8	397	236	136	185	122	810	473	266
10	4.68E+05	62.0	397	236	136	185	122	810	472	266
11	4.68E+05	62.1	397	235	136	185	122	810	471	266
12	4.69E+05	62.3	397	235	136	185	122	810	470	266
13	4.69E+05	62.3	397	235	136	185	122	810	470	266
14	4.69E+05	62.4	397	234	136	185	123	810	470	267
15	4.69E+05	62.5	397	234	136	185	123	810	469	267
16	4.69E+05	62.7	397	234	136	185	123	810	468	267
17	4.69E+05	62.8	398	233	136	185	123	810	466	267
18	4.69E+05	63.0	398	232	136	185	124	810	465	267
19	4.69E+05	63.0	398	232	136	185	124	810	465	267
20	4.69E+05	63.0	398	232	136	185	124	810	465	267
21	4.72E+05	60.9	5.39E-07	210	137	186	119	2.96E-02	420	267
22	4.72E+05	61.7	5.39E-07	205	137	186	121	2.96E-02	410	267

Table 5. Example of attack output values from (5, 1, 1) attack, values that can be read by AI for training data. Labelled from nodes 1-5 power and current.

While the three inputs of the DSK-RAMG variables are the most important, the other three still hold an important sway based on their influence on the equation. Authority and skills are both usable regarding the speed at which the attack occurs, which can determine the worst-case scenario and how quickly a response is necessary in some cases, or what happens if the attacker does have insider information and can enact a part of their plan instantaneously. Knowledge holds a similar influence on the decision side of it. It can decide how far of a reach the attacker holds and, in this case, will heavily change which nodes are attacked for each attacker. While some nodes are like the attacker's preferences, they could be enough of a distance away that it would not be worth it to reach that far away, unless abundant resources are invested into the attack.

Section 6.3: Summary of Findings

In general, the inclusion of different properties has vastly improved the model for attacker prediction. Originally, there are only two variables vaguely based on probabilities that were not going to be too effective, as the chances of something happening are not concrete. However, the inclusion of the model for attacker properties to determine what is the ideal place to go to is something that can be more readily based upon for decision-making and training. The fuzzy inference system can be updated as needed, and with enough research, the ruleset can be brought as close to the values of how attackers behave as possible. From there, it would be simple to look at the attacks and then make countermeasures from them by running the fuzzy inference system in reverse and determining the next move. Computers are particularly good at that, and while there are several different values to consider, they can run those possibilities based on the inputs well, with enough training and heuristics to investigate. Overall, however, this is a much better model that incorporates criminology into the subject quite well. It also allows the users to determine the severity of the attack and where the attack paths might lead quickly. The usage of fuzzy logic, therefore, is integral to the overall work and the advancement of attack determination. By using this, an algorithm has a much better chance to determine what kind of attack is being mounted, and then from there can strengthen the defense in critical locations if they know where they are going to strike next.

SECTION 7: CONCLUSION

In conclusion, the overall work in this thesis is to make a better testing platform for future work on cybersecurity for the power grid, allowing for more accurate modeling for attacks based on severity and attacker characteristics. Using fuzzy inference systems, a more fundamental usage of criminology allows for the possibility to determine what kind of attacker is making actions against the power grid and to determine what actions can be taken. The result is a process of taking the seven characteristics of an attacker and determining their ideal primary targets and the attack path from there. As it puts the attacks in order, it exports the statistics from the grid as they go through it so artificial intelligence can read it for training data, intended for creating a good environment for these tests to occur. Due to its modular nature, the algorithm can be applied to any power grid in general.

There are weaknesses to note about the proposed method. Despite the current improvements regarding character attributes, there still needs to be more work on the fuzzy inference system as it is critical to the work overall. The issue that required the usage of fuzzy inference systems remains, that getting data for specific attacks is a difficult conundrum that would require information from real sources and will usually be in the specific circumstance of that power grid. Fortunately, the algorithm can be applied to various grids to compensate for this, and with further tuning, it can work to the greatest accuracy. The fuzzy inference system provides a good basis for a few types of attackers and their general trends based on the logic and understanding of what would be good for an attacker. It is important to add that, the input to output is only as good as the system is made. Furthermore, there should be expansions upon the basis for deciding the importance of nodes. At the current moment, it mostly relies on power flow and things related to power flow, leading to them each having a linear relationship with each other. More testing should be done on that specific portion to ensure it is improved upon or to use a different method for measuring each. Finally, it is possible to analyze more attacks and relate the intentions of the attacker to them. Overall, for the future work, there should be some method to ensure that the attacker algorithm is as close to actual attackers as possible.

