CYBER THREAT PROPAGATION MODELING IN CYBER PHYSICAL SYSTEMS

Ph.D. Dissertation Defense

By

Yu-Cheng Chen

Adviser: Professor Vincent John Mooney

Co-adviser: Professor Santiago Grijalva

Georgia Institute Of Technology

Atlanta, GA, USA

Thursday, April 14th, 2022

Georgia Tech

Outline

- Introduction
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

2

Georgia Tech

Outline

- **Introduction**
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

3

Georgia Tech

Cyber-Physical System Security - Motivation

- Ukraine power grid attack (2015, 2016) were major wake up calls for the power grid industry [1]
- Using the power grid as an example of cyber-physical system
- Study the different ways in which the cyber-physical power grid can be compromised
- Develop techniques to evaluate and mitigate the propagation, and impact of a potential cyber-physical attack

Imagine source [2]

4

Georgia Tech

Recent Threats, Attacks and Concerns

- According to a U.S. Department of Energy report[3], in 2014, roughly 55% of the reported incidents involved advanced persistent threats (APT)
- In 2019, Siemens and the Ponemon Institute produced a cybersecurity report asserting that cyberthreats to utility operation systems are becoming increasingly significant
  - 54% of the 1726 utility professionals surveyed, anticipate at least one cyberattack on critical infrastructure in the coming year [4,5]

Power grid security – Taking action

- The Federal Energy Regulatory Commission (FERC) approves the following Critical Infrastructure Protection (CIP) reliability standards, which was submitted by the North American Electric Reliability Corporation (NERC) [6]:
  - CIP-013-1 (Cyber Security—Supply Chain Risk Management)
  - CIP-005-6 (Cyber Security—Electronic Security Perimeter(s))
  - CIP-010-3 (Cyber Security—Configuration Change Management and Vulnerability Assessments)
  - This rule is effective December 26, 2018
- On May 1st, 2020, President Donald Trump signed an executive order aimed at securing the U.S. bulk-power system [7]

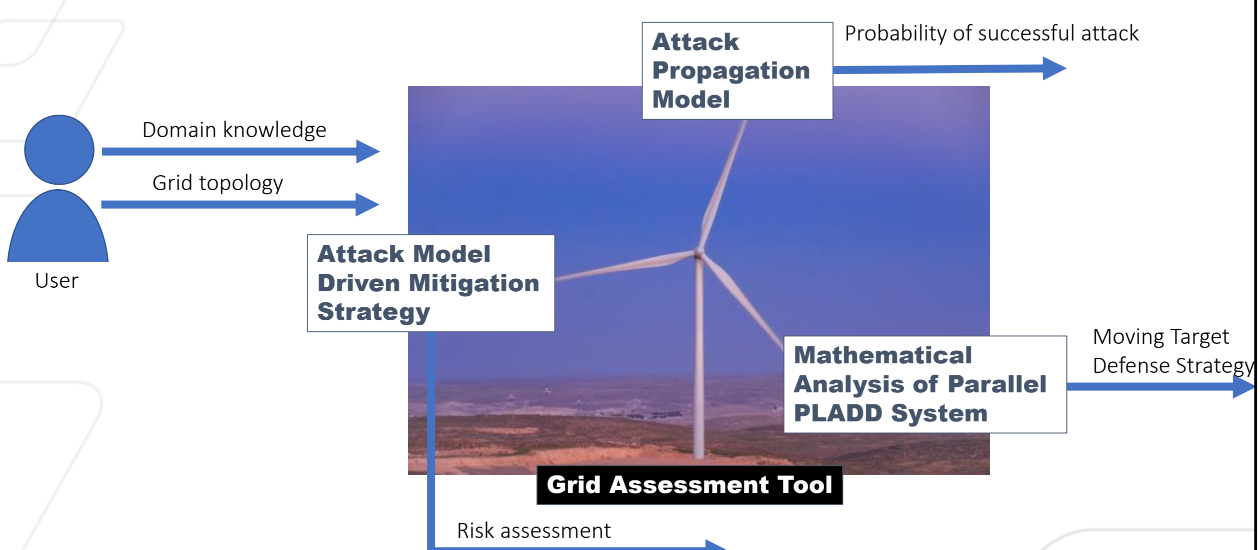
Outline

- Introduction
- **Research Overview**
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

7

Georgia Tech

Research Overview



Georgia Tech

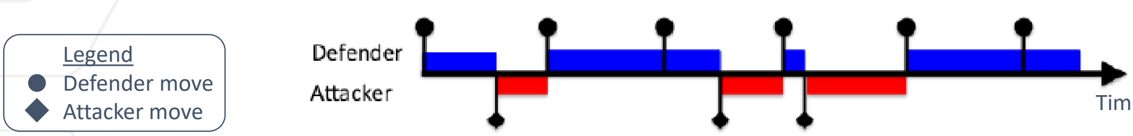
Outline

- Introduction
- Research Overview
- **Background and Prior Work**
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

9

Georgia Tech

Prior Work: FlipIt



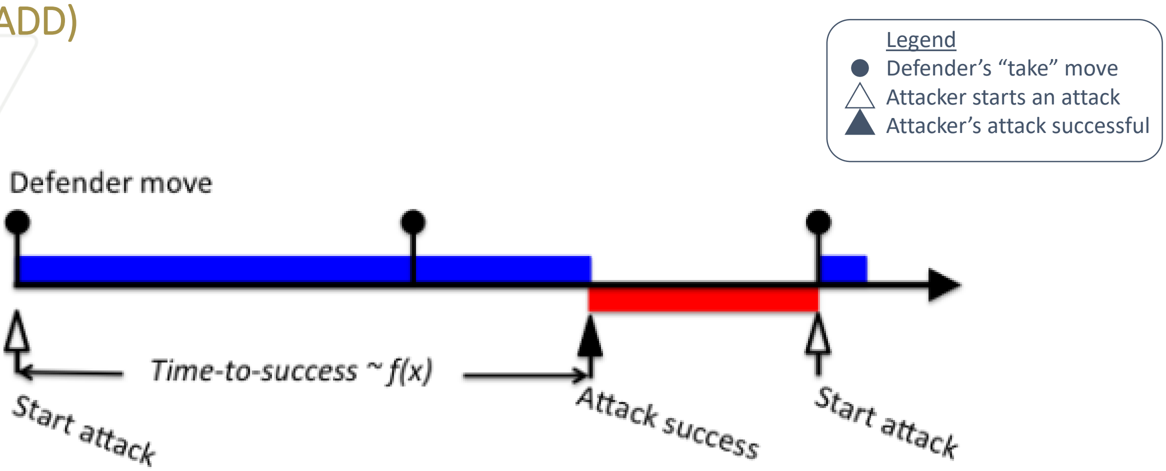
An Illustrative example of the FlipIt game showing the resource changing hands between the attacker (red) and the defender (blue) as time progresses from left to right

- FlipIt [8] provides insight into attack-defender interactions
- Two players, the defender and the attacker, content for control of a single shared resource
- The defender initially controls the resource
- When players move, they immediately gain control of the resource

10

Georgia Tech

Prior Work: Probabilistic Learning Attacker, Dynamic Defender (PLADD)

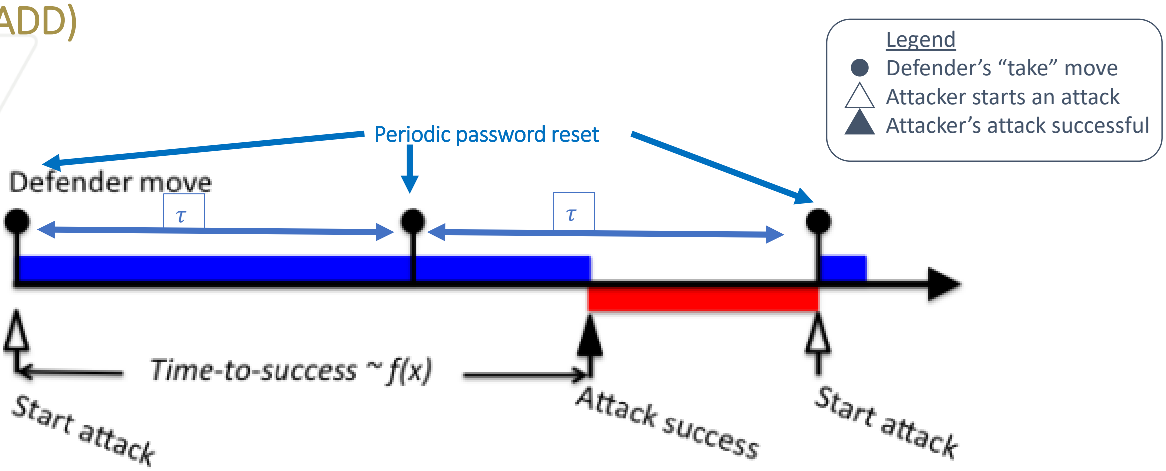


- A PLADD [9] game represents an access control or resource
- There is one attacker and one defender contesting for control of the resource

