cryptography

MDPI

Article

Grid Cyber-Security Strategy in an Attacker-Defender Model †

Yu-Cheng Chen [1,*], Vincent John Mooney III [1,2] and Santiago Grijalva [1]

[1] School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA; mooney@ece.gatech.edu (V.J.M.III); sgrijalva@ece.gatech.edu (S.G.)
[2] School of Computer Science, Georgia Institute of Technology, Atlanta, GA 30332, USA
* Correspondence: ychen414@gatech.edu
† This is an extended conference version that was presented at the 2020 Clemson University Power Systems Conference (PSC).

Abstract: The progression of cyber-attacks on the cyber-physical system is analyzed by the Probabilistic, Learning Attacker, and Dynamic Defender (PLADD) model. Although our research does apply to all cyber-physical systems, we focus on power grid infrastructure. The PLADD model evaluates the effectiveness of moving target defense (MTD) techniques. We consider the power grid attack scenarios in the AND configurations and OR configurations. In addition, we consider, for the first time ever, power grid attack scenarios involving both AND configurations and OR configurations simultaneously. Cyber-security managers can use the strategy introduced in this manuscript 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. Our mathematical proof for the OR configuration of multiple PLADD games shows that it is best if all access controls are reset simultaneously. For the AND configuration, our mathematical proof shows that it is best (in terms of minimizing the attacker's average probability of success) that the resets are equally spaced apart. We introduce a novel concept called hierarchical parallel PLADD system to cover additional attack scenarios that require combinations of AND and OR configurations.

Keywords: periodic reset; attack graph; cyber-physical systems; cyber-physical security; moving target defenses

Citation: Chen, Y.-C.; Mooney, V.J., III; Grijalva, S. Grid Cyber-Security Strategy in an Attacker-Defender Model . *Cryptography* **2021**, *5*, 12. https://doi.org/10.3390/cryptography5020012

Academic Editor: Jim Plusquellic

Received: 30 December 2020
Accepted: 22 March 2021
Published: 2 April 2021

1. Introduction

One set of mitigation techniques that defenders can use to shift their systems' attack surfaces is moving target defenses (MTDs). Moving target defenses can increase the attacker's costs and reduce the attacker's probability of success in performing attacks. The objective of moving target defenses (MTDs) is to increase uncertainty and complexity for attackers. Periodically resetting secret information is a crucial strategy of MTD. A cyber-physical system usually has implemented multiple MTDs by keeping secret information hidden.

Our previous work has shown that it is possible to decrease the attacker's probability of success by scheduling the periodic reset of MTDs in the cyber-physical system in a coordinated manner [1]. We expand on this previous work by adding additional examples to clarify key concepts and experiment results to validate our findings. We also introduce a novel concept called hierarchical parallel Probabilistic, Learning Attacker, and Dynamic Defender (PLADD) system to cover additional attack scenarios.

Critical infrastructure such as the power grid is a known target for adversaries that want to inflict damage on opposing nations. According to a U.S. Department of Energy report [2], cyber vulnerabilities remain a high-risk profile relative to grid reliability. Individual field cyber-components or the communications network can be potential targets in a cyber-physical attack. Therefore, it is crucial to strengthen the cyber-security of the power grid. Ukraine's power grid attack in December 2015 [3] is the first publicly known

successful cyber-attack on the power grid and resulted in a blackout that affected hundreds of thousands of people. Microsoft Office documents with embedded malware were used to steal credentials, providing access to the Ukraine power grid's industrial control system (ICS) network. Experts found that the Ukraine power grid's attackers were able to use the stolen credentials to access the ICS network from June 2015 to December 2015 [4]. This may imply that the credentials to the Ukraine power grid's ICS network were not changed for at least six months. One example of MTD is periodic credential reset. Periodically changing the internet protocol (IP) addresses of remote terminal units (RTUs) in the power grid is also an example of moving target defense. With the knowledge of an RTU's IP address, the adversary may be able to inject fake data to the control center by spoofing the IP address [5], perform malicious commands, etc. The motivation of this research is to understand how MTDs can be improved by making sure that MTDs in a cyber-physical system are working together to lower the attacker's probability of success.

2. Terminology

This section provides definitions used throughout the paper and includes basic concepts of probability for completeness and game theory for clarity.

2.1. Basic 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 [6]. 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.*

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:

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

Example 1. *If an exponential distribution function has a mean equal to 30, then the plot of the cumulative distribution function is shown in Figure 1.*

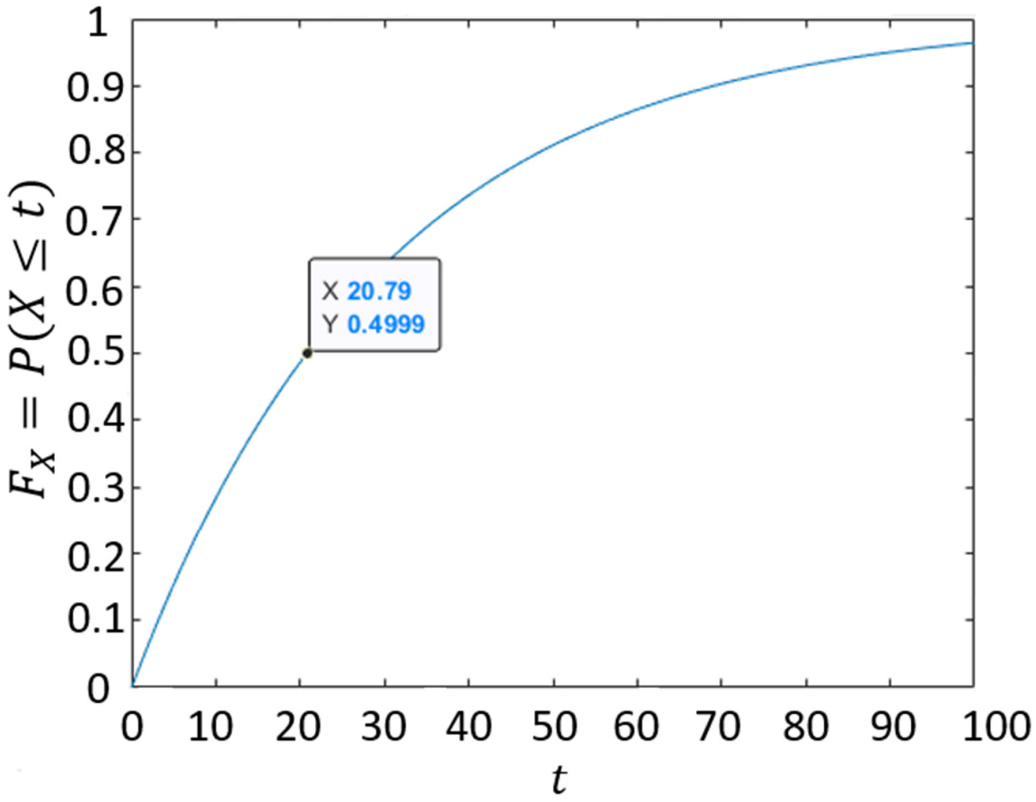

Figure 1. The cumulative distribution function of an exponential distribution with a mean $(\mu_k) = 30$. $P(X \leq t)$ is the probability that a random number is less than or equal to t. By plugging $m = 30 * \ln(2)$, we can see that the median is 20.79, which is where the probability is approximately 50%.

2.2. Basic Definitions in Game Theory

Game theory is the study of mathematical models of strategic interaction among rational decision-makers [7]. 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.*

Example 2. *Figure 2 shows an example attacker and defender interaction involving access to Computer 1 that controls a power generator. For this example, there are two players, which are the defender and the 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 1 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.

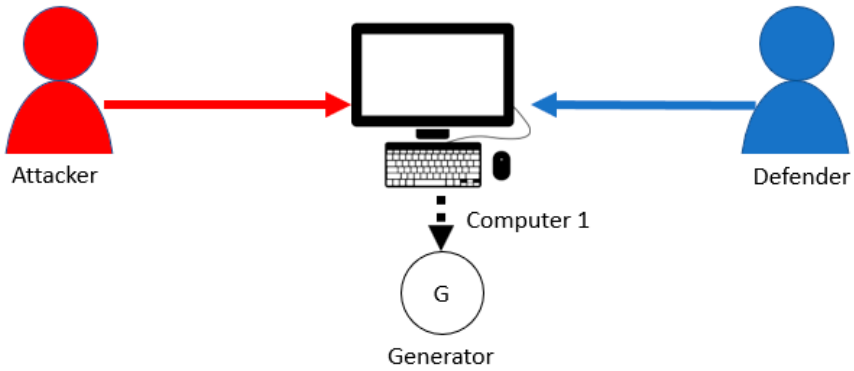

Figure 2. An example attacker and defender interaction involving a computer.

