

CYBER THREAT PROPAGATION MODELING IN CYBER PHYSICAL SYSTEMS

A Dissertation
Presented to
The Academic Faculty

by

Yu-Cheng Chen

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
May 2022

COPYRIGHT © YU-CHENG CHEN 2022

CYBER THREAT PROPAGATION MODELING IN CYBER PHYSICAL SYSTEMS

Approved by:

Dr. Vincent Mooney, Advisor
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Dr. Daniel Molzahn
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Dr. Santiago Grijalva, Co-advisor
School of Electrical and Computer
Engineering
Georgia Institute of Technology

Dr. Chelsea White
School of Industrial and Systems
Engineering
Georgia Institute of Technology

Dr. Lee Lerner
Georgia Tech Research Institute
Georgia Institute of Technology

Dr. Brandon Eames
Sandia National Laboratory

Date Approved: [April 14, 2022]

To my beloved parents,

Tuo-Ju and Jyh-Chern

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation to my advisor, Prof. Vincent J. Mooney III, for without his guidance and persistent help, this dissertation would have not been possible. I would also like to thank my coadvisor, Prof. Santiago Grijalva, for his encouragement, guidance and support especially in the early stages of my Ph.D. studies. Thank you both for your forthcoming novel ideas and suggestions and for providing me with your support and patience throughout my research.

Besides my advisor and co-advisor, I would also like to thank my Ph.D. dissertation committee members, Prof. Daniel Molzahn, Dr. Lee Lerner, Dr. Chelsea White, and Dr. Brandon Eames for their valuable suggestions and insightful comments.

I am also grateful for the Graduate Teaching Assistantship positions provided by the School of Electrical and Computer Engineering at the Georgia Institute of Technology. Without this source of financial support, I would have not been able to complete my research work and pursue my Ph.D. degree. I would also like to extend my thanks to the Sandia National Laboratories and the Department of Energy, which provided financial support towards my Ph.D degree.

Last but not least, I could not express how grateful I am to my parents, Jyh-Chern and Tuo-Ju, to whom I am forever indebted. Finally, I would like to thank my family, my friends and all those who contributed in any shape or form to the success of this work.

It is because of all these amazing people that I am here today. To all of you, I say, thank you!

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF SYMBOLS AND ABBREVIATIONS	xii
SUMMARY	xiii
CHAPTER 1. Introduction	1
1.1 Problem Statement	1
1.2 Terminology	3
1.2.1 Attack Graph Semantics	3
1.2.2 Basics Definitions In Probability Theory	5
1.2.3 Basic Definitions in Game Theory	7
1.3 Research Overview	10
1.4 Dissertation Organization	11
CHAPTER 2. Background	13
2.1 FlipIt	13
2.2 Probabilistic Learning Attacker, Dynamic Defender (PLADD)	14
2.3 Markov Chain	15
2.4 Attack Scenarios	18
2.4.1 Bad Data Injections Attack Scenario	18
2.4.2 Bad Data Detection	19
2.4.3 Single-Layer Parallel PLADD System Attack Scenarios	20
2.4.4 Hierarchical Parallel PLADD System Attack Scenarios	22

2.5	Risk Assessment in Cyber-Physical Systems	25
	CHAPTER 3. Attack Propagation Model for Cyber-Physical System	27
3.1	Components of Hybrid Attack Model	27
3.1.1	PLADD Modeling Bad Data Injection Attack in Power Grid	27
3.2	Attack Propagation In Power Delivery Systems	28
3.2.1	Motivation	28
3.2.2	Attack Propagation Model	29
3.2.3	Simulation Results	34
3.3	Attack Model Leveraging PLADD and Markov Chain Characteristics	37
3.3.1	Introduction	37
3.3.2	Hybrid Attack Model	37
3.3.3	Experimental Results	41
3.3.4	Discussion	44
	CHAPTER 4. Mathematical ANalysis of Parallel PLADD System	47
4.1	Introduction	47
4.2	Mathematical Model Basics	47
4.2.1	Notation and Definitions	48
4.2.2	Single PLADD Game	49
4.3	Overview of Major Theorems	52
4.3.1	Single-Layer Parallel PLADD System	52
4.3.2	Hierarchical parallel PLADD System	54
4.4	Mathematical Model in Detail	57
4.4.1	Single PLADD Game	57

4.4.2	Parallel PLADD System	73
4.5	Simulation Results	77
4.5.1	Single-Layer PLADD Simulation	80
4.5.2	Hierarchical PLADD Simulation	82
4.6	Discussion	84
CHAPTER 5.	Attack Model Driven Mitigation Strategies	86
5.1	Risk Assessment	86
5.2	4-bus Risk Assessment	88
5.2.1	Experiment Results	91
5.3	39-bus Risk Assessment	99
5.3.1	Experiment Results	101
5.4	Sensitivity Analysis	102
CHAPTER 6.	Conclusions	106
REFERENCES		108

LIST OF TABLES

Table 1	Mapping of attacker's tasks to each node.	18
Table 2	Notation and definition.	48
Table 3	PLADD parameters and attacker's expected probability of success in AND configuration for Testcases 1, 2, and 3.	53
Table 4	PLADD parameters and attacker's expected probability of success in OR configuration for Testcases 1, 2, and 3.	54
Table 5	PLADD parameters and attacker's expected probability of success in AND configuration for testcases 1 – 4.	54
Table 6	PLADD parameters and attacker's expected probability of success in AND configuration for testcases 1 – 4.	56
Table 7	Simulation of attacker's expected probability of success.	78
Table 8	Hierarchical PLADD simulation of attacker's expected probability of success, where the period of the defender's take move (τ) is 90 days and the attacker's mean-time-to-success (μ) is 30 days.	83
Table 9	PLADD parameters used to model the four-bus system.	91
Table 10	The severity of damage for each test cases	94
Table 11	DC power flow parameters	94
Table 12	Risk calculations of test case 1-5	94
Table 13	Average and worst case risk calculation for the 39-bus system	102

LIST OF FIGURES

Figure 1	Attack graph capturing attacker's strategy in performing BDI attack to the power grid.	6
Figure 2	The cumulative distribution function of an exponential distribution with a mean (μ_k) = 30.	6
Figure 3	An example attacker and defender interaction involving a computer.	8
Figure 4	An example of attacker and defender interaction involving two computers.	10
Figure 5	An Illustrative example of the FlipIt game showing the resource changing hands between the attacker (red) and the defender (blue) as time progresses from left to right.	14
Figure 6	Illustration of the impact of the time-to-success distribution on the control of the resource.	14
Figure 7	Markov chain capturing attacker's strategy for compromising the power system under attack assuming no defender.	16
Figure 8	Markov chain capturing attacker's strategy for compromising the power system under attack assuming defender with no state estimation.	17
Figure 9	Markov chain capturing attacker's strategy for compromising the power system under attack assuming defender with state estimation.	17
Figure 10	Cyber-physical system bad data injection attack path.	19
Figure 11	Two power grid attack scenarios.	22
Figure 12	Power grid topology where the control center communicates substations in two different regions.– Attack scenario involving two subsystems in the AND configuration while the two subsystems have an OR configuration relationship. This configuration is labeled as OR_AND_AND.	22
Figure 13	Attack scenario involving two subsystems in the AND configuration while the two subsystems have an OR configuration relationship. This configuration is labeled as OR_AND_AND.	23

Figure 14	Attack scenario involving two subsystems in the OR configuration while the two subsystems have an AND configuration relationship. This configuration is labeled as AND_OR_OR.	24
Figure 15	Two-bus case under bad data injection attack.	32
Figure 16	Probability of an attack being located at each node with respect to time for the case assuming no defender.– Probability of an attack being located at each node with respect to time for the case assuming defender exists, but not using state estimation.	35
Figure 17	Probability of an attack being located at each node with respect to time for the case assuming defender exists, and uses state estimation.	35
Figure 18	Probability of an attack being located at each node with respect to time for the case assuming defender exists, and uses state estimation.	36
Figure 19	Hybrid model attack graph, where the table shows the parameters used for each PLADD node.	40
Figure 20	State of each PLADD node with respect to time are shown from top to bottom, where the top plot represents the state of PLADD node 1 in Figure 19. The second plot from the top represents the state of PLADD node 2 in Figure 19. The third plot from the top represents the state of PLADD node 3 in Figure 19. The bottom plot represents the result of doing a logical AND on PLADD node 1-3's state.	43
Figure 21	(a) The preparation stage for day 1 through 40 is shown on the left. (b) The first execution stage happens on the 14 th day and the corresponding attack propagation is shown on the right.	43
Figure 22	(a) The preparation stage for days 1 through 40 is shown on the left. (b) On the right, the execution stage for days 1 through 40 is shown on the right. Note that attacker's progress is reset at the end of each attack-frame.	44
Figure 23	Four possible outcomes of a PLADD game, where the attacker starts an attack at time $t = 0$, and the time of inspection is at time t , $d_k < t < \tau_k$.	50
Figure 24	A hierarchical parallel PLADD system containing three PLADD games. This configuration is labeled as AND_OR.	55
Figure 25	A hierarchical parallel PLADD system containing three PLADD games. This configuration is labeled as OR_AND.	57

Figure 26	Timeline of events in PLADD game k , where the start of the most recent attack (relative to t) is at time 0.	59
Figure 27	Timeline of events in PLADD game k , where the start of the most recent attack (relative to t) is at time d_k .	60
Figure 28	Timeline of events in PLADD game k , where the start of the most recent attack (relative to t) is at time $d_k + (n_k - i)\tau_k$.	61
Figure 29	Implementation of a single PLADD game.	78
Figure 30	Simulation 1.c: We set $d_{RTU1} = 0$, $d_{RTU2} = 45$, $\mu_{RTU1} = \mu_{RTU2} = 90$, $\tau_{RTU1} = \tau_{RTU2} = 90$.	80
Figure 31	Simulation 1.c: We set $d_{computer1} = 0$, $d_{computer2} = 45$, $\mu_{computer1} = \mu_{computer2} = 90$, $\tau_{computer1} = \tau_{computer2} = 90$.	81
Figure 32	Four-bus power grid system.	88
Figure 33	Attacker's attack plan for a single substation.	89
Figure 34	Hybrid attack model for the four-bus system.	91
Figure 35	A hybrid attack model simulating an attack on Substation 3.	95
Figure 36	A hybrid attack model simulating an attack on Substation 4.	96
Figure 37	A hybrid attack model simulating an attack on Substation 1 and Substation 4 simultaneously.	97
Figure 38	A graphical view of a 39-bus system. This is drawn using [44].	99
Figure 39	The hybrid attack model of attacking one, two or three substations simultaneously.	101
Figure 40	Risk of Substation 1 being successfully attacked as the period of resets increases.	103
Figure 41	Risk of Substation 1 being successfully attacked as the attacker's mean-time-to-success increases.	103
Figure 42	Sensitivity of Substation 1 being successfully attacked as the period of resets increases.	104
Figure 43	Sensitivity of Substation 1 being successfully attacked as the attacker's mean-time-to-success increases.	105

LIST OF SYMBOLS AND ABBREVIATIONS

BDI	Bad Data Injection
CPS	Cyber-Physical System
HAM	Hybrid Attack Model
IP	Internet Protocol
MTU	Master Terminal Unit
PLADD	Probabilistic Learning Attacker, Dynamic Defender
PRESTIGE	PRactical Evaluation and Synthesis of Trust In Government systEms
RTU	Remote Terminal Unit
TCP	Transmission Control Protocol
AND	Logical AND Relationship
OR	Logical OR Relationship

SUMMARY

Cyber-physical attacks on critical industrial control systems are on the rise. These attacks may target individual field cyber-components or the communications network. In the electricity grid, cyber-physical attacks can modify or affect data or software applications such as state estimator demand response, frequency regulation and voltage control. As a result, a cyber-physical attack on the grid can trigger operators to take inappropriate actions which can lead to instability in the power grid and cascading failures with significant consequences. Hence, to ensure a secure and reliable power grid, it is imperative to study the different ways in which the cyber-physical power grid can be compromised and then develop techniques and mechanisms to detect, evaluate and mitigate the propagation and impact of a potential cyber-physical attack.

The objective of the research is to model the propagation of cyber-attack in cyber-physical systems. Note that our research should be applicable to all cyber-physical systems, but we use the electricity grid as the main exemplar for our work. We utilize three models:

(a) A model based on Markov principles. The Markov model uses a Markov chain to encapsulate the attacker's strategy and probabilities of success/failure of the attack propagating from one node to the next. Each node in the Markov model represents at least one attacker goal in the cyber-physical system.

(b) A game-theoretic probabilistic learning attacker, dynamic defender (PLADD) model [1]. PLADD models ongoing contention between defender and attacker for "ownership" of an access control, where attacker ownership implies the attacker has access

and defender ownership implies denied attacker access. The PLADD model leverages game theory similar to FlipIt [2] to analyze defender and attacker interactions.

(c) The hybrid attack model [3], which combines both Markov and PLADD model. The hybrid attack model (HAM) is a hybrid of (a) and (b). HAM consists of both PLADD games and Markov nodes. In HAM, an attack is split into preparation and execution stages. In HAM, PLADD games are used to model attacker actions in the preparation stage, and the Markov nodes are used to model attacker actions in the execution stage.

Additionally, the hybrid attack model is extended to assess risk in a cyber-physical system. The risk assessment allows cyber-physical system operators to quantitatively determine which area of the cyber-physical system is the most vulnerable and requires a security update. Lastly, sensitivity analysis is done on an example power grid scenario to determine the maximum risk value.

CHAPTER 1. INTRODUCTION

1.1 Problem Statement

A Cyber-Physical System (CPS) is an integration of computation and physical processes. Cyber-Physical Systems are widely used in critical national infrastructures, such as the communication, electric power, transportation, and petroleum industries [4]. As we move toward large-scale introduction of Information Technology (IT) in these sectors and automatic management, cyber threats can have a significant impact on these infrastructures [5]. For example, it has been shown that potential network intrusion by adversaries may lead to a variety of severe consequences in the smart grid, from customer information leakage to cascading failures [6]. Prior work by the research community has focused on reliability by protecting Cyber-Physical Systems against random, independent or benign faults, and failures of cyber/physical components [7]. However, these prior works did not focus on modeling attack propagation related issues.

Addressing the cybersecurity aspects of a CPS is very important. However, security analysts are often constrained by time and money. Security analysts need to determine a reasonable way of spending resources (time and/or money) to protect a CPS. In this thesis, we define an analysis that improves the efficiency of spending resources on increasing the overall security of CPS as a security investment analysis.

Securing a CPS goes beyond securing the individual system components. A motivated adversary often uses the inter-dependency of vulnerabilities to carry out

multistage attacks. While each individual phase of the attack may not pose a serious threat to the corresponding component, the combined effect, however, may be catastrophic.

Cyber-physical systems are complex and consist of technologies that span across different fields. To measure the security of a CPS, security analysts need to consider defender-related information such as when are the login credentials reset as well as attacker-related information such as how would the attacker gain access to the necessary information to exploit a vulnerability.

The power grid is a critical infrastructure that must continue to function even when under attack. Therefore, the security analysis of power grids is critical and has theoretical and practical significance [8]. The power grid has distinct features that create unique security challenges including a) transmission and distribution circuits over large geographic areas, b) unmanned substations, c) a broad range of modern and legacy components, and d) use of a variety of communications technologies and protocols.

According to a U.S. Department of Energy report [9], out of 245 total incidents reported across all sectors in FY 2014, roughly 55% involved advanced persistent threats (APT) or sophisticated actors. The 2015 Global State Information Security Survey reported that power companies and utilities around the world expressed a six-fold increase in the number of detected cyber incident over the previous year [10]. On May 1st, 2020, President Donald Trump signed an executive order aimed at securing the U.S. bulk-power system[11]. Cyber-physical security attacks may target individual field cyber-components or the communications network. Therefore, it is imperative to study the different ways in which the cyber-physical power grid can be compromised and then develop techniques and

mechanisms to detect, evaluate and mitigate the propagation and impact of a potential cyber-physical security attack.

Many works have been proposed to investigate the vulnerability of power grids by developing threat and attack models as well as simulating different attack scenarios in a controlled environment[12-15]. However, important challenges remain. Developing reasonable approaches and models that can mimic cyber-physical attacks in reality is still a critical challenge. Such models need to incorporate both the communications network and the power systems layer in order to detect and mitigate the effects of cyber-physical attacks, modelling and simulation of how these attacks may propagate through a cyber-physical power system need to be undertaken.

1.2 Terminology

In this section, we define terms used in this thesis, give examples of an attack propagation in power grid, and introduce probability theory.

1.2.1 Attack Graph Semantics

In this thesis, an attack graph contains nodes and edges. A node represents a malicious action that attackers want to complete in order to successfully reach their goal. A directional edge that connects node A to node B together shows that an attacker needs to successfully attack A before attacking B.

We represent the attacker's strategy in two phases. The first phase is the preparation phase, where the attacker needs to gather information and prepare all the necessary tools to execute an attack. Nodes one through five capture the preparation phase shown in

Figure 1. The second phase is the execution phase where the attacker executes the attack and interacts with the defender.

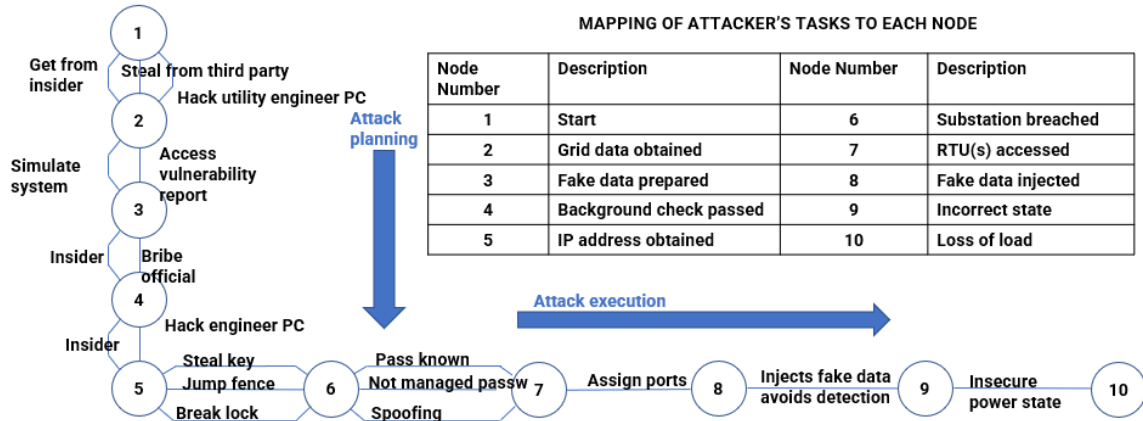


Figure 1 – Attack graph capturing attacker’s strategy in performing BDI attack to the power grid.

Example 1: Figure 1 shows an example of a bad data injection attack on the power grid. □

Bad data injection attacks have drawn wide concerns in cyber-physical power grids such as those proposed by Liu and Ning[16]. The attack graph in Figure 1 shows the attacker’s strategy in two phases, which are the planning and execution phase. Nodes 1 to 5 are actions that the attacker perform to plan for the BDI attack. Nodes 6 to 10 are actions that requires the attacker to interact with the power grid. Starting at Node 1, the attacker can either 1) simulate the power system, 2) steal from a third party that has access to the grid data, 3) hack an operator’s computer to get access to grid data. The attacker moves through the attack graph until Node 5, where the attacker has finished preparing for an attack, so the attacker has the option to 1) steal key to a substation, 2) jump the fence around the substation, or 3) break the lock to gain access to the substation. The attacker moves

through Nodes 6 through 10 in order to achieve load loss. Although we don't have realistic incident reports from the power grid, it is safe to assume that actions in the preparation phase requires significantly more time and resources for the attacker to complete relative to the execution phase. It is also noteworthy to point out that it is highly likely that the work the attacker has done in the preparation phase is a moving target due to security reasons such as periodic IP reset, password reset, or practical reasons such as changing power grid topology. Therefore, we think it is a safe assumption that the attacker would require more time in the preparation phase than the execution phase of the attack.

1.2.2 Basics Definitions In Probability Theory

Definition 1. *The cumulative distribution function (CDF) of a real-valued random variable X , or just distribution function of X , is evaluated at x . It is the probability that X will take a value less than or equal to x [17]. The cumulative distributive distribution function of a real-valued random variable X is the function given by*

$$F_X(x) = P(X \leq x)$$

where the right-hand side represents the probability that the random variable X takes on a value less than or equal to x . The probability that X lies in the semi-closed interval $(a, b]$, where $a < b$, is therefore

$$P(a < X \leq b) = F_X(b) - F_X(a)$$

Definition 2. *The exponential distribution is the probability distribution of the time between events in a Poisson point process, i.e., a process in which events occur continuously and independently at a constant average rate.*

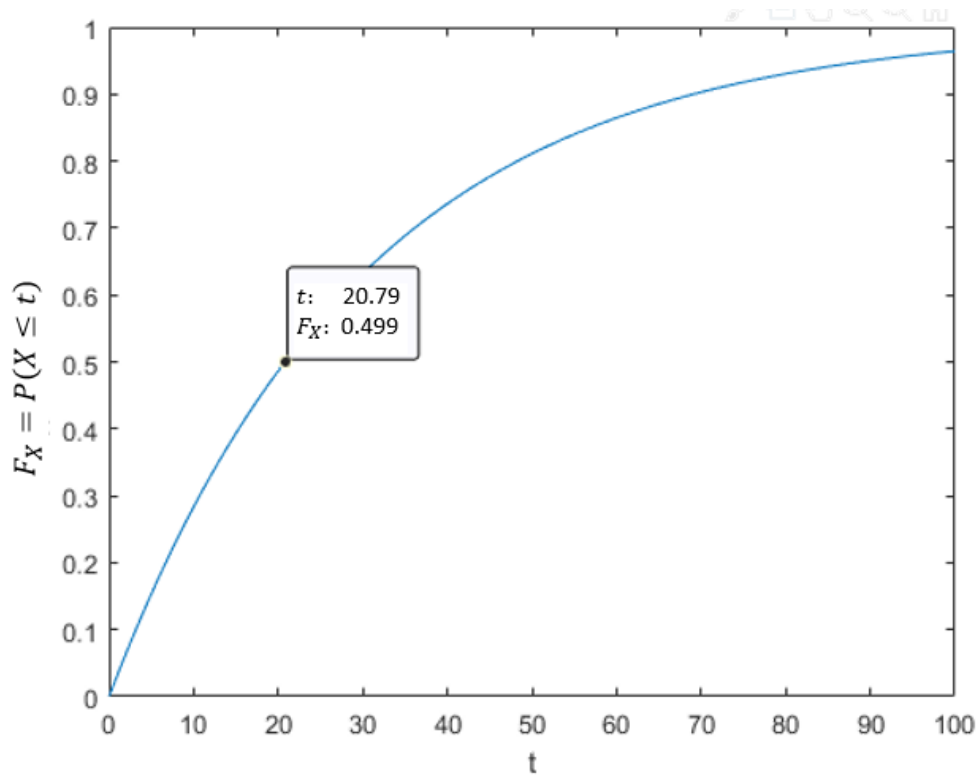


Figure 2 – The cumulative distribution function of an exponential distribution with a mean (μ_k) = 30.

Figure 2’s y-axis is $P(X \leq t)$, which is the probability that a random number is less than or equal to t . By plugging $m = \mu_k * \ln(2)$, we can see that the median is 20.79, which is where the probability is approximately 50%.

Definition 3. Suppose X is exponentially distributed. Then the CDF of X is given by

$$F_X(x; \lambda) = \begin{cases} 1 - e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

where λ is greater than 0 and is the parameter of the distribution, often called the rate parameter. The mean or expected value of an exponentially distributed random variable X with rate parameter λ is given by $\frac{1}{\lambda}$. Throughout this manuscript, we use the mean of an

exponential distribution (μ) instead of the rate parameter λ to define an exponentially distributed function. Note that the mean does not imply the probability is 50% at the mean. The median (m) of an exponential distribution function is defined as the center of mass of the probability density function. The median (m) is calculated as shown below:

$$m = \mu * \ln (2)$$

Example 2: If an exponential distribution function has a mean equal to 30, then the plot of the cumulative distribution function is shown in Figure 2. □

1.2.3 Basic Definitions in Game Theory

Game theory is the study of mathematical models of strategic interaction among rational decision-makers [18]. There are many variations of game theory models and strategies, but game theoretic models typically must define the players of the game, the information and actions available to each player at each decision time, and the payoffs of each outcome.

Definition 4. *A game consists of the following:*

- *a collection of decision-makers, called players;*
- *the possible information states of each player at each decision time;*
- *the collection of feasible moves (decisions, actions, etc.) that each player can choose to make in each of his possible information states;*
- *a procedure for determining how the move choices of all the players collectively determine the possible outcome of the game; and*

- *preferences of the individual players over these possible outcomes, typically measured by a utility or payoff function.*

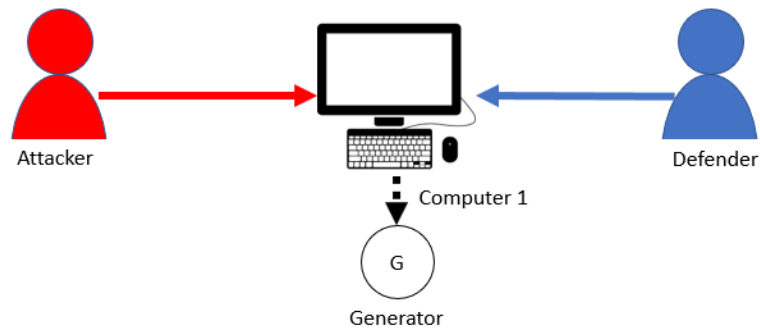


Figure 3 – An example attacker and defender interaction involving a computer.

Example 3: Figure 3 shows an example attacker and defender interaction involving access to Computer 1 that controls a power generator. □

In Example 3, there are two players, a defender and an attacker. For the current calendar year, the defender is required to change the computer password periodically, and the attacker can use password cracking software to gain access to the computer. Realistically, the defender can employ various cybersecurity measures to protect the computer, while the attacker can also employ various types of attacks to gain access to the computer. Therefore, instead of diving into what cybersecurity mechanisms the defender is implementing on the computer and exactly what the attacker is doing to gain access to the computer, we can derive a simple model. Specifically, the defender can do a “take” move, which can immediately regain control of the computer. In this example, the defender resets passwords every month (30 days), and each password reset immediately grants the

defender control of the computer. The attacker can attack the computer to gain access, but the attacker only gains access to the computer after some time has passed (such as one month) and with a given probability of success (such as 30%). The information available to the attacker consists of whether Computer 1 is controlled by the attacker or not. On the other hand, the defender only knows for sure that Computer 1 is controlled by the defender immediately after a take move. The amount of time each player controls Computer 1 determines the payoff (see Definition 4) of each player in this example.

Example 4: Figure 4 describes an example of attacker and defender interaction involving access to two computers. □

For this example, there is one defender and one attacker. There are two computers, but only Computer 2 can control the generator. Computer 1's one-time key is required for Computer 2 to control the generator. In this example, the attacker needs access to both Computer 1 and Computer 2 to execute commands on Computer 2. As was done in Example 3, the attacker's move is to start an attack (such as executing password cracking software) on a computer, which gives the attacker control of the computer after some time. The attacker can attack Computer 1 and/or Computer 2 independently. The defender's move is the same as in Example 3, which is called a "take" move that immediately regains control of a computer. The defender can execute a "take" move on Computer 1 or Computer 2 independently. The attacker knows if the attacker controls Computer 1 and/or Computer 2. The defender knows that a computer is controlled by the defender immediately after a take move. The amount of time each player can control the generator determines the payoff of each player.