11

Georgia Tech

Prior Work: Probabilistic Learning Attacker, Dynamic Defender (PLADD)

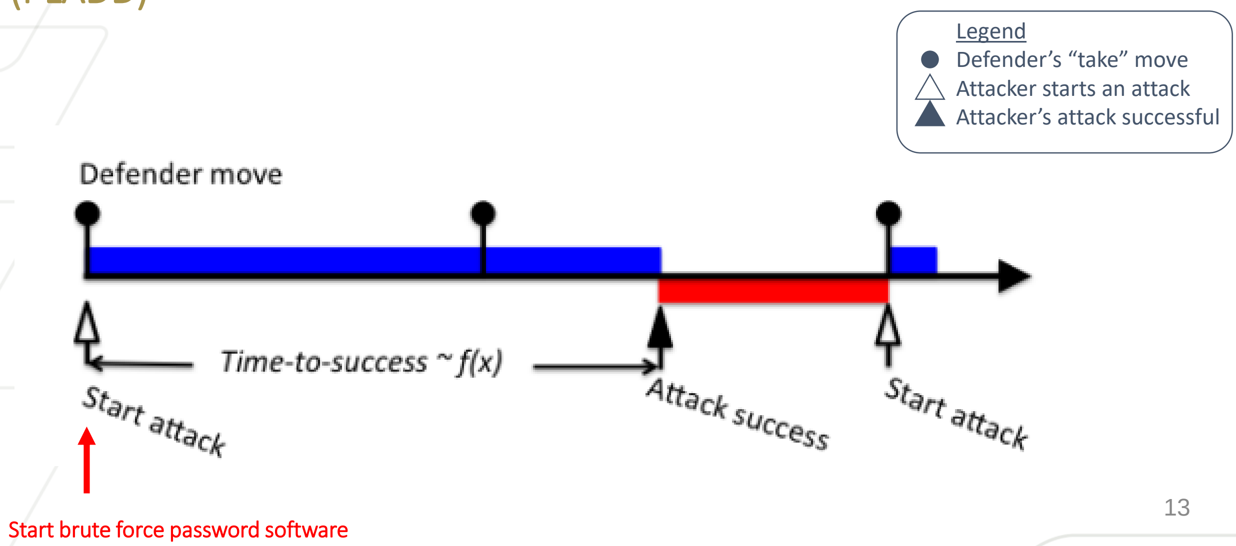


- Defender move: "Take" move, periodically take back control of resource

12

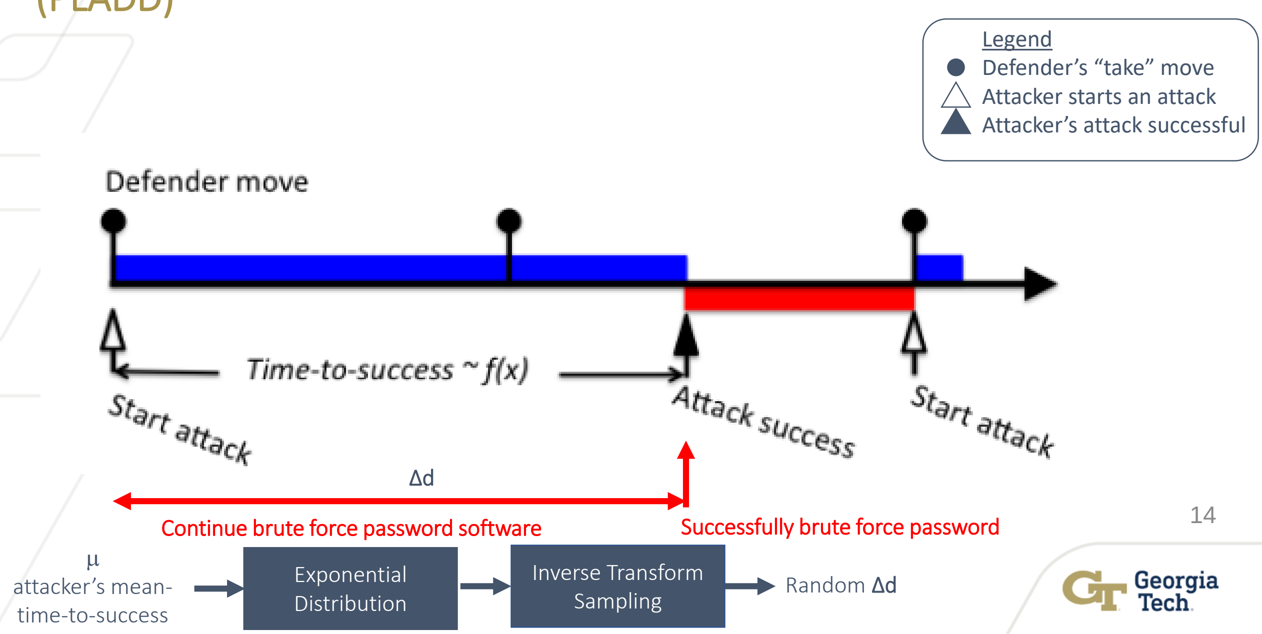
Georgia Tech

Prior Work: Probabilistic Learning Attacker, Dynamic Defender (PLADD)



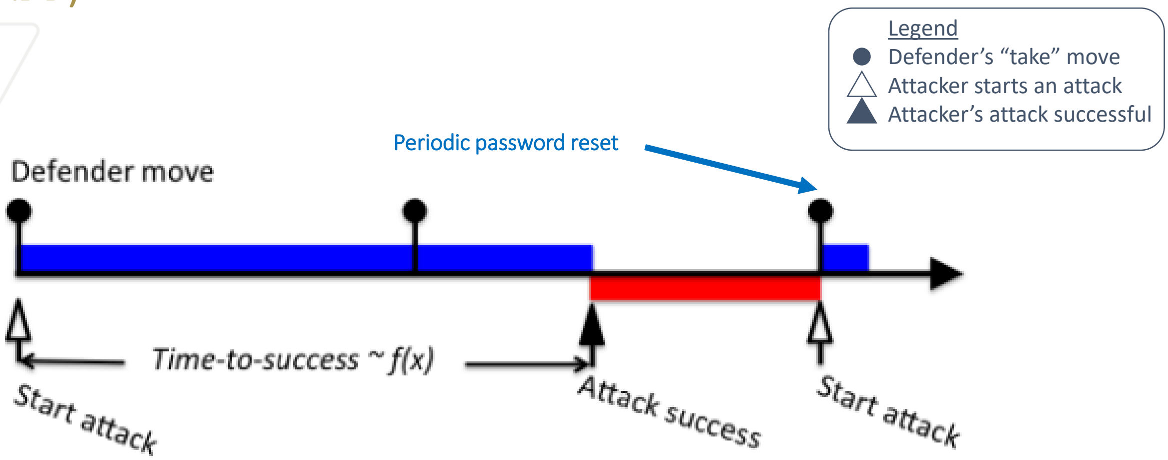
13

Prior Work: Probabilistic Learning Attacker, Dynamic Defender (PLADD)



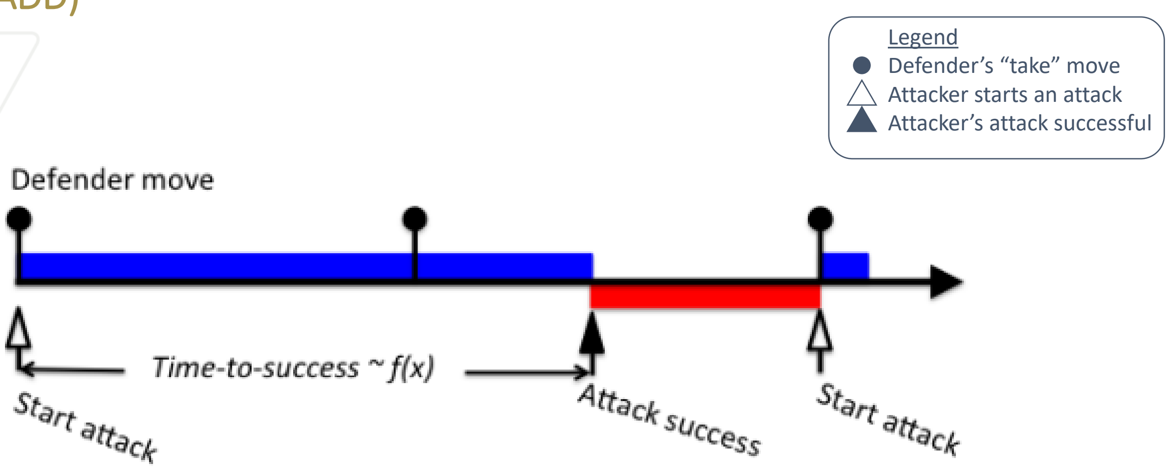
14

Prior Work: Probabilistic Learning Attacker, Dynamic Defender (PLADD)