Example 3. *Figure 3 describes an example of the 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. Likewise, in Example 2, the attacker's move is to start an attack (such as executing password cracking software [8]) on a computer, which gives the attacker control of the computer after some time. The attacker can attack Computer 1 or Computer 2 independently. The defender's move is the same as in Example 2, 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.*

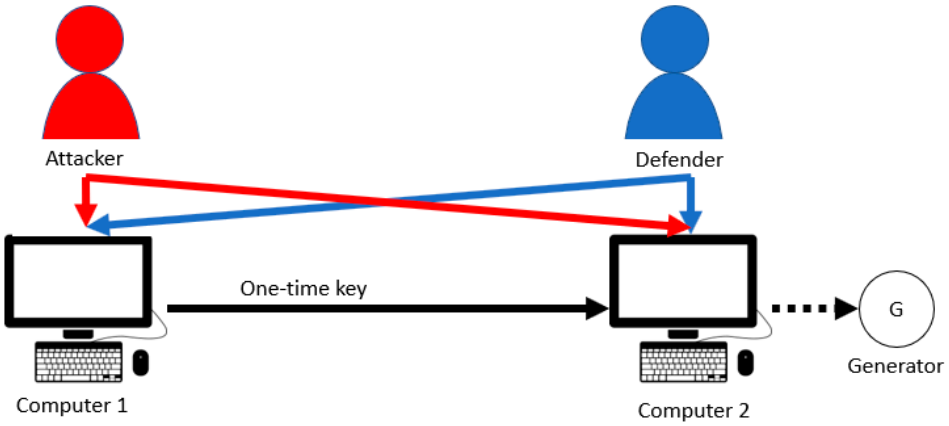

Figure 3. An example of an attacker and defender interaction involving two computers.

Examples 2 and 3 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 [8]). 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 10% of the time, while the defender may control 90% of the time.

3. Background and Prior Work

The concept of moving target defense (MTD) has recently emerged as a new paradigm for strengthening cybersecurity for computer networks and systems. One MTD example is IP address randomization [9]. IP address randomization is a technique that periodically randomizes each network packet's source IP address and destination IP address. A similar example of an MTD is address space layout randomization (ASLR [10]). If the randomization of the secret information (e.g., address space position of key data areas of a process) is not changed periodically, then these MTDs can be vulnerable over time. Another MTD example is periodically changing passwords or authentication keys. Multiple passwords usually protect the security of a system (e.g., the power grid). However, given enough time and resources, a strong password can be exploited. The attacker may use password cracking tools such as Openwall [8] and Hashcat [11] to steal passwords. These password-cracking tools may use a dictionary attack with a key logger to steal the user's passwords [12]. Note that a password reset from the user will not affect the password cracking tool's current progress because the key logger keeps a list of everything the user types. The password reset does not invalidate the key logger's list. Therefore, a password reset does not impair the password cracking tool's progress. If field cyber-components in a system implement MTDs, the security analysts may have the ability to coordinate each MTD to lower the attacker's probability of a successful attack.

The Probabilistic, Learning Attacker, and Dynamic Defender (PLADD) model was developed by Jones et al. to attempt to capture the essence of MTD [13]. They recognized that during cyber-attacks, (i) there is some information that, when held by the attacker, gives the attacker a competitive advantage and (ii) the defender can take away the information from the attacker (at least temporarily). In the PLADD model, an attacker and a defender contend to control a single resource. The resource in this context is the secret information that gives the attacker a competitive advantage. A stochastic process is used to model the evolution of attacks. A random variable models the time required for the attacker to gain control of the resource. Both the attacker and the defender perform a series of moves in the PLADD game. Note that an attack does not instantaneously finish because an attack takes a random amount of time to be successful. The attacker begins an attack on a resource at time 0 or immediately after losing control of a resource. In short, at any point in time, the attacker either (i) starts an attack, (ii) is carrying out an ongoing attack, or (iii) has control of the resource. The defender can regain control of the resource by executing a "take" move. The defender has no information about attacker progress. The defender decides when to execute a "take" move. Each PLADD game is defined by two parameters, which are (i) period (τ) of the defender's "take" move and (ii) the attacker's mean time (μ) required for a successful attack. Additional refinements to PLADD games are possible, but we only utilize the aforementioned features in this paper. An attacker and a defender contending to control a single PLADD game over time are illustrated in Figure 4 and Example 4. The PLADD game's unit of time can be any time units (seconds, hours, days, months, ... , etc.). However, we will use days as our time unit in our discussion of attack scenarios and experiments.

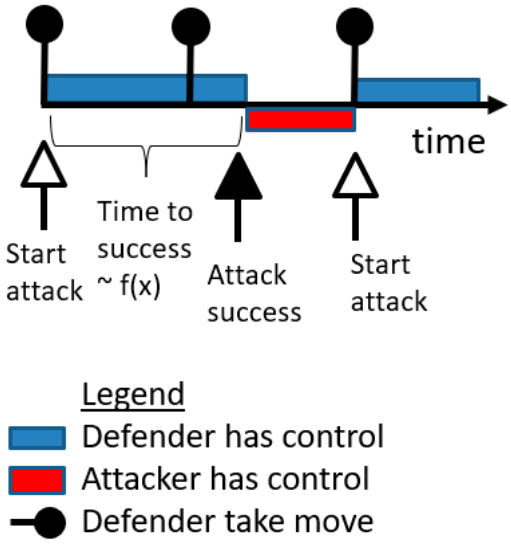

Figure 4. Illustration of an attacker and a defender contending for control of a single Probabilistic, Learning Attacker, and Dynamic Defender (PLADD) game over time.

Example 4. *Consider a single PLADD game. Figure 4 shows that a resource is initially controlled by the defender as shown in blue. The attack starts at the very beginning (immediately after the first "take" move at time zero). The time to successful attack is modeled by f(x), which is an exponential distribution function with a mean* (μ)*, i.e., rate parameter* $\lambda = \frac{1}{\mu}$*. After some time, the attack is successful, so the resource is controlled by the attacker as shown in red. The attacker retains control of the resource until the defender executes a "take" move (e.g., password reset) to regain control of the resource. Note that the defender's "take" move does not affect an on-going attack from the attacker. Therefore, if the defender executes a "take" move while the attacker's attack is on-going, the attacker's ongoing attack is not impaired by the defender's "take" move.*

4. Attack Scenarios

4.1. Single-Layer Parallel PLADD System

We consider a generic power grid topology shown in Figure 5. We focus on the attack scenarios in the power grid shown in Figure 6. 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 6 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 6 (see Section 3). 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 modeled 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 5, 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 6. 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.

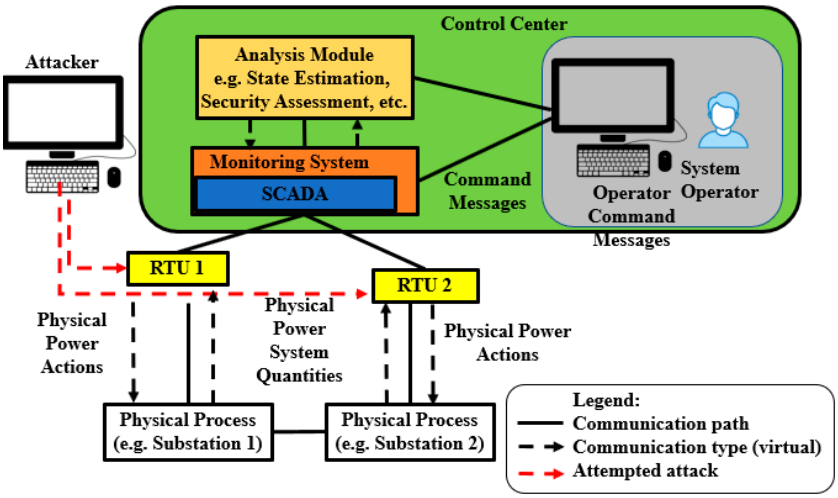

Figure 5. Power grid topology.

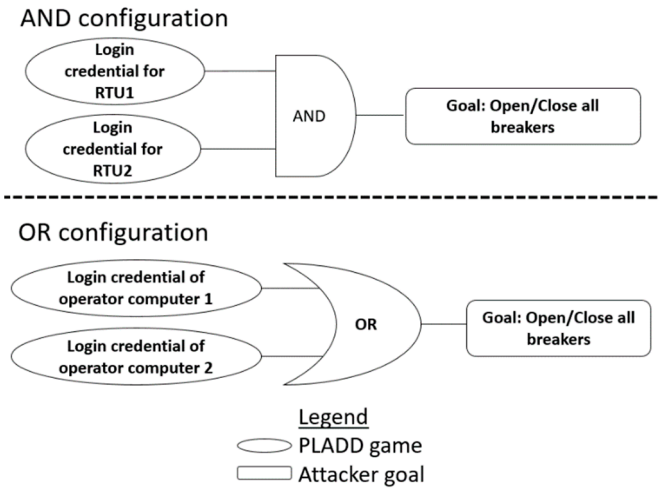

Figure 6. Two power grid attack scenarios.

4.2. Hierarchical Parallel PLADD System

In addition to the two attack scenarios shown in Figure 6 (involving two PLADD games in a 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 7. 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 7. 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 RTU 1, RTU 2, RTU 3, RTU

4, Operator Computer 1, Operator Computer 2, Operator Computer 3, and Operator Computer 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 modeled by an exponential distribution.