Future work should also focus on the improvement of the fuzzy inference system using real data to improve the model and make it more accurate overall, which will help reduce the limitations that are presented previously. As it is critical to have an accurate and optimal fuzzy inference system, it is the major step to improve the work further. However, it will require extensive research into the attacks to obtain data that would be difficult to acquire. Additionally, the development of artificial intelligence to read and act upon this data would also be effective to complete the entire system. While it can be done with any computer that can read the information readily, there is a need to know how to translate the information into decisions. Overall, this project is based on predicting attackers based on their properties, and due to human nature, it must define them in specific variables and ranges for them. Most future work will be to improve upon the current state, with improved models but still holding a fuzzy inference system basis.

REFERENCES

[1] J. E. Chadwick, "How a smarter grid could have prevented the 2003 U.S. cascading blackout," *2013 IEEE Power and Energy Conference at Illinois (PECI)*, Urbana, IL, USA, 2013, pp. 65-71, doi: 10.1109/PECI.2013.6506036.

[2] C. C. Sun, A. Hahn, and C. C. Liu, “Cyber security of a power grid: State-of-the-art”, International Journal of Electrical Power & Energy Systems, Volume 99, 2018, 45-56, ISSN 0142-0615, https://doi.org/10.1016/j.ijepes.2017.12.020.

[3] A. Shehod, “Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity implications of smart grid advancements in the US,” Working Paper CISL# 2016-22, December 2016, Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Room E62-422, Massachusetts Institute of Technology, Cambridge, MA

[4] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, “Cybersecurity in power grids: Challenges and opportunities,” *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021, doi: 10.3390/s21186225.

[5] I. Semertzis, V. S. Rajkumar, A. Ştefanov, F. Fransen and P. Palensky, "Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs," *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Milan, Italy, 2022, pp. 1-6, doi: 10.1109/MSCPES55116.2022.9770140.

[6] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[7] A. Prakash, M. Satish, T. S. Bhargav, and N. Bhalaji, “Detection and mitigation of denial of service attacks using stratified architecture,” *Procedia Computer Science*, vol. 87, pp. 275–280, 2016.

[8] J. Hong, Y. Chen, C.-C. Liu, and M. Govindarasu, “Cyber-physical security testbed for substations in a power grid,” *Cyber Physical Systems Approach to Smart Electric Power Grid*, pp. 261–301, 2015.

[9] A. Stefanov, C.-C. Liu, M. Govindarasu, and S.-S. Wu, “SCADA modeling for performance and Vulnerability Assessment of integrated cyber-physical systems,” *International Transactions on Electrical Energy Systems*, vol. 25, no. 3, pp. 498–519, 2013.

[10] S. Ahmad *et al.*, "Advanced Persistent Threat (APT)-style attack modeling and testbed for power transformer diagnosis system in a substation," *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2022, pp. 1-5, doi: 10.1109/ISGT50606.2022.9817518.

[11] C.-W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[12] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, “Review and insight on the behavioral aspects of cybersecurity,” *Cybersecurity*, vol. 3, no. 1, 2020.

[13] X. Peng and H. Zhao, “A framework of attacker centric cyber attack behavior analysis,” *2007 IEEE International Conference on Communications*, 2007.

[14] D. Maimon, O. Babko-Malaya, R. Cathey, and S. Hinton, “Re-thinking online offenders’ SKRAM: Individual traits and situational motivations as additional risk factors for predicting cyber attacks,” *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, 2017.

[15] B. Chen, Z. Yang, Y. Zhang, Y. Chen, and J. Zhao, “Risk assessment of cyber attacks on power grids considering the characteristics of attack behaviors,” *IEEE Access*, vol. 8, pp. 148331–148344, 2020.

[16] B. Dupont and C. Whelan, “Enhancing relationships between criminology and Cybersecurity,” *Journal of Criminology*, vol. 54, no. 1, pp. 76–92, 2021.

[17] A. Bilen and A. B. Özer, “Cyber-attack method and perpetrator prediction using machine learning algorithms,” *PeerJ Computer Science*, vol. 7, 2021.

[18] Graham Dudgeon (2023). Distribution System Model in Simscape: 123 Node Test Feeder (https://www.mathworks.com/matlabcentral/fileexchange/66599-distribution-system-model-in-simscape-123-node-test-feeder), MATLAB Central File Exchange. Retrieved January 30, 2023.