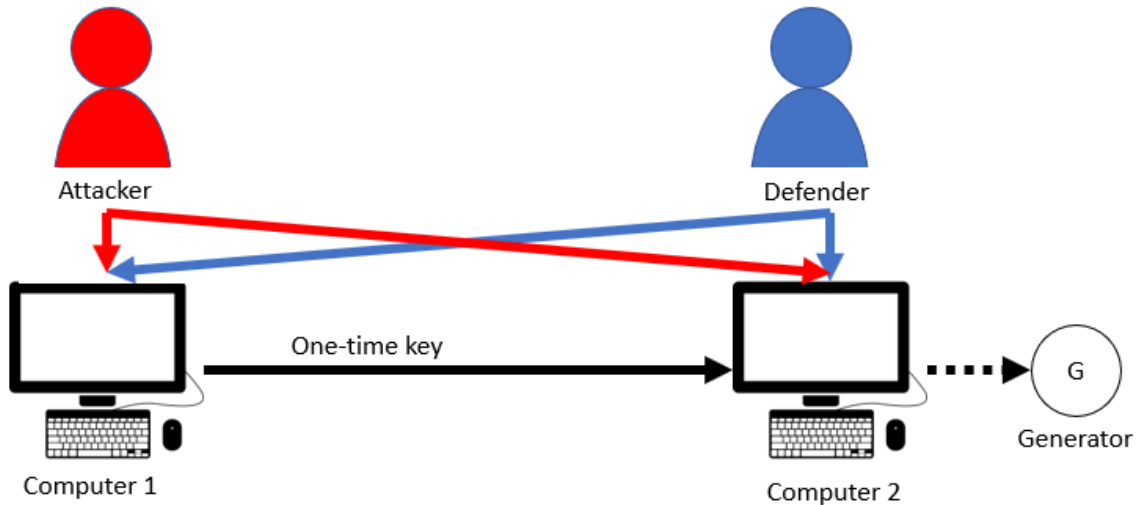


Figure 4 – An example of attacker and defender interaction involving two computers.

Example 3 and Example 4 showcase the following game theoretic terms. First, there are two players in each example. The information available to the attacker is whether the attacker controls each computer or not. The defender does not know whether the attacker controls the computer or not. The attacker can execute an attack on the computer (e.g., running password cracking software). The attack is successful after a delay, and then the attacker controls the computer. The defender can execute a “take” move (e.g., periodic credential reset) which immediately takes control of the computer. The amount of time each player controls the computer determines the payoff for each player. For example, the attacker may control the computer for 10% of the time, while the defender may control 90% of the time.

1.3 Research Overview

The objective of the research is to model CPS attack propagation including the effect of possible mitigations. Attack propagation in our context is defined as an attack that travels through different layers of CPS to achieve a malicious goal. It is well-known that a CPS

typically has five layers, which are configuration, cognition, cyber, conversion, and connection [19]. Bad data injection attack is an example of an attack that travels through different layers of a CPS. By modeling attack propagation in a CPS, we can identify the weak points in a CPS, and provide feedback to security analysts on how to increase the overall security of a CPS.

1.4 Dissertation Organization

The remaining chapters of this dissertation are organized as follows.

Chapter 2 presents some background and prior work related to game theoretic models and stochastic model. An overview of models are presented.

Chapter 3 discusses attack propagation modeling in cyber-physical system. The advantages and disadvantages of using Markov chain and PLADD is discussed, then the hybrid attack model is presented which is a combination of Markov chain and PLADD model.

Chapter 4 describes the mathematical analysis of a parallel PLADD system. Specifically, notations and definitions are defined, follow by mathematical model of a single PLADD game. We then expand the mathematical model of a single PLADD game to a single-layer parallel PLADD system. Next, we build on top of a single-layer PLADD system to get a hierarchical parallel PLADD system.

Chapter 5 presents risk assessment and sensitivity analysis on an example attack scenario in the power grid. The risk assessment shows how a power grid operator may use the hybrid attack model to determine the weak link in the power grid.

Finally, Chapter 6 concludes the work presented in this dissertation and highlights the major contributions of this research.

CHAPTER 2. BACKGROUND

In the power grid scenario, one example of vulnerability is called the bad data injection attack. Prior research on bad data injection attack usually assumes the attacker has access to old measurement data and can run power flow analysis to determine the bad data that can cause damage to the power grid. In addition, these prior works also assume that the attacker has the login credentials to access the power grid communication network. Although these prior works are important, they are not measuring the security of the CPS, but rather a single vulnerability in the CPS.

In this chapter, we present some background and literature review regarding the two major work related to HAM. We first start by introducing a model called FlipIt, which is then extended to create Probabilistic Learning Attacker, Dynamic Defender (PLADD) model. Next, we introduce Markov chain, which is combined with PLADD to create the HAM. Finally, we introduce some prior work on bad data detection and risk assessment.

2.1 FlipIt

FlipIt provides insight into certain kinds of adversarial cyber scenarios. In FlipIt, two players, the defender and the attacker, contend for control of a single shared resource. The defender initially controls the resource. Each player can make a move at any time by incurring a fixed cost. Defender and attacker costs are independent, and the magnitude of the costs is a game parameter. When players move, they immediately gain control of the resource if it was controlled by their opponent or retain control of the resource if they already controlled it. The move has no effect, but still incurs cost, if a player already has the control of the resource.

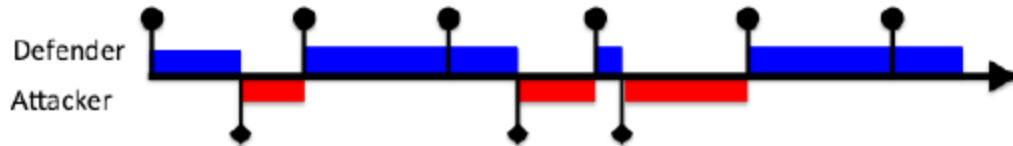


Figure 5 – An Illustrative example of the FlipIt game showing the resource changing hands between the attacker (red) and the defender (blue) as time progresses from left to right.

2.2 Probabilistic Learning Attacker, Dynamic Defender (PLADD)

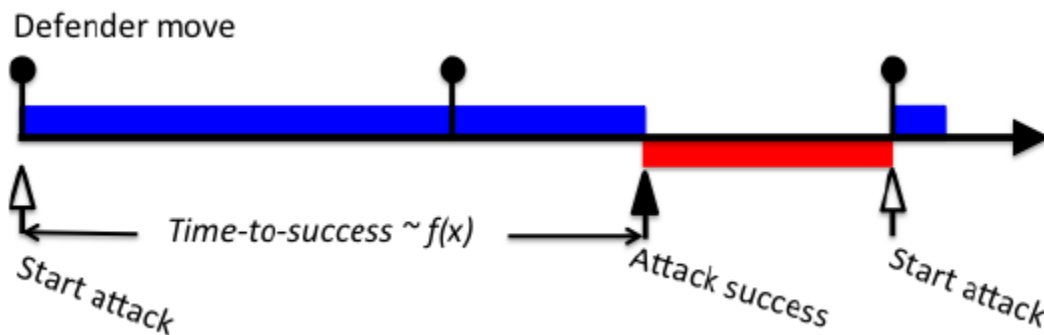


Figure 6 – Illustration of the impact of the time-to-success distribution on the control of the resource.

Unlike FlipIt, the attacker’s attack is not instantaneously successful, the attacker’s time-to-success is a random variable calculated from a probability distribution. In PLADD, a single attacker and defender contend for a resource. Attack dynamics is modeled as a stochastic process. The time required for the attacker to gain control is a random variable. The attacker “learns” from a successful attack, shortening the average time to complete subsequent attacks. The defender can regain the resource with (i) a lower cost “take” move that does not lessen the attacker’s knowledge level, or (ii) a higher cost “morph” move that in addition undoes attacker learning. The defender has no information about attacker progress and must decide (i) when to act and (ii) which moves to use to maximize defender

utility and minimize attacker utility. “Utility” for both players is defined as the cumulative duration of controlling the resource minus costs.

2.3 Markov Chain

A Markov chain [20] is a mathematical system that experiences transitions from one state to another according to certain probabilistic rules. The defining characteristic of a Markov chain is that no matter how the process arrived at its present state, the possible future states are fixed. In other words, the probability of transitioning to any particular state is dependent solely on the current state and the time elapsed. The state space, or set of all possible states, can be anything: letters, numbers, weather conditions. In this manuscript, state space of Markov chain represents successful attacker action.

The Markov chain encapsulates the attacker’s strategy and probabilities of success/failure of the attack propagating from one node to the next. In Figure 1, we assume that the tasks are sequential, which means that only one task is being executed at any point in time. We also assume that the system has bad data detection capability from the state estimator. This detects and tries to prevent an ongoing attack from becoming successful; however, it does not reset the attacker’s current progress. Therefore, a successful detection of an attack at any node only pushes the attacker back to the immediate previous node. It is noteworthy to point out that the example scenario (see Figure 1) does not show the possibility that a successful detection by the defender may cause the attacker’s progress to be set back by more than one node. Each node in the Markov chain can connect with any nodes. Each edge (directed) represents the attacker’s attempt to complete the next task given that the current task is completed. The values on the edges represent the probability

that the attacker will successfully complete the next task. The probabilities used in Figure 7 to Figure 9 are informally assigned since we do not have access to real world data. However, an expert in the power grid field has agreed that the probabilities make sense. The probability assigned to each edge only depends on each individual vulnerability, which is similar to many existing metric, such as Common Vulnerability Scoring System (CVSS) [21]. The CVSS gives a way to capture the characteristics of a vulnerability and create a numerical score reflecting its seriousness. The numerical score can be translated into a qualitative representation (such as low, medium, high, and critical) to assist organizations evaluate and prioritize their vulnerability management processes. Table 1 shows the mapping of an attacker’s tasks to each node in Figure 1 to Figure 9. Figure 1 is the attack graph representation of the Markov chains shown in Figure 7 to Figure 9.

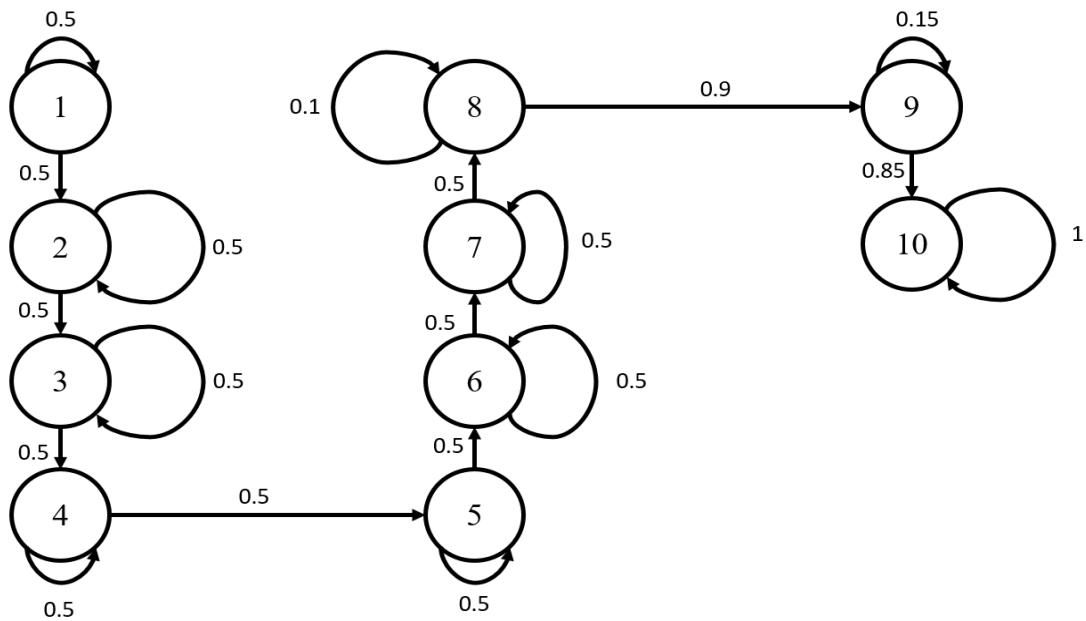


Figure 7 – Markov chain capturing attacker’s strategy for compromising the power system under attack assuming no defender.

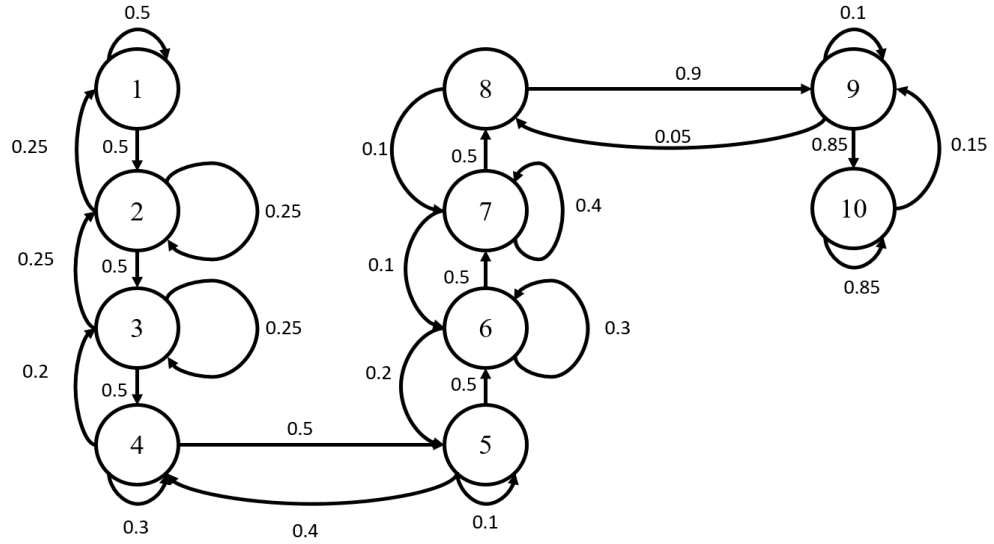


Figure 8 – Markov chain capturing attacker’s strategy for compromising the power system under attack assuming defender with no state estimation.

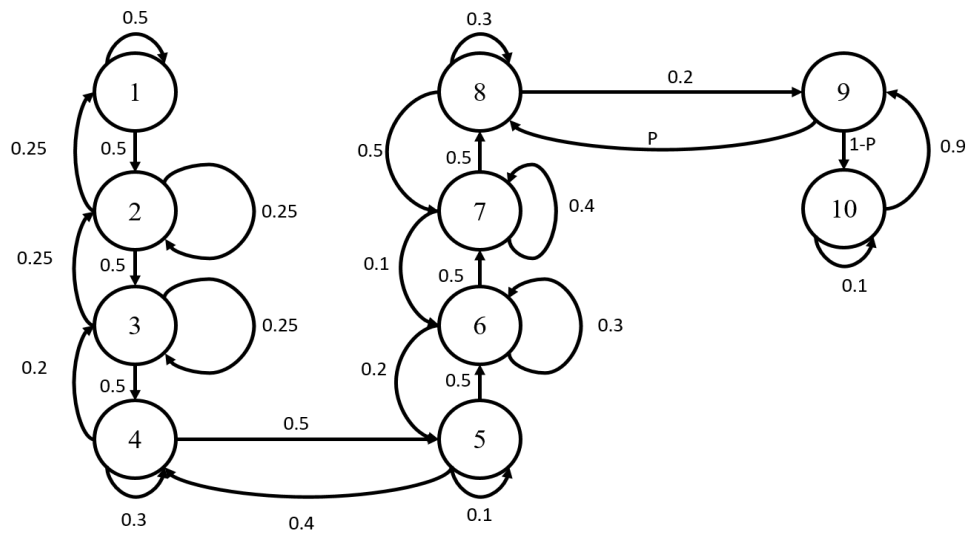


Figure 9 – Markov chain capturing attacker’s strategy for compromising the power system under attack assuming defender with state estimation.

Example 5: Figure 7 through Figure 9 are examples of Markov chain that models the bad data injection attack of Figure 1 with various different assumptions. Figure 7 assumes there is no defender. Figure 8 assumes that state estimation is not used to detect bad data. Figure 9 assumes that state estimation is available to

detect bad data. The success or failure of the attack propagating from the source to the operator at the control center is modelled by the Markov chain with various assumptions with regards to Example 1. □

Table 1 – Mapping of attacker’s tasks to each node.

Node Number	Description
1	Start
2	Grid Data Obtained
3	Fake data Prepared
4	Background Check passed
5	IP Address Obtained
6	Substation Breached
7	RTU(s) Accessed
8	Fake Data Injected
9	Incorrect State
10	Loss of Load

2.4 Attack Scenarios

2.4.1 Bad Data Injections Attack Scenario

A simplistic diagram for my example power grid scenario is shown in Figure 10. In this diagram, there are two Remote Terminal Unit (RTU) and two substations. At the control center, there are Analysis Modules, Monitoring Systems and Operators. The Analysis Modules are tools such state estimation, security assessment, etc. The Monitoring System are equipment that send and receive data packets such as the SCADA system. The operators are the human making decisions such as increasing generation of power at a substation to meet demand. We assume the attacker is executing a bad data injection attack by accessing the RTU. The adversary may access the RTU to inject well-crafted fake data to the control center that passes the state estimation checks and cause incorrect data to be presented to the system operator. This incorrect data may cause the system operator to issue

an incorrect command that may damage the power grid. We assume that the attacker has full knowledge of the power system topology and in the planning state obtains IP addresses/TCP ports of the Monitoring System and the Remote Terminal Units (RTU) at the substations. The attacker breaks into the substation enclosure containing the RTUs and communication radio, connects a malicious computing device to RTU and is able to access the RTUs. The attacker compromises the measurements polled by the Monitoring System by constructing packets containing fake field readings and transmitting said readings to the Monitoring System as shown in Figure 10 below. We also assume that the attacker’s goal is to cause the System Operator to issue an incorrect command as a result of the fake data injection attack rather than to completely disable the RTUs.

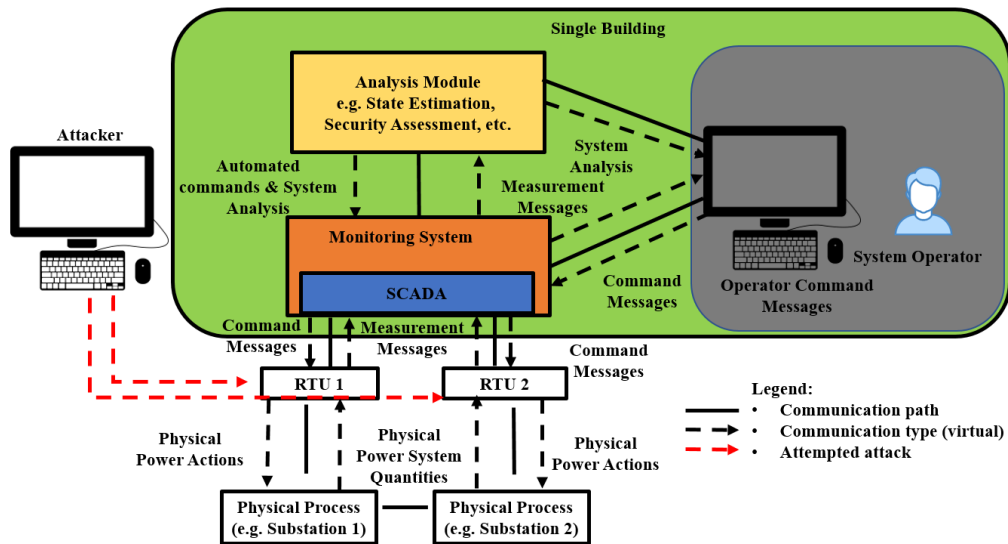


Figure 10 – Cyber-physical system bad data injection attack path.

2.4.2 Bad Data Detection

The goal of this thesis is not to design undetectable bad data injection attacks or to develop better bad data detection tests, but rather the goal is to study how bad data injection

attacks propagate in the system before they are identified and contained or mitigated by the operator.

The traditional bad data detection [22] in power system is based on the residual between the real values of measurements and the estimated ones. If the difference between estimated measurements \hat{z} and the real measurement z exceeds the tolerance threshold x , i.e. $|\hat{z} - z| > x$, the bad data will be detected. However, there Liu [23] showed that it is possible to create undetectable bad data injection (BDI) attack. The basic idea of the undetectable BDI is to construct the attack vector a on DC model as follows:

$$z = Hx + e + a = H(x + c) + e \quad (1)$$

Where H is the Measurement Jacobian Matrix of $h(x)$ since there is an approximate linear relationship between state variable and measurements in DC model. The attack vector satisfies $a = Hc$, so that the residual between the injected measurements and the true value will never exceed the detection threshold.

2.4.3 Single-Layer Parallel PLADD System Attack Scenarios

We consider a generic power grid topology shown in Figure 10. We focus on the attack scenarios in the power grid shown in Figure 11. We assume the attacker's goal is to have the ability to open and/or close breakers in the power grid. For simplicity, in Figure 11 we assume that there are two remote terminal units (RTUs) and two operator computers in the power grid (but our results apply to any number of RTUs and/or operator computers). A PLADD game models each credential in Figure 11. In our experiment, we

assume the period (τ) of the defender “take” move for RTU 1, RTU 2, Operator Computer 1, and Operator Computer 2 is 90 days each. We will also perform parameter sweeps on the period (τ) of RTU 1, RTU 2, Operator Computer 1, and Operator Computer 2 by setting the period (τ) to 90 days as well as 180 days. For the attacker’s mean time required for a successful attack (μ), we assume it is 90 days. Our experiment will also do a parameter sweep by setting the attacker’s mean time required for a successful attack (μ) to 90 days and 180 days. In addition, we assume the attacker’s time to success is modelled by an exponential distribution. The cumulative distribution function of an exponential distribution is shown below:

$$F_k(t) = \begin{cases} 1 - e^{-\frac{1}{\mu_k}t} & t \geq 0 \\ 0 & t < 0 \end{cases}$$

where μ_k is the mean of the exponential distribution. In the context of our attack scenario, μ_k is the attacker’s mean time-to-success of an attack in game k .

From the attacker’s point of view with regard to Figure 10, the attacker needs to control i) both RTU 1 and RTU 2, or ii) either Operator Computer 1 or Operator Computer 2 to have the ability to open/close all breakers. We define a single-layer parallel PLADD system as a system containing at least two PLADD games in a single configuration of AND or OR. The PLADD games in a parallel PLADD system start at the same time and interact simultaneously with the same attacker and defender. The attacker and defender can make moves in each game independently. The topology of two single-layer parallel PLADD system configurations is shown in Figure 11. If a system is in the AND configuration, then the attacker is considered to control the system when the attacker

controls all resources. If a system is in the OR configuration, then the attacker is considered to control the system when the attacker controls at least one resource.

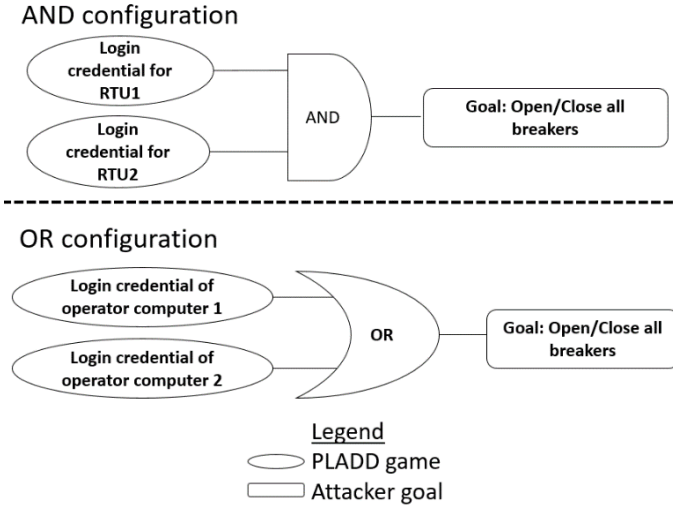


Figure 11 – Two power grid attack scenarios.

2.4.4 Hierarchical Parallel PLADD System Attack Scenarios

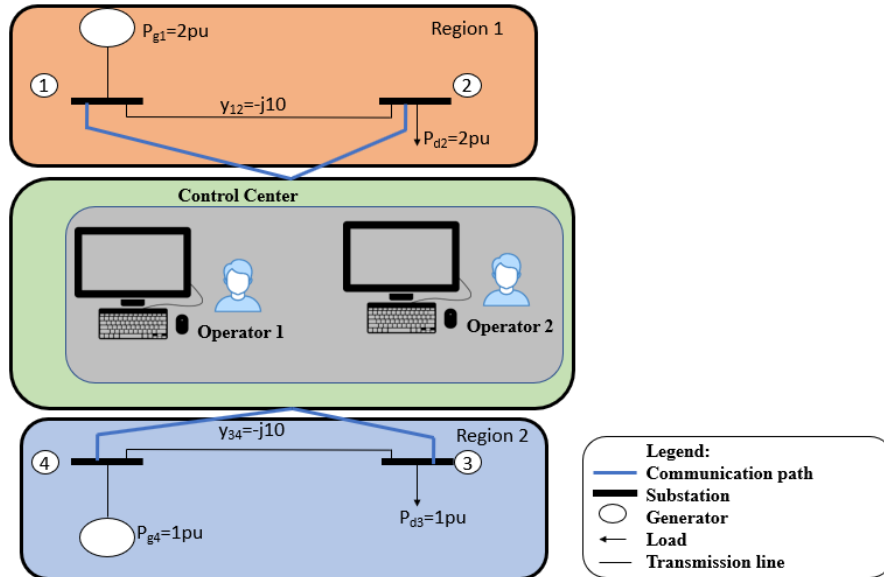


Figure 12 – Power grid topology where the control center communicates substations in two different regions.

OR_AND_AND

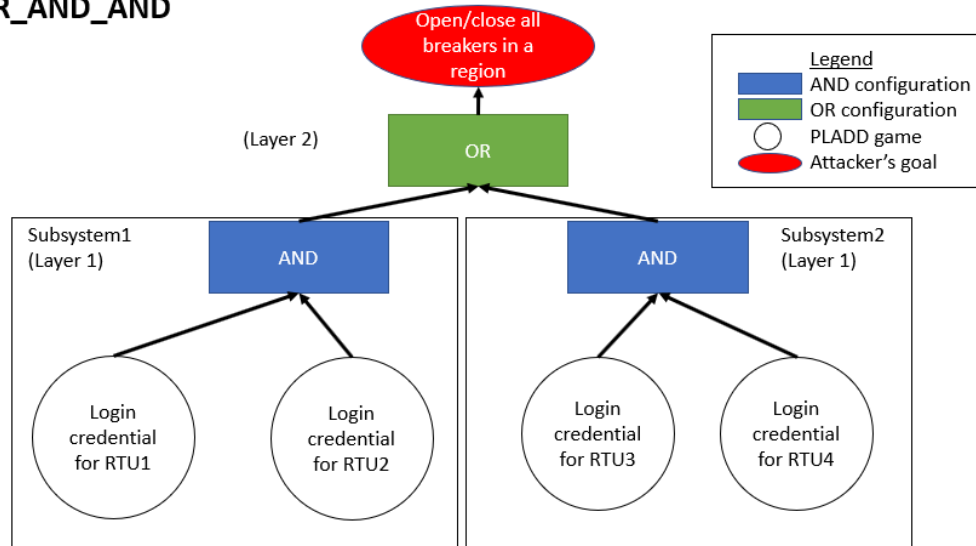


Figure 13 – Attack scenario involving two subsystems in the AND configuration while the two subsystems have an OR configuration relationship. This configuration is labeled as OR_AND_AND.

In addition to the two attack scenarios shown in Figure 11 (involving two PLADD games in parallel PLADD system), we also consider scenarios involving combinations of both AND configurations and OR configurations within a hierarchical parallel PLADD system. For example, consider a generic power grid topology that controls two separate regions, as shown in Figure 12. Substation 1 and Substation 2 are in Region 1, while Substation 3 and Substation 4 are in Region 2. The control center communicates with all Substations shown in Figure 12. We also assume the operator computers are in a room that is accessible by either Operator 1's keycard or Operator 2's keycard. In our experiment, we assume the period (τ) of the defender "take" move for RTUs (1, 2, 3 and 4) and Operator Computers (1, 2, 3 and 4) is 90 days each. We also assume the attacker's mean time required for a successful attack (μ) is 30 days. In addition, we assume the attacker's time to success is modelled by an exponential distribution.

From the attacker’s point of view with regard to Figure 12, the attacker needs to control either i) both RTU 1 and RTU 2 or ii) both RTU 3 and RTU 4 to have the ability to open/close all breakers in a region. We define a parallel PLADD system involving at least two layers as a hierarchical parallel PLADD system. Figure 13 and Figure 14 show parallel PLADD systems involving two layers of AND and OR configurations within a single overall parallel PLADD system.