From the attacker's point of view with regard to Figure 7, 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. Figures 8 and 9 show parallel PLADD systems involving two layers of AND and OR configurations within a single overall parallel PLADD system.

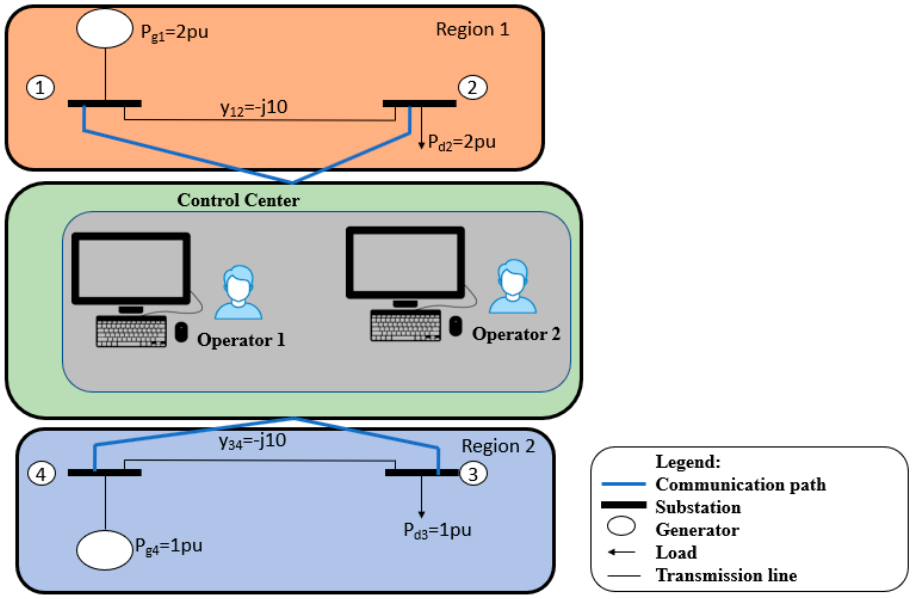

Figure 7. Power grid topology where the control center communicates substations in two different regions.

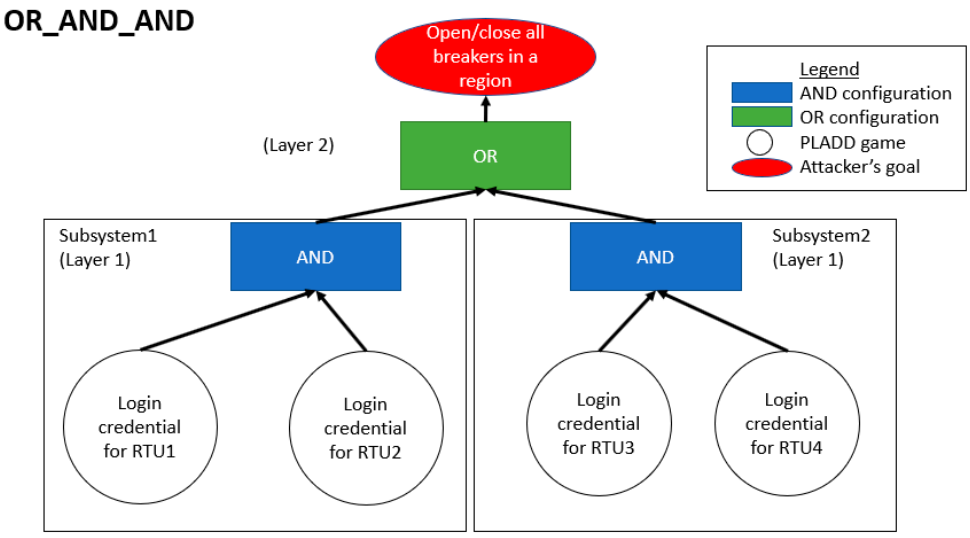

Figure 8. Attack scenario involving two subsystems in the AND configuration while the two subsystems have an OR configuration relationship. This configuration is labeled as OR_AND_AND.

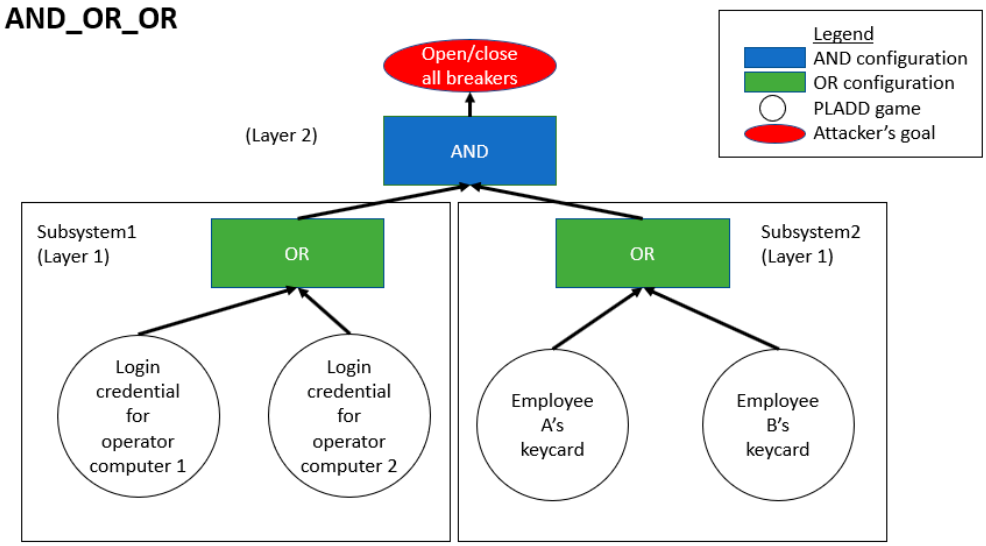

Figure 9. Attack scenario involving two subsystems in the OR configuration while the two subsystems have an AND configuration relationship. This configuration is labeled as AND_OR_OR.

Example 5. *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 7. 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 8 shows an illustration of this attack scenario modeled in the hierarchical parallel PLADD system.*

Example 6. *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 7. 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 5 and Example 6 describe two attack scenarios in a hierarchical parallel PLADD system. Figure 8 illustrates Example 5 and exhibits a hierarchical parallel PLADD system involving the AND of two subsystems with each subsystem in the OR configuration. Figure 9 illustrates Example 6 and displays a hierarchical parallel PLADD system involving the OR of two subsystems with each subsystem in the AND configuration.

5. 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 (as described in Section 4.2). With our model, a security analyst can refine the reset policy to minimize the attacker's mean probability of controlling a parallel PLADD system.

5.1. Notation and Definitions

The notation used in this manuscript is summarized in Table 1.

Table 1. 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 a 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 a game with index k.
$F_k(t)$	The cumulative distribution function of the attacker′s time-to-success in a 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.
$t_k\prime$	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 $\lim_{t \to t^-} P_k(t)$.
$R(t)$	The probability that the attacker controls the parallel PLADD system at time t.
EPS	Expected probability of success. It is computed as shown below: $EPS = \lim_{T \to \infty} \frac{1}{T} \int_0^T R(t)\, dt$
τ-periodic	A τ-periodic function is a function with period equal to τ.

5.2. 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 we consider:

(a) The defender executes "take" moves periodically; specifically, the defender executes "take" moves at $\{d_k,\ d_k + \tau_k,\ d_k + 2\tau_k,\ \ldots,\ d_k + n_k\tau_k,\ \ldots\}$.
(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 (1). 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.

$$P_k(t) = F_k(t), \text{ where } t < d_k \tag{1}$$

Example 7. *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.*

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

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 10.

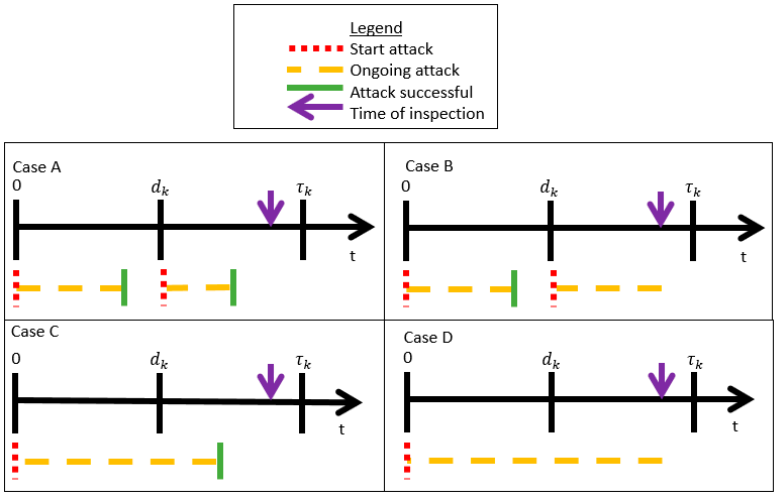

Figure 10. Four possible outcomes of a PLADD game, where the attacker starts an attack at time $t = 0$, and the time of inspection is at time t, $d_k < t < \tau_k$.