APPENDIX A: Additional Data

Most of this appendix will focus on the additional results from various tests. This starts with the sensitivity tests and goes on to the cyber-physical system tests. Additionally, there is the list of nodes in the tests. The order of the nodes in the IEEE 13-Node system is 692, 671_684, 632_633, 650_632, and 670_671. For the IEEE 123-Node system, the order of nodes is 13_152, 18_135, 60_160, 60_61, 97_197, and 149_1.

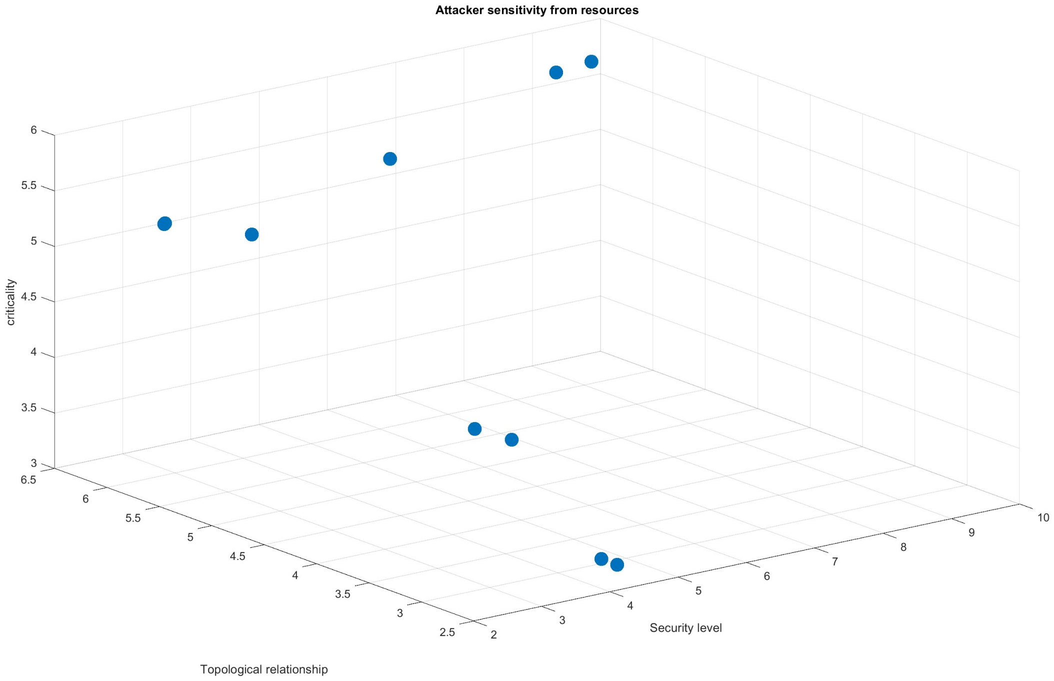


Fig. 23. Attacker sensitivity from resources.