15

Prior Work: Probabilistic Learning Attacker, Dynamic Defender (PLADD)



- PLADD is good at modelling the notion of time, but PLADD assumes that defender cannot do detection to know if there's an ongoing attack or whether the attacker has control
- In addition, actions such breaking a lock at the substation is difficult to model

16

Prior Work: Markov Chain Model

Markov Chain Equation [10]

- $x^{(T)} = x^{(T-1)} * P$
  $= \left(x^{(T-2)} * P\right) * P \ \dots = x^{(0)} * P^T$
- x^T is the probability (event of interest) occurring at each node
- T is time unit (seconds, minutes, hours,..., etc)
- P is the transitional matrix

17

Georgia Tech

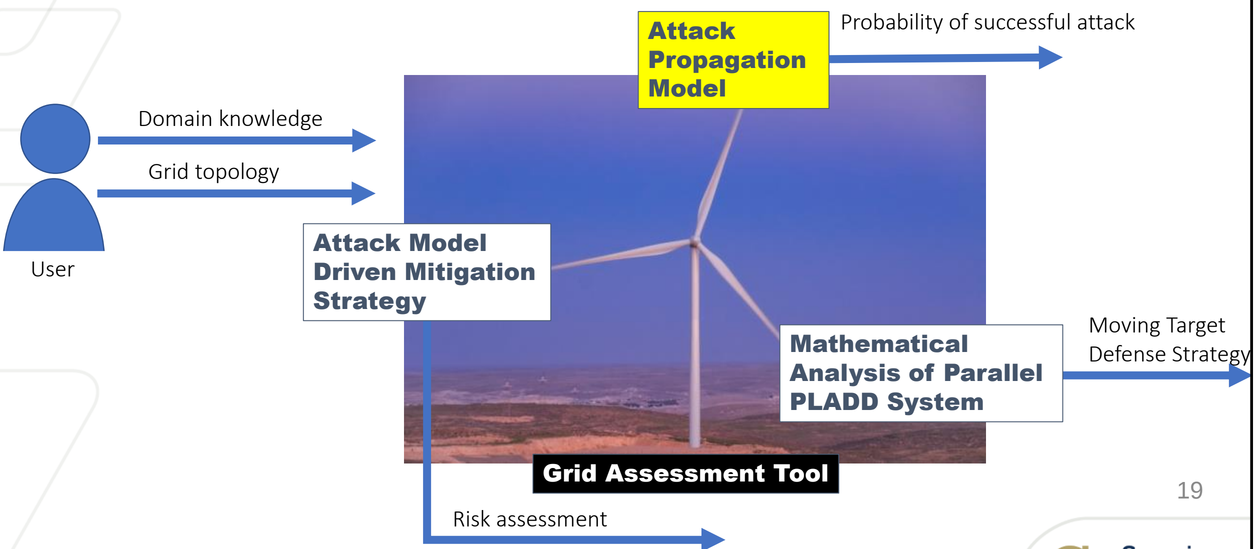
Outline

- Introduction
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
  - **Attack Propagation Model with Markov Chain**
  - Attack Propagation Model with Hybrid Attack Model
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

18

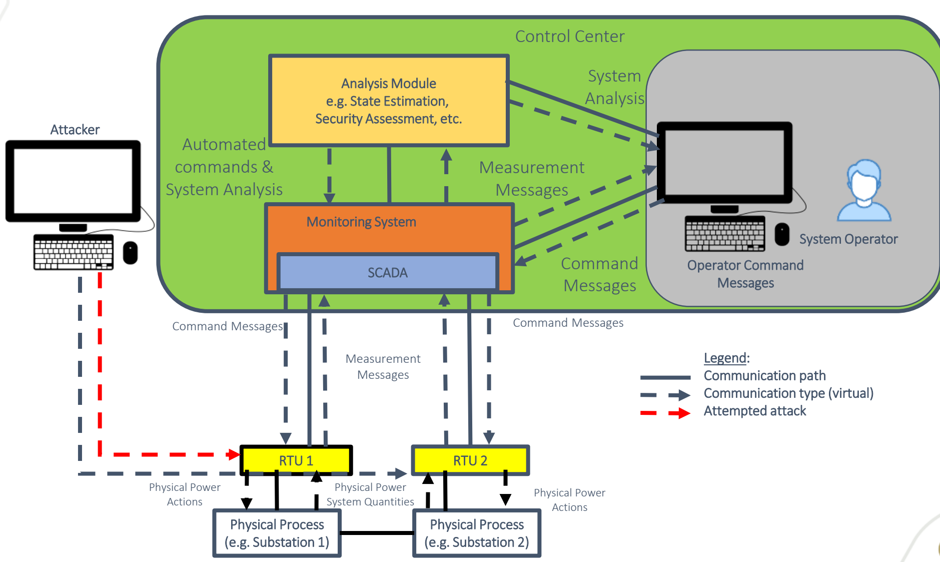
Georgia Tech

Research Overview



19

Bad Data Injection Scenario



20

Substation (Satellite view)