One possible outcome is Case A in Figure 10, 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 10, 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 10, 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 10, 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 10, 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 $P_k(d_k)F_k(t_k\prime)$, 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 $t_k\prime$ (recall that $t_k\prime$ is the time since the last defender "take" move, see Table 1). In Case C of Figure 10, 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 Equation (2).

$$P_k(t) = F_k(t) - F_k(d_k) + P_k(d_k) \times F_k(t_k'), \text{ where } d_k < t < \tau_k \quad (2)$$

Example 8. *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.*

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

6. Overview of Major Theorems

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

6.1. Single-Layer Parallel PLADD System

The following two theorems are proved in detail in Section 7.

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.*

Please note that Theorem 1 will be fully explained in Section 7. Our intention here is to briefly give an overview of the main theorems proven and simulated in this paper.

Example 9. *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 6. 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 probabilities of success of three of these possible reset patterns are shown in Table 2.*

Table 2. 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

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 10. *Consider two PLADD games with index "1" and "2" in the OR configuration as shown in the bottom half of Figure 6. We simulate three different reset patterns, which are as follows: (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 probabilities of success of these three possible reset patterns are shown in Table 3.*

Table 3. 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 is fully explained in Section 7. Our intention here is to briefly give an overview of the main theorems proven and simulated in this paper.

Based on the results shown in Tables 2 and 3, 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.

6.2. Hierarchical Parallel PLADD System

A hierarchical parallel PLADD system (see Section 4.2) 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 obtain minimized attacker's expected probability of success, and (b) each upper layer also applies Theorem 1 and Theorem 2 to obtain minimized attacker's expected probability of success.

Example 11. *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 11. Let us also assume the defender's "take" move periods* (τ) *are 90 time units and the attacker's mean time-to-successes* (μ) *are 30 time units. We simulate four different reset patterns, which are the following:*

i. The resets of each PLADD game in the hierarchical parallel PLADD system are at the same time.
ii. 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 $\frac{\tau}{2}$.
iii. 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.
iv. 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.

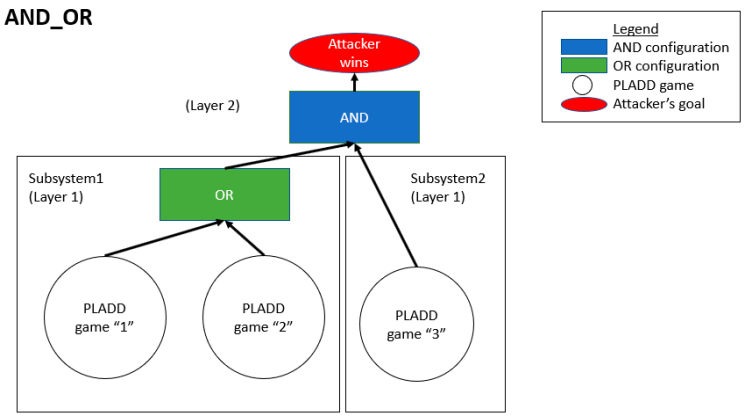

Figure 11. A hierarchical parallel PLADD system containing three PLADD games. This configuration is labeled as AND_OR.

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 OR-AND configuration as shown in Figure 12. Let us also assume the defender's "take" move periods* (τ) *are 90 time units and the attacker's mean time-to-successes* (μ) *are 30 time units. We simulate four different reset patterns, which are the following:*

i. The resets of each PLADD game in the hierarchical parallel PLADD system are at the same time.
ii. 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 $\frac{\tau}{2}$.
iii. 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.
iv. 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.

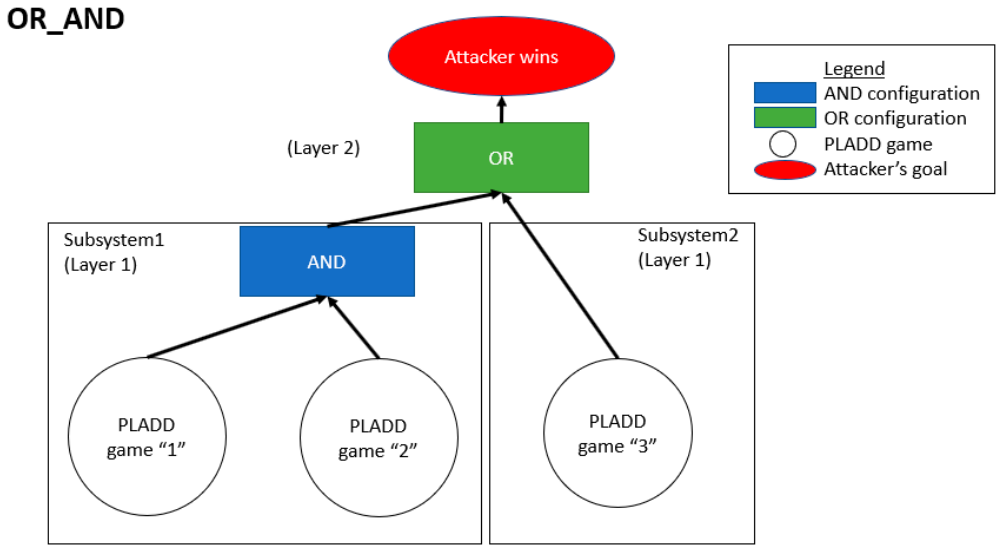

Figure 12. A hierarchical parallel PLADD system containing three PLADD games. This configuration is labeled as OR_AND.

The simulation result for Example 11 is shown in Table 4. The simulation result for Example 11 is shown in Table 5. Based on the results shown in Tables 4 and 5, 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.

Table 4. 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

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_{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

7. Mathematical Model in Detail

In this section, we discuss the detailed mathematical proofs.

7.1. 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 $t\prime$ be the time since the last defender "take" move. $n_k \in [0, \mathbb{N})$ and $t\prime \in (0, \tau_k]$ are the unique values such that $t = d_k + n_k\tau_k + t_k\prime$. Then, the probability that the attacker controls the game with index k at time t is given by Equation (3).*

$$P_k(t) = F_k(t) - F_k(d_k + n_k\tau_k) + \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)(F_k(t_k\prime + i\tau_k) - F_k(i\tau_k)) \quad (3)$$

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 (4).

$$P_k(t) = F_k(t) - F_k(0) = F_k(t),\ 0 \leq t \leq d_k \quad (4)$$

For time $t > d_k$, 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 $0,\ d_k,\ d_k + \tau_k,\ \ldots,\ d_k + n_k\tau_k$ (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 13.

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 within the range $(d_k + n_k\tau_k,\ t]$.

Equation (5) shows the probability that the time used in a successful attack is within the range $(d_k + n_k\tau_k,\ t]$. Notice that Equation (5) comprises the first two terms in Equation (3).

$$F_k(t) - F_k(d_k + n_k\tau_k) \tag{5}$$

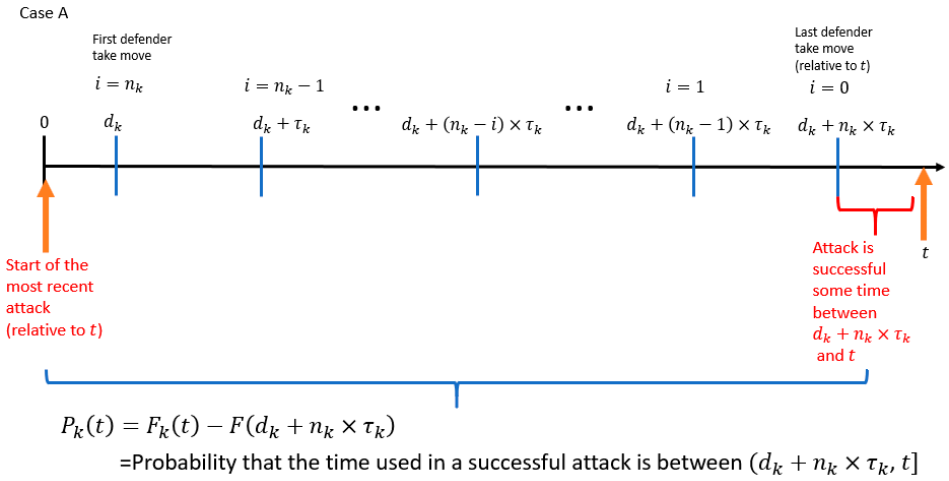

Figure 13. Timeline of events in PLADD game k, where the start of the most recent attack (relative to t) is at time 0.

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 14.