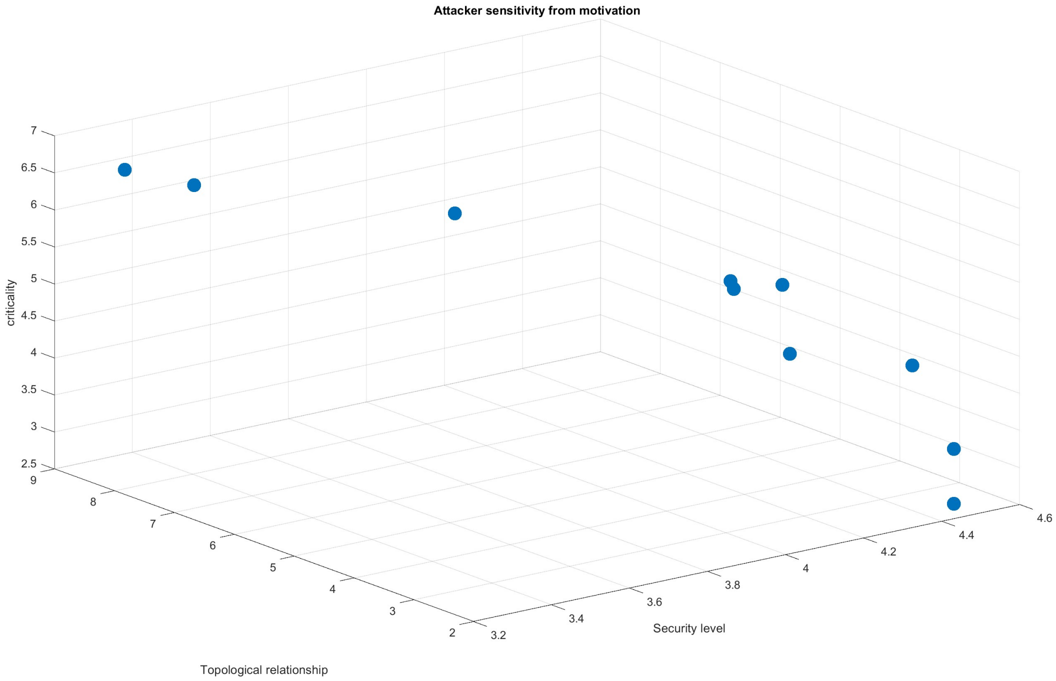


Fig. 24. Attack sensitivity from motivation.

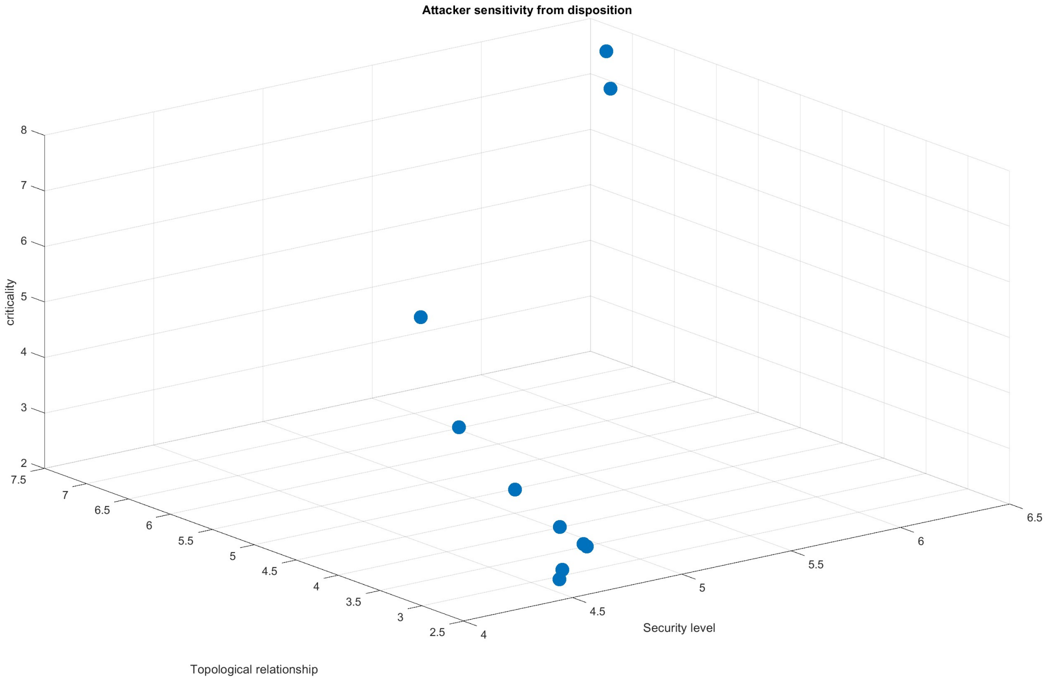


Fig. 25. Attack sensitivity from disposition.

The three types of attacks involved and their inputs are used to create the three sensitivity graphs, as it goes through a loop of resources, motivation, then disposition increasing. These also dictate the value ranges used.

- Efficient attacks: motivated parties that have notable resources, but not too many, with the skill and interest that coincides with the attacker. In fuzzy logic from 1-10, they have resources from 3-6, motivation from 3-6, and disposition will typically be careful, 1 - 5. Their goal is to look for areas with high topology and low security.
- Ordinary attacks: They are singular people who just want to test code or gain notoriety. All values, therefore, are low, from 1-3 for resources, motivation, and disposition. They are low on resources, do not want to cause trouble, and do not want to be caught.
- Terror attacks: The worst case scenario, where every value is high, from 7 - 10 for resources and motivation, and 5 - 10 for disposition. They are not only intending to fully attack the grid but are willing to do so in more obvious ways, less willing to cover their tracks. They will also typically have high knowledge as it has been planned for some time, and potentially more authority involved.