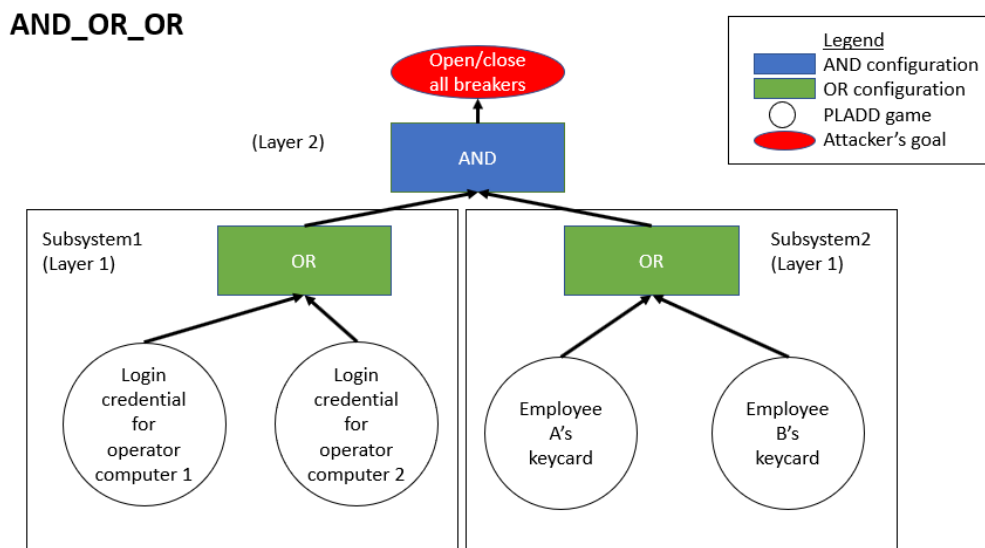


Figure 14 – Attack scenario involving two subsystems in the OR configuration while the two subsystems have an AND configuration relationship. This configuration is labeled as AND_OR_OR.

Example 6: Consider an attack scenario where the attacker’s goal is to have the ability to open/close all breakers in a region. In this scenario, we consider the power grid topology as shown in Figure 12. The attacker needs to control either i) both RTU 1 and RTU 2 or ii) both RTU 3 and RTU 4 in order to have control of all RTUs in a region. Figure 13 shows an illustration of this attack scenario modelled in the hierarchical parallel PLADD system. □

Example 7: Consider an attack scenario where the attacker's goal is to have the ability to open/close all breakers in Region 1 and Region 2. In this scenario, we consider the power grid topology as shown in Figure 12. The attacker needs to control i) either Operator Computer 1 or Operator Computer 2 in the control center, and ii) either Employee A's keycard or Employee B's keycard, to have the ability to open/close all breakers in both Region 1 and Region 2. □

Example 6 and Example 7 describe two attack scenarios in a hierarchical parallel PLADD system. Figure 13 illustrates Example 6 and exhibits a hierarchical parallel PLADD system involving the AND of two subsystems with each subsystem in the OR configuration. Figure 14 illustrates Example 7 and displays a hierarchical parallel PLADD system involving the OR of two subsystems with each subsystem in the AND configuration.

2.5 Risk Assessment in Cyber-Physical Systems

The methodology proposed in [24], by using attack tree provides an effective way to model the attack sceneries and quantify the risk values of CPS. In [25], an enhanced attacks tree is used to evaluate the security risk of CPS. In [26], the authors propose a methodology of security assessment for electrical industrial systems and power systems based on petri net. A game-theoretic framework to model cyber-physical security from a coordinated cyber-attack perspective is proposed in [27]. In [28], a quantitative security analysis model based on the combination of Petri net and game theory is proposed to reflect not only the hybrid of cyber and physical world but the behaviors of attacks and defenders. However, due to the constantly changing external environment, managers cannot find the real threat

from the huge amounts of alarm data. Besides that, the static assessment methods can only roughly estimate the risk over a period of time, but it cannot assess the risk at some specific time points accurately.

Researchers have investigated the vulnerability of power grids by evaluating a set of plausible physical events, such as loss of transmission lines or generating units, and by evaluating their impact. Traditionally, power system operational security involves investigating $N-1$, $N-2$, and $N-1-1$ events [29]. In the field of power systems, “ $N-1$ ” means that the grid shall be capable of experiencing outage of a single transmission line, cable, transformer, or generator without causing losses in electricity supply. “ $N-2$ ” means that the grid shall be capable of experiencing two transmission line, cable, transformer or generator without causing losses in electricity supply. “ $N-1-1$ ” means that the grid shall be capable of experiencing outage of a single transmission line, cable, transformer or generator, follow by another outage of a single transmission line, cable, transformer or generator without causing losses in electricity supply. In [30], a security assessment platform for the electric power system is presented which consists of risk data acquisition, risk identification, and analysis. However, the risk, generated as an output of the analysis, is not estimated based on any actual simulation of the response from the electric power system. Another similar work [31] uses the power system data such as the maximum voltage of each substation and the number of connection lines to calculate risk. In general, the calculation of risk consists of two stages such as determination of probability and severity. The formula to calculate risk can be calculated as follows:

$$risk = \text{Pr}(\text{event happening}) \times \text{Severity}(\text{event happening}) \quad (2)$$

CHAPTER 3. ATTACK PROPAGATION MODEL FOR CYBER-PHYSICAL SYSTEM

In this chapter, we will discuss the advantages and disadvantages of PLADD and Markov chain model, follow by the motivation for combining the PLADD and Markov chain to create the Hybrid Attack Model. Then the bad data injection attack scenario shown in Figure 1 is simulated with Markov chain and Hybrid Attack Model. The bad data injection attack scenario is not simulated with only the PLADD model because the PLADD model cannot properly model the execution stage of the bad data injection attack.

3.1 Components of Hybrid Attack Model

3.1.1 PLADD Modeling Bad Data Injection Attack in Power Grid

The PLADD model is a good fit for a persistent attack where the interaction between an attacker and defender is important for risk assessment. However, for our purposes, modeling an attack exclusively using PLADD does not appear feasible because certain actions may not interact with a defender such as “jumping a fence” or “breaking into a substation” which is unmanned and unsupervised in our scenario. More formally, PLADD models as defined have the following two requirements for any game being modeled:

- The defender does not know who owns the resource and is unable to use detection techniques;
- The defender has a fixed periodic action capable of retaking the resource.

3.2 Attack Propagation In Power Delivery Systems

3.2.1 Motivation

The coupling between information, communication and computing elements with the physical components of power systems introduces new cyber and cyber-physical security concerns. Addressing these concerns requires novel methods that complement the legacy and existing security solutions. Attacks such as bad data injection can cause disruptions that transcend the cyber realm and affect the physical world. This section introduces a graph-based attack propagation model that simulates a bad data injection attack and executes a heuristic defense strategy using power system state estimation. We use the state estimator to identify maliciously injected data and adopt physical security metrics to decide attack mitigation actions. Visualization from analysis performed by this propagation simulation can guide the operator at the control center to take appropriate action to minimize disruption of the physical power system operation due to bad data injection attacks. The work in this section is published on IEEE [32].

Unauthorized access and/or manipulation of cyber-physical power delivery assets by an insider or disgruntled employee is the biggest threat to SCADA, Energy Management Systems (EMS) and bulk electric systems (BES) [33]. Notable cyber-physical attacks on SCADA and EMS systems in recent years include Maroochy Shire sewage spill attack in January 2000 [33], the Davis-Beese Ohio nuclear plant and Slammer Worm attack in January 2003 [33], the Stuxnet malware attack on electrical equipment powering Iran's Nuclear facilities in November 2010 [33, 34], and the cyber-attacks on Ukraine's power grid in December 2015 and February 2016 [35] which caused a blackout affecting 225,000

customers. These attacks have brought more attention to power system threats and vulnerabilities, and the impact of cyber-physical attacks on critical power delivery systems. The consequences and impact of power grid cyber-physical attacks can be worsened by cascading failures. A cascading failure refers to a sequence of dependent events, where the initial failure of one or more components (i.e., substations and transmission lines) triggers the sequential failure of other components [36]. The cause of the initial failures can be a cyber-physical attack, falling of a tree branch, equipment failure, aging equipment, human errors, software, or hardware faults. These cyber-physical attack events stress the need to determine and deploy mechanisms to minimize their risk.

3.2.2 Attack Propagation Model

The attack propagation model is a combined Markovian process and system state estimator model. As shown in Figure 1, we study attack propagation from the substation to the operator using a Markovian process. For a set of simulation time steps $t \in [1, T]$ the final state is obtained as shown in Equation (3).

$$\begin{aligned}
 x^{(T)} &= x^{(T-1)} \times P \\
 &= x^{(T-2)} \times P \times P \\
 &\cdot \\
 &\cdot \\
 &\cdot \\
 &= x^{(0)} \times P^T
 \end{aligned} \tag{3}$$

The x in Equation (3) is a vector representing the state of each node. Therefore, the x in our simulation is a vector of 10 elements, which represents the ten nodes in our attack graph. Each element in x is either “0” for uncompromised, or “1” for compromised. P is a matrix that contains probability values shown in in Figure 7 to Figure 9. The row number in P is the node number at the tail-end of the edge. The column number in P is the node

number at the head-end of the edge. If there is no edge connecting two nodes, the corresponding value in the matrix is 0. An example P matrix which is used in Figure 8 is shown below.

$$\mathbf{P} = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.25 & 0.25 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.25 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.2 & 0.3 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.4 & 0.1 & 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.2 & 0.3 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.1 & 0.4 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.1 & 0 & 0.9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.05 & 0.1 & 0.85 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.15 & 0.85 \end{bmatrix}$$

The model incorporates both the Markov chain that captures attack propagation and a state estimation with bad data detection capabilities. The bad data detection algorithm is implemented at node nine of Figure 9. We investigate three cases – no defender, defender without state estimation, and defender with state estimation. In the attack graph shown in Figure 1, nodes one through five represent the attacker’s preparation process, which is described in Table 1. Nodes six through ten represent the tasks executed by the attacker on to the power grid. Without defender, the Markov chain representation of the attack graph is shown in Figure 7 . There is no edge that shows an attacker’s attack is pushed back to the previous node. In Figure 8, the Markov chain representation of the attack graph shows the existence of a defender, but without a state estimation. Node eight represents an attacker injecting fake data from the RTU. Node nine represents the Analysis Module and Monitoring System in Figure 10. Without state estimation, there is a 0.9 (90%) chance that the fake data injected cause the Analysis Module to reach an incorrect system state, and then the Monitoring System displays the incorrect system state to the system operator.

Furthermore, there is a 0.05 (5%) chance that the attack may be identified by the system operator, and the attacker's progress is pushed back to node eight. Finally, there is also a 0.05 (5%) chance that the attack stays in node eight, because the fake data has not reached the Analysis Module at node nine. The probabilities are chosen to reflect the attacker's chances of successfully carrying out a bad data injection attack in the real world. Without a state estimator, the operator would have to rely on experience and intuition in analyzing the massive amounts of data received at the control center which means the chance of detecting bad data injection is low. In Figure 9, the Markov chain representation of the attack graph assumes the existence of a defender with state estimation in node nine. In this case, the state estimator can detect and eliminate the bad data. The bad data detection of the state estimation enhances the detection capabilities of the power system, therefore, the edge from node nine to node eight has the probability P . P is a variable probability of detection which is calculated by the state estimator using Chi-square cumulative distribution function. The existence of a state estimator provides a means to mitigate the attack by attempting to prevent the attack from propagating to the next node.

For simplicity, we model the bad data injection attack propagation using a two-bus system with a generator and load as shown in Figure 15. The field measurements from each bus are polled by two separate RTUs. The attacker compromises RTU1 measurements before compromising RTU2 measurements. RTU2 also acts as a Master Terminal Unit (MTU). An MTU can be an RTU that accepts different inputs such as field measurements from several RTUs and then transmits the measurements over the network to the analysis module for computational analysis.

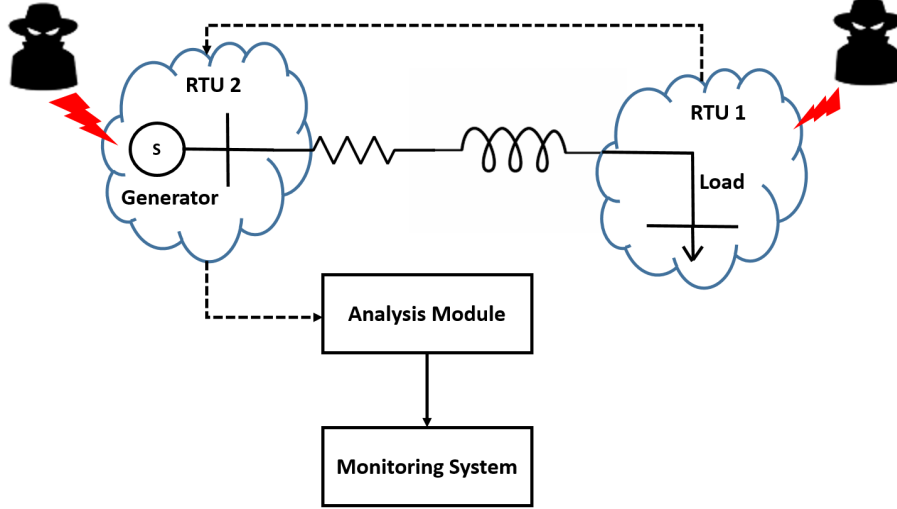


Figure 15 – Two-bus case under bad data injection attack.

The monitoring system collates the measurements by concatenating the measurements into a single measurement vector as shown in Equation (4).

$$z = [z_{RTU_1}; z_{RTU_2}] \quad (4)$$

$$z = h(x) + e \quad (5)$$

$$z = Hx + e \quad (6)$$

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \quad (7)$$

$$r = z - H\hat{x} \quad (8)$$

$$\|r = z - H\hat{x}\| \leq \tau \quad (9)$$

$$z_{attack} = z + a \quad (10)$$

$$\|z_{attack} - H\hat{x}\| \leq \tau \quad (11)$$

Using a standardized weighted least-squares state estimation model, Equation (5) shows how the various field measurements denoted by z are related to the state variables x (i.e. the voltages and phase angles) and the measurement error e . $h(\cdot)$ is a non-linear vector function expression of the measurements in terms of the state variables. Equation (6) shows the linear relationship between z , and x under DC power flow model assumptions. Equation (7) denotes the state estimates, where z is the vector of measurements, H is the measurement Jacobian matrix, R is the error covariance matrix, x , \hat{x} are the vectors of state

variables and state estimates respectively, and \mathbf{e} is the vector measurement error. The state estimates are considered valid only if the measurement residuals \mathbf{r} are less than a threshold (τ) as shown in Equation (8) and Equation (9). The threshold is set based on state estimation residual information obtained from historical data when the system is operating normally. The attacker compromises measurements in the measurement vector \mathbf{z} by changing measurement values as shown in Equation (10) thus corrupting existing legitimate measurements. For this simulation, the available measurements are taken to be

$$\mathbf{z} = \begin{bmatrix} V_1 (kV) \\ V_2 (kV) \\ P_{12}(MW) \\ Q_{12}(MVar) \\ P_2(MW) \end{bmatrix}$$

and the quantities being estimated are $\mathbf{x} = [\theta_2, V_1, V_2]$. RTU1 measurements are relayed to RTU2 which collates those measurements with its own and send the collated measurements over the backbone communication network to the monitoring center. A synthetic load profile with peak load at mid-day is adopted to drive the simulation. Equation (10) is adopted in the formulation for minimizing the weighted least squares state estimator objective function shown in Equation (12) where $h_i(\mathbf{x})$ are components of the measurement Jacobian, and R_{ii} is the diagonal matrix elements representing the standard deviation of each measurements i .

$$J(\mathbf{x}) = \sum_{i=1}^m \frac{[z_{attack,i} - h_i(\mathbf{x})]^2}{R_{ii}} = [\mathbf{z}_{attack} - \mathbf{h}(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z}_{attack} - \mathbf{h}(\mathbf{x})] \quad (12)$$

At the minimum, the first-order optimality conditions must be satisfied thus requiring the following:

$$\mathbf{g}(\mathbf{x}) = \frac{\partial J(\mathbf{x})}{\partial \mathbf{x}} = [\mathbf{H}(\mathbf{x})]^T \mathbf{R}^{-1} [\mathbf{z}_{attack} - \mathbf{h}(\mathbf{x})] \quad (13)$$

where $\mathbf{H}(\mathbf{x}) = \left[\frac{\partial h_i(\mathbf{x})}{\partial x_j} \right]$ is the measurement Jacobian. Expanding the nonlinear function $g(x)$ around a guess state vector \mathbf{x}^k and dropping the higher order of terms leads to a newton iterative solution:

$$\mathbf{x}^{k+1} = \mathbf{x}^k - [\mathbf{G}(\mathbf{x}^k)]^{-1} \mathbf{g}(\mathbf{x}^k) \quad (14)$$

It is imperative to note that the estimated state of the system would be the compromised states that do not reflect the true state of the statement as a result of the field measurements being compromised.

3.2.3 Simulation Results

As described in the previous sections, the attacker's strategy to compromise the power grid is broken down into multiple tasks that the attacker has to complete in order to reach a certain outcome. In the example attack graph shown in Figure 1, the attacker's goal is to inject bad data into the power grid, in order to fool the system operator to issue an incorrect command, which can damage the power grid itself. The attacker manipulates field measurements to be telemetered from the RTUs to the Analysis module for execution of important grid functions such as state estimation as illustrated in Figure 10. The attacker

compromises measurements from both RTUs. For detecting bad data, the Chi-squared distribution is used to identify the presence of bad data followed by the largest normalized residual test that identifies the actual measurements to be removed. The operator at the monitoring center is notified when the residual is higher than normal.

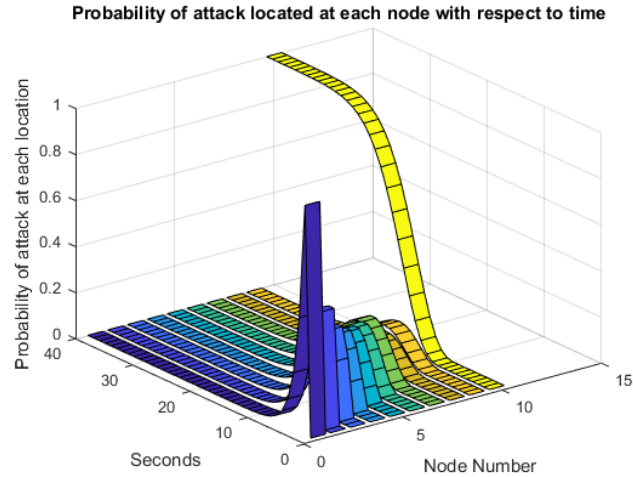


Figure 16 – Probability of an attack being located at each node with respect to time for the case assuming no defender.

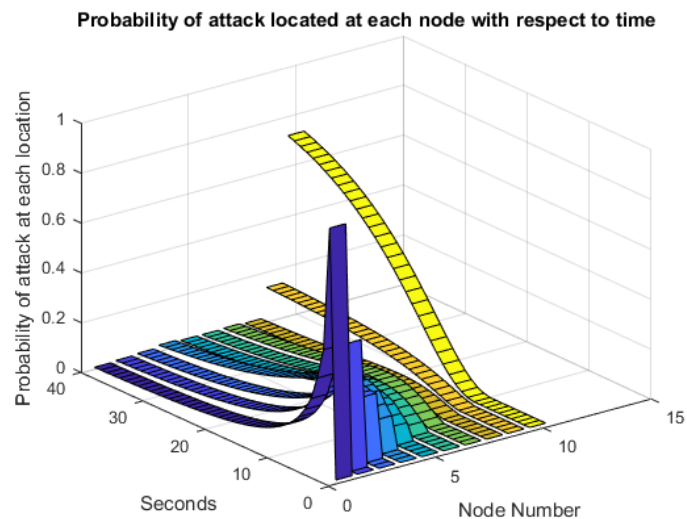


Figure 17 – Probability of an attack being located at each node with respect to time for the case assuming a defender exists, but not using state estimation.

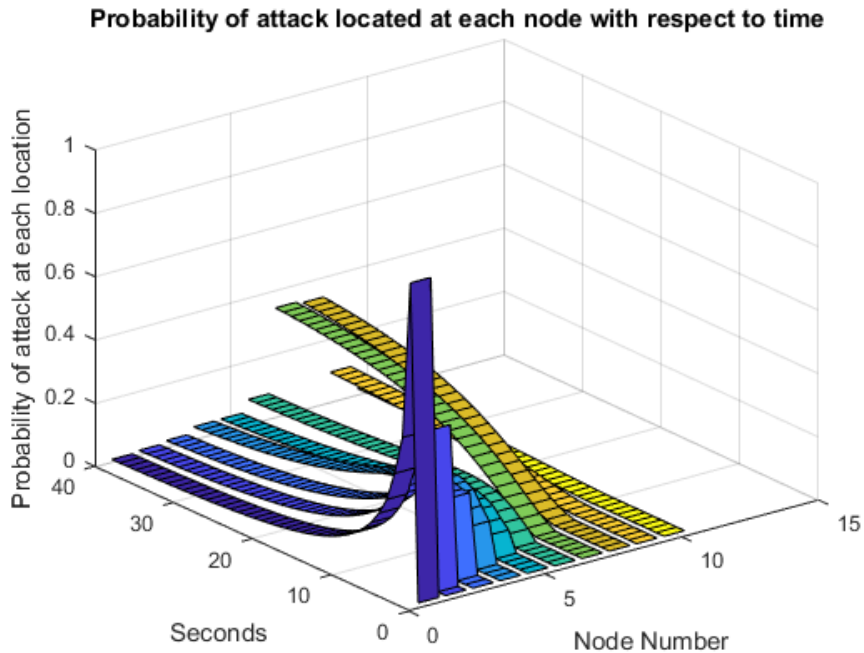


Figure 18 – Probability of an attack being located at each node with respect to time for the case assuming defender exists, and uses state estimation.

By using the Markov chain equation (1), we are able to find the probability of bad data due to attack being present at a given node for a specific time step. We present three simulation scenarios: 1) no defender, 2) with defender but no state estimation, and 3) with defender and use of state estimation.

All of the simulation cases have the attacker starting their attack at time equals to 2 seconds. In Figure 16, the simulation shows that the attack quickly propagates through nodes one through ten, and so the probability of the attack being in node ten is 1 after only a few seconds. In this case, the attack propagates all the way through with the operator being presented with the incorrect state of the system thus causing the operator to take an incorrect action. In Figure 17, the simulation shows that the attack takes longer to reach node ten, and after the simulation ends, the probability of attack reaching node ten is less

than 1. This means that with consideration of defender in the power grid, the attacker does not always reach the goal with certainty. In Figure 18, the simulation shows that the attack still propagates through nodes one through five, but due to an increase in detection capability, the probability that the attacker's attack stays at node seven and eight is very high. In this case, the state estimation provides a viable means of increasing the defender's capabilities through the bad data detection functionality of the system state estimator. As a result, it is highly unlikely that the bad data propagates all the way to the control center forcing the operator to make a decision based on inaccurate data.

3.3 Attack Model Leveraging PLADD and Markov Chain Characteristics

3.3.1 Introduction

A detailed model of an attack on the power grid involves both a preparation stage as well as an execution stage of the attack. This section introduces a novel Hybrid Attack Model (HAM) that combines Probabilistic Learning Attacker, Dynamic Defender (PLADD) model and a Markov chain model to simulate the planning and execution stages of a bad data injection attack in power grid. We discuss the advantages and limitations of the prior work models and of our proposed Hybrid Attack Model and show that HAM is more effective compared to individual PLADD or Markov chain models.

3.3.2 Hybrid Attack Model

We will first discuss the two models we combine – a Markov model and a game theoretic model – separately. Then we will explain how we combine the Markov model and the game theoretic model into a Hybrid Attack Model (HAM).

The Markov model described in Section 2.3 incorporates both attack propagation as well as state estimation with bad data detection capabilities. However, this model has several limitations. First, the serial nature of nodes does not properly reflect the possibility of completing these tasks in parallel. In general, n nodes have $n!$ orderings, and so we would prefer to have parallelism easily expressed. Second, the time frame of nodes 2 through 4 can occur over months or even up to a year, while nodes 5 through 7 should occur quickly, preferably on the same day and perhaps even in less than an hour in order to not be noticed. To consider parallelism and time more effectively, we next consider a game-theoretic approach.

3.3.2.1 Hybrid Model Characteristics

The motivation behind our proposed hybrid attack model is that while the PLADD model is good at modeling long interactions found in the planning phase between the attacker and the defender, the Markov model is a better match for the execution stage of the attack. In addition, PLADD has the capability of modeling the scenario where the attacker decides to attack all nodes in the preparation stage simultaneously. Although the Markov chain model also has the capability of modeling the scenario where the attacker attacks all preparation nodes simultaneously, the Markov chain would have a problem of state space explosion where the number of nodes in the preparation stage of an attack increases in super-linear fashion. For example, to model the scenario where three preparation nodes (called A, B and C) can be simultaneously carried out by an attacker, the Markov chain stage diagram would need to have seven states, namely, A, B, C, A&B, A&C, B&C, and A&B&C.

HAM consists of both PLADD nodes and Markov state nodes. Each PLADD node represents a single PLADD game where the attacker and defender contend to control the PLADD node. The PLADD games can be played for any period of time, although we limit the time to a year or less in the scenarios we consider in this thesis. The attacker must have the control of all PLADD nodes, which represent the preparation for an attack, to be able to execute an attack by traversing through the Markov states. The result of the PLADD simulations yields a time frame for executing an attack (i.e., for attempting to traverse the Markov states), e.g., one day or more days. Given this time frame, the execution stage must be completed in the specified time, else the attacker loses possession of the preparation items and hence loses the game. To interface the PLADD model and the Markov chain model, the number of time steps in the Markov chain model per unit time in the PLADD model must be specified by a domain expert.

A major advantage of the hybrid model in comparison to the individual PLADD model and Markov chain model is the case where the “time resolution” in the preparation stage and the execution differs significantly. For example, it may be possible that the attacker needs to run keyboard logger for months before being able to determine the correct password to a cloud system. However, once the attacker has determined the correct password, the actual attack which is to steal data from the cloud, may take less than a day to complete. The PLADD model and the Markov chain model as defined in this thesis do not have the means to run a simulation where the time-to-completion of an action for each player (attacker and defender) can be significantly different (e.g., orders of magnitude) in the preparation stage and the execution stage.

3.3.2.2 Hybrid Model Of The BDI Attack

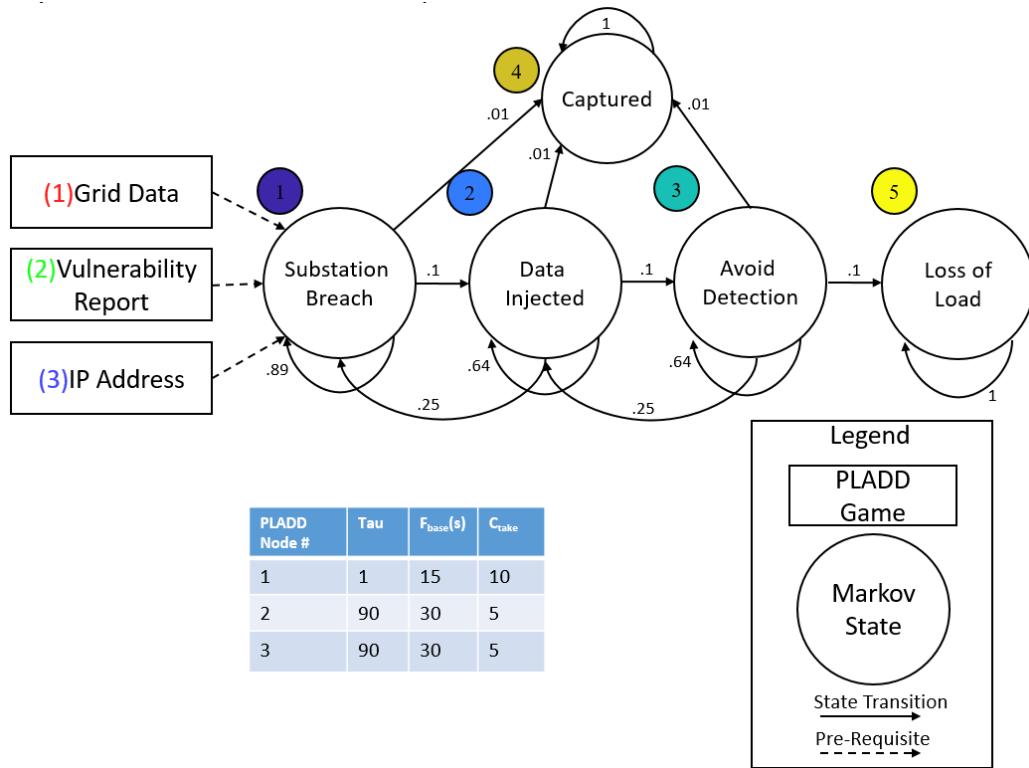


Figure 19 – Hybrid model attack graph, where the table shows the parameters used for each PLADD node.