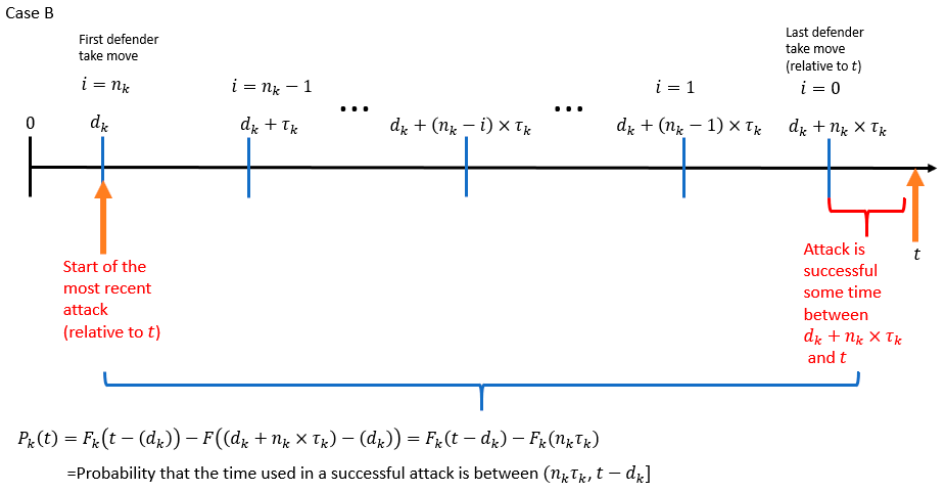

Figure 14. Timeline of events in PLADD game k, where the start of the most recent attack (relative to t) is at time d_k.

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 $(n_k\tau_k,\ t - d_k]$.

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 15. Note that for some $i \in \{0,\ 1,\ \ldots,\ n_k\}$, 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 $(i\tau_k,\ t - (d_k + (n_k - i)\tau_k)]$.

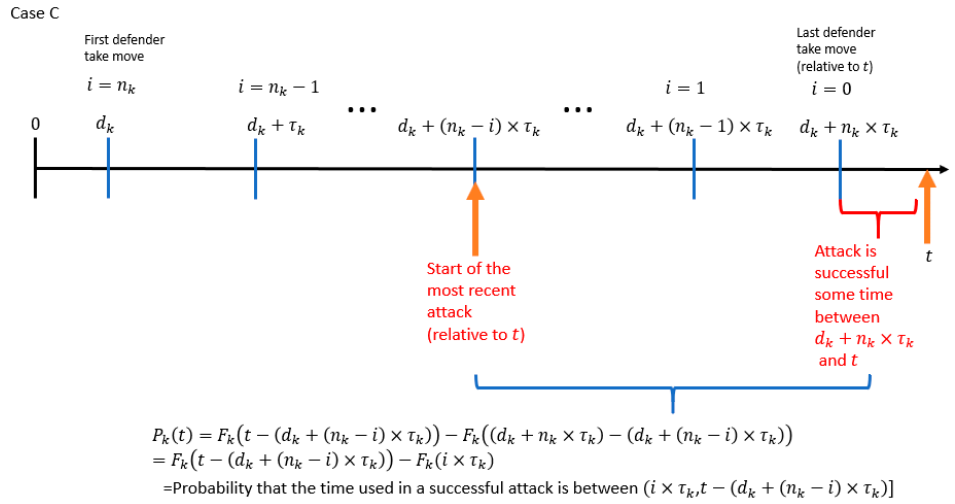

Figure 15. Timeline of events in PLADD game k, where the start of the most recent attack (relative to t) is at time $d_k + (n_k - i)\tau_k$.

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:

i. 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).
ii. The probability that the time used in a successful attack is within the range $(i\tau_k,\ t - (d_k + (n_k - i) \times \tau_k)]$.

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 (6). Note that Equation (6) is the third term in Equation (3).

$$\begin{aligned} P_k(d_k + (n_k - i)\tau_k) \times (F_k(t - (d_k + (n_k - i)\tau_k)) - F((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k))) \\ = P_k(d_k + (n_k - i)\tau_k) \times \left(F_k\left(t'_k + i\tau_k\right) - F_k(i\tau_k)\right) \end{aligned} \quad (6)$$

The description for Equation (6) is 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 $t - (d_k + (n_k - i)\tau_k)$.
- $F((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k))$ is the probability that the time used in a successful attack is less than or equal to $(d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k)$.
- $(F_k(t - (d_k + (n_k - i)\tau_k)) - F((d_k + n_k\tau_k) - (d_k + (n_k - i)\tau_k)))$ 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 (7) shows the summation of all times the previous attack could have started. Theorem 1 is summarized in Equation (7).

$$P_k = \begin{cases} F_k(t), & 0 \le t \le d_k \\ F_k(t) - F_k(d_k + n_k\tau_k) + \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)(F_k(\tau'_k + i\tau_k) - F_k(i\tau_k)) & t > d_k \end{cases} \tag{7}$$

□

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: $\mathbb{R} \to \mathbb{R}^+$ *such that for all* $t \in \mathbb{R}$,

$$Q_k(t) = \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)\big(F_k(t'_k + i\tau_k) - F_k(i\tau_k)\big) \tag{8}$$

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 $t \to \infty$, the first two terms in $P_k(t)$ in Equation (7) 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 $\lim_{t \to (d_k + (n_k - i)\tau_k)^-} Q_k(t)$.

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

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 $c \ge 0$, if we let $Q_k(d_k + (n_k - 1)\tau_k) = c$ for all $n_k \in [0, \mathbb{N})$, then Equation (9) shows $Q_k(t)$ converges to a constant c.

$$\begin{aligned} Q_k(t) = \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)\big(F_k(t'_k + i\tau_k) - F_k(i\tau_k)\big) &= \sum_{i=0}^{\infty} c \times \big(F_k(t'_k + i\tau_k) - F_k(i\tau_k)\big) \\ &= c \times \sum_{i=0}^{\infty} \big(F_k(t'_k + i\tau_k) - F_k(i\tau_k)\big) = c \lim_{t\to\infty} F_k(t) = c \end{aligned} \tag{9}$$

□

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 (7): if there is no defender "take" move between t_1 and t_2, then $P_k(t_1) \le P_k(t_2)$ 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 $t'_{k1} = t_1 - (d_k + n_k\tau_k)$ and $t'_{k2} = t_2 - (d_k + n_k\tau_k)$. Since F_k is a cumulative distribution function, it is monotonically increasing. In particular, for all $i \in \mathbb{N}$,

$$F_k(t'_{k1} + i\tau_k) \le F_k(t'_{k2} + i\tau_k) \tag{10}$$

We arrive at Equation (11) by subtracting $F_k(i\tau_k)$ from both sides of the inequality in Equation (8).

$$F_k(t'_{k1} + i\tau_k) - F_k(i\tau_k) \le F_k(t'_{k2} + i\tau_k) - F_k(i\tau_k) \tag{11}$$

We arrive at Equation (12) by multiplying $\sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)$ to both sides of Equation (9).

$$\sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)\Big(F_k\Big(t'_{k_1} + i\tau_k\Big) - F_k(i\tau_k)\Big) \leq \sum_{i=0}^{\infty} Q_k(d_k + (n_k - i)\tau_k)\Big(F_k\Big(t'_{k_2} + i\tau_k\Big) - F_k(i\tau_k)\Big) \tag{12}$$

By Definition 5, we obtain Equation (13) from Equation (12).

$$Q_k(t_1) \leq Q_k(t_2) \tag{13}$$

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

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 $t \to \infty$, $P_k(t)$ converges to a steady-state solution.*

Proof. Recall Equation (7), which is reproduced below.

$$P_k = \begin{cases} F_k(t), & 0 \leq t \leq d \\ F_k(t) - F_k(d_k + n_k\tau_k) + & \\ \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)(F_k(\tau'_k + i\tau_k) - F_k(i\tau_k)), & t > d_k \end{cases} \tag{14}$$

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 (7) approaches zero.

Equation (15) is in the form of $Q_k(t)$. By Proposition 1, $P_k(t)$ also converges to a steady-state solution.

$$\begin{aligned} \lim_{t\to\infty} P_k(t) &= \lim_{t\to\infty} \sum_{i=0}^{n_k} P_k(d_k + (n_k - i)\tau_k)\big(F_k\big(t'_k + i\tau_k\big) - F(i\tau_k)\big) \\ &= \sum_{i=0}^{\infty} P_k(d_k + (n_k - i)\tau_k)(F_k(t'_k + i\tau_k) - F(i\tau_k)) \end{aligned} \tag{15}$$

□

Lemma 2. *Let $p_1(t), \ldots, p_N(t) : \mathbb{R} \to \mathbb{R}$ be nonnegative τ-periodic functions that are all monotonically increasing or all monotonically decreasing on $(0, \tau]$. Then the mean of Equation (16) is maximized when $d_1 = d_2 = \ldots = d_N$.*

$$s(t) = \prod_{k=1}^{N} p_k(t + d_k) \tag{16}$$

Proof. We will do a proof by contradiction. Assume that the value $s'(t)$ is achieved with values of $d_1 = d_2 = \ldots = d_N = d$ where $d \in [0, \mathbb{R}^+)$; then Equation (17) is the mean of $s'(t)$.

$$E\big(s'(t)\big) = \lim_{T\to\infty} \frac{1}{T} \int_0^T \prod_{k=1}^{N} p_k(t + d)dt \tag{17}$$

Let $\Delta t \to 0$, and for some $i \in \{1, 2, \ldots, N\}$, the value $s(t)$ is achieved with values of $d_1 = d_2 = \ldots = d_{i-1} = d_{i+2} = \ldots = d_N = d$. Let $d_i = d + \Delta t$ and $d_{i+1} = d - \Delta t$; then Equation (18) shows the value $E(s(t))$.

$$E(s(t)) = \lim_{T\to\infty} \frac{1}{T} \int_0^T \left(\prod_{k=1}^{i-1} p_k(t + d_k)\right) \times p_i(t + d_i) \times p_{i+1}(t + d_{i+1}) \times \left(\prod_{k=i+1}^{N} p_k(t + d_k)\right) dt \tag{18}$$

Let us assume that $E(s'(t))$ is not optimal. Thus, a deviation such as $E(s(t)) > E(s'(t))$ is shown in Equation (19).