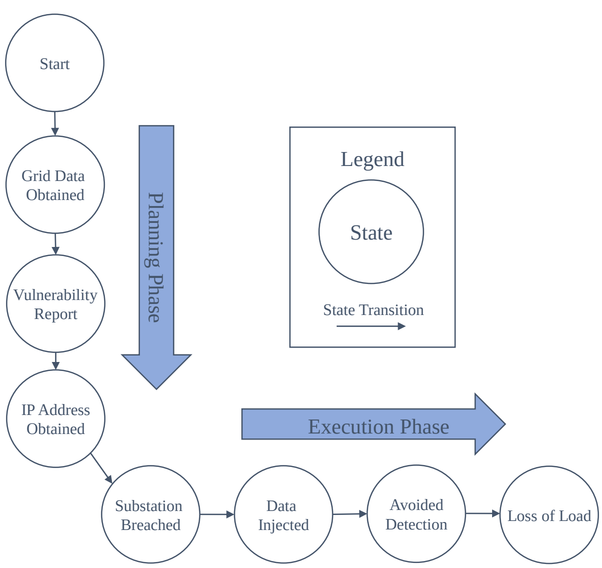
Marietta Power Substation

Substation Room

21

Georgia Tech

Generic Bad Data Injection Attack Graph



22

Georgia Tech

Attack Graph

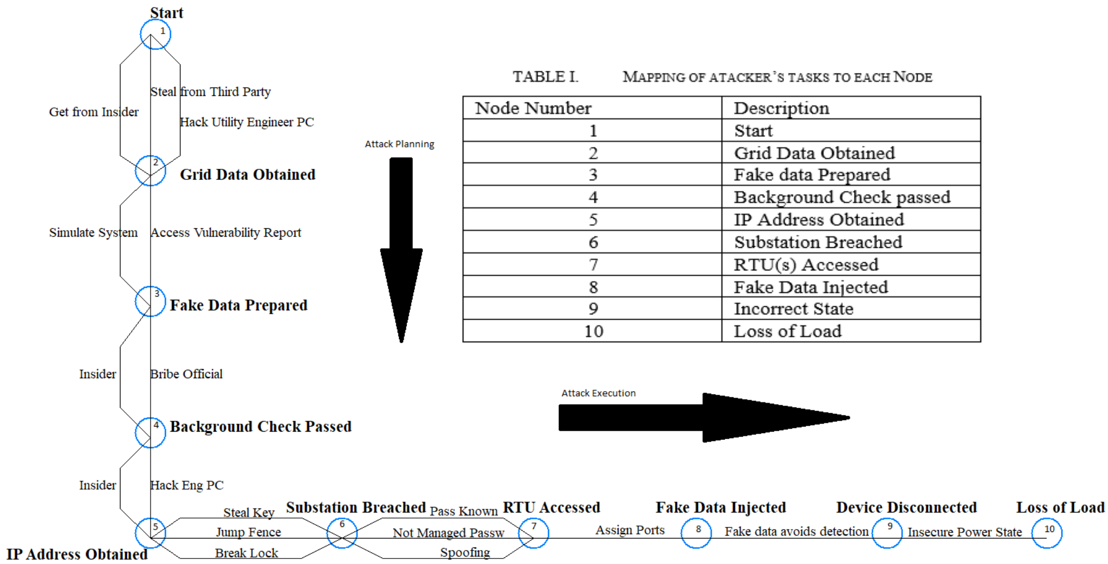


TABLE I. MAPPING OF ATACKER'S TASKS TO EACH NODE

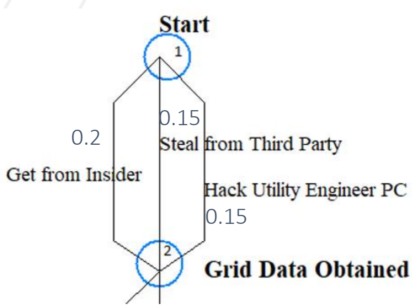
Node Number	Description
1	Start
2	Grid Data Obtained
3	Fake data Prepared
4	Background Check passed
5	IP Address Obtained
6	Substation Breached
7	RTU(s) Accessed
8	Fake Data Injected
9	Incorrect State
10	Loss of Load

Attack graph capturing attacker's strategy

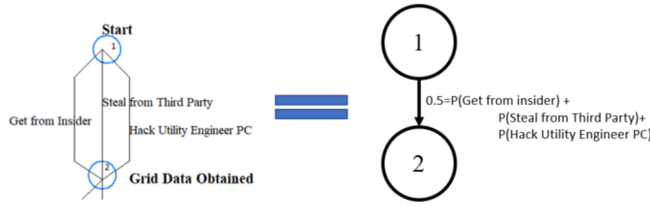
23

Georgia Tech

Attack Graph



- Vertex – Attacker's sub-goal
- Edge – Action performed by the attacker
  - Each edge has a probability parameter associated with it
  - Represents the probability of success in carrying out the action
  - Edges are directed (i.e., have an associated arrow)



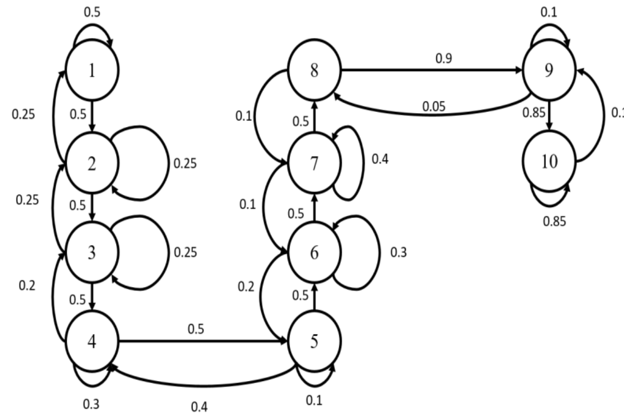
24

Georgia Tech

Markov Chain Model

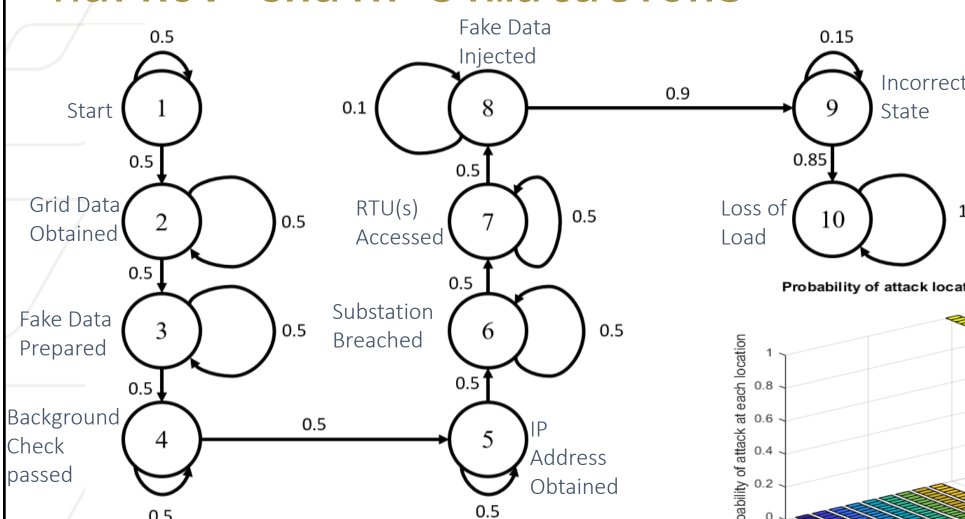
- Markov Chain capturing attacker's strategy for compromising the power system under attack assuming defender with no state estimation

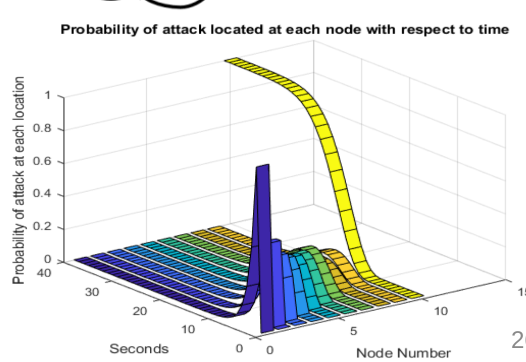
$$P = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.25 & 0.25 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.25 & 0.5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.2 & 0.3 & 0.5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.4 & 0.1 & 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.2 & 0.3 & 0.5 & 0 & 0 &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