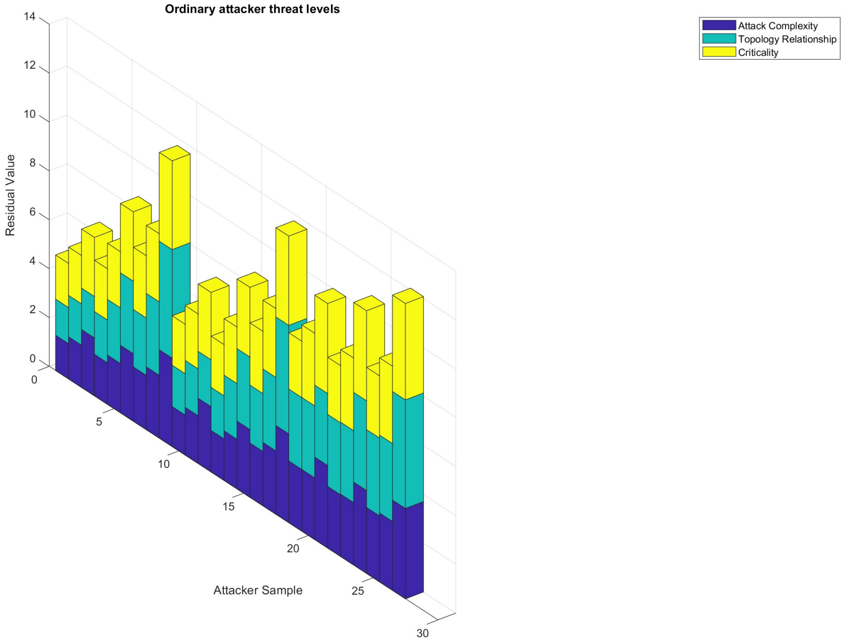


Fig. 26. Values for AC, TR, and PO for ordinary attackers.

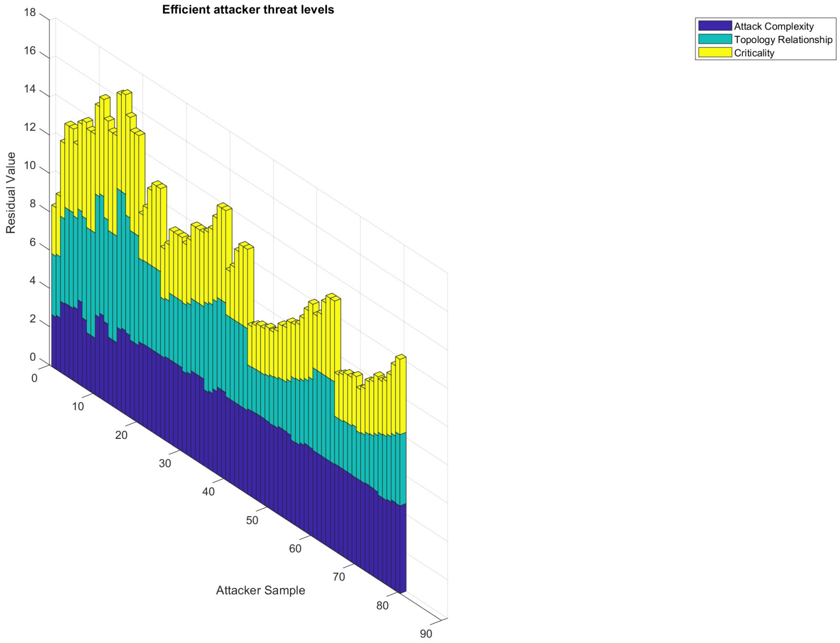


Fig. 27. Values for AC, TR, and PO for efficient attackers.