In the scenario described in Section 2.4.1 and shown in Figure 19, the attacker/adversary needs access to RTU data, Vulnerability Report and IP address to be able to carry out a bad data injection attack on the power grid. Each of these attempts by the adversary to gain necessary information is modeled as a PLADD node. For simplicity, we assume that the RTU data is stored in a cloud drive and the adversary must run a password cracking program to gain access. We also assume that the vulnerability report is stored in a utility engineer’s computer, so the adversary must gain access by cracking the engineer’s password. Lastly, we assume that the IP address is stored in a computer located at the control center, and the adversary must gain access by password cracking. Once the

adversary has gained access to all the nodes in the preparation stage, this means the adversary is ready to execute the attack, and then the adversary immediately starts to attack the power grid by moving through the Markov states in Figure 19. Finally, to interface the PLADD model and the Markov chain model, the number of time steps in the Markov chain model occurs within a time unit specified by the PLADD model. For the bad data injection attack scenario, the PLADD model uses one day as the smallest unit of time. If we assume that each step of the Markov chain is estimated to require, on average, four hours, this would mean that six time steps in the Markov chain model would occur within a day of PLADD model. Each time step of traversal of the Markov chain is done using Equation (3).

3.3.3 *Experimental Results*

We implemented HAM for our scenario shown in Figure 19 using MATLAB. Each PLADD node requires the parameters shown in Figure 19. The parameters are nice numbers because we do not have incident reports from the power grid. With incident reports from the power grid, we can extract probability parameters by dividing the number of incidents of a certain attack by 365 days to get a probability of successful attack per day. HAM simulation starts by having the attacker attempt all PLADD nodes simultaneously on the first day. Note that attacks are not instantaneous; the time-to-successful attack is generated by using a well-known technique called Inverse Transform Sampling[37]. The purpose of inverse transform sampling is to generate pseudo-random number samplings from any probability distribution given its cumulative distribution function. For the purpose of this simulation, this pseudo-random number represents the amount of time needed to successfully take over a PLADD node as the attacker. The defender in the simulation takes the control of each PLADD node at a periodic period with respect to the

τ shown in Figure 19. Note that the defender's action to take the control of PLADD node is instantaneous.

Shown in Figure 20 are the PLADD nodes in the preparation stage. Each PLADD node can be represented as a state where "0" means the defender has the control of the node and "1" means the attacker has the control of the node. The result in Figure 20 shows that the attacker's efforts do not always provide the attacker with any benefit. For example, in Figure 20, the attacker gained control of PLADD node 2 on the 7th day and continues to hold control of PLADD node 2 until the 9th day. However, the defender was able to take back the control of PLADD node 2 on the 10th day. It is noteworthy to point out that during the time from the 7th day to 9th day, the attacker was not able to continue to do the execution stage of the attack because PLADD node 1 is still controlled by the defender for the duration of the 7th to the 9th day. Therefore, it can be concluded that the attacker may have to attack the same PLADD node multiple times before being able to carry out the actual execution of the attack on the power grid. The bottom plot in Figure 20 shows the days where the attacker is able to execute attack on the power grid because the bottom plot shows the product of all three PLADD states. Figure 21 shows the result of the hybrid model where on the left of Figure 21, the bottom plot of Figure 20 is reproduced for comparison. On the right side of Figure 21 is shown the attack propagation on Markov nodes 1-5 of Figure 4 for the duration of one attack, which happens to be one day long. As described in Section III. B, the reason that the duration of attack is one day long for the first effort to carry out the execution stage of the attack (on the 14th day) is because the defender takes back control of PLADD node 2 (the vulnerability report) on the next day (the 15th day). Figure 21 (b) also shows that at the end of the day, the probability that the

attacker has reached node 5 in Figure 4 is 32.38%, and the probability that the attacker is captured by the defender is 5.36%.

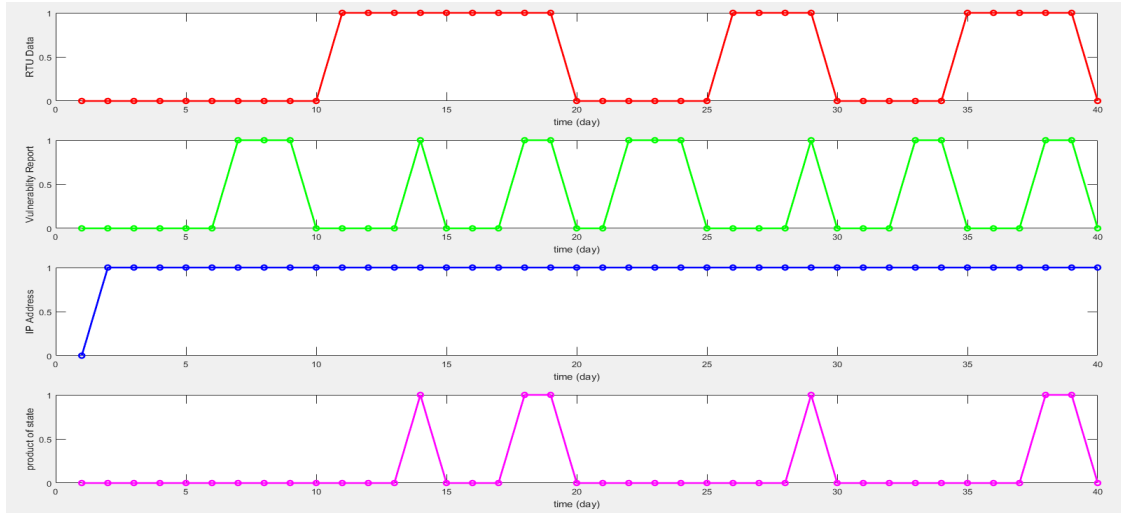


Figure 20 – State of each PLADD node with respect to time are shown from top to bottom, where the top plot represents the state of PLADD node 1 in Figure 19. The second plot from the top represents the state of PLADD node 2 in Figure 19. The third plot from the top represents the state of PLADD node 3 in Figure 19. The bottom plot represents the result of doing a logical AND on PLADD node 1-3’s state.

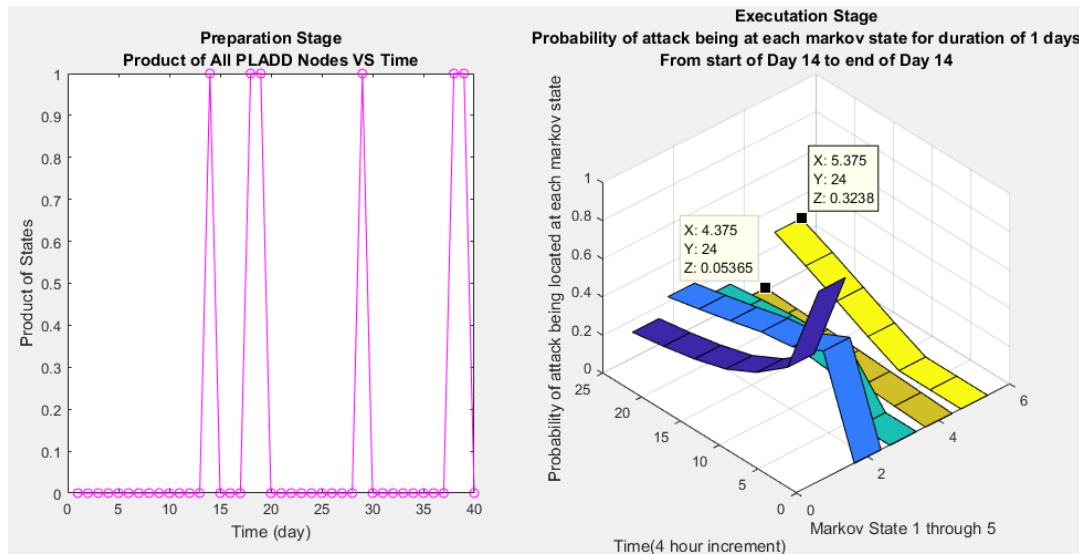


Figure 21 – (a) The preparation stage for day 1 through 40 is shown on the left. (b) The first execution stage happens on the 14th day and the corresponding attack propagation is shown on the right.

As shown in Figure 22(b), we see that because the 2nd attack allows the adversary more time to attack the power grid, the probability that the attacker has reached node 5 (which is the “load loss” node which is very bad) at the end of the attack is 63.04%, which is significantly higher than the first attack, which happened on the 14th day.

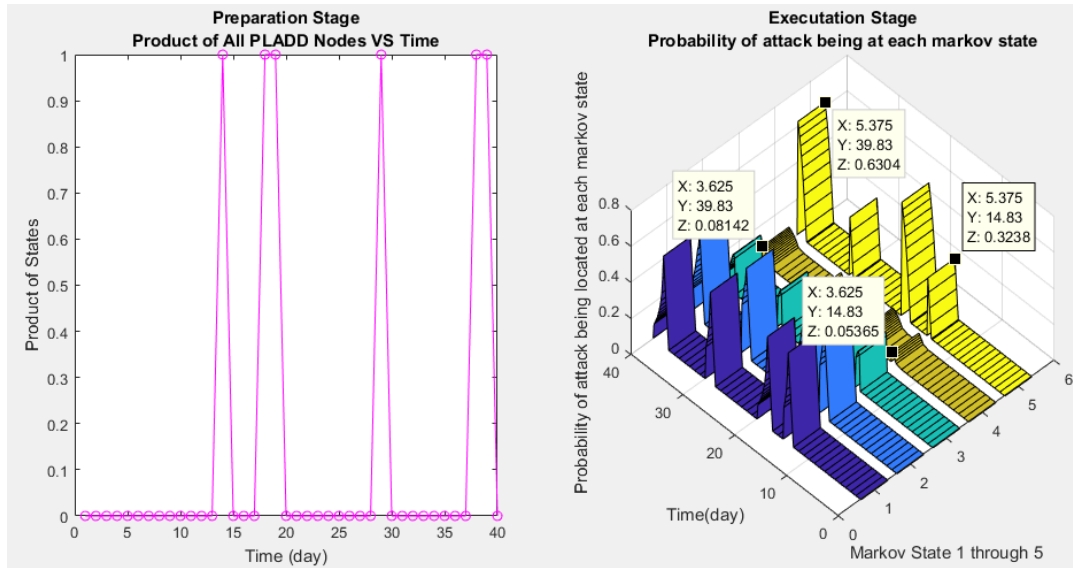


Figure 22 – (a) The preparation stage for days 1 through 40 is shown on the left. (b) On the right, the execution stage for days 1 through 40 is shown on the right. Note that attacker’s progress is reset at the end of each attack-frame.

We argue that HAM is more realistic than the Markov chain model because the hybrid model can show the attacker being forced to abandon an attack in the execution stage and restart attack in the preparation stage due to the defender taking back the control of PLADD nodes in the preparation stage.

3.3.4 Discussion

Our experimental results clearly show the advantages of the hybrid model with respect to the handling of time. Specifically, HAM can run simulations where the attacker

takes significantly longer time to prepare for an attack in comparison to the actual execution of the attack (i.e., injection of bad data).

3.3.4.1 Hybrid Model Choices For PLADD Nodes

Currently, the hybrid model assumes that during the preparation stage the adversary always starts an attack if the PLADD node is not controlled by the adversary and there is no ongoing attack on the node. Note that it is possible for the attacker to increase the probability of being in the last node (attacker goal) by strategically delaying the start of an attack on the PLADD nodes to make sure the time that the attacker owns all the PLADD nodes are maximized. In addition, the assumption that the attacker must abandon an attack because the defender takes back the control of one or more nodes in the preparation stage is an oversimplification of the problem scenario. It may be possible when the defender takes back the control of one or more nodes in the preparation stage, the attacker does not abandon the current attack, and so the attacker may then be able to temporarily pause the current attack and come back to the attack once the attacker has gained the control of all the nodes in the preparation stage again.

3.3.4.2 Hybrid Model Choices For Markov Nodes

The motivation behind HAM is to show that if the difference between the time spent in preparing for an attack is significantly longer than the time spent in executing the said attack, then the behavior of the attacker may become less straightforward than one might think. Therefore, we use PLADD to model the preparation stage and Markov chain to model the execution stage. The challenge of using a hybrid model is how to come up with a good interface between the PLADD and Markov chain model. Both PLADD and Markov

chain model have a notion of “time”, although the “time” in PLADD may not necessarily be the same “time” in the Markov chain. In order to simulate the hybrid model, we must define how many Markov chain model time-step is equivalent to a time-step in PLADD model. In the simulation result shown in Figure 21 to Figure 22, we assumed that six Markov chain model time-steps are equivalent to one time-step in PLADD model. This is because we choose preparation stage’s time-step to be equivalent to one day based on our estimate that each action in the preparation stage would need at least one day to complete, hence the smallest unit is one day. We also estimated the average time of an action in the execution stage to be four hours, which means there are six Markov chain time-step in one day. Note that using four hours to represent one time-step in execution stage may be appropriate for bad data injection attack scenario, but this is not true for all attack scenarios. Our hybrid model can be applied to model attacks such as botnets in a network, however, the appropriate time-step in the execution stage should be seconds or minutes, rather than four hours.

CHAPTER 4. MATHEMATICAL ANALYSIS OF PARALLEL PLADD SYSTEM

4.1 Introduction

As discussed in the earlier sections, the progression of cyber-attacks on the cyber-physical system is analyzed by the Probabilistic, Learning Attacker, and Dynamic Defender (PLADD) model. The PLADD model evaluates the effectiveness of moving target defense (MTD) techniques. Cyber-security managers can use the strategy introduced in this section to optimize their defense strategies. Specifically, our research provides insight into when to reset access controls (such as passwords, internet protocol addresses, and session keys), to minimize the probability of a successful attack. This work has been published in MDPI Cryptography Journal [38].

4.2 Mathematical Model Basics

In this section, we introduce mathematical model basics such as notation and definitions used throughout this manuscript. We then present a mathematical model for the attacker's probability of controlling a single PLADD game with respect to time. Next, we expand the mathematical model for a single PLADD game to model a single layer parallel PLADD system with at least two PLADD games in an AND configuration or in an OR configuration (as described in Section 4.1). Finally, we expand the single layer parallel PLADD system to a hierarchical parallel PLADD system with at least three PLADD games. With our model, a security analyst can refine the reset policy to minimize the attacker's mean probability of controlling a parallel PLADD system.

4.2.1 Notation and Definitions

The notation used in this manuscript is summarized in Table 2.

Table 2 – Notation and definition.

Notation	Definition
\mathbb{N}	Natural numbers (1, 2, 3, 4, etc.).
N	The number of PLADD games in parallel PLADD system.
k	The index of a PLADD game in parallel PLADD system; note that $1 \leq k \leq N$.
t	Time; we allow time to begin at 0 and proceed to infinity.
τ_k	The defender “take” period of a single game with index k in a parallel PLADD system.
d_k	The time of occurrence of the first defender take move in game with index k in a parallel PLADD system. A “take” move resets control to the defender.
$f_k(t)$	The probability density function of the attacker’s time-to-success in game with index k .
$F_k(t)$	The cumulative distribution function of the attacker’s time-to-success in game with index k .
n_k	The number of defender “take” moves between time $d_k + \tau_k$ and t ; in other words, the first “take” move that is counted by n_k is the “take” move at time $d_k + \tau_k$; thus, the “take” moves at times $t = 0$ and $t = d_k$ are not counted in n_k .
t'_k	The time since the last defender “take” move in a PLADD game with index k , assuming the last defender “take” move before time t occurred either at time 0 or at time $d_k + n_k\tau_k$. $t'_k = \begin{cases} t & 0 \leq t \leq d_k \\ t - d_k - n_k\tau_k & t > d_k \end{cases}$
$P_k(t)$	The probability that the attacker controls a PLADD game with index k at time t . Note that if t is at an exact time where a defender “take” move occurs (i.e., instantaneously), we define $P_k(t)$ as equal to $\lim_{t \rightarrow t^-} P_k(t)$.
$R(t)$	The probability that the attacker controls the parallel PLADD system at time t .
EPS	Expected probability of success. It is computed as shown below: $EPS = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T R(t) dt$
τ -periodic	A τ -periodic function is a function with period equal to τ .

4.2.2 Single PLADD Game

A PLADD game models a resource that an attacker and a defender contend to control. We make the following assumptions about each PLADD game:

- a) The defender executes “take” moves periodically; specifically, the defender executes “take” moves at $d_k, d_k + \tau_k, d_k + 2\tau_k, \dots, d_k + n_k\tau_k$.
- b) d_k is less than τ_k .
- c) The attacker is persistent, i.e., starts an attack at time 0 and immediately after anytime the defender takes back the resource.

The probability that the attacker controls the PLADD game with index k at time t before the first defender “take” move is given by equation (15). Since there is no defender “take” move (except at exactly d_k), the probability that the attacker controls the resource at time t is equal to the probability that the time used in a successful attack is less than or equal to t , which is the cumulative distribution function.

$$P_k(t) = F_k(t), \text{ where } t < d_k \quad (15)$$

Example 8: Consider a PLADD game k with $d_k = 5$, $\tau_k = 10$, and $\mu_k = 30$. The probability that the attacker controls the PLADD game at time 4 is calculated as shown below.

$$P_k(4) = F_k(4) = 1 - e^{-\frac{1}{30} \cdot 4} = 0.1248$$

□

To find the probability that the attacker controls the PLADD game with index k at time t , where $d_k < t < \tau_k$, we need to consider four possible cases shown in Figure 23.

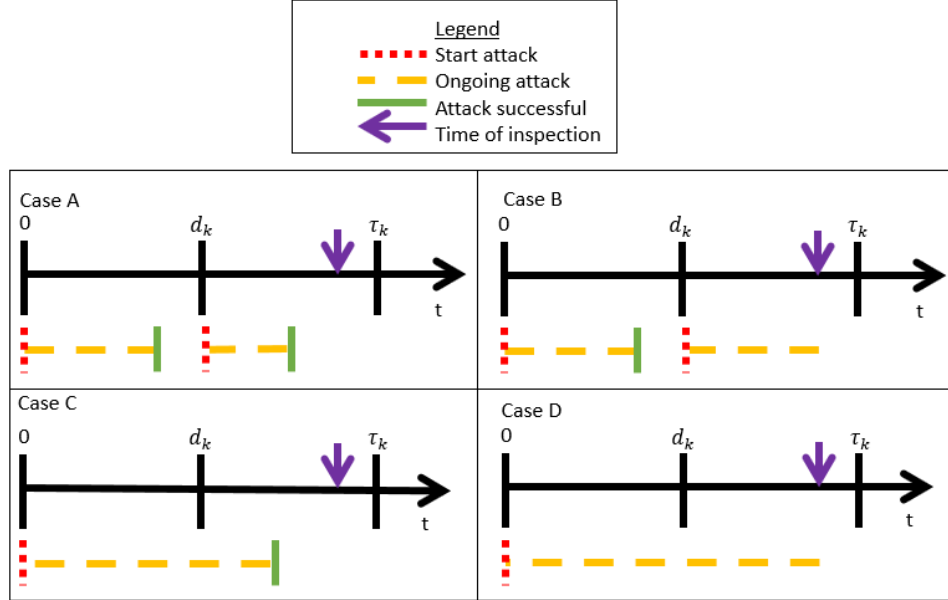


Figure 23 – Four possible outcomes of a PLADD game, where the attacker starts an attack at time $t = 0$, and the time of inspection is at time t , $d_k < t < \tau_k$.

One possible outcome is Case A in Figure 23 where the attacker’s first attack (which occurred at $t = 0$) is successful before time d_k and the attacker’s second attack is also successful before the time of inspection at time t , $d_k < t < \tau_k$. The second possible outcome is Case B in Figure 23, where the attacker’s first attack is successful before time d_k and the attacker’s second attack is ongoing (not successful) before the time of inspection at time t , $d_k < t < \tau_k$. The third possible outcome is Case C in Figure 23 where the attacker’s first attack is successful after time d_k and before the time of inspection at time t , $d_k < t < \tau_k$. Finally, the last possible outcome is Case D in Figure 23 where the attacker’s first attack is not successful before time d_k and is also not successful before the time of inspection at time $t < \tau_k$. Since we are only interested in calculating the probability

that the attacker controls the PLADD game at time t , we can disregard the cases where the attacker is not successful (attack is ongoing) at the time of inspection, which are Case B and Case D.

In Case A of Figure 23, the attacker's last attack started right after the defender's take move at d_k . In this case, the probability that the attacker controls the PLADD game is $P_k(d_k)F_k(t_k')$, which is the probability that the attacker controls the PLADD game at d_k multiplied by the probability that the time used in a successful attack is less than or equal to t_k' (recall that t_k' is the time since the last defender take move, see Table 2). In Case C of Figure 23, the attacker's last attack started at $t = 0$. In this case, the probability that the attacker controls the PLADD game is $F_k(t) - F_k(d_k)$, which is the probability that the time used in a successful attack is $(d_k, t]$. Note that Case A accounts for the probability that the attacker controls the PLADD game when the attacker's most recent attack (relative to t) is right after d_k and Case C accounts for the probability that the attacker controls the PLADD game when the attacker's most recent attack began at $t = 0$. By adding the probability that the attacker controls the PLADD game at time t in Cases A and C, the probability that the attacker controls the PLADD game with index k at time t , $d_k < t < \tau_k$, is given by (16).

$$P_k(t) = F_k(t) - F_k(d_k) + P_k(d_k) * F_k(t_k'), \text{ where } d_k < t < \tau_k \quad (16)$$

Example 9: Consider a PLADD game with index k with $d_k = 5$, $\tau_k = 10$, and $\mu_k = 30$. The probability that the attacker controls the PLADD game at time 7 is calculated as shown below.

$$\begin{aligned}
P_k(7) &= F_k(7) - F_k(5) + P_k(5) * F_k(2) \\
&= \left(1 - e^{-\frac{1}{30} * 7}\right) - \left(1 - e^{-\frac{1}{30} * 5}\right) + \left(1 - e^{-\frac{1}{30} * 5}\right) * \left(1 - e^{-\frac{1}{30} * 2}\right) \\
&= 0.0644
\end{aligned}$$

□

4.3 Overview of Major Theorems

In this section, we discuss the overall results of this paper in a summary fashion.

4.3.1 Single-Layer Parallel PLADD System

The following two theorems are proved in detail in Section 4.4.

Theorem 1. *Consider a single-layer parallel PLADD system with N games in the AND configuration where the period τ_k of defender take moves for all PLADD games are equal. The steady-state solution of the attacker's expected probability of success is minimized when the resets (i.e., take moves) of each PLADD game in the parallel PLADD system are equally spaced apart.*

Example 10: Consider two PLADD games with index "1" and "2". The two PLADD games are in the AND configuration as shown in the top half of Figure 11. We simulate three different reset patterns, which are 1) the resets of each PLADD game in the parallel PLADD system are at the same time, 2) the resets of each PLADD game in the parallel PLADD system are equally spaced apart, and 3) the resets of each PLADD game in the parallel PLADD system are at different times

but are not equally spaced apart. The expected probability of success of three of these possible reset patterns are shown in Table 3. □

Table 3 – PLADD parameters and attacker’s expected probability of success in AND configuration for Testcases 1, 2, and 3.

Testcases	d_1	d_2	τ_1	τ_2	μ_1	μ_2	EPS_{AND}
1	0	0	90	90	30	30	0.5372
2	0	45	90	90	30	30	0.4194
3	30	45	90	90	30	30	0.4236

Please note that Theorem 1 will be fully explained in Section 4.4. Our intention here is to briefly give an overview of the main theorems proven and simulated in this thesis.

Theorem 2. *Consider a single-layer parallel PLADD system in the OR configuration where the period τ_k of defender take moves for all PLADD games are equal. The steady-state solution of the attacker’s expected probability of success is minimized when the resets (i.e., take moves) of each PLADD game in the parallel PLADD system are done at the same time.*

Example 11: Consider two PLADD games with index “1” and “2” in the OR configuration as shown in the bottom half of Figure 11. We simulate three different reset patterns, which are 1) the resets of each PLADD game in the parallel PLADD system are at the same time, 2) the resets of each PLADD game in the parallel PLADD system are equally spaced apart, and 3) the resets of each PLADD game in the parallel PLADD system are at different times but are not equally spaced apart. The expected probability of success of three these possible reset patterns are shown in Table 4. □

Table 4– PLADD parameters and attacker’s expected probability of success in OR configuration for Testcases 1, 2, and 3.

Testcases	d_1	d_2	τ_1	τ_2	μ_1	μ_2	EPS_{OR}
1	0	0	90	90	30	30	0.8348
2	0	45	90	90	30	30	0.8991
3	30	45	90	90	30	30	0.8494

Note that Theorem 2 will be fully explained in Section 4.4. Our intention here is to briefly give an overview of the main theorems proven and simulated in this thesis.

Based on the results shown in Table 3 and Table 4, we see that a) the steady-state solution of the attacker’s expected probability of success is *minimized* when the resets of each PLADD game in the parallel PLADD system in the AND configuration are equally spaced apart, and b) the steady-state solution of the attacker’s expected probability of success is *minimized* when the resets of each PLADD game in the parallel PLADD system in the OR configuration are done at the same time.

4.3.2 Hierarchical parallel PLADD System

Table 5 – PLADD parameters and attacker’s expected probability of success in AND configuration for testcases 1 – 4.

Testcases	d_1	d_2	d_3	τ_1	τ_2	τ_3	μ_1	μ_2	μ_3	$EPS_{AND OR}$
1	0	0	0	90	90	90	30	30	30	0.62909
2	0	0	45	90	90	90	30	30	30	0.52004
3	0	45	0	90	90	90	30	30	30	0.63435
4	0	45	45	90	90	90	30	30	30	0.58903

A hierarchical parallel PLADD system follows the same rules as single-layer parallel PLADD system. The steady-state solution of the attacker’s expected probability of success is minimized when a) each individual subsystem (which is a single-layer parallel PLADD system) applies Theorem 1 and Theorem 2 to have minimized attacker’s expected

probability of success, and b) each upper layer also applies Theorem 1 and Theorem 2 to have minimized attacker's expected probability of success.

AND_OR

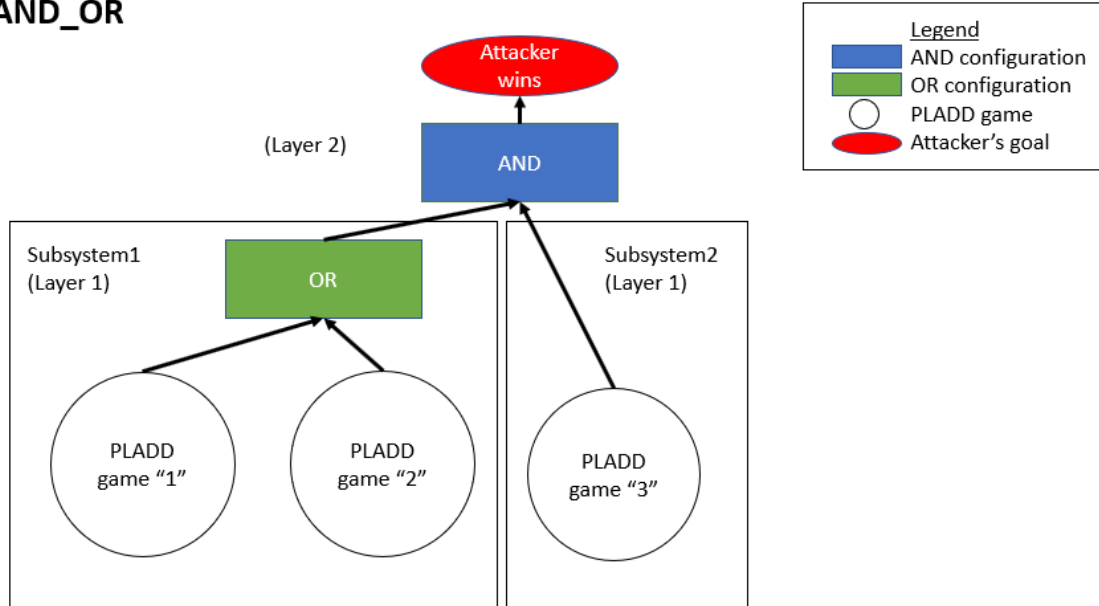


Figure 24 – A hierarchical parallel PLADD system containing three PLADD games. This configuration is labeled as AND_OR.