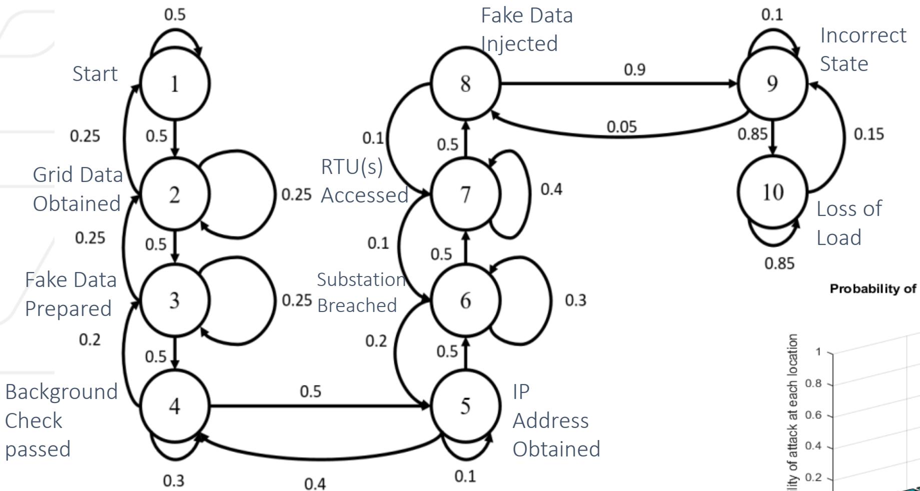
Georgia Tech

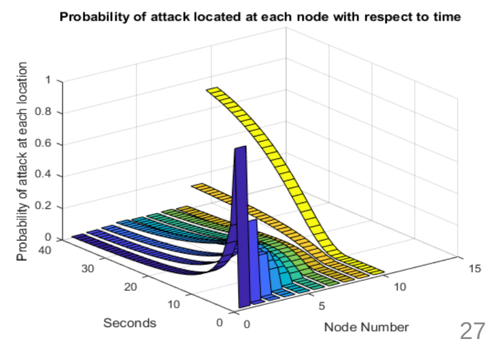
Markov Chain Simulations





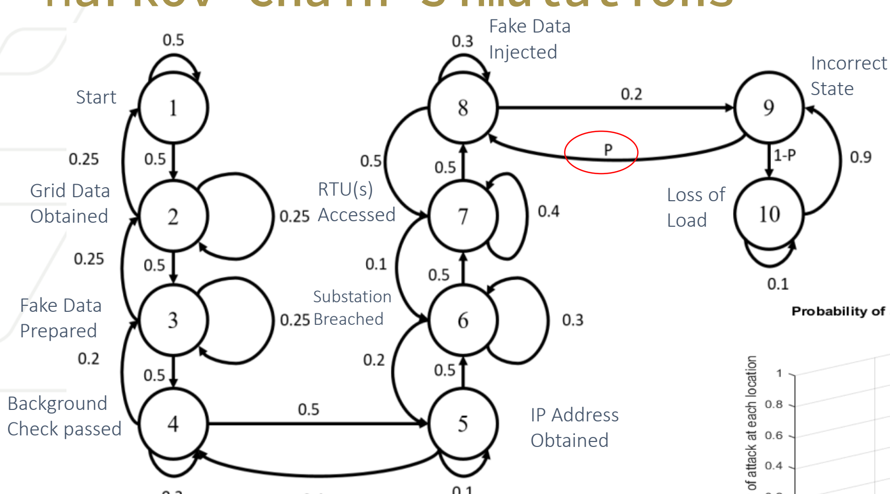
Markov Chain Simulations

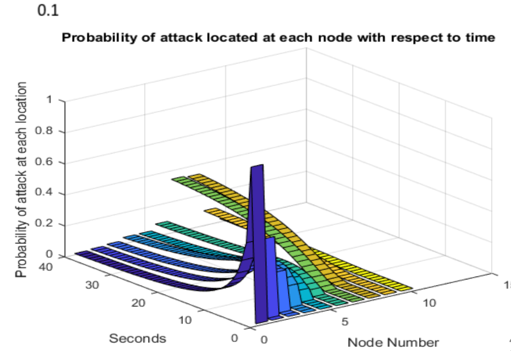




27

Markov Chain Simulations





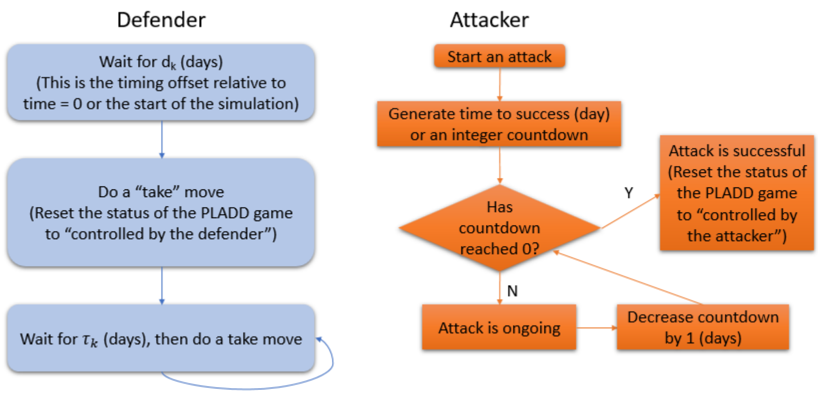
28

Outline

Motivation of Hybrid Attack Model

- Analysis of attacks on the cyber physical system should consist of both an attack planning and execution phase
  - Attack planning phase: Gather information with regards to the target of the attack
  - Attack execution phase: Execute attack on the target using information gathered from the planning phase
- We propose an attack model that can simulate the propagation of attack from the attacker's attack planning phase to execution phase
- The Markov Chain model is good at modelling attack propagation, however, it is not so great at modeling the back and forth interaction between the attacker and the defender in the planning stage

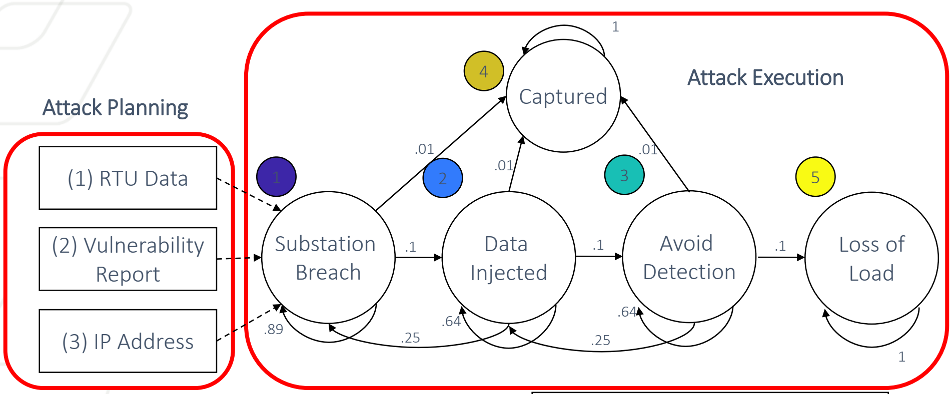
Implementation of a single PLADD game

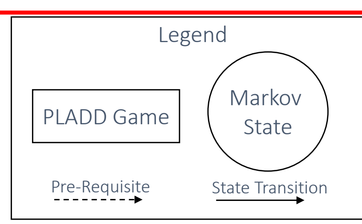


31

Georgia Tech

Hybrid Attack Model



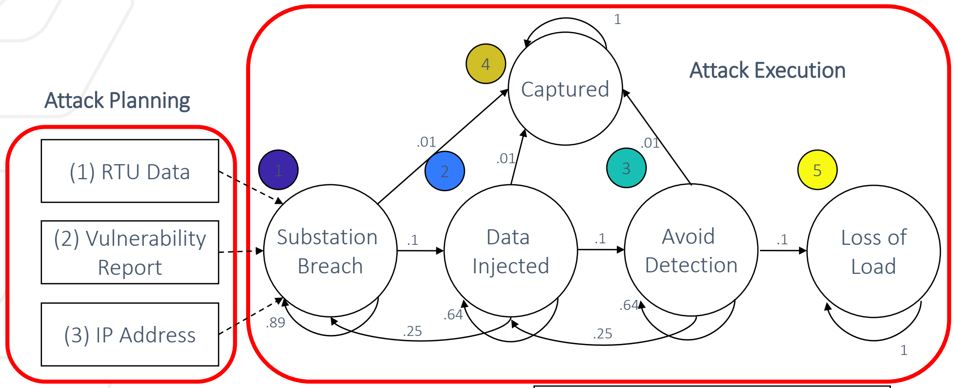


- The hybrid attack model consists of both PLADD game and Markov state
- Assumed attacker need to have control of all PLADD game to be in the execution phase

32

Georgia Tech

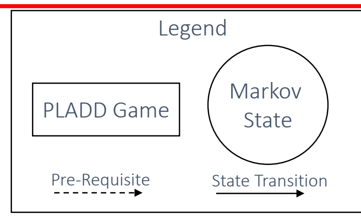
Hybrid Attack Model



Time between each defender's move

Average time of attack completion

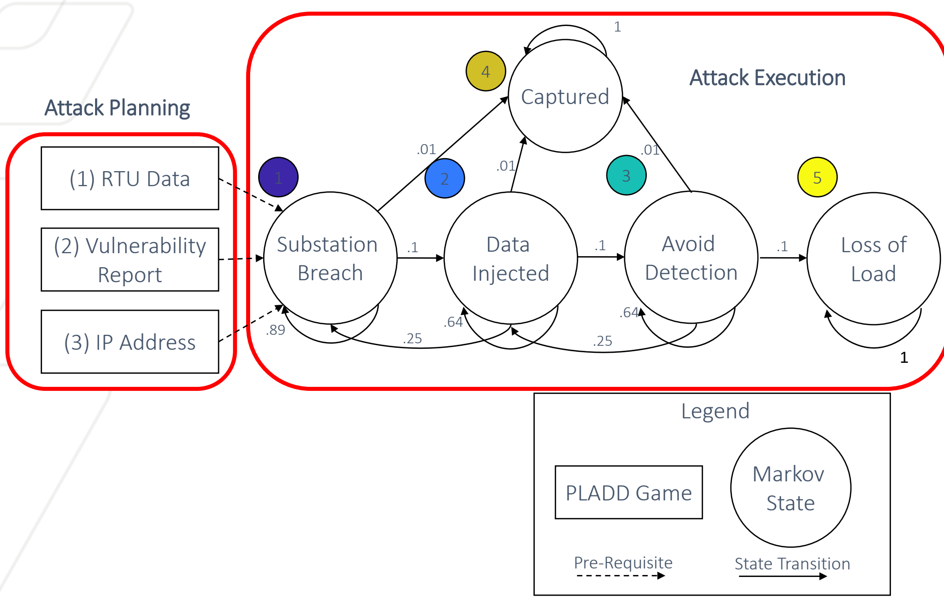
PLADD Node #	τ (day)	μ (day)
1	10	5
2	5	3
3	90	1