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T\left[\prod_{k=1}^{i-1}p_k(t+d_k)\times p_i(t+d_i)\times p_{i+1}(t+d_{i+1})\times\prod_{k=i+2}^{N}p_k(t+d_k)\right]dt > \lim_{T\to\infty}\frac{1}{T}\int_0^T\left[\prod_{k=1}^{N}p_k(t+d_k)\right]dt \tag{19}$$

Equation (19) implies Equation (20).

$$\prod_{k=1}^{i-1}p_k(t+d_k)\times p_i(t+d_i)\times p_{i+1}(t+d_{i+1})\times\prod_{k=i+2}^{N}p_k(t+d_k) > \prod_{k=1}^{N}p_k(t+d_k) \tag{20}$$

We simplify Equation (20) to obtain Equation (21).

$$p_i(t+d_i)\times p_{i+1}(t+d_{i+1}) > p_i(t+d)\times p_{i+1}(t+d) \tag{21}$$

Equation (22) is obtained by substituting $d_i = d$ and $d_{i+1} = d$ into Equation (21) because the right side of the inequality corresponds to $E(s'(t))$ where $d_1 = d_2 = \ldots = d_N = d$.

$$p_i(t+d+\Delta t)\times p_{i+1}(t+d-\Delta t) > p_i(t+d)\times p_{i+1}(t+d) \tag{22}$$

Since $p_i(t+d_i)$ and $p_{i+1}(t+d_{i+1})$ are monotonic, and for $\Delta t\to 0$, we can expand Equation (22) to obtain Equation (23).

$$\left[p_i(t+d)+\Delta t\times\frac{\partial p_i(t+d)}{\partial t}\right]\times\left[p_{i+1}(t+d)-\Delta t\times\frac{\partial p_{i+1}(t+d)}{\partial t}\right] > p_i(t+d)\times p_{i+1}(t+d) \tag{23}$$

By carrying out the multiplication rearranging terms from Equation (23), we obtain Equation (24).

$$\begin{aligned} p_i(t+d)\times p_{i+1}(t+d)+\Delta t\Big(\Big(\tfrac{\partial p_i(t+d)}{\partial t}\times p_{i+1}(t+d)\Big)-\Big(\tfrac{\partial p_{i+1}(t+d)}{\partial t}\times p_i(t+d)\Big)\Big) \\ -\Big(\Delta t^2\times\tfrac{\partial p_i(t+d)}{\partial t}\times\tfrac{\partial p_{i+1}(t+d)}{\partial t}\Big) > p_i(t+d)\times p_{i+1}(t+d) \end{aligned} \tag{24}$$

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.

$$\frac{\partial p_i(t+d)}{\partial t} = \frac{\partial p_{i+1}(t+d)}{\partial t} \tag{25}$$

Equation (24) can be simplified into Equation (26) using Equation (25).

$$-\left(\Delta t^2\times\frac{\partial p_i(t+d)}{\partial t}\times\frac{\partial p_{i+1}(t+d)}{\partial t}\right) > 0 \tag{26}$$

Equation (26) 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. □

Lemma 3. *Let* $p_1(t), \ldots, p_N(t) : \mathbb{R}\to\mathbb{R}$ *be nonnegative* τ*-periodic functions that are all monotonically increasing or all monotonically decreasing on* $(0,\tau]$*. Then the mean of Equation (27) is minimized when* $d_k = \frac{\tau}{N}*(k-1)$ *for* $k \in \{1, 2, \ldots, N\}$.

$$s(t) = \prod_{k=1}^{N}p_k(t+d_k) \tag{27}$$

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 $k \in \{1, 2, \ldots, N\}$; then, Equation (28) is the mean of $s'(t)$.

$$E(s'(t)) = \lim_{T\to\infty} \frac{1}{T} \int_0^T \prod_{k=1}^{N} p_k(t+d_k)dt \tag{28}$$

Let $\Delta t \to 0$, and for some $i \in \{1, 2, \ldots, N\}$; the value $s(t)$ is achieved with values of $d_1 = \frac{\tau}{N} \times 0$, $d_2 = \frac{\tau}{N} \times 1$, $\ldots$, $d_{i-1} = \frac{\tau}{N} \times (i-2)$, $\ldots$, $d_{i+2} = \frac{\tau}{N} \times (i+1)$, $\ldots$, $d_N = \frac{\tau}{N} \times (N-1)$. In addition, let $d_i = \frac{\tau}{N} \times (i-1+\Delta t)$, $d_{i+1} = \frac{\tau}{N} \times (i-\Delta t)$; then Equation (29) shows the value $E(s(t))$.

$$\begin{aligned} E(s(t)) = \lim_{T\to\infty} \tfrac{1}{T} \int_0^T \Big(\textstyle\prod_{k=1}^{i-1} p_k(t+d_k)\Big) \times p_i\big(t + \tfrac{\tau}{N} \times (i-1+\Delta t)\big) \times p_{i+1}\big(t + \tfrac{\tau}{N} * (-\Delta t)\big) \\ \times \Big(\textstyle\prod_{k=i+1}^{N} p_k(t+d_k)\Big)dt \end{aligned} \tag{29}$$

Let us assume $E(s'(t))$ is not optimal. Thus, a deviation such as $E(s(t)) < E(s'(t))$ is shown in Equation (30).

$$E(s(t)) < E\big(s'(t)\big) \tag{30}$$

We obtain Equation (31) by substituting Equations (28) and (29) into Equation (30).

$$\begin{aligned} \lim_{T\to\infty} \tfrac{1}{T} \int_0^T \Big(\textstyle\prod_{k=1}^{i-1} p_k(t+d_k))\Big) \times p_i\big(t + \tfrac{\tau}{N} \times (i-1+\Delta t)\big) \times p_{i+1}\big(t + \tfrac{\tau}{N} \times (i-\Delta t)\big) \\ \times \Big(\textstyle\prod_{k=i+1}^{N} p_k(t+d_k))\Big)d \;<\; \lim_{T\to\infty} \tfrac{1}{T} \int_0^T \textstyle\prod_{k=1}^{N} p_k(t+d_k)dt \end{aligned} \tag{31}$$

Equation (31) can be simplified into Equation (32).

$$p_i\Big(t + \frac{\tau}{N} \times (i-1+\Delta t)\Big) \times p_{i+1}\Big(t + \frac{\tau}{N} \times (i-\Delta t)\Big) < p_i\Big(t + \frac{\tau}{N} \times (i-1)\Big) \times p_{i+1}\Big(t + \frac{\tau}{N} \times i\Big) \tag{32}$$

Since $p_i(t+d_i) and\ p_{i+1}(t+d_{i+1})$ are monotonic, and $\Delta t \to 0$, we can expand Equation (32) to obtain Equation (33).

$$\begin{aligned} \Big(p_i\big(t + \tfrac{\tau}{N}(i-1)\big) + \tfrac{\tau}{N} \times \Delta t \tfrac{dp_i\left(t+\frac{\tau}{N}\right)}{dt}\Big) \times \Big(p_{i+1}\big(t + \tfrac{\tau}{N}(i)\big) - \tfrac{\tau}{N}\Delta t \times \tfrac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}\Big) \\ < \; p_i\big(t + \tfrac{\tau}{N} \times (i-1)\big) \times p_{i+1}\big(t + \tfrac{\tau}{N} \times i\big) \end{aligned} \tag{33}$$

By carrying out the multiplication in Equation (33), we arrive at Equation (34).

$$\begin{aligned} \big(p_i\big(t + \tfrac{\tau}{N}(i-1)\big) \times p_{i+1}\big(t + \tfrac{\tau}{N}(i)\big)\big) - \Big(p_i\big(t + \tfrac{\tau}{N}(i-1)\big) \times \tfrac{\tau}{N}\Delta t \times \tfrac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}\Big) \\ + \Big(p_{i+1}\big(t + \tfrac{\tau}{N}(i)\big) \times \tfrac{\tau}{N} \times \Delta t \tfrac{dp_i\left(t+\frac{\tau}{N}\right)}{dt}\Big) - \Big(\tfrac{\tau}{N} \times \Delta t \tfrac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \times \tfrac{\tau}{N}\Delta t \times \tfrac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}\Big) \\ < p_i\big(t + \tfrac{\tau}{N} \times (i-1)\big) \times p_{i+1}\big(t + \tfrac{\tau}{N} \times i\big) \end{aligned} \tag{34}$$

We obtain Equation (35) by subtracting $p_i\big(t + \frac{\tau}{N} \times (i-1)\big) \times p_{i+1}\big(t + \frac{\tau}{N} \times (i)\big)$ on both sides of the inequality.