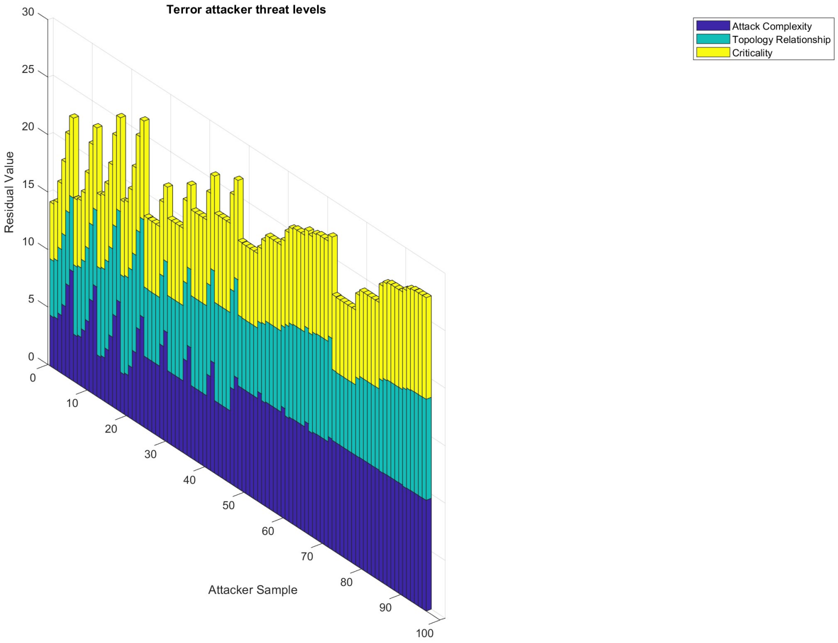


Fig. 28. Values for AC, TR, and PO for terror attackers.

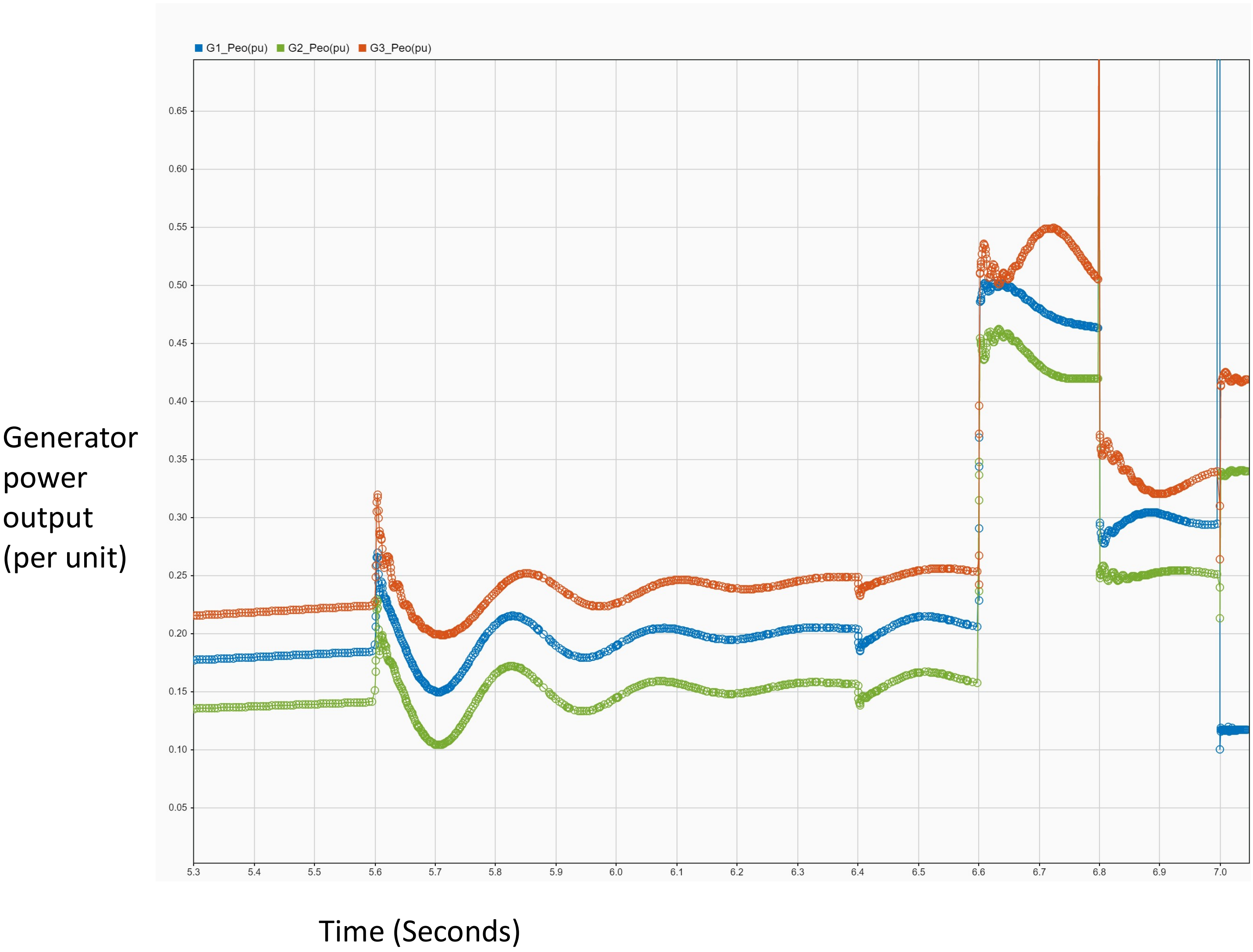


Fig. 29. 5, 5, 5 attacks, knowledge = 1, skill = 5, authority = 0.