Example 12: Consider three PLADD games with indices “1”, “2”, and “3”. Assume the three PLADD games are in a hierarchical parallel PLADD system in an AND-OR configuration as shown in Figure 24. Let's also assume the defender's take move periods (τ) are 90 time unit and the attacker's mean time-to-successes (μ) are 30 time unit. We simulate 4 different reset patterns, which are the following:

- The resets of each PLADD game in the hierarchical parallel PLADD system are at the same time.
- The resets of each PLADD game in subsystem 1 are at the same time, and the PLADD game in subsystem 2 is offset by 45, which is $\frac{\tau}{2}$.

- The resets of each PLADD game in subsystem 1 are offset by 0 and 45, and the PLADD game in subsystem 2 is offset by 0.
- The resets of each PLADD games in subsystem 1 are offset by 0 and 45, and the PLADD game in subsystem 2 is offset by 45. □

Example 13: Consider three PLADD games with indices “1”, “2”, and “3”. Assume the three PLADD games are in a hierarchical parallel PLADD system in an OR-AND configuration as shown in Figure 25. Let’s also assume the defender’s take move periods (τ) are 90 time unit and the attacker’s mean time-to-successes (μ) are 30 time unit. We simulate 4 different reset patterns, which are the following:

- The resets of each PLADD game in the hierarchical parallel PLADD system are at the same time.
- The resets of each PLADD game in subsystem 1 are at the same time, and the PLADD game in subsystem 2 is offset by 45, which is $\frac{\tau}{2}$.
- The resets of each PLADD game in subsystem 1 are offset by 0 and 45, and the PLADD game in subsystem 2 is offset by 0.
- The resets of each PLADD game in subsystem 1 are offset by 0 and 45, and the PLADD game in subsystem 2 is offset by 45. □

Table 6 – PLADD parameters and attacker’s expected probability of success in AND configuration for testcases 1 – 4.

Testcases	d_1	d_2	d_3	τ_1	τ_2	τ_3	μ_1	μ_2	μ_3	EPS_{OR_AND}
1	0	0	0	90	90	90	30	30	30	0.77963
2	0	0	45	90	90	90	30	30	30	0.84917
3	0	45	0	90	90	90	30	30	30	0.75229
4	0	45	45	90	90	90	30	30	30	0.75229

OR_AND

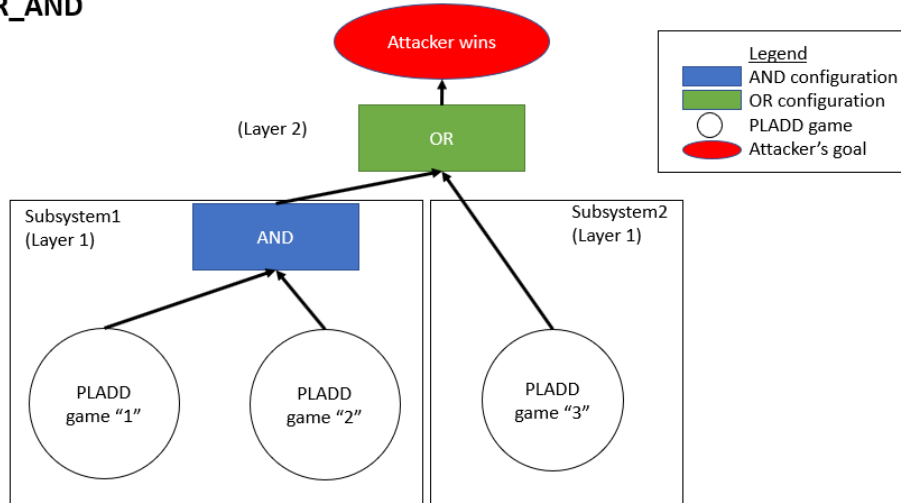


Figure 25 – A hierarchical parallel PLADD system containing three PLADD games. This configuration is labeled as OR_AND.

The simulation result for Example 12 is shown in Table 5. The simulation result for Example 13 is shown in Table 6. Based on the results shown in Table 5 and Table 6, we show that the steady-state solution of the attacker's expected probability of success is minimized when a) each individual subsystem applies Theorem 1 and Theorem 2 to minimize an attacker's expected probability of success and b) the upper layers of the hierarchical parallel PLADD system also apply Theorem 1 and Theorem 2 to minimize an attacker's expected probability of success.

4.4 Mathematical Model in Detail

In this section, we discuss the detailed mathematical proofs.

4.4.1 Single PLADD Game

Theorem 3. Consider a PLADD game labeled as index k . Given time t , $0 \leq t \leq d_k$, the probability that the attacker controls the game at time t is $F_k(t)$. For time $t > d_k$, suppose

that the last defender take move before time t was at time $d_k + n_k\tau_k$ and let t' be the time since the last defender take move. $n_k \in [0, \mathbb{N})$ and $t' \in (0, \tau_k]$ are the unique values such that $t = d_k + n_k\tau_k + t'$. Then, the probability that the attacker controls the game with index k at time t is given by Equation (17).

$$P_k(t) = F_k(t) - F_k(d_k + n_k\tau_k) \tag{17}$$

$$+ \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)(F_k(t_k' + i\tau_k) - F_k(i\tau_k))$$

Proof. For time $0 \leq t \leq d_k$, there is no defender “take” move (except at exactly d_k), and so the attacker controls the resource if and only if the initial attack at time 0 has succeeded. By definition of the cumulative distribution function, $F_k(0) = 0$. Thus, we obtain equation (18).

$$P_k(t) = F_k(t) - F_k(0) = F_k(t), 0 \leq t \leq d_k \tag{18}$$

For time $> d_k$, we proceed by considering all possible start times of the last attack before time t . By our assumptions in Section 5, the attacker starts an attack at time 0 and immediately after the defender takes back the resource. Thus, the last attack must have started at one of $0, d_k, d_k + \tau_k, \dots, d_k + n_k\tau_k$ (where $t > d_k + n_k * \tau_k$). For time $t > d_k$, there are three cases to consider, which are labeled as case A, case B, and case C below.

For case A, the start of the most recent attack (relative to t) is at time 0 and the attack is successful sometime after $d_k + n_k\tau_k$ and before time t . An illustration for case A is shown in Figure 26.

The probability that the attacker controls the PLADD game k at time t is equal to the probability that the time used in a successful attack is between $(d_k + n_k \tau_k, t]$. Equation (19) shows the probability that the time used in a successful attack is between $(d_k + n_k \tau_k, t]$. Notice that equation (19) comprises the first two terms in equation (17).

$$F_k(t) - F_k(d_k + n_k \tau_k) \tag{19}$$

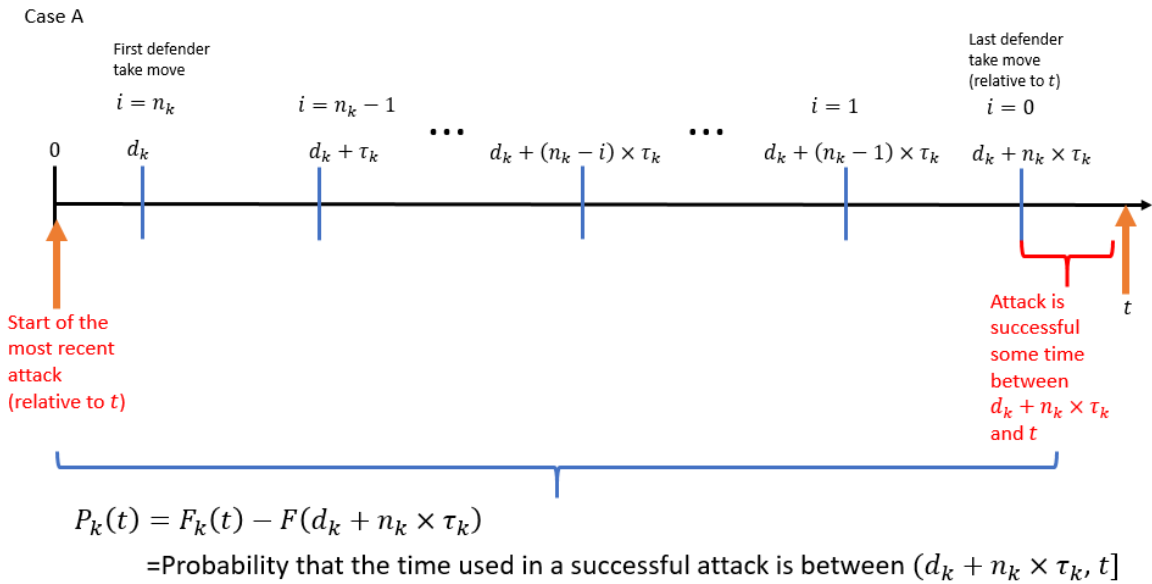


Figure 26 – Timeline of events in PLADD game k , where the start of the most recent attack (relative to t) is at time 0.

For case B, the start of the most recent attack (relative to t) is at time d_k and the attack is successful sometime after $d_k + n_k \tau_k$ and before time t . An illustration for case B is shown in Figure 27. The probability that the attacker controls the PLADD game k at time t is equal to the probability that the time used in a successful attack is between $(n_k \tau_k, t - d_k]$.

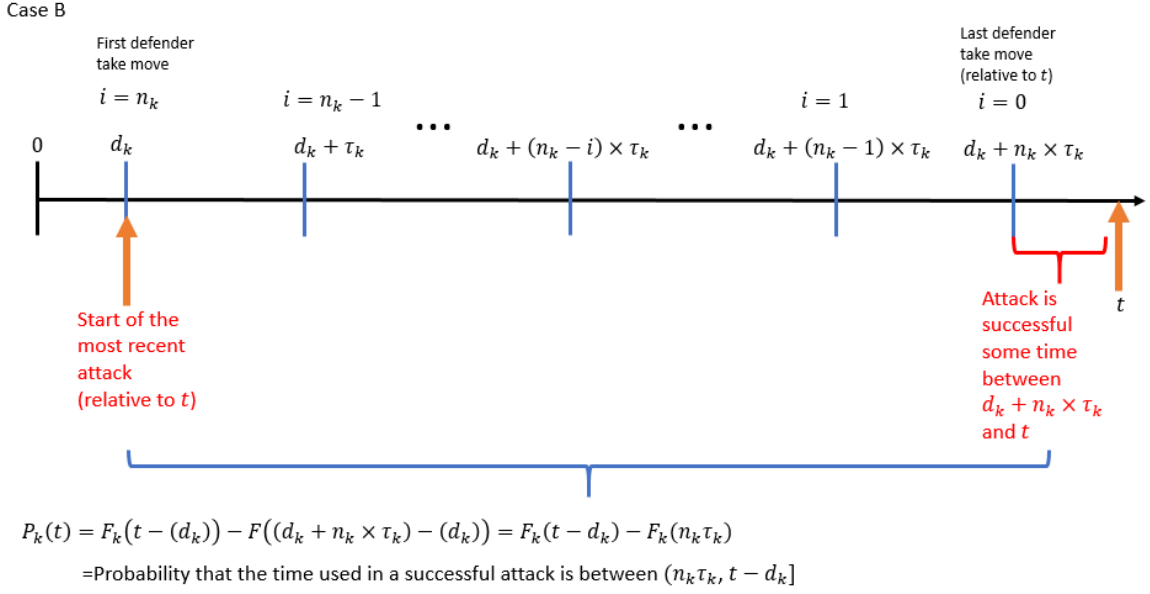


Figure 27 – Timeline of events in PLADD game k , where the start of the most recent attack (relative to t) is at time d_k .

For case C, the start of the most recent attack (relative to t) is at time $d_k + (n_k - i)\tau_k$ and the attack is successful sometime after $d_k + n_k\tau_k$ and before time t . An illustration for case C is shown in Figure 28. Note that for some $i \in \{0, 1, \dots, n_k\}$, the attacker starts an attack at time $d_k + (n_k - i)\tau_k$ if and only if the defender took the resource from the attacker at time $d_k + (n_k - i)\tau_k$. Furthermore, the defender takes back the resource from the attacker at time $d_k + (n_k - i)\tau_k$ if and only if the attacker controlled the resource at time $d_k + (n_k - i)\tau_k$, which by definition has the probability $P_k(d_k + (n_k - i)\tau_k)$. For this attack (which starts at time $d_k + (n_k - i)\tau_k$) to be the most recent attack (relative to time t), the attack must not be successful by the last defender “take” move at time $d_k + n_k\tau_k$. Additionally, for the attacker to control the resource at time t , the attack must have resolved by time t . The probability that the attacker controls the PLADD game k at time t , is equal to the probability that the time used in a successful attack is between $(i\tau_k, t - (d_k + (n_k - i)\tau_k)]$.

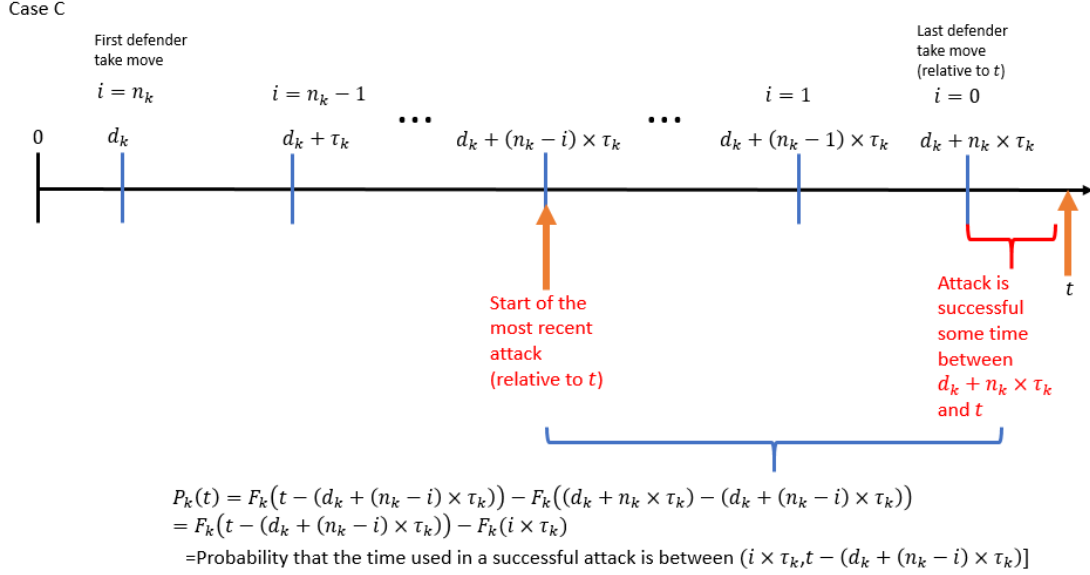


Figure 28 – Timeline of events in PLADD game k , where the start of the most recent attack (relative to t) is at time $d_k + (n_k - i)\tau_k$.

Therefore, the probability that the attacker controls the resource at time t and the last attack started at time $d_k + (n_k - i)\tau_k$ is found by accounting for the components below:

- The probability that the attacker controls the resource at time $d_k + (n_k - i)\tau_k$ (which is the time of the attacker's most recent attack relative to t).
- The probability that the time used in a successful attack is between $(i\tau_k, t - (d_k + (n_k - i) * \tau_k)]$.

Therefore, the probability that the attacker controls the resource at time t and the last attack started at time $d_k + (n_k - i)\tau_k$ is shown in equation (20). Note that equation (20) is the third term in equation (17).

$$P_k(d_k + (n_k - i)\tau_k) \times (F_k(t - (d_k + (n_k - i)\tau_k)) - F_k((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k))) = P_k(d_k + (n_k - i)\tau_k) \times (F_k(t' + i\tau_k) - F_k(i\tau_k)) \quad (20)$$

The description for equation (20) are listed below:

- $d_k + (n_k - i)\tau_k$ is the start time of the attacker's most recent attack relative to the variable t .
- $t - (d_k + (n_k - i)\tau_k)$ is the amount of time between the start time of the attacker's most recent attack relative to the variable t .
- $d_k + n_k\tau_k$ is the time of the last defender take move relative to the variable t .
- $(d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k)$ is the amount of time between the start of the attacker's most recent attack relative to the time of the last defender take move.
- $P_k(d_k + (n_k - i)\tau_k)$ is the probability that the attacker controls the resource at $d_k + (n_k - i)\tau_k$.
- $F_k(t - (d_k + (n_k - i)\tau_k))$ is the probability that the time used in a successful attack is less than or equal to $t - (d_k + (n_k - i)\tau_k)$.
- $F_k((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k))$ is the probability that the time used in a successful attack is less than or equal to $(d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k)$.
- $(F_k(t - (d_k + (n_k - i)\tau_k)) - F_k((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k)))$ is the probability that the time used in a successful attack is between $((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k), t - (d_k + (n_k - i)\tau_k)]$.

Equation (21) shows the summation of all times the previous attack could have started.

Theorem 1 is summarized in equation (21).

$$P_k = \begin{cases} F_k(t), & 0 \leq t \leq d_k \\ F_k(t) - F_k(d_k + n_k \tau_k) + \sum_{i=0}^{n_k} P_k(d_k + (n_k - i) \tau_k) (F_k(\tau'_k + i \tau_k) - F_k(i \tau_k)) & t > d_k \end{cases} \quad (21)$$

□

Next, Definition 5 defines a steady-state solution of a single PLADD game.

Definition 5. *A steady-state solution to a PLADD game with index k is a bounded function $Q_k: \mathbb{R} \rightarrow \mathbb{R}^+$ such that for all $t \in \mathbb{R}$,*

$$Q_k(t) = \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i) \tau_k) (F_k(t'_k + i \tau_k) - F_k(i \tau_k)) \quad (22)$$

where $n_k \in [0, \mathbb{N})$, $t'_k \in (0, \tau_k]$ are the unique values such that $t = d_k + n_k \tau_k + t'_k$.

The steady-state solution can be thought of as how $P_k(t)$ should behave after infinite time.

As $t \rightarrow \infty$, the first two terms in $P_k(t)$ in equation (21) approach zero. Note that $d_k + (n_k - i) \tau_k$ is at exactly the time where the defender “take” move occurs. So

$Q_k(d_k + (n_k - i) \tau_k)$ is equal to $\lim_{t \rightarrow (d_k + (n_k - i) \tau_k)^-} Q_k(t)$.

Proposition 1. *The steady-state solution of a PLADD game converges to a constant $1 \geq c \geq 0$.*

Proof. Since a steady-state solution to a PLADD game with index k is τ -periodic, the steady-state solution to a PLADD game will have the same value at all occurrences of

defender “take” move. Note that for any fixed $c \geq 0$, if we let $Q_k(d_k + (n_k - 1)\tau_k) = c$ for all $n_k \in [0, \mathbb{N})$, then equation (23) shows $Q_k(t)$ converges to a constant c .

$$\begin{aligned}
Q_k(t) &= \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)(F_k(t'_k + i\tau_k) - F_k(i\tau_k)) \\
&= \sum_{i=0}^{\infty} c \times (F_k(t'_k + i\tau_k) - F_k(i\tau_k)) \\
&= c \times \sum_{i=0}^{\infty} (F_k(t'_k + i\tau_k) - F_k(i\tau_k)) = c \lim_{t \rightarrow \infty} F_k(t) = c
\end{aligned} \tag{23}$$

Lemma 1. Consider $P_k(t)$ and $Q_k(t)$ on $(d_k + n_k\tau_k, d_k + (n_k + 1)\tau_k]$ for all $n_k \in [0, \mathbb{N})$, then both $P_k(t)$ and $Q_k(t)$ are monotonically increasing functions.

Proof. For a given $n_k \in [0, \mathbb{N})$, let $t_1, t_2 \in (d_k + n_k\tau_k, d_k + (n_k + 1)\tau_k]$ and $t_1 < t_2$. There is no defender “take” move between t_1 and t_2 . If the attacker controls the resource at time t_1 , then the attacker must also control the resource at time t_2 . Recall equation (21), if there is no defender take move between t_1 and t_2 , then $P_k(t_1) \leq P_k(t_2)$ must be true. Therefore, $P_k(t)$ is monotonic on $(d_k + n_k\tau_k, d_k + (n_k + 1)\tau_k]$.

For some $n_k \in [0, \mathbb{N})$, let $t_1, t_2 \in (d_k + n_k\tau_k, d_k + (n_k + 1)\tau_k]$ and $t_1 < t_2$. Let $t'_{k_1} = t_1 - (d_k + n_k\tau_k)$ and $t'_{k_2} = t_2 - (d_k + n_k\tau_k)$. Since F_k is a cumulative distribution function, it is monotonically increasing. In particular, for all $i \in \mathbb{N}$,

$$F_k(t'_{k_1} + i\tau_k) \leq F_k(t'_{k_2} + i\tau_k) \tag{24}$$

We arrive at equation (25) by subtracting $F_k(i\tau_k)$ from both sides of the inequality in equation (22).

$$F_k(t'_{k_1} + i\tau_k) - F_k(i\tau_k) \leq F_k(t'_{k_2} + i\tau_k) - F_k(i\tau_k) \quad (25)$$

We arrive at equation (26) by multiplying $\sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)$ to both sides of equation (23).

$$\begin{aligned} \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k) \left(F_k(t'_{k_1} + i\tau_k) - F_k(i\tau_k) \right) \\ \leq \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k) \left(F_k(t'_{k_2} + i\tau_k) - F_k(i\tau_k) \right) \end{aligned} \quad (26)$$

By Definition 5, we obtain equation (27) from equation (26).

$$Q_k(t_1) \leq Q_k(t_2) \quad (27)$$

Thus, $Q_k(t)$ is monotonic on $(d_k + n_k\tau_k, d_k + (n_k + 1)\tau_k]$ for some $n_k \in [0, \mathbb{N})$. \square

Theorem 4. Consider a PLADD game with index k where $d_k = 0$ and $F_k(T) \cong 1$ for some $T > 0$. Then as $t \rightarrow \infty$, $P_k(t)$ converges to a steady-state solution.

Proof. Recall equation (21), which is reproduced below.

$$P_k = \begin{cases} F_k(t), & 0 \leq t \leq d \\ F_k(t) - F_k(d_k + n_k \tau_k) + \\ \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)(F_k(\tau'_k + i\tau_k) - F_k(i\tau_k)), & t > d_k \end{cases} \quad (28)$$

As t approaches ∞ , n_k also approaches ∞ , because n_k is defined as the number of “take” moves before t starting at $d_k + \tau_k$.

Therefore, $F_k(t) - F_k(d_k + n_k \tau_k)$ in equation (21) approaches zero.

Equation (29) is in the form of $Q_k(t)$. By Proposition 1, $P_k(t)$ also converges to a steady-state solution.

$$\begin{aligned} \lim_{t \rightarrow \infty} P_k(t) &= \lim_{t \rightarrow \infty} \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)(F_k(t'_k + i\tau_k) - F_k(i\tau_k)) \\ &= \sum_{i=0}^{\infty} P_k(d_k + (n_k - i)\tau_k)(F_k(t'_k + i\tau_k) - F_k(i\tau_k)) \end{aligned} \quad (29)$$

□

Lemma 2. *Let $p_1(t), \dots, p_N(t): \mathbb{R} \rightarrow \mathbb{R}$ be nonnegative τ -periodic functions that are all monotonically increasing or all monotonically decreasing on $(0, \tau]$. Then the mean of equation (30) is maximized when $d_1 = d_2 = \dots = d_N$.*

$$s(t) = \prod_{k=1}^N p_k(t + d_k) \quad (30)$$

Proof. We will do a proof by contradiction. Assume that the value $s'(t)$ is achieved with values of $d_1 = d_2 = \dots = d_N = d$ where $d \in [0, \mathbb{R}^+)$, then equation (31) is the mean of $s'(t)$.

$$E(s'(t)) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \prod_{k=1}^N p_k(t+d) dt \quad (31)$$

Let $\Delta t \rightarrow 0$, and for some $i \in \{1, 2, \dots, N\}$, the value $s(t)$ is achieved with values of $d_1 = d_2 = \dots = d_{i-1} = d_{i+2} = \dots = d_N = d$. Let $d_i = d + \Delta t$ and $d_{i+1} = d - \Delta t$, then equation (32) shows the value $E(s(t))$.

$$E(s(t)) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \left(\prod_{k=1}^{i-1} p_k(t+d_k) \right) \times p_i(t+d_i) \times p_{i+1}(t+d_{i+1}) \times \left(\prod_{k=i+1}^N p_k(t+d_k) \right) dt \quad (32)$$

Let us assume $E(s'(t))$ is not optimal. Thus, a deviation such as $E(s(t)) > E(s'(t))$ is shown in equation (33).

$$\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \left[\prod_{k=1}^{i-1} p_k(t+d_k) \times p_i(t+d_i) \times p_{i+1}(t+d_{i+1}) \times \prod_{k=i+2}^N p_k(t+d_k) \right] dt > \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \left[\prod_{k=1}^N p_k(t+d_k) \right] dt \quad (33)$$

Equation (33) implies equation (34).

$$\begin{aligned} \prod_{k=1}^{i-1} p_k(t + d_k) \times p_i(t + d_i) \times p_{i+1}(t + d_{i+1}) \times \prod_{k=i+2}^N p_k(t + d_k) & \quad (34) \\ & > \prod_{k=1}^N p_k(t + d_k) \end{aligned}$$

We simplify equation (34) to obtain equation (35).

$$p_i(t + d_i) \times p_{i+1}(t + d_{i+1}) > p_i(t + d) \times p_{i+1}(t + d) \quad (35)$$

Equation (36) is obtained by substituting $d_i = d$ and $d_{i+1} = d$ into equation (35) because the right side of the inequality corresponds to $E(s'(t))$ where $d_1 = d_2 = \dots = d_N = d$.

$$p_i(t + d + \Delta t) \times p_{i+1}(t + d - \Delta t) > p_i(t + d) \times p_{i+1}(t + d) \quad (36)$$

Since $p_i(t + d_i)$ and $p_{i+1}(t + d_{i+1})$ are monotonic, and for $\Delta t \rightarrow 0$, we can expand equation (36) to obtain equation (37).

$$\begin{aligned} \left[p_i(t + d) + \Delta t \times \frac{\partial p_i(t + d)}{\partial t} \right] \times \left[p_{i+1}(t + d) - \Delta t \times \frac{\partial p_{i+1}(t + d)}{\partial t} \right] & \quad (37) \\ & > p_i(t + d) \times p_{i+1}(t + d) \end{aligned}$$

By carrying out the multiplication rearranging terms from equation (37), we obtain equation (38).

$$p_i(t + d) \times p_{i+1}(t + d) \tag{38}$$

$$\begin{aligned}
& + \Delta t \left(\left(\frac{\partial p_i(t + d)}{\partial t} \times p_{i+1}(t + d) \right) \right. \\
& \left. - \left(\frac{\partial p_{i+1}(t + d)}{\partial t} \times p_i(t + d) \right) \right) \\
& - \left(\Delta t^2 \times \frac{\partial p_i(t + d)}{\partial t} \times \frac{\partial p_{i+1}(t + d)}{\partial t} \right) \\
& > p_i(t + d) \times p_{i+1}(t + d)
\end{aligned}$$

If the probability distribution p_i and p_{i+1} are the same, then the derivative of p_i and p_{i+1} are the same.

$$\frac{\partial p_i(t + d)}{\partial t} = \frac{\partial p_{i+1}(t + d)}{\partial t} \tag{39}$$

Equation (38) can be simplified into equation (40) using equation (39).

$$- \left(\Delta t^2 \times \frac{\partial p_i(t + d)}{\partial t} \times \frac{\partial p_{i+1}(t + d)}{\partial t} \right) > 0 \tag{40}$$

Equation (40) cannot be true. We have arrived at a contradiction. Therefore, $E(s(t))$ cannot be greater than $E(s'(t))$. Thus, $E(s'(t))$ is the optimal policy. \square

Lemma 3. Let $p_1(t), \dots, p_N(t): \mathbb{R} \rightarrow \mathbb{R}$ be nonnegative τ -periodic functions that are all monotonically increasing or all monotonically decreasing on $(0, \tau]$. Then the mean of equation (41) is minimized when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$.