$$\begin{aligned} -\Big(p_i\big(t + \tfrac{\tau}{N}(i-1)\big) \times \tfrac{\tau}{N}\Delta t \times \tfrac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}\Big) + \Big(p_{i+1}\big(t + \tfrac{\tau}{N}(i)\big) \times \tfrac{\tau}{N} \times \Delta t \tfrac{dp_i\left(t+\frac{\tau}{N}\right)}{dt}\Big) \\ -\Big(\tfrac{\tau}{N} \times \Delta t \tfrac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \times \tfrac{\tau}{N}\Delta t \times \tfrac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}\Big) < 0 \end{aligned} \tag{35}$$

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.

$$\frac{\partial p_i(t+d)}{\partial t} = \frac{\partial p_{i+1}(t+d)}{\partial t} \tag{36}$$

We obtain Equation (37) by substituting (36) into Equation (35) and factor out $\frac{\tau}{N}\Delta t \times \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt}$.

$$\frac{\tau}{N}\Delta t \times \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \times \left(p_{i+1}\left(t+\frac{\tau}{N}(i)\right) \ - p_i\left(t+\frac{\tau}{N}(i-1)\right)\right) - \left(\frac{\tau}{N} \times \Delta t \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt}\right)^2 < 0 \tag{37}$$

We obtain Equation (38) by dividing Equation (37) by $\Delta t \frac{dp_{i+1}\left(t+\frac{\tau}{N}\right)}{dt}$.

$$\left(p_{i+1}\left(t+\frac{\tau}{N}(i)\right) - p_i\left(t+\frac{\tau}{N}(i-1)\right)\right) < \frac{\tau}{N} \times \Delta t \frac{dp_i\left(t+\frac{\tau}{N}\right)}{dt} \tag{38}$$

Since $\Delta t \to 0$, Equation (38) 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. □

7.2. 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 (39).*

$$\lim_{T\to\infty} \frac{1}{T} \int_0^T R(t)\, dt \tag{39}$$

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 (40).*

$$R_{AND}(t) = P_1(t) \times P_2(t) \times \ldots P_N(t) \tag{40}$$

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 (41).*

$$R_{OR}(t) = 1 - ((1 - P_1(t)) \times (1 - P_2(t)) \ \times \ldots (1 - P_N(t))) \tag{41}$$

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 (42).*

$$EPS_{AND} = \lim_{T\to\infty} \frac{1}{T} \int_0^T R_{AND}(t)dt \tag{42}$$

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 (43).*

$$EPS_{OR} = \lim_{T\to\infty} \frac{1}{T} \int_0^T R_{OR}(t)dt \tag{43}$$

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

Proof. Let $Q_1(t+d_1),\ Q_2(t+d_2),\ldots,\ Q_N(t+d_N)$ be the steady-state solutions of the N-PLADD games. Then, $Q_1(t+d_1),\ Q_2(t+d_2),\ldots,\ Q_N(t+d_N)$ are τ-periodic functions that are monotonically increasing on $(0,\tau]$. The attacker's EPS when $d_1 = d_2 = \ldots = d_N$ is the mean of Equation (44).

$$\prod_{k=1}^{N} Q_k(t+d_k) \tag{44}$$

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

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

Proof. Let $Q_1(t+d_1),\ Q_2(t+d_2),\ldots,\ Q_N(t+d_N)$ be the steady-state solutions of the N-PLADD games. Then, $Q_1(t+d_1),\ Q_2(t+d_2),\ldots,\ Q_N(t+d_N)$ are τ-periodic functions that are monotonically increasing on $(0,\tau]$. The attacker's EPS when $d_k = \frac{\tau}{N} \times (k-1)$ for $k \in \{1,\ 2,\ldots,\ N\}$ is the mean of Equation (44).

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

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

Proof. Let $Q_1(t+d_1),\ Q_2(t+d_2),\ldots,\ Q_N(t+d_N)$ be the steady-state solutions of the N-PLADD games. Then, $1 - Q_1(t+d_1), 1 - Q_2(t+d_2)\ldots,\ 1 - Q_N(t+d_N)$ 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 (45).

$$\prod_{k=1}^{N} 1 - (Q_k(t+d_k)) \tag{45}$$

The steady-state solution of the probability that the attacker controls at least one resource at time t is given by Equation (46).

$$1 - \prod_{k=1}^{N} 1 - (Q_k(t+d_k)) \tag{46}$$

By **Lemma 2**, the mean of Equation (45) is maximized when $d_1 = d_2 = \ldots = d_N$. Thus, the attacker's EPS for Equation (46) is minimized when $d_1 = d_2 = \ldots = d_N$. □

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

Proof. Let $Q_1(t+d_1),\ Q_2(t+d_2),\ldots,\ Q_N(t+d_N)$ be the steady-state solutions of the N-PLADD games. Then, $1 - Q_1(t+d_1), 1 - Q_2(t+d_2)\ldots,\ 1 - Q_N(t+d_N)$ 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 (45). The steady-state solution of the probability that the attacker controls at least one resource at time t is given by Equation (46).

By **Lemma 3**, the mean of Equation (45) is minimized when $d_k = \frac{\tau}{N} \times (k-1)$ for $k \in \{1, 2, \ldots, N\}$. Thus, the attacker's EPS for Equation (46) is maximized when $d_k = \frac{\tau}{N} \times (k-1)$ for $k \in \{1, 2, \ldots, N\}$. □

8. Experimental Results

The implementation of a single PLADD game is shown in Figure 16. The time unit used in Figure 16 is days, but this can be switched to another 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.

Given the attack scenarios as described in Section 4, the attacker's goal is to open/close breakers to cause a blackout. As shown in Figures 5 and 6, 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.

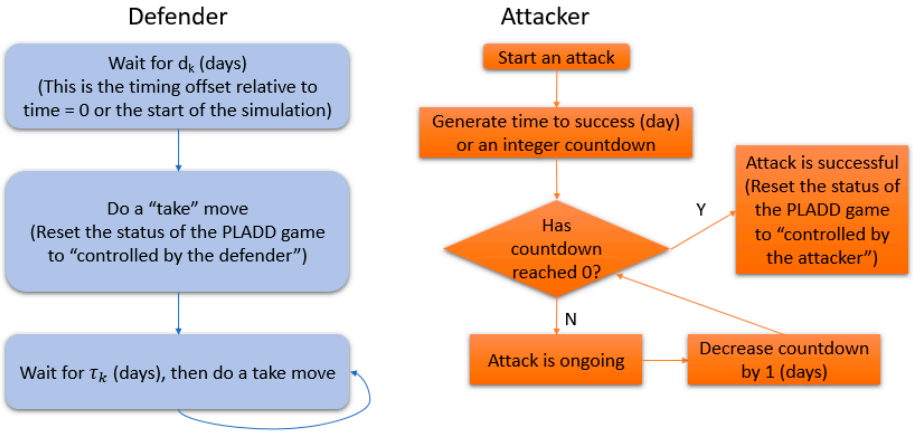

Figure 16. Implementation of a single PLADD game.

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 (40) and (41) to calculate the attacker's probability of a successful attack on the parallel PLADD system with respect to time. Then, we use Equations (42) and (43) 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 6.

To quantify the improvement shown in the experiment results, we define an equation for the percent improvement in Equation (47).

$$Percent\ improvement = \frac{Maximum\ EPS - Minimum\ EPS}{Maximum\ EPS} \times 100\% \quad (47)$$

Table 6. Simulation of attacker's expected probability of success.

	Simulation #	Player Parameters (Days)	PLADD Game Offsets (Days)	EPS	Percent Improvement
Figure 6 AND configuration	1.a		$d_{RTU1} = 0$, $d_{RTU2} = 0$	0.169	
	1.b	$\tau = 90$, $\mu = 90$	$d_{RTU1} = 0$, $d_{RTU2} = 30$	0.121	33.1
	1.c		$d_{RTU1} = 0$, $d_{RTU2} = 45$	0.113	
	1.d		$d_{RTU1} = 0$, $d_{RTU2} = 60$	0.117	
	2.a		$d_{RTU1} = 0$, $d_{RTU2} = 0$	0.059	
	2.b	$\tau = 90$, $\mu = 180$	$d_{RTU1} = 0$, $d_{RTU2} = 30$	0.040	37.3
	2.c		$d_{RTU1} = 0$, $d_{RTU2} = 45$	0.037	
	2.d		$d_{RTU1} = 0$, $d_{RTU2} = 60$	0.038	
	3.a		$d_{RTU1} = 0$, $d_{RTU2} = 0$	0.379	
	3.b	$\tau = 180$, $\mu = 90$	$d_{RTU1} = 0$, $d_{RTU2} = 60$	0.281	30.6
	3.c		$d_{RTU1} = 0$, $d_{RTU2} = 90$	0.263	
	3.d		$d_{RTU1} = 0$, $d_{RTU2} = 120$	0.270	
Figure 6 OR configuration	1.a		$d_{computer1} = 0$, $d_{computer2} = 0$	0.567	
	1.b	$\tau = 90$, $\mu = 90$	$d_{computer1} = 0$, $d_{computer2} = 30$	0.585	3.57
	1.c		$d_{computer1} = 0$, $d_{computer2} = 45$	0.588	
	1.d		$d_{computer1} = 0$, $d_{computer2} = 60$	0.586	
	2.a		$d_{computer1} = 0$, $d_{computer2} = 0$	0.3672	
	2.b	$\tau = 90$, $\mu = 180$	$d_{computer1} = 0$, $d_{computer2} = 30$	0.3673	0.08
	2.c		$d_{computer1} = 0$, $d_{computer2} = 45$	0.3675	
	2.d		$d_{computer1} = 0$, $d_{computer2} = 60$	0.3674	
	3.a		$d_{computer1} = 0$, $d_{computer2} = 0$	0.749	
	3.b	$\tau = 180$, $\mu = 90$	$d_{computer1} = 0$, $d_{computer2} = 60$	0.766	3.10
	3.c		$d_{computer1} = 0$, $d_{computer2} = 90$	0.773	
	3.d		$d_{computer1} = 0$, $d_{computer2} = 120$	0.772	