33

Georgia Tech

Hybrid Attack Model



$$Equation\ 1{:}\ x^{(T)} = x^{(0)} \times P^{T}$$

if attacker controls all PLADD nodes

$$x^{(0)} = [1, 0, 0, 0, 0]$$

else

$$x^{(0)} = [0, 0, 0, 0, 0]$$

$$P = \begin{bmatrix} .89 & .1 & 0 & .01 & 0 \\ .25 & .64 & .1 & .01 & 0 \\ 0 & .25 & .64 & .01 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

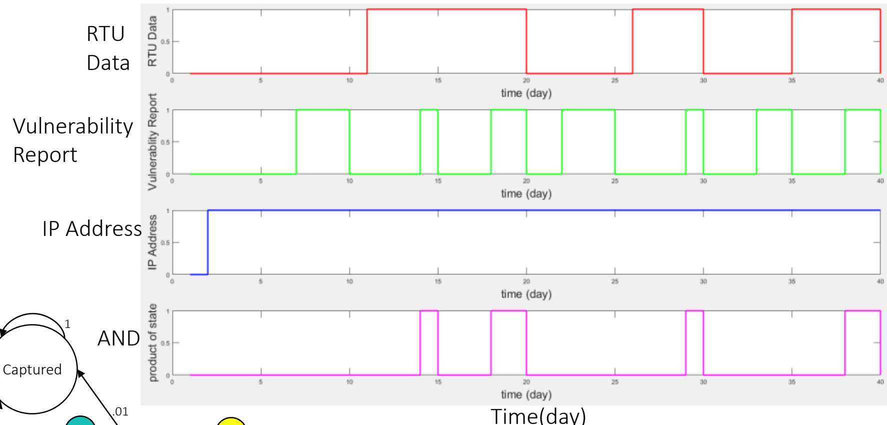
$T = time\ step$

34

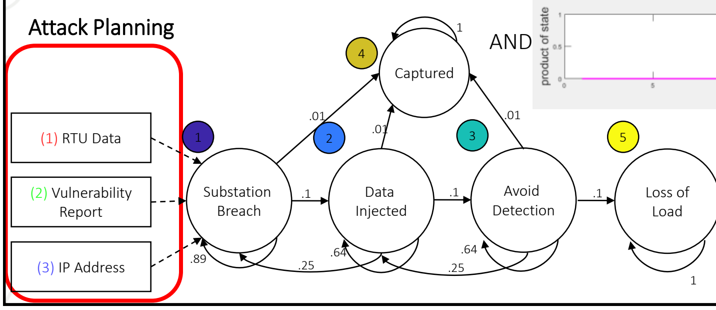
Georgia Tech

Simulation Result (Planning)

- State of each PLADD game with respect to time is shown
- State = 1 means attacker have access to the resource
- State = 0 means defender have access to the resource



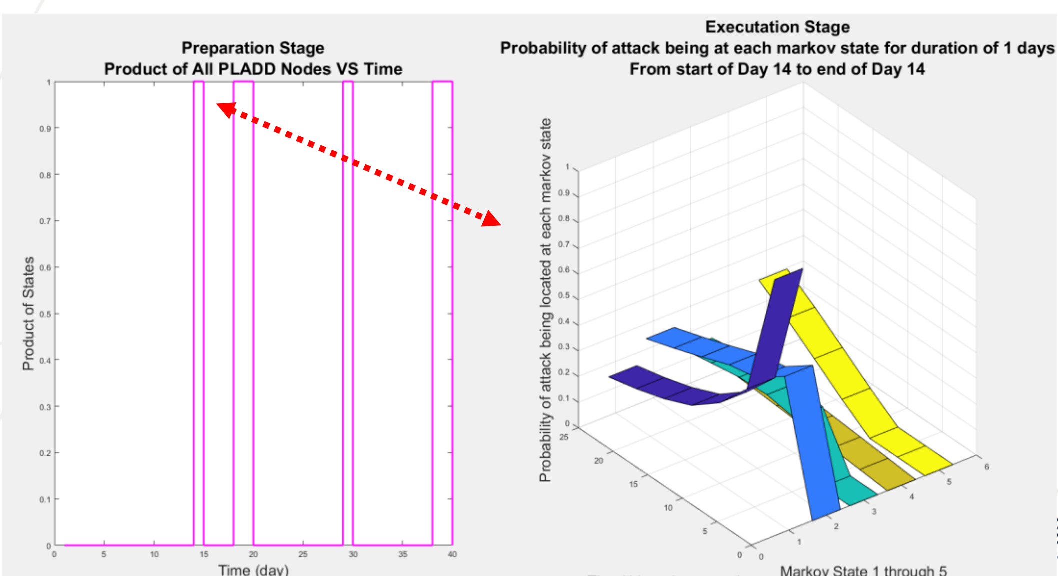
Attack Planning



35

Georgia Tech

Simulation Result (Execution)

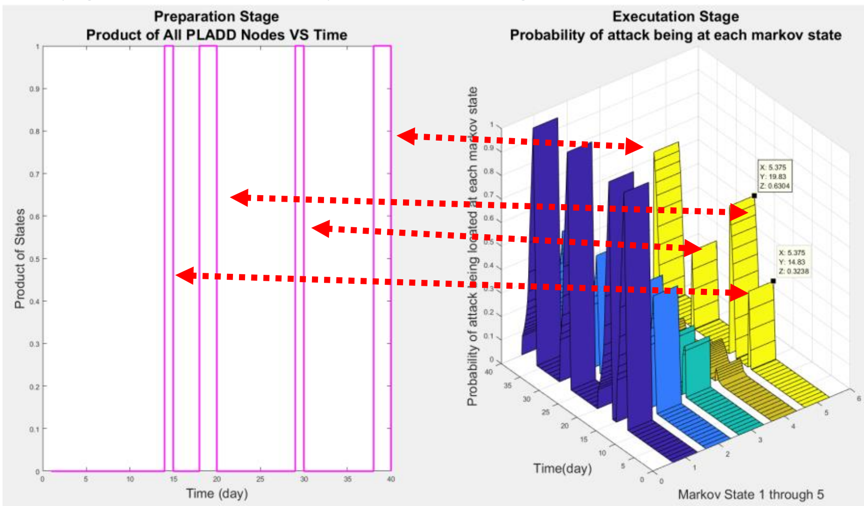


36

Georgia Tech

Simulation Result (Execution)

- Product-of-all-state is reproduced on the left
- Attacker is in execution phase on 14th, 18th-19th, 29th , 38th -39th
- Propagation of attack for 40 days is drawn on the right



37

Georgia Tech

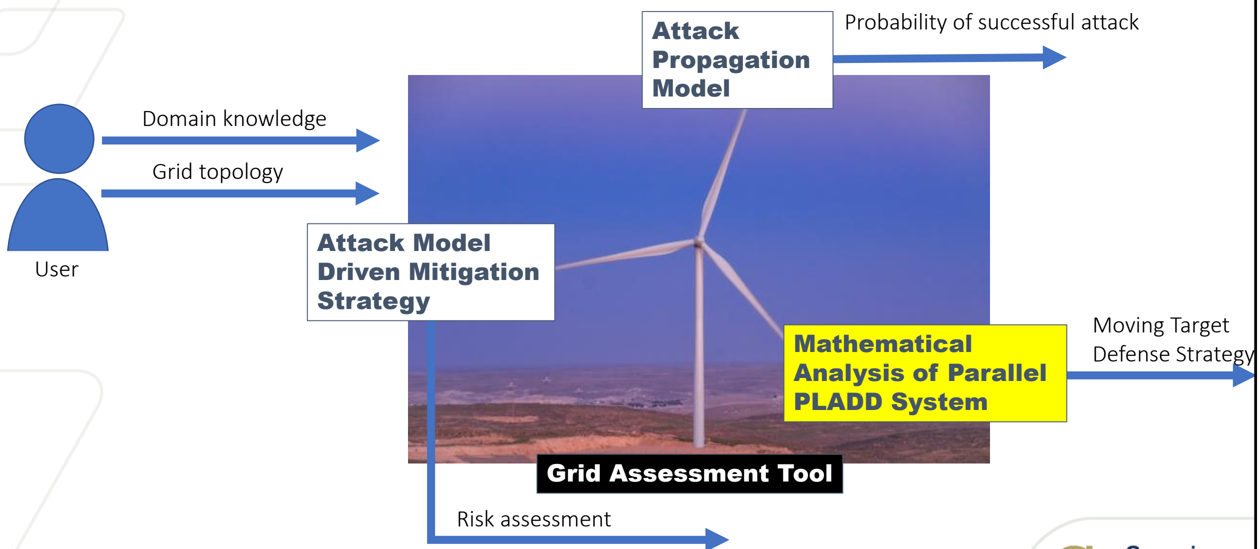
Outline

- Introduction
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
  - **Overview of Major Theorems**
  - Simulation Results
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