$$s(t) = \prod_{k=1}^N p_k(t + d_k) \quad (41)$$

Proof. We will do a proof by contradiction. Assume that the value $s'(t)$ is achieved with values of $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$, then equation (42) is the mean of $s'(t)$.

$$E(s'(t)) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \prod_{k=1}^N p_k(t + d_k) dt \quad (42)$$

Let $\Delta t \rightarrow 0$, and for some $i \in \{1, 2, \dots, N\}$, the value $s(t)$ is achieved with values of $d_1 = \frac{\tau}{N} * 0, d_2 = \frac{\tau}{N} * 1, \dots, d_{i-1} = \frac{\tau}{N} * (i - 2), \dots, d_{i+2} = \frac{\tau}{N} * (i + 1), \dots, d_N = \frac{\tau}{N} * (N - 1)$. And let $d_i = \frac{\tau}{N} * (i - 1 + \Delta t), d_{i+1} = \frac{\tau}{N} * (i - \Delta t)$ then equation (43) shows the value $E(s(t))$.

$$\begin{aligned} E(s(t)) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T & \left(\prod_{k=1}^{i-1} p_k(t + d_k) \right) \times p_i \left(t + \frac{\tau}{N} * (i - 1 + \Delta t) \right) \\ & \times p_{i+1} \left(t + \frac{\tau}{N} * (-\Delta t) \right) \times \left(\prod_{k=i+1}^N p_k(t + d_k) \right) dt \end{aligned} \quad (43)$$

Let us assume $E(s'(t))$ is not optimal. Thus, a deviation such as $E(s(t)) < E(s'(t))$ is shown in equation (44).

$$E(s(t)) < E(s'(t)) \quad (44)$$

We obtain equation (45) by substituting equation (42) and (43) into equation (44).

$$\begin{aligned} \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \left(\prod_{k=1}^{i-1} p_k(t + d_k) \right) \times p_i \left(t + \frac{\tau}{N} \times (i - 1 + \Delta t) \right) \times p_{i+1}(t) & \quad (45) \\ + \frac{\tau}{N} \times (i - \Delta t) \times \left(\prod_{k=i+1}^N p_k(t + d_k) \right) dt & \\ < \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \prod_{k=1}^N p_k(t + d_k) dt & \end{aligned}$$

Equation (45) can be simplified into equation (46).

$$\begin{aligned} p_i \left(t + \frac{\tau}{N} \times (i - 1 + \Delta t) \right) \times p_{i+1} \left(t + \frac{\tau}{N} \times (i - \Delta t) \right) & \quad (46) \\ < p_i \left(t + \frac{\tau}{N} \times (i - 1) \right) \times p_{i+1} \left(t + \frac{\tau}{N} \times i \right) & \end{aligned}$$

Since $p_i(t + d_i)$ and $p_{i+1}(t + d_{i+1})$ are monotonic, and $\Delta t \rightarrow 0$, we can expand equation (46) to obtain equation (47).

$$\begin{aligned}
& \left(p_i \left(t + \frac{\tau}{N} (i-1) \right) + \frac{\tau}{N} \times \Delta t \frac{dp_i \left(t + \frac{\tau}{N} \right)}{dt} \right) \times \left(p_{i+1} \left(t + \frac{\tau}{N} (i) \right) - \frac{\tau}{N} \Delta t \times \right. \\
& \left. \frac{dp_{i+1} \left(t + \frac{\tau}{N} \right)}{dt} \right) \\
& < p_i \left(t + \frac{\tau}{N} \times (i-1) \right) \times p_{i+1} \left(t + \frac{\tau}{N} \times i \right)
\end{aligned} \tag{47}$$

By carrying out the multiplication in equation (47), we arrive at equation (48).

$$\begin{aligned}
& \left(p_i \left(t + \frac{\tau}{N} (i-1) \right) \times p_{i+1} \left(t + \frac{\tau}{N} (i) \right) \right) \\
& - \left(p_i \left(t + \frac{\tau}{N} (i-1) \right) \times \frac{\tau}{N} \Delta t \times \frac{dp_{i+1} \left(t + \frac{\tau}{N} \right)}{dt} \right) \\
& + \left(p_{i+1} \left(t + \frac{\tau}{N} (i) \right) \times \frac{\tau}{N} \times \Delta t \frac{dp_i \left(t + \frac{\tau}{N} \right)}{dt} \right) \\
& - \left(\frac{\tau}{N} \times \Delta t \frac{dp_i \left(t + \frac{\tau}{N} \right)}{dt} \times \frac{\tau}{N} \Delta t \times \frac{dp_{i+1} \left(t + \frac{\tau}{N} \right)}{dt} \right) \\
& < p_i \left(t + \frac{\tau}{N} \times (i-1) \right) \times p_{i+1} \left(t + \frac{\tau}{N} \times i \right)
\end{aligned} \tag{48}$$

We obtain equation (49) by subtracting $p_i \left(t + \frac{\tau}{N} \times (i-1) \right) \times p_{i+1} \left(t + \frac{\tau}{N} \times (i) \right)$ on both sides of the inequality.

$$\begin{aligned}
& - \left(p_i \left(t + \frac{\tau}{N} (i-1) \right) \times \frac{\tau}{N} \Delta t \times \frac{dp_{i+1} \left(t + \frac{\tau}{N} \right)}{dt} \right) \\
& + \left(p_{i+1} \left(t + \frac{\tau}{N} (i) \right) \times \frac{\tau}{N} \times \Delta t \frac{dp_i \left(t + \frac{\tau}{N} \right)}{dt} \right) \\
& - \left(\frac{\tau}{N} \times \Delta t \frac{dp_i \left(t + \frac{\tau}{N} \right)}{dt} \times \frac{\tau}{N} \Delta t \times \frac{dp_{i+1} \left(t + \frac{\tau}{N} \right)}{dt} \right) < 0
\end{aligned} \tag{49}$$

If the probability distribution p_i and p_{i+1} are the same, then the derivative of p_i and p_{i+1} are the same.

$$\frac{\partial p_i(t+d)}{\partial t} = \frac{\partial p_{i+1}(t+d)}{\partial t} \quad (50)$$

We obtain equation (51) by substituting (50) into equation (49) and factor out $\frac{\tau}{N}\Delta t *$

$$\frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt}.$$

$$\begin{aligned} \frac{\tau}{N}\Delta t \times \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \times \left(p_{i+1}\left(t+\frac{\tau}{N}(i)\right) - p_i\left(t+\frac{\tau}{N}(i-1)\right) \right) & \quad (51) \\ - \left(\frac{\tau}{N} \times \Delta t \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \right)^2 & < 0 \end{aligned}$$

We obtain equation (52) by dividing equation (51) by $\Delta t \frac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}$.

$$\left(p_{i+1}\left(t+\frac{\tau}{N}(i)\right) - p_i\left(t+\frac{\tau}{N}(i-1)\right) \right) < \frac{\tau}{N} * \Delta t \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \quad (52)$$

Since $\Delta t \rightarrow 0$, equation (52) cannot be true. Hence, we have arrived at a contradiction.

Therefore, $E(s(t))$ cannot be less than $E(s'(t))$. Thus, $E(s'(t))$ is the optimal policy.

□

4.4.2 Parallel PLADD System

Definition 6. A parallel PLADD system consists of at least two PLADD games that start at the same time and interact simultaneously with the same attacker and defender in each

game. The attacker and defender can make moves in each game independently. If the parallel PLADD system is in the AND configuration, then the attacker is considered to control the system when the attacker controls all resources. If the parallel PLADD system is in the OR configuration, then the attacker is considered to control the system when the attacker controls at least one resource.

Definition 7. We will consider the attacker's expected probability of success (EPS) as a metric for attacker success. The attacker's EPS is the mean of $R(t)$ for $t \in [0, \infty)$. The attacker's EPS is computed as shown in equation (53).

$$\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T R(t) dt \quad (53)$$

Definition 8. The probability that the attacker controls a parallel PLADD system in the AND configuration is R_{AND} , which is computed as shown in equation (54).

$$R_{AND}(t) = P_1(t) \times P_2(t) \times \dots \times P_N(t) \quad (54)$$

Definition 9. The probability that the attacker controls a parallel PLADD system in the OR configuration is R_{OR} , which is computed as shown in equation (55).

$$R_{OR}(t) = 1 - \left((1 - P_1(t)) \times (1 - P_2(t)) \times \dots \times (1 - P_N(t)) \right) \quad (55)$$

Definition 10. The attacker's EPS for a parallel PLADD system in the AND configuration is EPS_{AND} , which is computed as shown in equation (56).

$$EPS_{AND} = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T R_{AND}(t) dt \quad (56)$$

Definition 11. *The attacker's EPS for a parallel PLADD system in the OR configuration is EPS_{OR} , which is computed as shown in equation (57).*

$$EPS_{OR} = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T R_{OR}(t) dt \quad (57)$$

Theorem 5. *Consider a parallel PLADD system in the AND configuration where $\tau_1 = \tau_2 = \dots = \tau_N = \tau$ for some $\tau > 0$. The steady-state solution of the attacker's EPS is maximized when $d_1 = d_2 = \dots = d_N$.*

Proof. Let $Q_1(t + d_1), Q_2(t + d_2), \dots, Q_N(t + d_N)$ be the steady-state solutions of the N -PLADD games. Then $Q_1(t + d_1), Q_2(t + d_2), \dots, Q_N(t + d_N)$ are τ -periodic functions that are monotonically increasing on $(0, \tau]$. The attacker's EPS when $d_1 = d_2 = \dots = d_N$ is the mean of equation (58).

$$\prod_{k=1}^N Q_k(t + d_k) \quad (58)$$

By **Lemma 2**, the attacker's EPS is maximized when $d_1 = d_2 = \dots = d_N$. \square

Theorem 6. *Consider a parallel PLADD system in the AND configuration where $\tau_1 = \tau_2 = \dots = \tau_N = \tau$ for some $\tau > 0$. The steady-state solution of the attacker's EPS is minimized when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$.*

Proof. Let $Q_1(t + d_1), Q_2(t + d_2), \dots, Q_N(t + d_N)$ be the steady-state solutions of the N -PLADD games. Then $Q_1(t + d_1), Q_2(t + d_2), \dots, Q_N(t + d_N)$ are τ -periodic functions that are monotonically increasing on $(0, \tau]$. The attacker's EPS when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$ is the mean of equation (58).

By **Lemma 3**, the attacker's EPS is minimized when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$. \square

Theorem 7. Consider a parallel PLADD system in the OR configuration where $\tau_1 = \tau_2 = \dots = \tau_N = \tau$ for some $\tau > 0$. The steady-state solution of the attacker's EPS is minimized when $d_1 = d_2 = \dots = d_N$.

Proof. Let $Q_1(t + d_1), Q_2(t + d_2), \dots, Q_N(t + d_N)$ be the steady-state solutions of the N -PLADD games. Then $1 - Q_1(t + d_1), 1 - Q_2(t + d_2) \dots, 1 - Q_N(t + d_N)$ are τ -periodic functions that are monotonically decreasing on $(0, \tau]$. The steady-state solution of the probability that the attacker does not control any resource at time t is given by equation (59).

$$\prod_{k=1}^N 1 - (Q_k(t + d_k)) \quad (59)$$

The steady-state solution of the probability that the attacker controls at least one resource at time t is given by equation (60).

$$1 - \prod_{k=1}^N 1 - (Q_k(t + d_k)) \quad (60)$$

By **Lemma 2**, the mean of equation (59) is maximized when $d_1 = d_2 = \dots = d_N$. Thus, the attacker's EPS for equation (60) is minimized when $d_1 = d_2 = \dots = d_N$.
 \square

Theorem 8. *Consider a parallel PLADD system in the OR configuration where $\tau_1 = \tau_2 = \dots = \tau_N = \tau$ for some $\tau > 0$. The steady-state solution of the attacker's EPS is maximized when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$.*

Proof. Let $Q_1(t + d_1), Q_2(t + d_2), \dots, Q_N(t + d_N)$ be the steady-state solutions of the N-PLADD games. Then $1 - Q_1(t + d_1), 1 - Q_2(t + d_2) \dots, 1 - Q_N(t + d_N)$ are τ -periodic functions that are monotonically decreasing on $(0, \tau]$. The steady-state solution of the probability that the attacker does not control any resource at time t is given by equation (59). The steady-state solution of the probability that the attacker controls at least one resource at time t is given by equation (60).

By **Lemma 3**, the mean of equation (59) is minimized when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$. Thus, the attacker's EPS for equation (60) is maximized when $d_k = \frac{\tau}{N} * (k - 1)$ for $k \in \{1, 2, \dots, N\}$. \square

4.5 Simulation Results

The implementation of a single PLADD game is shown in Figure 29. The time unit used in Figure 29 is days, but this can be switched to other time unit. Note that d_k is the offset to the defender's first take move (relative to the start of the simulation). τ_k is the

period of the defender’s take move. For the attacker, the time unit of the integer countdown is also days.

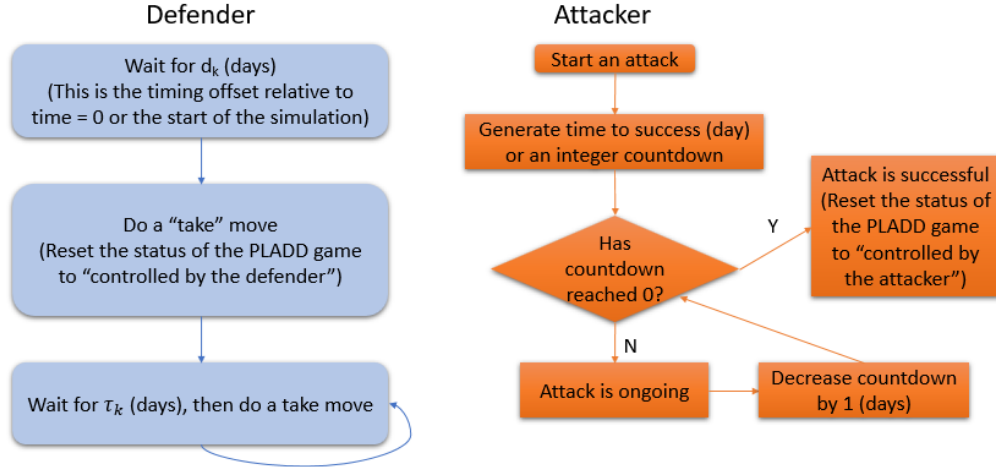


Figure 29 – Implementation of a single PLADD game.

Table 7 – Simulation of attacker’s expected probability of success.

Figure 11 AND configuration	Simulation #	Player parameters (days)	PLADD game offsets (days)	EPS	Percent improvement
	1.a	$\tau = 90,$ $\mu = 90$	$d_{RTU1}=0, d_{RTU2}=0$	0.169	33.1
	1.b		$d_{RTU1}=0, d_{RTU2}=30$	0.121	
	1.c		$d_{RTU1}=0, d_{RTU2}=45$	0.113	
	1.d		$d_{RTU1}=0, d_{RTU2}=60$	0.117	
	2.a	$\tau = 90,$ $\mu = 180$	$d_{RTU1}=0, d_{RTU2}=0$	0.059	37.3
	2.b		$d_{RTU1}=0, d_{RTU2}=30$	0.040	
	2.c		$d_{RTU1}=0, d_{RTU2}=45$	0.037	
	2.d		$d_{RTU1}=0, d_{RTU2}=60$	0.038	
	3.a	$\tau = 180,$ $\mu = 90$	$d_{RTU1}=0, d_{RTU2}=0$	0.379	30.6
	3.b		$d_{RTU1}=0, d_{RTU2}=60$	0.281	
	3.c		$d_{RTU1}=0, d_{RTU2}=90$	0.263	
	3.d		$d_{RTU1}=0, d_{RTU2}=120$	0.270	

Table 7 (Continued)

Figure 11 OR configuration	1.a	$\tau = 90,$ $\mu = 90$	$d_{\text{computer1}}=0, d_{\text{computer2}}=0$	0.567	3.57
	1.b		$d_{\text{computer1}}=0, d_{\text{computer2}}=30$	0.585	
	1.c		$d_{\text{computer1}}=0, d_{\text{computer2}}=45$	0.588	
	1.d		$d_{\text{computer1}}=0, d_{\text{computer2}}=60$	0.586	
	2.a	$\tau = 90,$ $\mu = 180$	$d_{\text{computer1}}=0, d_{\text{computer2}}=0$	0.3672	0.08
	2.b		$d_{\text{computer1}}=0, d_{\text{computer2}}=30$	0.3673	
	2.c		$d_{\text{computer1}}=0, d_{\text{computer2}}=45$	0.3675	
	2.d		$d_{\text{computer1}}=0, d_{\text{computer2}}=60$	0.3674	
	3.a	$\tau = 180,$ $\mu = 90$	$d_{\text{computer1}}=0, d_{\text{computer2}}=0$	0.749	3.10
	3.b		$d_{\text{computer1}}=0, d_{\text{computer2}}=60$	0.766	
	3.c		$d_{\text{computer1}}=0, d_{\text{computer2}}=90$	0.773	
	3.d		$d_{\text{computer1}}=0, d_{\text{computer2}}=120$	0.772	

Given the attack scenarios as described in 2.4, the attacker's goal is to open/close breakers to cause a blackout. As shown in Figure 10 and Figure 11, if the attacker attacks the RTUs, then the attacker needs to attack both RTU 1 and RTU 2 to have the ability to open/close all breakers. If the attacker attacks operator computers, then the attacker only needs to succeed in an attack on either Operator Computer 1 or Operator Computer 2.

The defender needs to decide how to schedule password resets on RTU 1, RTU 2, Operator Computer 1, and Operator Computer 2. Based on Theorem 6, assuming the password reset period for RTU 1 is equal to the password reset period for RTU 2, the defender should not reset passwords for RTU 1 and RTU 2 simultaneously. The time between the password reset of RTU 1 and the password reset of RTU 2 should equal half of the password reset period. Based on Theorem 7, assuming the password reset period for Operator Computer 1 and the password reset period for Operator Computer 2 are equal, the

defender should reset passwords for Operator Computer 1 and Operator Computer 2 simultaneously. We have simulated our example attack scenarios for 365 days. The simulation uses equations (54) and (55) to calculate the attacker’s probability of successful attack on the parallel PLADD system with respect to time. Then, we use equations (56) and (57) to calculate the attacker’s EPS for a parallel PLADD system in the AND configuration and the attacker’s EPS for a parallel PLADD system in the OR configuration. We fixed d_{RTU1} and $d_{computer1}$ to zero and varied d_{RTU2} and $d_{computer2}$ as shown in Table 7. To quantify the improvement shown in the experiment results, we define an equation for the percent improvement in equation (61).

$$\text{Percent improvement} = \frac{\text{Maximum EPS} - \text{Minimum EPS}}{\text{Maximum EPS}} * 100\% \quad (61)$$

4.5.1 Single-Layer PLADD Simulation

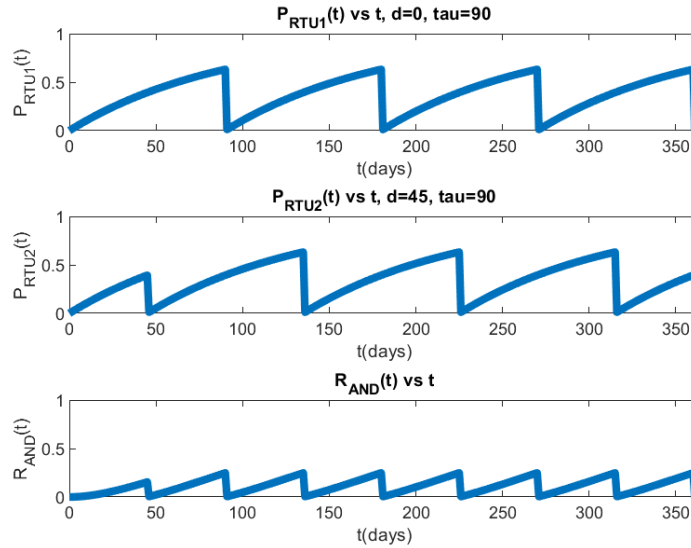


Figure 30 – Simulation 1.c: We set $d_{RTU1} = 0$, $d_{RTU2} = 45$, $\mu_{RTU1} = \mu_{RTU2} = 90$, $\tau_{RTU1} = \tau_{RTU2} = 90$.

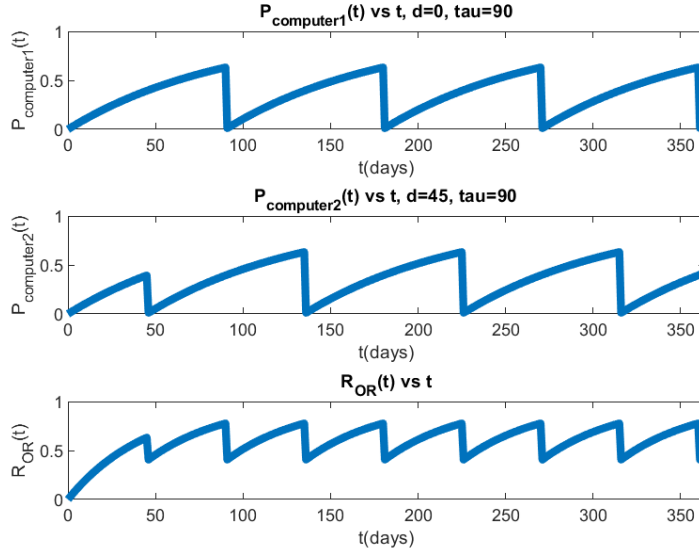


Figure 31 – Simulation 1.c: We set $d_{computer1} = 0$, $d_{computer2} = 45$, $\mu_{computer1} = \mu_{computer2} = 90$, $\tau_{computer1} = \tau_{computer2} = 90$.

For each configuration, we have simulated three different sets of player parameters. For simulations 1.a through 1.d, the defender’s take move period (τ) is 90 days, and the attacker’s mean-time-to-success (μ) is also 90 days. For simulations 2.a through 2.d, the defender’s take move period is 90 days, and the attacker’s mean-time-to-success is 180 days. For simulations 3.a through 3.d, the defender’s take move period is 180 days, and the attacker’s mean-time-to-success is 90 days. For each set of player parameters, we have simulated four different d_k (as shown in Table 7). Simulations 1.a, 2.a, and 3.a assume the defender executes “take” moves on all PLADD games with the same period simultaneously. Simulations 1.b and 2.b assume the defender executes “take” moves on all PLADD games with the same period but with an offset of 30 days between each PLADD game. Simulations 1.c and 2.c assume the defender executes “take” moves on all PLADD games with the same period, but with an offset of 45 days between each PLADD game. Simulations 1.d and 2.d assume the defender executes “take” moves on all PLADD games

with the same period, but with an offset of 60 days between each PLADD game. Simulation 3.b assumes the defender executes “take” moves on all PLADD games with the same period but with an offset of 60 days between each PLADD game. Simulation 3.c assumes the defender executes “take” moves on all PLADD games with the same period but with an offset of 90 days between each PLADD game. Simulation 3.d assumes the defender executes “take” moves on all PLADD games with the same period but with an offset of 120 days between each PLADD game. Simulations 3.b through 3.d have different offsets ($d_{Computer2}$) as compared to simulation 1.b, 1.c, and 1.d because the defender’s take move period is doubled. Therefore, PLADD game offsets ($d_{Computer2}$) in simulations 3.b through 3.d are also doubled for consistency of the experiment. We show the probability that the attacker controls the parallel PLADD system with respect to time for simulation 1.c in Figure 30 and Figure 31. As described in Section 7, equations (54) and (55) are used to plot R_{AND} and R_{OR} in Figure 30 and Figure 31.

4.5.2 Hierarchical PLADD Simulation

The hierarchical PLADD simulations are shown in Table 8, and illustrations of the OR_AND_AND and AND_OR_OR configuration are shown in Figure 13 and Figure 14. We have simulated our example attack scenarios with 11 different sets of d_k (as shown in Table 8). Simulation 1 assumes the defender executes “take” moves on all PLADD games with the same period simultaneously. Simulation 2 assumes the defender in Subsystem 2 executes “take” moves on all PLADD games with an offset of 45 days. Simulation 3 assumes the defender executes “take” moves on all PLADD games with an offset of 22.5 days between each PLADD game. Simulation 4 assumes all PLADD games have the same

offset, except PLADD game 2 has an offset of 22.5 days. Simulation 5 assumes all PLADD games have the same offset, except PLADD game 2 has an offset of 45 days. Simulation 6 assumes PLADD games 1 and 3 have offset equal to zero, while PLADD games 2 and 4 have offset equal to 45 days. Simulation 7 assumes PLADD games 1, 2, 3, and 4 have offset equal to 0, 45, 9, and 54, respectively. Simulation 8 assumes PLADD game 1 and 4 have the same offset, while PLADD game 2 has an offset of 45 days and PLADD game 3 has an offset of 22.5 days. Simulation 9 assumes PLADD games 1 and 4 have offset equal to zero, while PLADD games 2 and 3 have an offset of 45 days. Simulation 10 assumes PLADD game 1 has an offset of zero, PLADD game 2 and 3 have an offset of 45 days, and PLADD game 4 has an offset of 22.5 days. Finally, simulation 11 assumes PLADD game 1 has an offset of zero, while the other PLADD games have an offset of 45 days. Using equation (61), the percent improvement in OR_AND_AND configuration is 19.4%, and the percent improvement in AND_OR_OR configuration is 18.4%.

Table 8 – Hierarchical PLADD simulation of attacker’s expected probability of success, where the period of the defender’s take move (τ) is 90 days and the attacker’s mean-time-to-success (μ) is 30 days.

Simulation	Subsystem 1		Subsystem 2		$EPS_{OR_AND_AND}$	$EPS_{AND_OR_OR}$
	d_1	d_2	d_3	d_4		
1	0	0	0	0	0.696	0.751
2	0	0	45	45	0.814	0.695
3	0	22.5	45	67.5	0.743	0.806
4	0	22.5	0	0	0.687	0.761
5	0	45	0	0	0.712	0.781
6	0	45	0	45	0.656	0.852
7	0	45	9	54	0.688	0.844
8	0	45	22.5	0	0.679	0.834
9	0	45	45	0	0.656	0.852
10	0	45	45	22.5	0.699	0.823
11	0	45	45	45	0.712	0.781

4.6 Discussion

Based on Table 7, EPS_{AND} is the largest when the password reset of RTU1 and RTU 2 is done simultaneously. EPS_{AND} is the smallest when RTU1's password reset and RTU's password reset are equally spaced apart. EPS_{OR} is the smallest when the password resets of Operator Computer 1 and Operator Computer 2 are done simultaneously. EPS_{OR} is the largest when RTU 1's password reset and RTU 2's password reset are equally spaced apart on the interval τ (the period of the password resets). For both AND configuration and OR configuration, the experimental results show that it is possible to decrease the attacker's expected probability of success by making sure the defender's take moves occur with respect to the aforementioned method. However, the percent improvement in the AND configuration is around 30%, while the percent improvement for the OR configuration is around 3% or less. It is noteworthy that a shift in the reset schedule is typically cheaper than other mitigations.

Based on the attacker's EPS in Table 8, we show that the hierarchical parallel PLADD system also follows the same rules proved in Theorems 5 - 8. Let's represent Subsystem 1's offsets (d_1 and d_2) as tuple α and Subsystem 2's offset (d_3 and d_4) as tuple β . The EPS of hierarchical parallel PLADD system is minimized when i) the individual subsystems applies Theorems 6 and 7 to minimize EPS and ii) tuple α and tuple β minimized also applies Theorems 6 and 7 to minimize EPS. Therefore, $EPS_{OR_AND_AND}$ is minimized when i) the resets of Subsystem 1 are equally spaced apart (e.g., $d_1 = 0$, $d_2 = 45$), ii) the resets of Subsystem 2 are equally spaced apart (e.g., $d_3 = 45$, $d_4 = 0$), and iii) tuple α and tuple β are equal (e.g., $\alpha = \beta = (d_1 = 0, d_2 = 45) =$

($d_3 = 0, d_4 = 45$). The $EPS_{AND_OR_OR}$ is minimized when i) the resets of Subsystem 1 are at the same time (e.g., $d_1 = 0, d_2 = 0$), ii) the resets of Subsystem 2 are at the same time (e.g., $d_3 = 45, d_4 = 45$), and iii) tuples α and β are equally spaced apart (e.g., $\alpha = (d_1 = 0, d_2 = 0)$ and $\beta = (d_3 = 45, d_4 = 45)$).