Residual	0.512	0.986	0.999	1.316	4.361
Node number	3	4	5	2	1

Table 6. Residual from above attacks sorted.

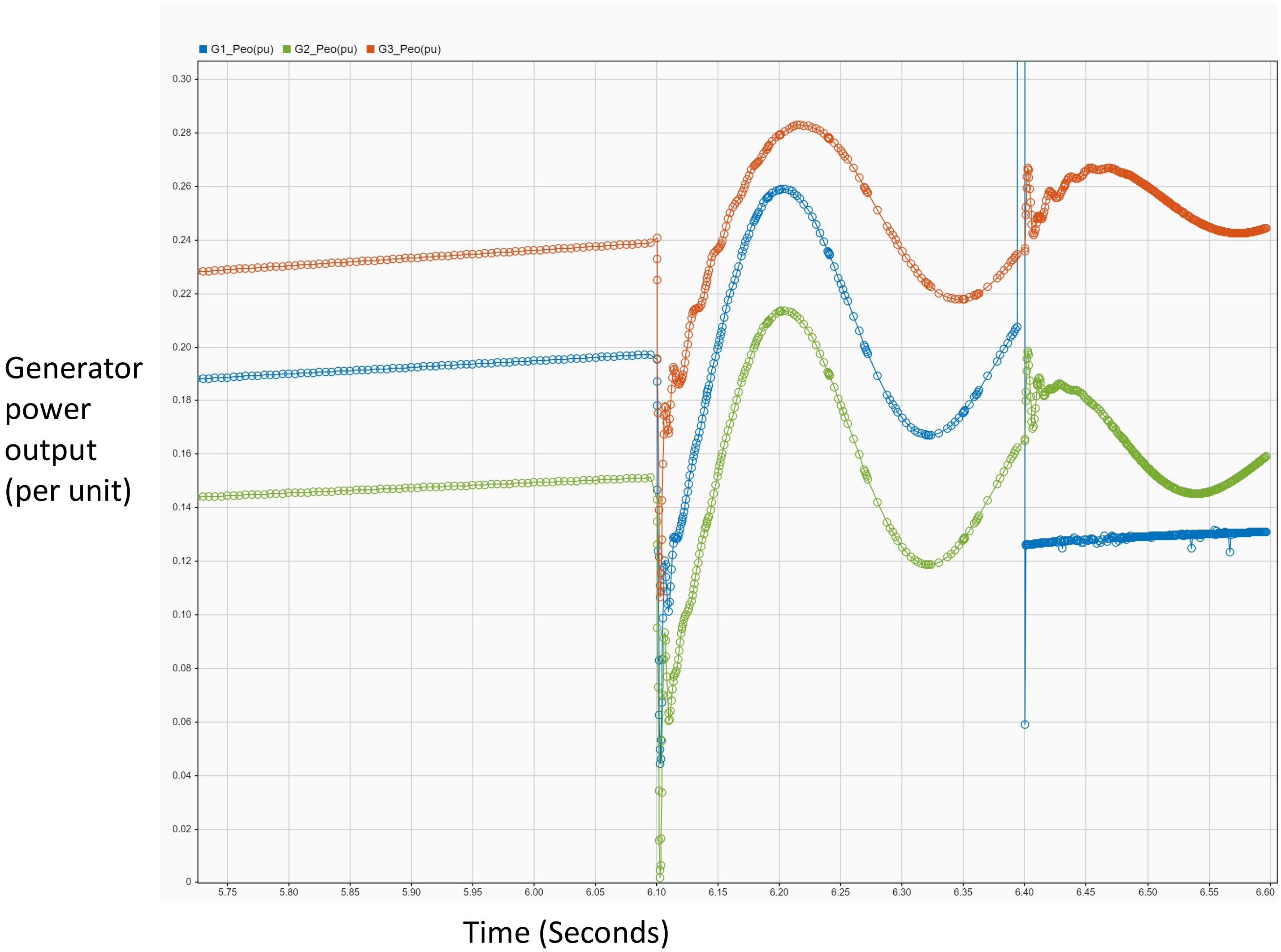


Fig. 30. 3, 7, 3, authority = 2, skill = 7, knowledge = 1.