38

Georgia Tech

Research Overview



Georgia Tech

PLADD Node (Mathematical Representation)

- A PLADD game models a resource that an attacker and a defender contend to control
- A parallel PLADD system is a system with multiple PLADD games that the attacker and defender simultaneously contend to control
- We make the following assumptions about each PLADD game:
- The defender executes "take" moves periodically; specifically, the defender executes "take" moves at $d_k, d_k + \tau_k, d_k + 2\tau_k, \ldots, d_k + n_k\tau_k$
- d_k is less than τ_k
  - 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
  - τ_k: The defender "take" period of a single game with index k in a parallel PLADD system
- The attacker is persistent, i.e., starts an attack at time 0 and immediately after anytime the defender takes back the resource

40

Georgia Tech

PLADD Node (Mathematical Representation)

- **The probability that the attacker controls the PLADD game with index k at time t is given below**

- $P_k(t)$: **The probability that the attacker controls a PLADD game with index k at time t.**
- $F_k(t)$: **The cumulative distribution function of the attacker's time-to-success in game with index k.**

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

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

Georgia Tech

Overview of Major Theorems

- **Theorem 1.** *Consider a 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*
- **Theorem 2.** *Consider a 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*

Georgia Tech

Example 1: AND Configuration

- We simulate three different defender 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
  3. the resets of each PLADD game in the parallel PLADD system are at different times but are not equally spaced apart

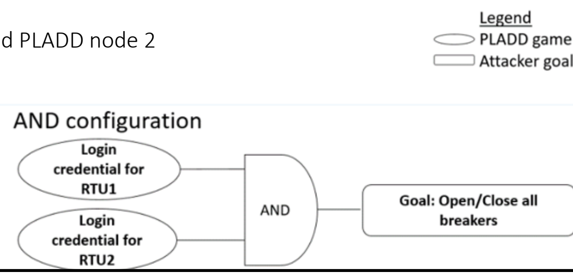
Table Legend

d_1, d_2: Delay counting from time = 0, for PLADD node 1 and PLADD node 2

τ_1, τ_2 : Period of defender reset, for PLADD node 1 and PLADD node 2

μ_1, μ_2: Attacker's mean-time-to-successful attack, for PLADD node 1 and PLADD node 2

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



Example 2: OR Configuration

- 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,
  3. the resets of each PLADD game in the parallel PLADD system are at different times but are not equally spaced apart

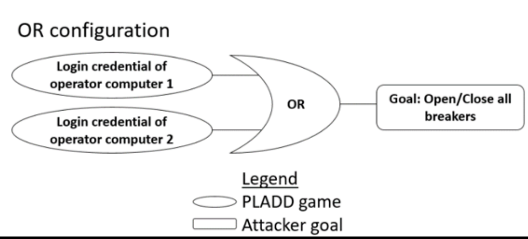
Table Legend

d_1, d_2: Delay counting from time = 0, for PLADD node 1 and PLADD node 2

τ_1, τ_2 : Period of defender reset, for PLADD node 1 and PLADD node 2

μ_1, μ_2: Attacker's mean-time-to-successful attack, for PLADD node 1 and PLADD node 2

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



Hierarchical Parallel PLADD System

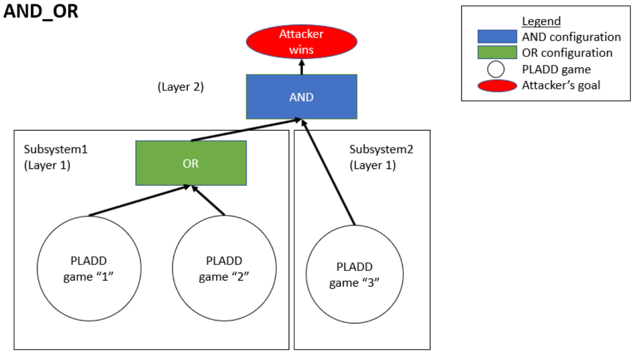
- A hierarchical parallel PLADD system follows the same rules as single-layer parallel PLADD system
- The steady-state solution of the attacker's expected probability of success is minimized under the following conditions:
  1. Each individual subsystem (which is a single-layer parallel PLADD system) applies Theorem 1 and Theorem 2 to have minimized attacker's expected probability of success
  2. Each upper layer also applies Theorem 1 and Theorem 2 to have minimized attacker's expected probability of success

Hierarchical Parallel PLADD System: Example 1 (AND_OR Configuration)

We simulate 4 different reset patterns, which are the following:

1. The resets of each PLADD game in the hierarchical parallel PLADD system are at the same time
2. 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 τ/2
3. 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
4. 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

AND_OR



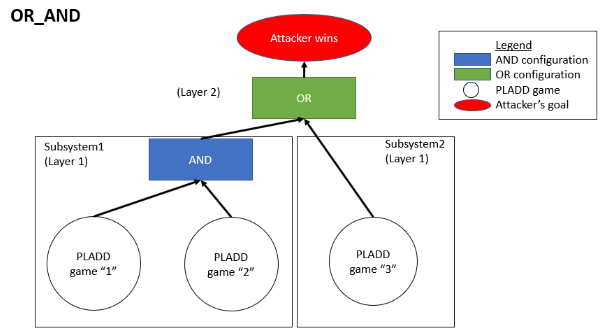
Testcases	d_1	d_2	d_3	τ_1	τ_2	τ_3	μ_1	μ_2	μ_3	EPS_{AND_OR}
1	0	0	0	90	90	90	30	30	30	0.62909
2	0	0	45	90	90	90	30	30	30	0.52004
3	0	45	0	90	90	90	30	30	30	0.63435
4	0	45	45	90	90	90	30	30	30	0.58903

OR configuration: Same time
AND configuration: Spaced apart

Hierarchical Parallel PLADD System: Example 2 (OR_AND Configuration)

We simulate 4 different reset patterns, which are the following:

1. The resets of each PLADD game in the hierarchical parallel PLADD system are at the same time
2. 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 $\tau/2$
3. 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
4. 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



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

AND configuration: Spaced apart
OR configuration: Same time

47

Outline

- Introduction
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
  - Overview of Major Theorems
  - **Simulation Results**
- Attack Model Driven Mitigation Strategies
- Conclusions
- List of Publications
- Reference

48

Simulation Result Of Two PLADD Nodes In AND Configuration

AND configuration of two PLADD nodes	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	

49

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

Georgia Tech

Simulation Result Of Two PLADD Nodes In OR Configuration

OR configuration of two PLADD nodes	Simulation #	Player parameters (days)	PLADD game offsets (days)	EPS	Percent improvement
	1.a	$\tau = 90, \quad \mu = 90$	$d_{computer1}$=0, $d_{computer2}$=0	0.567	3.57
	1.b		$d_{computer1}$=0, $d_{computer2}$=30	0.585	
	1.c		$d_{computer1}$=0, $d_{computer2}$=45	0.588	
	1.d		$d_{computer1}$=0, $d_{computer2}$=60	0.586	
	2.a	$\tau = 90, \quad \mu = 180$	$d_{computer1}$=0, $d_{computer2}$=0	0.3672	0.08
	2.b		$d_{computer1}$=0, $d_{computer2}$=30	0.3673	
	2.c		$d_{computer1}$=0, $d_{computer2}$=45	0.3675	
	2.d		$d_{computer1}$=0, $d_{computer2}$=60	0.3674	
	3.a	$\tau = 180, \quad \mu = 90$	$d_{computer1}$=0, $d_{computer2}$=0	0.749	3.10
	3.b		$d_{computer1}$=0, $d_{computer2}$=60	0.766	
	3.c		$d_{computer1}$=0, $d_{computer2}$=90	0.773	
	3.d		$d_{computer1}$=0,$d_{computer2}$=120	0.772	