Security analysts may use the proofs this paper to provide insights and refine reset policies in a system that is protected by multiple resources. Although we have provided a way to decrease the attacker's expected probability of success in the OR configuration, our OR configuration result shows that the mitigations are relatively small compared to the AND configuration. Therefore, if possible, the security analysts should adjust their system such that attack scenarios do not have OR configuration. Finally, suppose a cyber-physical system is in the AND configuration. In that case, the defender should reset the MTD's secret information equally spaced apart within the time frame of a single reset period. If a cyber-physical system is in the OR configuration, the defender should reset the MTD's secret information simultaneously.

CHAPTER 5. ATTACK MODEL DRIVEN MITIGATION STRATEGIES

In this chapter, a novel risk assessment method that combines simulations of cyber-attack models and the potential physical impact on the power infrastructure is described. The proposed method assesses the risk of physical operational disruption caused by propagating cyber-attacks, and then recommends mitigating solutions.

5.1 Risk Assessment

Unlike the prior risk assessment work such as $N-1$ discussed in Section II, our risk assessment of the power grid is specific to the attacker's goal. An example attacker's goal could be to overload a particular transmission line with the intent of activating power relays that would disconnect the line and cause loss of load. In order to create a risk assessment tool that incorporates a realistic grid response to an attack, we have integrated power flow analysis with the hybrid attack model.

We use a simplified DC power flow model as shown in Equation (62).

$$\theta = [B']^{-1}P_{injection} \quad (62)$$

where B' is the reduced susceptance matrix describing the topology and parameters of the power grid, θ is the bus voltage angle with respect to the system reference (slack) bus, and $P_{injection}$ is the vector of bus power injections at a given point in time. A positive entry in the $P_{injection}$ vector represents power produced by a generator, and a negative value

corresponds to the power consumed by a load at that bus. The flow of active power on a given transmission line between buses j and k is

$$P_{jk} = B_{jk}(\theta_j - \theta_k) \quad (63)$$

where B_{jk} is the value in susceptance matrix B' located at row k and column j . θ_k and θ_j are the angle of active power at bus k and bus j respectively.

We note that depending on the topology of the system, the disconnection of one or more lines can cause loss of load at more than one substation, e.g. substations have a radial topology from generation to loads, where the loads are downstream with respect to the attacked substation.

As described in Section 3.3.2, the hybrid attack model combines the advantages of the PLADD model's timing information to improve the Markov model's ability to assess the security risk against a specific attack. In this thesis, we evaluate the risk of each substation against a specific attack. Similar to the prior work [39] [40] on risk assessment described in Section 2.5, we define risk as the probability of successful attack multiplied by the severity of the damage. The probability of a successful attack (P) is calculated as shown in Equation (64).

$$P = \frac{\textit{Number of days the attacker has the ability to open breakers}}{\textit{Number of days in the simulation}} \quad (64)$$

It is noteworthy to point out that prior work on risk assessment requires a domain expert to input the severity. There are many ways to evaluate the severity of a successful

attack. In this thesis, we present two straightforward ways to calculate severity: 1) use the percentage of power loss to represent the severity of the damage and 2) use the actual load loss in MW. The severity equations for 1) and 2) are shown in Equation (65) and Equation (66) respectively.

$$Severity = \frac{Load\ loss\ (MW)}{Total\ load\ in\ the\ grid\ (MW)} \quad (65)$$

$$Severity = Load\ loss\ (MW) \quad (66)$$

The equation to calculate risk is shown in Equation (67).

$$Risk = P * Severity \quad (67)$$

5.2 4-bus Risk Assessment

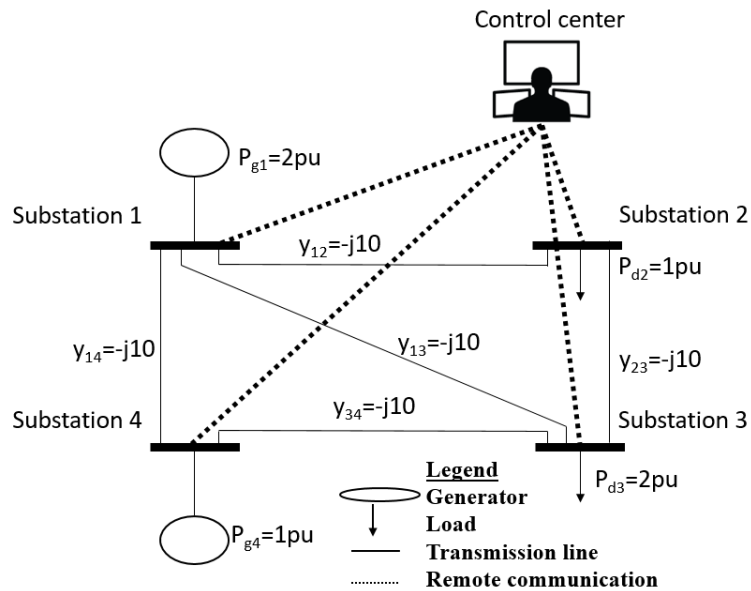


Figure 32 – Four-bus power grid system.

substation. We assume the attacker requires access to a “Vulnerability Report,” “RTU credentials” and “IP address of the RTU.” The Vulnerability Report represents a set of relevant information about the system that is important in order to implement the attack. The Vulnerability Report consists of other information regarding items such as (1) equipment type and/or design, (2) criticality of load, and (3) number and/or types of customers. We assume the Vulnerability Report for the entire power grid is stored on a utility engineer’s computer. We further assume that the attacker will need to run password cracking software to gain access to the vulnerability report. The attacker may use a brute force or phishing attack on each RTU to gain control. Each RTU is assumed to have different login credentials, so if an attacker gains access to one RTU does not mean the attacker has access to all other similar RTUs. We also assume the attacker does not want the control center to remotely control a substation that is under the attacker’s control. Therefore, the attacker would execute Address Resolution Protocol (ARP) cache poisoning [41] or a similar technique in order to prevent communication between the control center and the substation. After the attacker has gathered the necessary information, the attacker executes the attack by the following steps: (1) breaching the substation room’s locked door, (2) accessing the RTU, (3) disabling communication between the substation and control center, and (4) opening breaker(s) of transmission lines at a substation. We also assume that multiple substations can be attacked simultaneously, given that the attacker has all the necessary information. In our attack scenario, we assume the attacker’s goal is to maximize the loss of power to customers in the grid. The attacker can attack any of the four substations shown in Figure 32. In addition, we also consider the scenario where the

attacker knows that Substation 1 and Substation 4 generate power in the power grid, and the attacker decides to cause a blackout for the entire four-bus grid.

5.2.1 Experiment Results

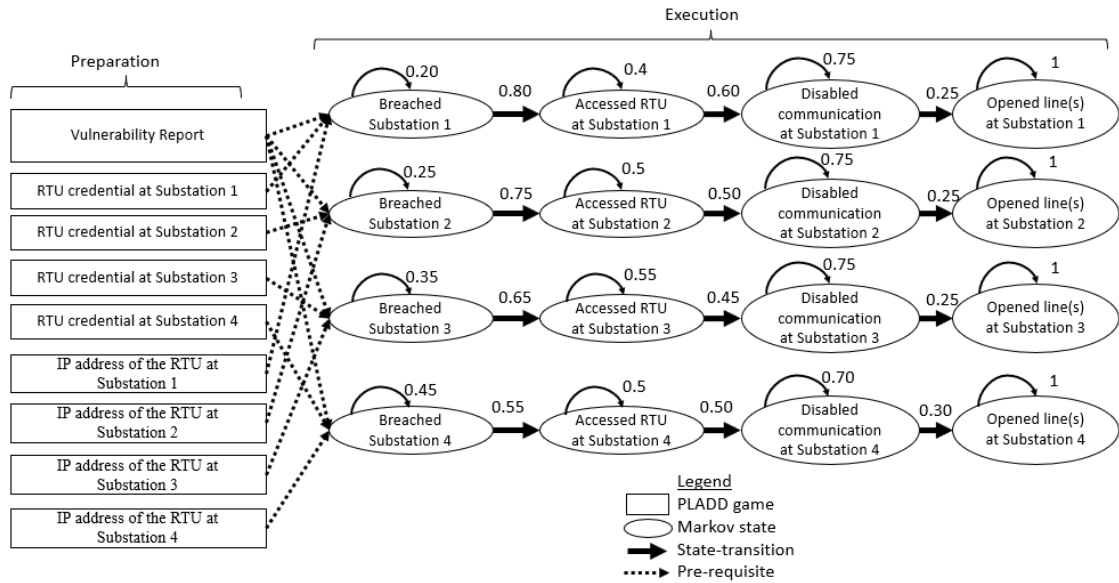


Figure 34 – Hybrid attack model for the four-bus system.

Table 9 – PLADD parameters used to model the four-bus system.

PLADD game type	τ (day)	μ (day)
Vulnerability report	180	90
RTU credentials at Substation 1, Substation 2 and Substation 3	90	45
IP addresses of the RTU at Substation 1, Substation 2 and Substation 3	360	180
RTU credential at Substation 4	45	45
IP address of the RTU at Substation 4	180	180

As described in Section 2.2, each PLADD game is modeled by two parameters, τ and $f_{base}(t)$, where τ is the defender's period to periodically execute a take move and $f_{base}(t)$ is the probability density function describing the attacker's time-to-success of an attack. Our experiments assume $f_{base}(t)$ is an exponential distribution, so $f_{base}(t) = \frac{1}{\mu} e^{-\frac{t}{\mu}}$ where μ is the average. Therefore, instead of using τ and $f_{base}(t)$ to model a PLADD game, we will be using τ and μ to model a PLADD game. Figure 34 shows the hybrid attack model of the four-bus system. The probability of transitioning from one state to the next is shown on the state transition edges in Figure 34. Once the attacker has gathered all the necessary information in the preparation stage, the attacker will move forward by attacking the power grid. In the execution stage, we assume the attacker will (1) breach the substation fences, (2) access the RTU at the substation, (3) disable communication at the substation, and (4) open line(s) at the substation. For simplicity, we assume the attacker is making six state transitions in Figure 34 per day. Our risk assessment tool can change the number of transitions per day by changing a single input parameter. The PLADD parameters used to model the four-bus system are shown in Table 9.

With regards to Table 9, the vulnerability report is changed every 180 days (approximately six months). The average time-to-success of the attacker's password cracking software is 90 days (approximately three months). The RTU credentials at Substation 1, Substation 2, and Substation 3 are changed every 90 days. For Substation 4, we assume the RTU is a newer model as compared to other substations, which allows the operator to change the login credentials every 45 days. The average time-to-success of the attacker's brute force attack on the RTUs in Substation 1, Substation 2, Substation 3, and Substation 4 is 45 days. The IP addresses of the RTUs at Substation 1, Substation 2, and

Substation 3 are changed every 360 days. For Substation 4, we assume the RTU is a newer model as compared to other substations, which allows the operator to change the login credentials every 180 days. We assume the attacker needs to analyze network packets to figure out the IP addresses of RTUs. Therefore, the average time required to figure out the IP address of an RTU from analyzing network packets is 180 days.

Our experiment is implemented in Matlab. In our experiment, we simulate an attack using the hybrid attack model and calculate the probability of success using Equation (64). When an attack is successful against a substation, the attacker disconnects the transmission line(s) connected to the substation. Next, we use the DC power flow analysis to calculate the power on each transmission line and at each substation after a successful attack from the attacker. As a result, we calculate the loss of power due to a successful attack. Using the four-bus power grid system as shown in Figure 32 as our example scenario, we have implemented five test cases for comparison of risk. Note that when we say “line₁₂”, it means line between Substation 1 and Substation 2. A quick description of each test case is shown below:

- Test case 0: Normal power grid operation (base case).
- Test case 1: Attacker attempts to disconnect Substation 1 from the grid, which forces the operator to shed 2 pu load between Substation 2 and Substation 3.
- Test case 2: Attacker attempts to disconnect line₁₂ and line₂₃, which disconnects Substation 2 and causes a power loss of 1 pu.
- Test case 3: Attacker attempts to disconnect line₁₃, line₂₃, and line₃₄, which disconnects Substation 3 and which causes a power loss of 2 pu.

- Test case 4: Attacker attempts to disconnect line₁₄ and line₃₄, which disconnects Substation 4 and forces the operator to shed 1 pu load between Substation 2 and Substation 3.
- Test case 5: Attacker attacks Substation 1 and Substation 4 to cause blackouts at Substation 2 and Substation 3.

Table 10 – The severity of damage for each test cases

Test cases	Severity (percentage of power loss)
1	0.66
2	0.33
3	1
4	0.33
5	1

Table 11 – DC power flow parameters

Test case	y ₁₂	y ₁₃	y ₁₄	y ₂₃	y ₃₄	P ₁	P ₂	P ₃	P ₄
0	10	10	10	10	10	2	-1	-2	1
1	0	0	0	10	10	2	-1	-2	1
2	0	10	10	0	10	2	-1	-2	1
3	10	10	10	10	0	2	-1	-2	1
4	10	10	0	10	0	2	-1	-2	1
5	0	0	10	10	0	2	-1	-2	1

Table 12 – Risk calculations of test case 1-5

Test case	Number of successful attacks in simulation	Total number of days in simulation	Probability of successful attack	Severity (Percentage of power loss)	Risk
1	164	720	0.2278	0.66	0.1503
2	217	720	0.3014	0.33	0.0995
3	272	720	0.3778	1.00	0.3778
4	49	720	0.0681	0.33	0.0225
5	40	720	0.0556	1.00	0.0556

Next, we use the DC power flow analysis to calculate the loss of power as a result of a successful attack from the attacker. The severity of each test cases are shown in

Table 10. The DC power flow parameters are shown in Table 11. The symbol y is admittance, so y_{12} is the admittance between bus 1 and bus 2 of the four-bus power grid system in Figure 32.

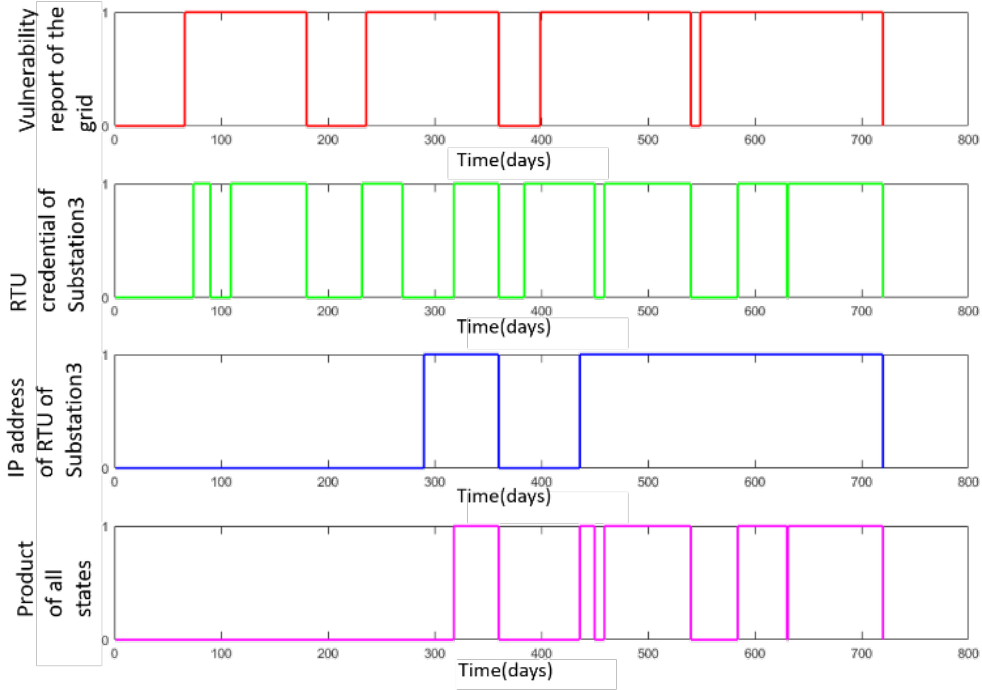


Figure 35 – A hybrid attack model simulating an attack on Substation 3.

The risk calculation of test cases 1-5 are shown in Table 12. The simulation covers calendar time of for 720 days (or approximately two years) with the result that Substation 3 has the highest risk and Substation 4 has the lowest risk (the clock time taken by our simulator is less than an hour). Figure 35 through Figure 37 show the simulation results of the hybrid attack model. Figure 35 shows simulation results of the hybrid attack model for attacking Substation 3. Figure 36 shows simulation results of the hybrid attack model for attacking Substation 4. Figure 37 shows simulation results of the hybrid attack model for attacking Substation 1 and Substation 4. Each PLADD game is represented as a state where

“0” means the defender has control of the node and “1” means the attacker has control of the node. The top three plots in each of Figure 35 through Figure 37 show the state of each PLADD game with respect to time, and the bottom subplot in each shows the product of all PLADD game states with respect to time. The product of all PLADD game states is calculated by multiplying the state of each PLADD game. When the product of all PLADD game states is equal to 1, the attacker has all the necessary information to execute an attack on the grid. By comparing the product of all PLADD states in Figure 36 and Figure 37, we can see that the attacker is spending less time in the execution stage when the attacker is attacking Substation 4. This is an expected result because we assumed the RTU at Substation 4 is a newer model as compared to the RTUs at Substation 1, Substation 2, and Substation 3. The operator can reset the RTU’s password and IP address at Substation 4 at a faster pace. By comparing the product of all PLADD states in Figure 35 and Figure 36 against Figure 37, we can see that it is more difficult to attack two substations instead of one substation.

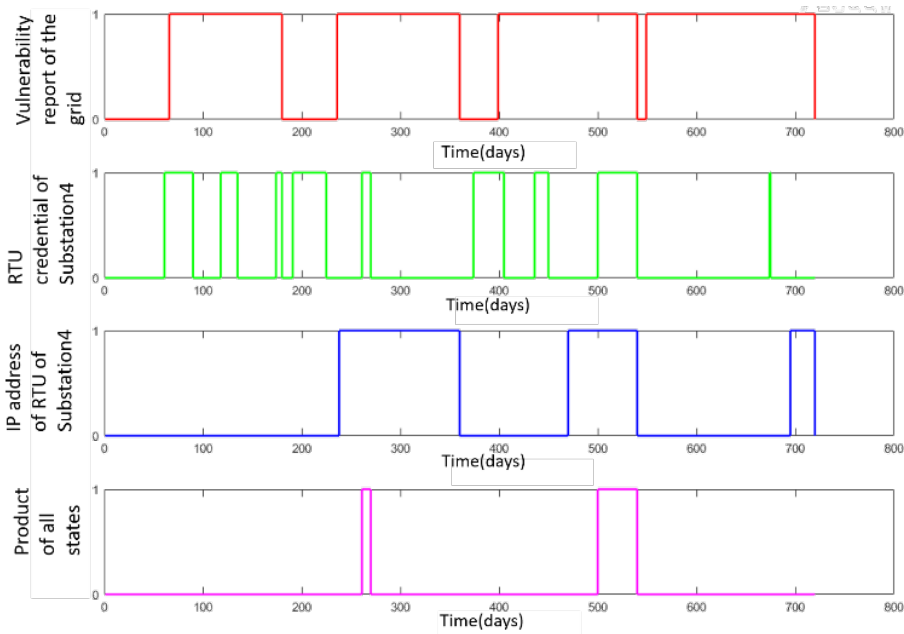


Figure 36 – A hybrid attack model simulating an attack on Substation 4.

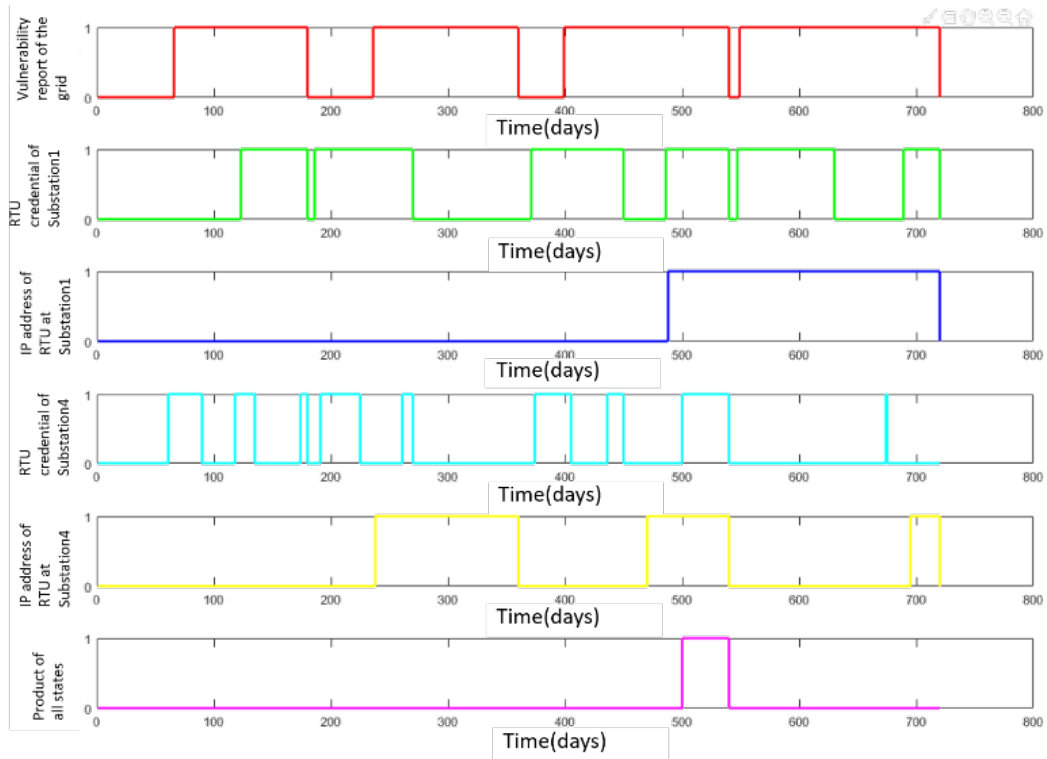


Figure 37 – A hybrid attack model simulating an attack on Substation 1 and Substation 4 simultaneously.

The risk calculation in Table 12 provides a way to compare (1) the probability of success of different attacks, (2) risk of individual substations, and (3) the risk of a combination of substations. Intuitively, since the parameters used to model Substation 1, Substation 2, and Substation 3 are the same, the probability of success for attacking Substation 1, Substation 2 and Substation 3 should be the same. However, as described in Section 2.2, the attacker’s time-to-successful attack is based on an exponential distribution function. The exponential distribution function is used as an input to a pseudo-random sampling technique called inverse transform sampling [37]. The inverse transform sampling technique generates pseudo-random numbers following an exponential distribution. The random number generation is the reason that the probability of a successful attack on Substation 1, Substation 2, and Substation 3 are different, even though

the PLADD parameters used to model Substation 1, Substation 2, and Substation 3 are the same. By comparing test case 1, test case 2, and test case 3, we can see that the risk of test case 3 is the highest and the risk of test case 2 is the lowest, which reflects the severity of each attack. By comparing test case 1 (attack on Substation 1) and test case 4 (attack on Substation 4) with test case 5 (attack on both Substation 1 and Substation 4), we can see that the probability of success for simultaneously attacking Substation 1 and Substation 4 is less than the probability of success for attacking Substation 1 and Substation 4 independently. Therefore, even though the severity of test case 5 is higher than test case 1 and test case 4, the risk of test case 5 is less than test case 1 and test case 4. In addition, due to the assumption that Substation 4 has a newer RTU model, the probability of a successful attack on Substation 4 is lower than the other substations. Of course, in a practical application of the approach proposed in this thesis, many additional test cases beyond the five explained here would need to be carried out to provide proper coverage of the attack surface, and such coverage invariably relies on expert domain knowledge. With the information in Table 12, security analysts can relate a risk value to the percentage of power loss after a successful attack on a substation. For example, the damage associated with test case 1's risk is load shedding of 2 pu between Substation 2 and Substation 3. In this thesis, a risk value is related to parameters associated with the defender, the attacker, and the power loss of the grid. For example, security analysts may decide that the highest acceptable risk is 0.1503 (test case 1's risk). This means the security analysts need to reduce the risk of Substation 3 by (1) increasing the frequency of credential resets for Substation 3, (2) increasing the average time the attacker needs to perform a successful

attack (e.g., increase length of passwords) and/or (3) implementing redundant transmission lines to reduce the severity of Substation 3.

5.3 39-bus Risk Assessment

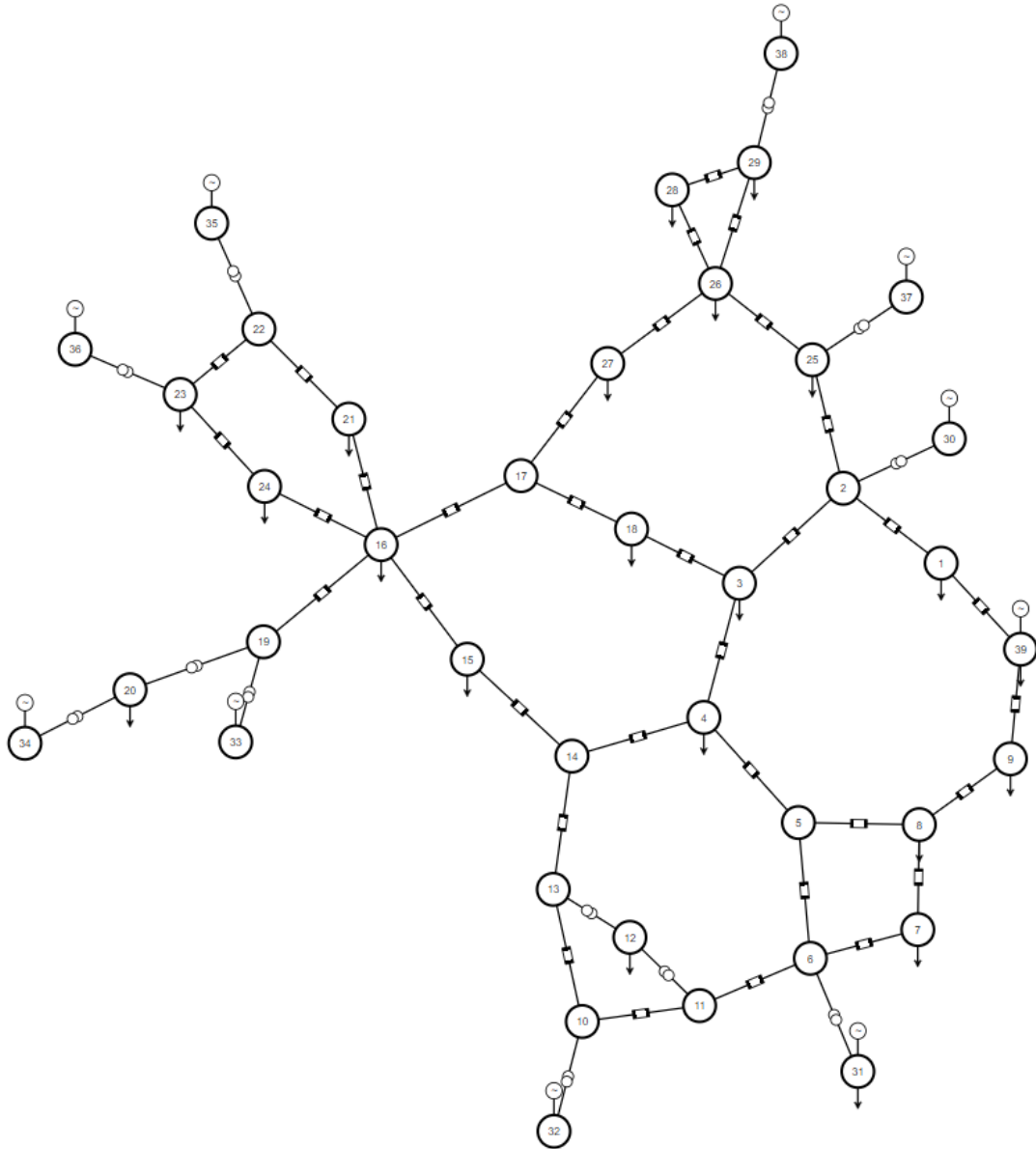


Figure 38 – A graphical view of a 39-bus system. This is drawn using Network Visualization [44].