Residual	1.981	2.156	2.279	2.474	4.370
Node number	3	5	4	2	1

Table 7. Above attack, attacked 4, 5, then 3. 2 had too much security to attack.

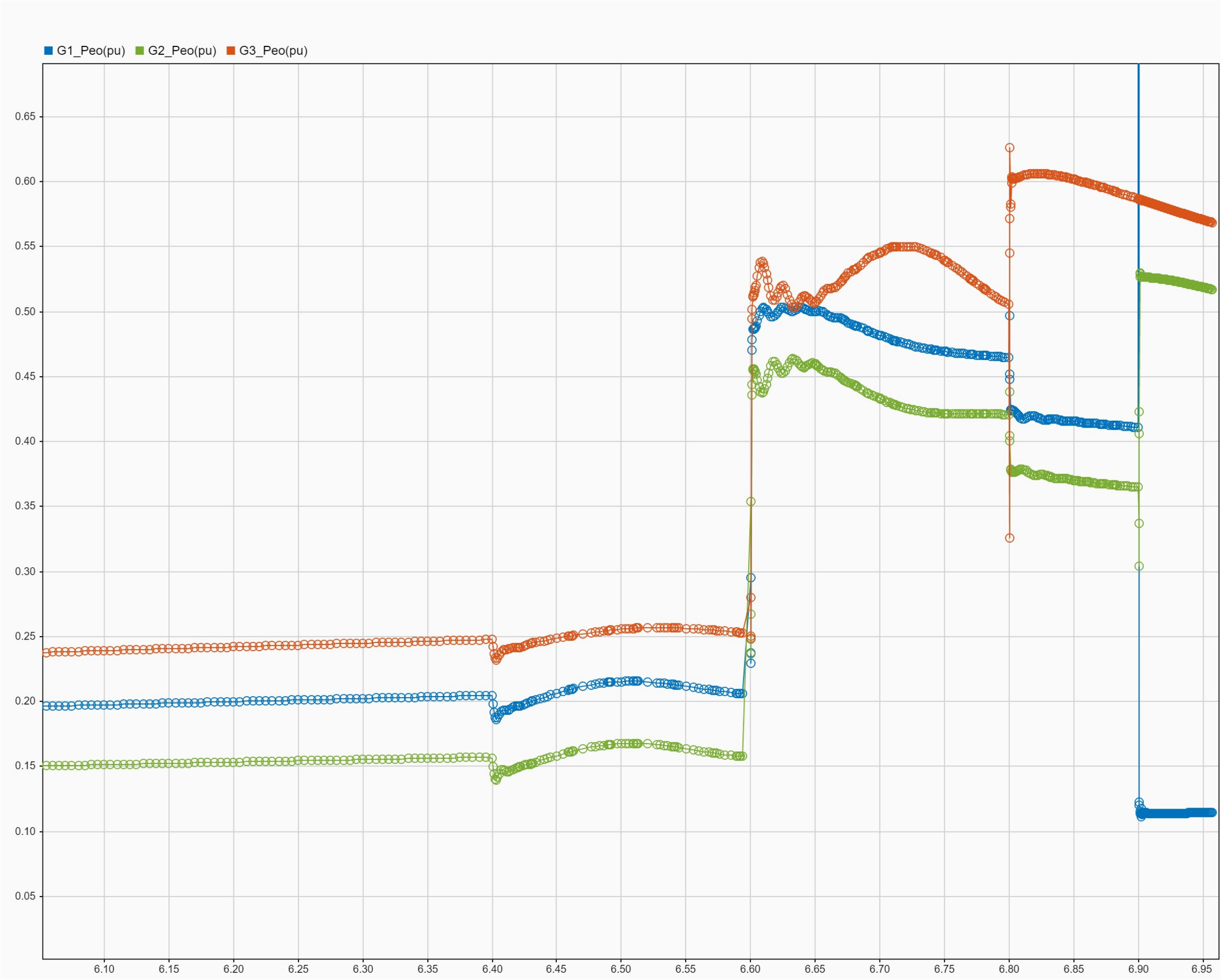


Fig. 31. 8, 8, 8, authority = 0, knowledge = 2, skill = 5.

Residual	3.052	1.784	3.356	3.445	3.763
Node number	3	4	1	5	2

Table 8. Residual from above attacks sorted.