8.1. Single-Layer PLADD Simulation

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 6). 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 Figures 17 and 18. As described in Section 7, Equations (40) and (41) are used to plot R_{AND} and R_{OR} in Figures 17 and 18. Table 6 shows the attacker's EPS in our simulations.

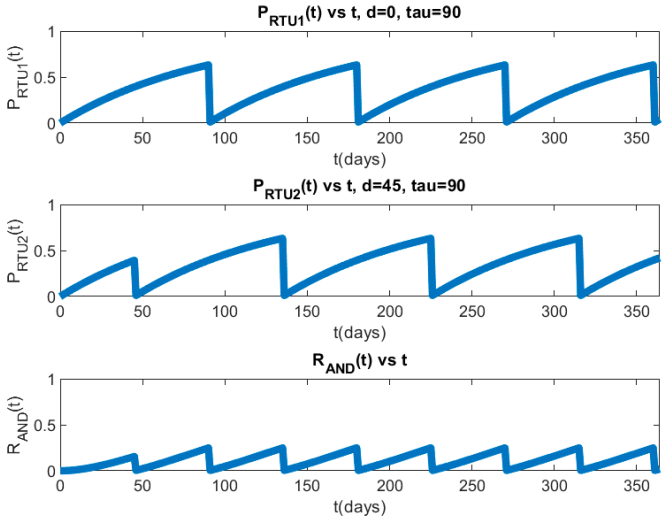

Figure 17. Simulation 1.c: We set $d_{RTU1} = 0$, $d_{RTU2} = 45$, $\mu_{RTU1} = \mu_{RTU2} = 90$, $\tau_{RTU1} = \tau_{RTU2} = 90$.

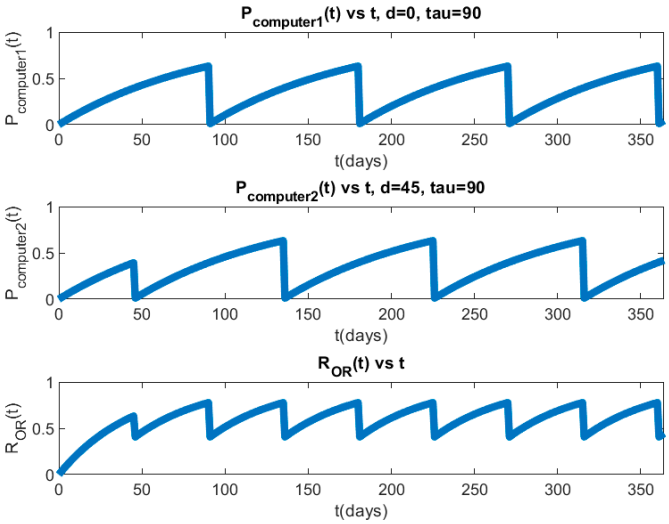

Figure 18. Simulation 1.c: We set $d_{computer1} = 0$, $d_{computer2} = 45$, $\mu_{computer1} = \mu_{computer2} = 90$, $\tau_{computer1} = \tau_{computer2} = 90$.

8.2. Hierarchical PLADD Simulation

The hierarchical PLADD simulations are shown in Table 7, and illustrations of the OR_AND_AND and AND_OR_OR configurations are shown in Figures 8 and 9. We have simulated our example attack scenarios with 11 different sets of d_k (as shown in Table 7). 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 offsets 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 offsets 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 offsets equal to zero, while PLADD games 2 and 3 have offsets of 45 days. Simulation 10 assumes PLADD game 1 has an offset of zero, PLADD game 2 and 3 have offsets 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 offsets of 45 days. Using Equation (47), the percent improvement in OR_AND_AND configuration is 19.4%, and the percent improvement in AND_OR_OR configuration is 18.4%.

Table 7. 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

9. Discussion

Based on Table 6, 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 the AND configuration and the 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 7, we show that the hierarchical parallel PLADD system also follows the same rules proved in Theorems 5–8. Let us 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 apply Theorems 6 and 7 to minimize EPS and (ii) tuple α and tuple β minimized also applies Theorems 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 in 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.

10. Conclusions

Various access controls protect cyber-physical systems. These access controls can be a combination of passwords, keycards, internet protocol addresses, and more. While it is important to focus on hardening the security of individual access controls, it is also noteworthy to look at the entire system's security. Our research can determine whether the access controls in a cyber-physical system are working together to improve the overall security. Specifically, our research's contribution is a mathematical approach to determine security policy recommendations for a cyber-physical system. Based on the assumption that all MTDs have the same reset period, the reset of secret information for all MTDs in the AND should be equally spaced apart. The reset of secret information for all MTDs in the OR configuration should be at the same time. This paper introduces a novel concept of a hierarchical parallel PLADD system to cover attack scenarios that are not described in prior articles. In conclusion, we have clarified key concepts and provided experimental results to validate our findings.

Author Contributions: Conceptualization, Y.-C.C., V.J.M.III, and S.G.; methodology, Y.-C.C., V.J.M.III, and S.G.; software, Y.-C.C.; validation, Y.-C.C., V.J.M.III, and S.G.; formal analysis, Y.-C.C., V.J.M.III, S.G.; investigation, Y.-C.C., V.J.M.III, and S.G.; writing—original draft preparation, Y.-C.C.; writing—review and editing, Y.-C.C., V.J.M.III, and S.G.; visualization, Y.-C.C.; supervision, V.J.M.III and S.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by Sandia National Laboratory under Contract #1838573 and the Depart of Energy under Contract # DE-CR0000004.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chen, Y.; Mooney, V.; Grijalva, S. Grid Cyber-Security Strategy in an Attacker-Defender Model. In Proceedings of the 2020 Clemson University Power Systems Conference (PSC), Clemson, SC, USA, 10–13 March 2020; pp. 1–8. [CrossRef]
2. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Available online: https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf (accessed on 26 December 2020).
3. Lee, R.M.; Assante, M.J.; Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid. 2016. Available online: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed on 26 December 2020).
4. Styczynski, J. When the Lights Went Out. Available online: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf (accessed on 26 December 2020).
5. Chukwuka, V.; Chen, Y.; Grijalva, S.; Mooney, V. Bad Data Injection Attack Propagation in Cyber-Physical Power Delivery Systems. In Proceedings of the 2018 Clemson University Power Systems Conference (PSC), Charleston, SC, USA, 4–7 September 2018; pp. 1–8. [CrossRef]
6. Dario, B. Game Theory: Models, Numerical Methods and Applications. *Found. Trends® Syst. Control* **2014**, *1*, 379–522.
7. Deisenroth, M.P.; Faisal, A.A.; Ong, C.S. Mathematics for Machine Learning: Cambridge University Press. Available online: https://mml-book.github.io/book/mml-book.pdf (accessed on 28 December 2020).
8. John the Ripper Password Cracker. Openwall. Available online: https://www.openwall.com/john/ (accessed on 15 November 2019).

9. Ulrich, J.; Drahos, J.; Govindarasu, M. A symmetric address translation approach for a network layer moving target defense to secure power grid networks. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 163–169. [CrossRef]
10. Evtyushkin, D.; Ponomarev, D.; Abu-Ghazaleh, N. Jump over ASLR: Attacking branch predictors to bypass ASLR. In Proceedings of the 2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), Taipei, Taiwan, 15–19 October 2016; pp. 1–13. [CrossRef]
11. Hashcat-Advanced Password Recovery. Hashcat. Available online: https://hashcat.net/hashcat/ (accessed on 15 November 2019).
12. Bošnjak, L.; Sreš, J.; Brumen, B. Brute-force and dictionary attack on hashed real-world passwords. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1161–1166. [CrossRef]
13. Jones, S.; Outkin, A.; Gearhart, J.; Hobbs, J.; Siirola, J.; Phillips, C.; Verzi, S.; Tauritz, D.; Mulder, S.; Naugle, A. Evaluating Moving Target Defense with PLADD. Available online: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2015/158432r.pdf (accessed on 29 December 2020).