The simulation in Section 5.2 was a simplistic system that did not consider branch (or transmission line) overflow and cascading failures, since the calculation for severity

was simply the percentage of load loss. For the 4-bus system, the attacker only needs to successfully attack one substation to guarantee a physical impact on the power grid. In this section, we expand the experiment to a 39-bus system as shown in Figure 38. In reality, sometimes, taking down a substation (and then disconnecting all related transmission lines) does not necessarily mean there is load loss. For example, if the attacker only takes down a single generating substation, then it is possible that no load loss occurs, because the impact of the said attack results in more stress on other transmission lines, but the stress is not enough to overload transmission lines. In this section, we analyze the difference between (1) immediately attacking one substation when the preparations are complete, (2) waiting until the preparations for attacking two substations are complete, and (3) waiting until the preparations for attacking three substations are complete. Therefore, the experiment involves analyzing (1) the load loss of choosing one bus out of 39 buses, which is $C(39,1) = 39$ load loss calculations, (2) the load loss of choosing two buses out of 39 buses, which is $C(39,2) = 741$ load loss calculations, and (3) the load loss of choosing three buses out of 39 buses, which is $C(39,3) = 9139$ load loss calculations. We do not consider cases that involves attacking four buses or more, because the probability of successfully attacking four buses simultaneously is, in theory, very low. The experiment utilizes Matpower [42] for DC power flow calculations while taking account of cascading failures due to branch overflows. The cascading failures is done by repeatedly removing transmissions lines that are overflowed, and then reruning the DC power flow simulation on individual islands (if the said islands exist) until either there is no transmission line overflow or the island does not have a generator to support the load. More sophisticated cascading failure analysis [43] could be implemented in the future, but for simplicity, we

choose to leave it out of the experiment. The hybrid attack model of attacking one, two or three substations simultaneously is shown in Figure 39. Note that in Figure 39, we assume the PLADD parameters for Substations A, B and C are the same as Substations 1, 2 and 3 in Table 9.

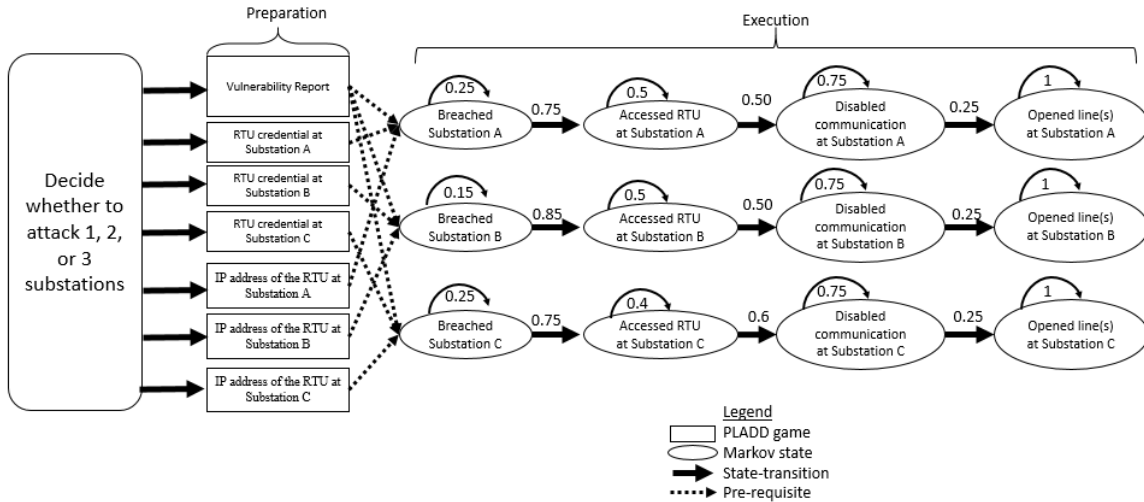


Figure 39 – The hybrid attack model of attacking one, two or three substations simultaneously.

5.3.1 Experimental Results

The experimental results are shown in Table 13. For clarity, not all experimental data is shown in Table 13. However, the average and worst case risk calculations are shown in Table 13. The equation to calculate risk is the same as in Section 5.2. It is also interesting to note that regardless of whether the attacker is successful in taking down one, two or three substations, there are always scenarios where no load loss has occurred in the 39-bus system. As the number of simultaneously attacked substation increases, the probability of successful attack decreases. As the number of simultaneously attacked substations increases, the worst case and average case load loss also increases. Unexpectedly, the risk

to attack two substations simultaneously has the highest worst case and average case risk. It is also interesting to note that Substation 6 has occurred in the worst case scenario for attacking two and three buses simultaneously. This finding implies that Substation 6 may be a critical substation to cause higher load loss for attack scenarios involving simultaneously attacking two and three substations.

Table 13 – Average and worst case risk calculation for the 39-bus system

Number of simultaneously attacked substations	Substations taken offline for the worst case scenario (Substation ID)	Probability of successful attack	Worst case load loss (MW)	Average load loss (MW)	Worst case risk	Average case risk
1	38	0.275	3858.4	374.93	1061.1	103.11
2	6, 29	0.20972	5246	1305.8	1100.2	273.85
3	6, 37, 39	0.14722	6245.7	2000	919.51	294.45

5.4 Sensitivity Analysis

Sensitivity analysis is done on all four buses in Figure 32; however, only Substation 1’s results are shown for simplicity. We assume that the attacker’s attack plan for a single substation is as shown in Figure 33. This means that there are three parameters that the defender can control: 1) when to reset the password to a computer hosting the vulnerability report, 2) when to reset the password to the RTU credential at the substation, and 3) when to reset IP address of the RTU at the substation. The Markov chain part Figure 33 is not included in the sensitivity analysis because the Markov chain is a linear system. Assuming the resets above are done periodically, then the defender can only control the periods at which the resets happen. Figure 40 and Figure 41 show the risk of Substation 1 being successfully attacked as the period of resets for vulnerability report, RTU credential at Substation 1, and IP address of RTU at Substation 1 increases. Figure 42

and Figure 43 show the sensitivity of Substation 1 being successfully attacked as the period of resets for vulnerability report, RTU credential at Substation 1, and IP address of RTU at Substation 1 increases.

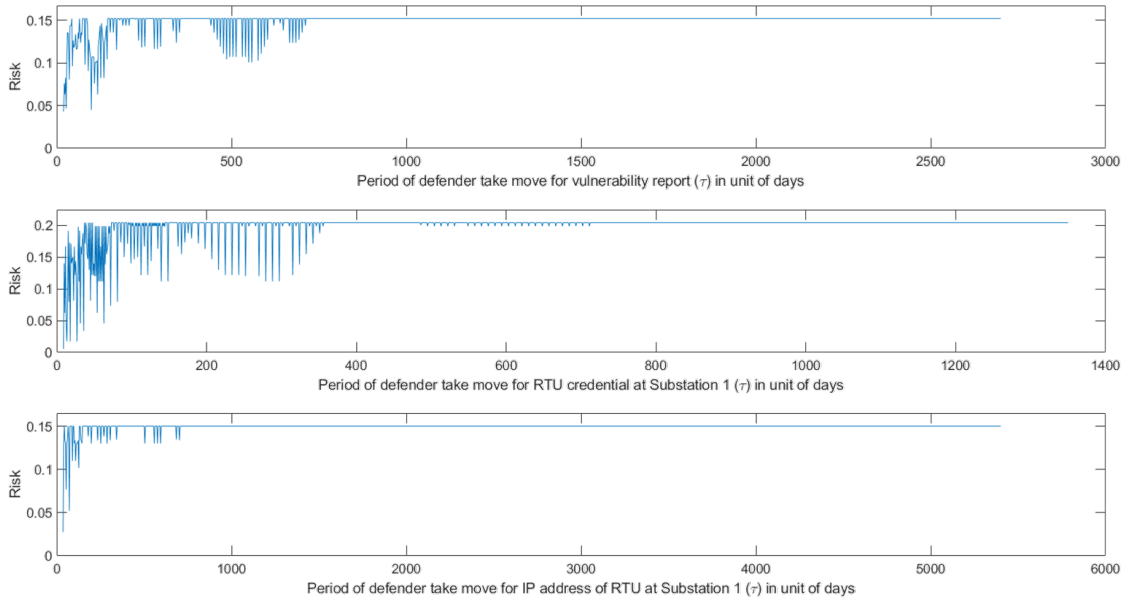


Figure 40 – Risk of Substation 1 being successfully attacked as the period of resets increases.

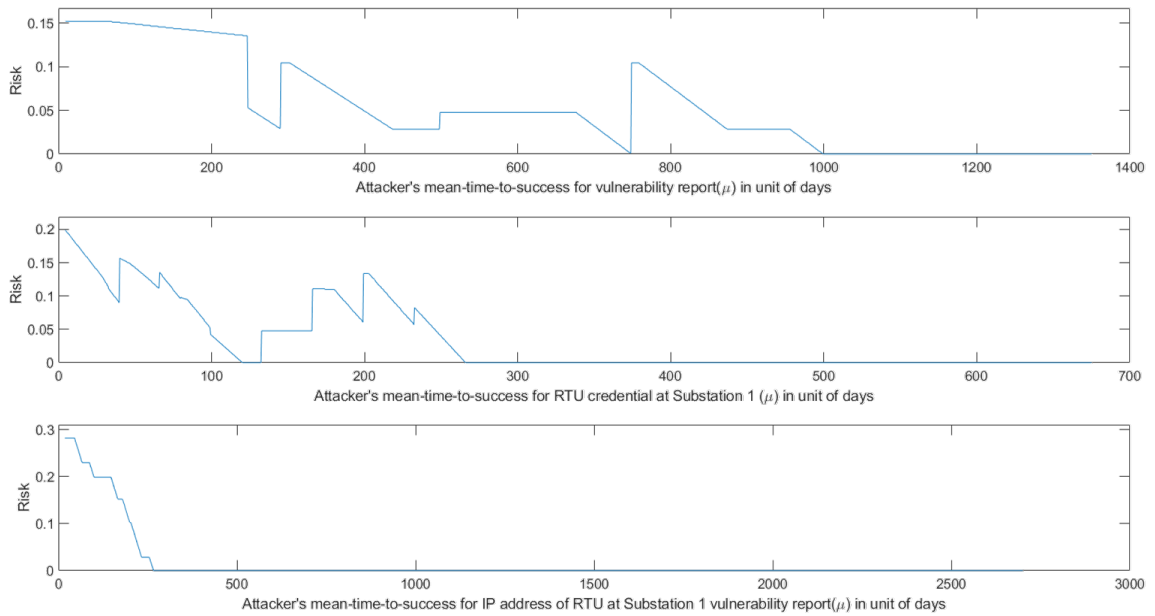


Figure 41 – Risk of Substation 1 being successfully attacked as the attacker's mean-time-to-success increases.

Base on Figure 40, it can be concluded that as the period of defender’s periodic reset increases, there is a threshold for the risk value. This is an important discovery for two reasons. First, if the defender is satisfied with the threshold, the defender can choose to not reset at all. This means that even if the attack on Substation 1 is successful, the impact of the attack is acceptable to the defender. Second, this threshold is a reference point for the defender. In prior works related to risk assessment, a single risk value by itself does not have an important meaning. However, the difference between each risk values provide context to the defender with regards to which part of the cyber-physical system is more at risk as compared to another part of the cyber-physical system. In this work, the threshold of the risk is the risk for not defending at all. Base on Figure 41, it can concluded that as the attacker’s mean-time-to-success increases, there will be a point where the defender’s periodic reset can absolutely prevent a successful attack from the attacker. Based on Figure 42, the sensitivity of risk to defender’s periodic reset is close to zero. Based on Figure 43, the sensitivity of risk to attacker’s mean-time-to-success is also close to zero.

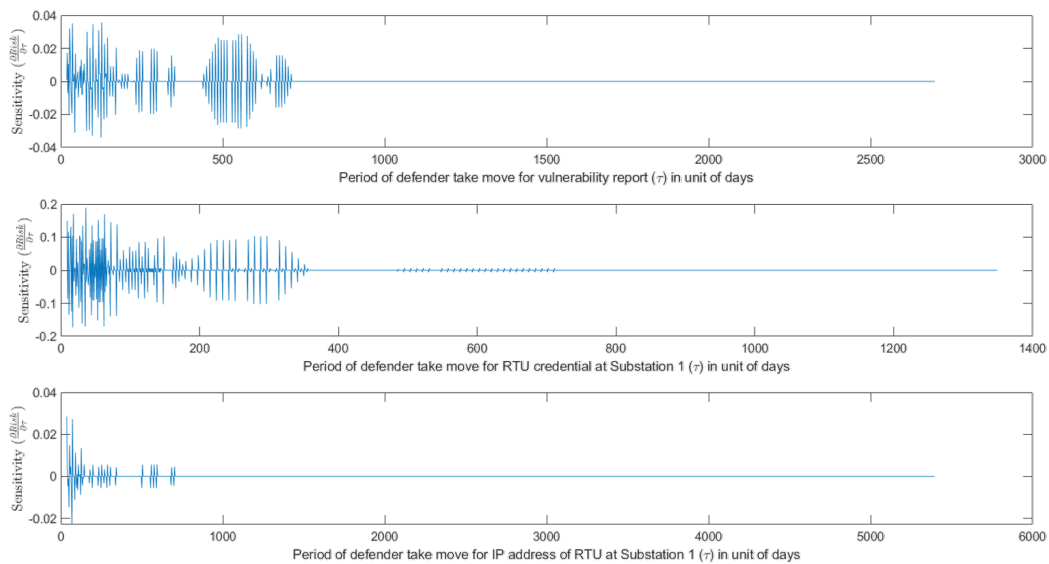


Figure 42 – Sensitivity of Substation 1 being successfully attacked as the period of resets increases.

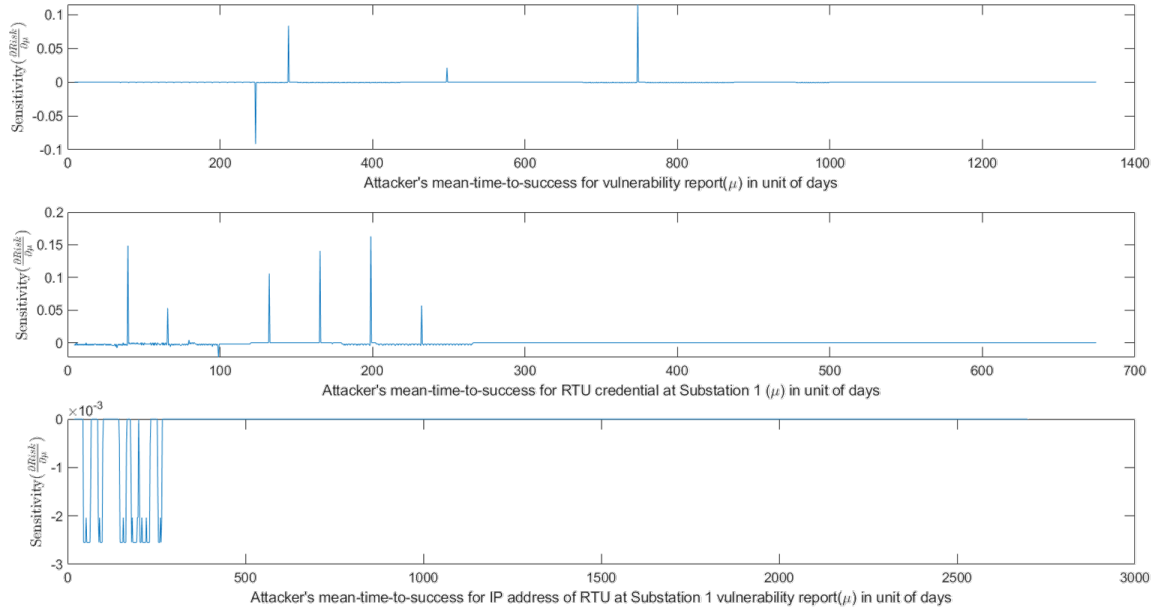


Figure 43 – Sensitivity of Substation 1 being successfully attacked as the attacker’s mean-time-to-success increases.

Figure 40 through Figure 43 show dramatic change earlier in the plot relative to later in the plot. In addition, besides having a risk threshold and converging to near zero as x-axis increases, Figure 40 through Figure 43 do not seem to follow any pattern. One reason for this characteristic is likely due to the random component in a PLADD node. Specifically, the attacker’s time-to-success is a random number. Therefore, the attacker’s time-to-success may be beneficial to either the attacker or the defender. For example, the attacker’s time-to-success may be very short, or the defender’s periodic take move may happen right after the attacker’s successful.

CHAPTER 6. CONCLUSIONS

In this thesis, we presented the advantages and disadvantages of PLADD and Markov chain models for the analysis of cyberattacks on a 4-bus power grid system and then we introduced a hybrid attack model that combines the advantages of the PLADD and Markov chain models. We discovered that the Markov chain assumes each action can only be completed with the same amount of time. This assumption works well in the execution phase because the time it takes to go through the execution phase is much less in comparison to the preparation phase. We also discovered that while the PLADD model is good at modeling attacker and defender interaction for a long period of time, the PLADD model does not have an easy and straightforward way to model quick and simple actions such “jumping a fence” to obtain access to a substation.

To gain a deeper understanding into the PLADD model, the mathematical model of a single PLADD game, a single-layer parallel PLADD system, and a hierarchical parallel PLADD system are created. We mathematically prove that for both AND configurations and OR configuration, it is possible to decrease the attacker’s expected probability of success by making sure the defender’s take moves occur with respect to the aforementioned method. This is a significant finding because the security analysts may be able to use our methodology to decrease the probability of successful attack by simply shifting the time of resets for critical resources such as computer passwords, IP addresses, etc.

We also present a risk assessment method that combines our Hybrid Attack Model and DC power analysis to determine the weak link in a power grid for 4-bus and 39-bus system. The techniques presented in this dissertation can be further expanded for larger

cyber-physical systems because each PLADD node is of linear complexity. Our risk assessment method could use either the percentage of load loss or the load loss to calculate risk. With the discussed attack scenarios, we found that the risks to attack two substations simultaneously is higher than only attacking one substation or waiting until the preparations to attack three substations is complete.

For future work, a more sophisticated method to calculate risk in combination with our Hybrid Attack Model could be to take into account of results from contingency analysis, state estimator and weather data. In addition, since we only considered loss load in the risk calculation, it is difficult to practically evaluate the impact of an attack. Data such as the cost to replace overloaded transmission lines and reconnecting disconnected substation(s) back to the grid should be considered. Given the discussed scenario in Section 5.3, we found that Substation 6 may be a critical substation for attacks involving more than one substation. However, the results are preliminary, since we only considered attack scenarios involving attacking one, two, or three substations simultaneously. If we increase the number of simultaneously attacked substations further, we may have a clearer view of which substations are critical. In addition, we only considered the absolute worst case and the average case physical impact for all successful attacks. A data mining expert may be able to gather more useful conclusions from the rest of the attack simulations. Lastly, our experiment does not consider the cost for the attacker's actions. In theory, as the number of simultaneously attacked substations increases, the cost to successfully implement attacks also increases, and probably not linear as well, since failed attacks still accumulate costs for the attacker.

REFERENCES

- [1] S. Jones *et al.*, "Evaluating Moving Target Defense with PLADD." [Online]. Available: <https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2015/158432r.pdf>
- [2] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FlipIt: The Game of "Stealthy Takeover"," *Journal of Cryptology*, vol. 26, no. 4, pp. 655-713, 2013/10/01 2013, doi: 10.1007/s00145-012-9134-5.
- [3] Y. Chen, T. Giesecking, D. Campbell, V. Mooney, and S. Grijalva, "A Hybrid Attack Model for Cyber-Physical Security Assessment in Electricity Grid," in *2019 IEEE Texas Power and Energy Conference (TPEC)*, 7-8 Feb. 2019 2019, pp. 1-6, doi: 10.1109/TPEC.2019.8662138.
- [4] W. Wu, R. Kang, and Z. Li, "Risk assessment method for cyber security of cyber physical systems," in *2015 First International Conference on Reliability Systems Engineering (ICRSE)*, 21-23 Oct. 2015 2015, pp. 1-5, doi: 10.1109/ICRSE.2015.7366430.
- [5] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer*, vol. 44, no. 4, pp. 91-93, 2011, doi: 10.1109/MC.2011.115.
- [6] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, 2013/04/07/ 2013, doi: <https://doi.org/10.1016/j.comnet.2012.12.017>.
- [7] A. Guo, D. Yu, H. Du, Y. Hu, Z. Yin, and H. Li, "Cyber-physical failure detection system: Survey and implementation," in *2016 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 19-22 June 2016 2016, pp. 428-432, doi: 10.1109/CYBER.2016.7574863.
- [8] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, <https://doi.org/10.1049/iet-cps.2016.0019> vol. 1, no. 1, pp. 13-27, 2016/12/01 2016, doi: <https://doi.org/10.1049/iet-cps.2016.0019>.
- [9] (2016). *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*.
- [10] "Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015." [Online]. Available: <https://www.pwc.lu/en/information-risk-management/docs/pwc-irm-managing-cyber-risks-in-an-interconnected-world.pdf>

- [11] Y. Dvorkin. "Executive Order Shines a Light on Cyberattack Threat to the Power Grid." *IEEE Spectrum*. <https://spectrum.ieee.org/executive-order-shines-a-light-on-cyberattack-threat-to-the-power-grid> (accessed November 17, 2021).
- [12] H. Zhu, Z. Ma, X. Cai, J. Chen, R. Jin, and L. Yang, "Dynamic Attack and Defense Security Situation Assessment Model for Power Information Physical Fusion System," in *2019 IEEE International Conference on Industrial Internet (ICII)*, 11-12 Nov. 2019 2019, pp. 152-155, doi: 10.1109/ICII.2019.00039.
- [13] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," in *2017 IEEE Power & Energy Society General Meeting*, 16-20 July 2017 2017, pp. 1-1, doi: 10.1109/PESGM.2017.8274329.
- [14] Y. Pei, H. Zhang, X. Gu, and H. Wang, "Research on Power Grid Information Model Based on Artificial Intelligence," in *2019 International Conference on Computer Network, Electronic and Automation (ICCNEA)*, 27-29 Sept. 2019 2019, pp. 321-328, doi: 10.1109/ICCNEA.2019.00067.
- [15] T. R. Sharafeev, O. V. Ju, and A. L. Kulikov, "Cyber-Security Problems in Smart Grid Cyber Attacks Detecting Methods and Modelling Attack Scenarios on Electric Power Systems," in *2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, 15-18 May 2018 2018, pp. 1-6, doi: 10.1109/ICIEAM.2018.8728654.
- [16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. Article 13, 2011, doi: 10.1145/1952982.1952995.
- [17] B. Dario, *Game Theory: Models, Numerical Methods and Applications* (Game Theory: Models, Numerical Methods and Applications). now, 2014, p. 1.
- [18] M. P. Deisenroth, A. A. Faisal, and C. S. Ong, *Mathematics for Machine Learning*: Cambridge University Press. [Online]. Available: <https://mml-book.github.io/book/mml-book.pdf>.
- [19] J. Lee, B. Bagheri, and H.-A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18-23, 2015/01/01/ 2015, doi: <https://doi.org/10.1016/j.mfglet.2014.12.001>.
- [20] P. A. Gagniuc, *Markov Chains: From Theory to Implementation and Experimentation*. John Wiley & Sons, 2017.
- [21] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85-89, 2006, doi: 10.1109/MSP.2006.145.

- [22] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, and Y. Liu, "A survey on bad data injection attack in smart grid," in *2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, 8-11 Dec. 2013 2013, pp. 1-6, doi: 10.1109/APPEEC.2013.6837157.
- [23] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," presented at the Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2009. [Online]. Available: <https://doi.org/10.1145/1653662.1653666>.
- [24] F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, and Y. Gao, "Security Analysis on Cyber-physical System Using Attack Tree," in *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 16-18 Oct. 2013 2013, pp. 429-432, doi: 10.1109/IIH-MSP.2013.113.
- [25] S.-H. Yang, X. Lyu, and Y. Ding, "Safety and Security Risk Assessment in Cyber-Physical Systems," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, 03/01 2019, doi: 10.1049/iet-cps.2018.5068.
- [26] G. Ramos, J. L. Sanchez, A. Torres, and M. A. Rios, "Power Systems Security Evaluation Using Petri Nets," *IEEE Transactions on Power Delivery*, vol. 25, no. 1, pp. 316-322, 2010, doi: 10.1109/TPWRD.2009.2035422.
- [27] A. Ashok, A. Hahn, and M. Govindarasu, "Cyber-Physical Security of Wide-Area Monitoring, Protection and Control in a Smart Grid Environment," *Journal of Advanced Research*, vol. 5, 12/27 2013, doi: 10.1016/j.jare.2013.12.005.
- [28] H. Orojloo and M. Abdollahi Azgomi, "Modeling and Evaluation of the Security of Cyber-Physical Systems Using Stochastic Petri Nets," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, 07/18 2018, doi: 10.1049/iet-cps.2018.0008.
- [29] Z. Qiqi, S. Gang, F. Yuyao, and S. Yun, "Network topology of urban grid considering N-1-1 criterion," in *12th IET International Conference on AC and DC Power Transmission (ACDC 2016)*, 28-29 May 2016 2016, pp. 1-5, doi: 10.1049/cp.2016.0440.
- [30] Y. Yu and W. Lin, "Study on the security assessment platform for electric power secondary system," in *2006 International Conference on Power System Technology*, 22-26 Oct. 2006 2006, pp. 1-6, doi: 10.1109/ICPST.2006.321797.
- [31] F. Farzan, M. A. Jafari, D. Wei, and Y. Lu, "Cyber-related risk assessment and critical asset identification in power grids," in *ISGT 2014*, 19-22 Feb. 2014 2014, pp. 1-5, doi: 10.1109/ISGT.2014.6816371.
- [32] V. Chukwuka, Y. Chen, S. Grijalva, and V. Mooney, "Bad Data Injection Attack Propagation in Cyber-Physical Power Delivery Systems," in *2018 Clemson*

- University Power Systems Conference (PSC)*, 4-7 Sept. 2018 2018, pp. 1-8, doi: 10.1109/PSC.2018.8664024.
- [33] R. Tsang, "Cyberthreats, Vulnerabilities and Attacks on SCADA Networks," 01/01 2010.
- [34] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210-219, 2017/08/01/ 2017, doi: <https://doi.org/10.1016/j.epsr.2017.04.018>.
- [35] M. J. A. R. M. Lee, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Industrial Control Systems, 2016.
- [36] R. Baldick *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures," in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 20-24 July 2008 2008, pp. 1-8, doi: 10.1109/PES.2008.4596430.
- [37] T. Zhou, Y. Li, and C. Wu, "An Efficient and Accurate Complex Nakagami Samples Generator Based on Inverse Transform Method," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 16-19 Oct. 2019 2019, pp. 102-106, doi: 10.1109/ICCT46805.2019.8947236.
- [38] Y.-C. Chen, V. J. Mooney, and S. Grijalva, "Grid Cyber-Security Strategy in an Attacker-Defender Model," *Cryptography*, vol. 5, no. 2, p. 12, 2021. [Online]. Available: <https://www.mdpi.com/2410-387X/5/2/12>.
- [39] M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *IEEE Transactions on Power Systems*, vol. 18, no. 1, pp. 258-265, 2003.
- [40] N. Aminudin, N. M. Ramli, M. Marsadek, N. M. Ramli, and T. K. A. Rahman, "Classification of risk of voltage collapse using risk matrix," in *2016 IEEE International Conference on Power System Technology (POWERCON)*, Wollongong, NSW, 2016.
- [41] M. Al-Hemairy, S. Amin, and Z. Trabelsi, "Towards more sophisticated ARP Spoofing detection/prevention systems in LAN networks," in *International Conference on the Current Trends in Information Technology (CTIT)*, Dubai, 2009.
- [42] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12-19, 2011, doi: 10.1109/TPWRS.2010.2051168.

- [43] I. Dobson, "Where is the edge for cascading failure?: challenges and opportunities for quantifying blackout risk," in *2007 IEEE Power Engineering Society General Meeting*, 24-28 June 2007 2007, pp. 1-8, doi: 10.1109/PES.2007.385773.
- [44] Monash University. <https://immersive.erc.monash.edu/stac/> (accessed February 16th, 2022).