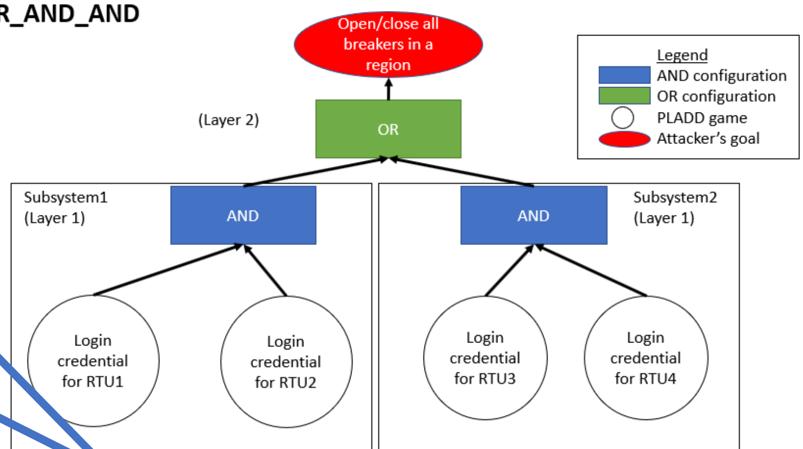
50

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

Georgia Tech

Simulation Result Of Four PLADD Nodes In OR_AND_AND Configuration

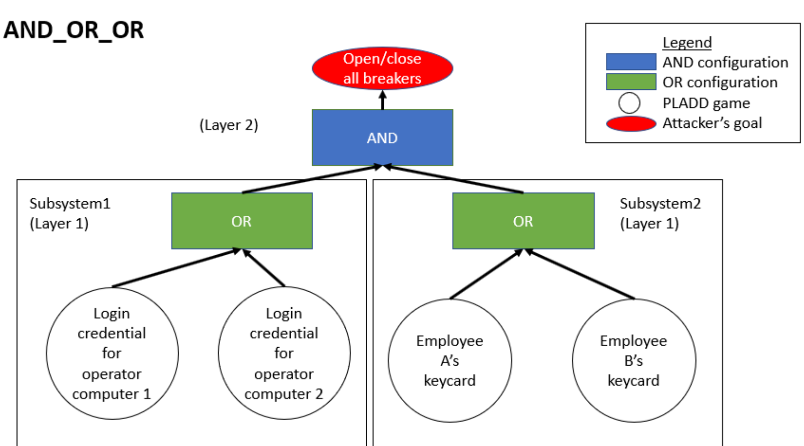
Simulation	Subsystem 1		Subsystem 2		$EPS_{OR\_AND\_AND}$
	d_1	d_2	d_3	d_4	
1	0	0	0	0	0.696
2	0	0	45	45	0.814
3	0	22.5	45	67.5	0.743
4	0	22.5	0	0	0.687
5	0	45	0	0	0.712
6	0	45	0	45	**0.656**
7	0	45	9	54	0.688
8	0	45	22.5	0	0.679
9	0	45	45	0	**0.656**
10	0	45	45	22.5	0.699
11	0	45	45	45	0.712



AND configuration: Resets are equally spaced apart
OR configuration: Resets are at the same time

Simulation Result Of Four PLADD Nodes In AND_OR_OR Configuration

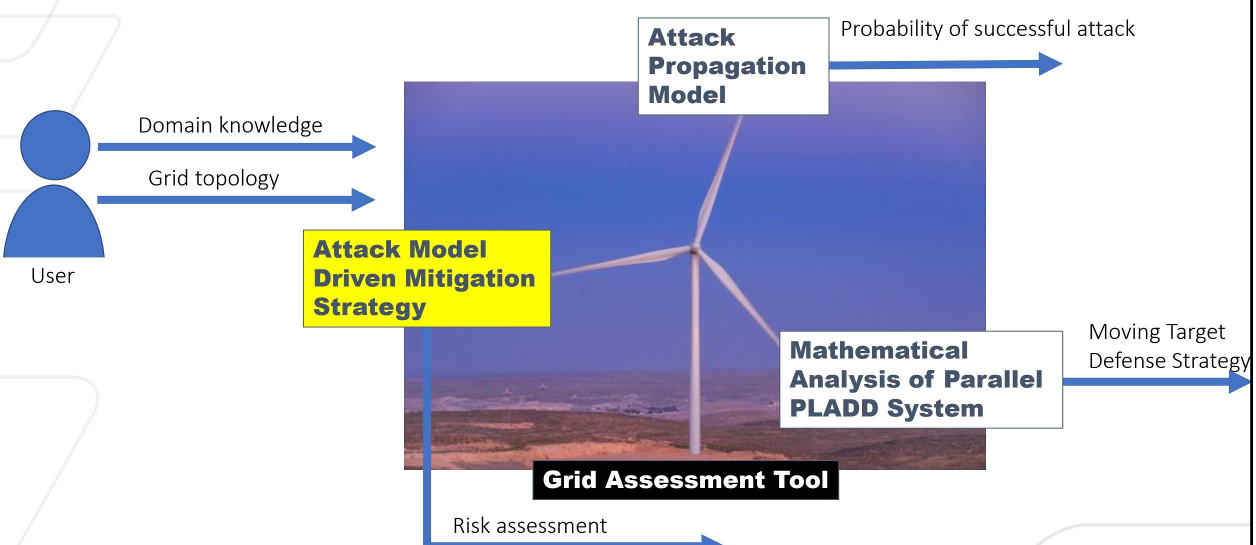
Simulation	Subsystem 1		Subsystem 2		$EPS_{AND\_OR\_OR}$
	d_1	d_2	d_3	d_4	
1	0	0	0	0	0.751
2	0	0	45	45	0.695
3	0	22.5	45	67.5	0.806
4	0	22.5	0	0	0.761
5	0	45	0	0	0.781
6	0	45	0	45	0.852
7	0	45	9	54	0.844
8	0	45	22.5	0	0.834
9	0	45	45	0	0.852
10	0	45	45	22.5	0.823
11	0	45	45	45	0.781



OR configuration: Resets are at the same time
AND configuration: Resets are equally spaced apart

Outline

Research Overview



Risk Assessment

- Typical risk assessment tool uses domain expert's knowledge to assign probability of success of attacks, and values of impact
- Our risk assessment of the power grid is specific to the attacker's goal and uses attack model to calculate probability of success
- An example attacker's goal could be to overload the transmission line and cause loss of load

$$P = \frac{\text{Number of days the attacker has the ability to open breakers}}{\text{Number of days in the simulation}}$$

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

$$Risk = P * Severity$$

55

Georgia Tech

Outline

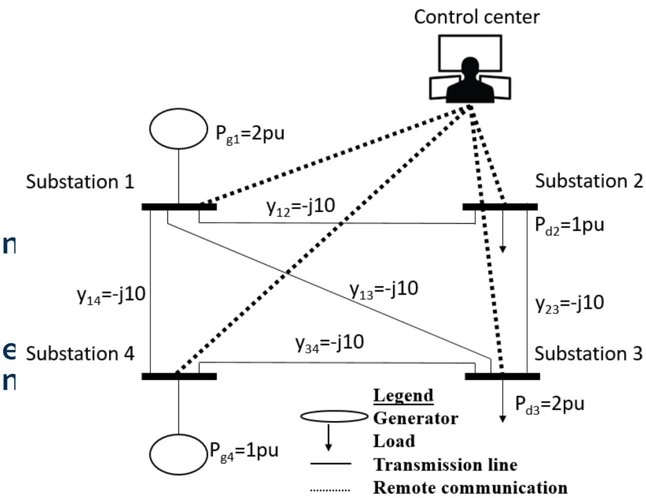
- Introduction
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
  - Risk Assessment
  - **4-bus Risk Assessment Example Scenario**
  - 39-bus Risk Assessment Example Scenario
- Conclusions
- List of Publications
- Reference

56

Georgia Tech

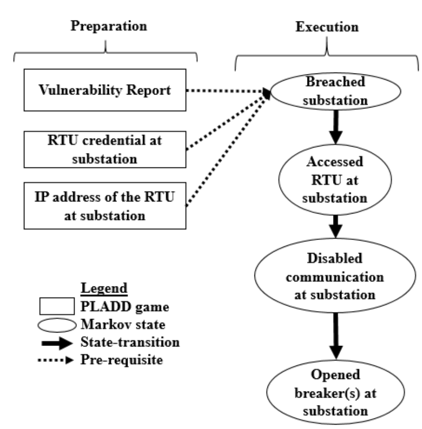
4-Bus Risk Assessment

- Substation 1 and Substation 4 are generating power while Substation 2 and Substation 3 have loads that consume power
- Assume that each substation has one remote terminal unit (RTU) that collects data from the substation sensors and can execute control center commands
- Specifically, RTUs are capable of opening/closing breakers on the transmission lines

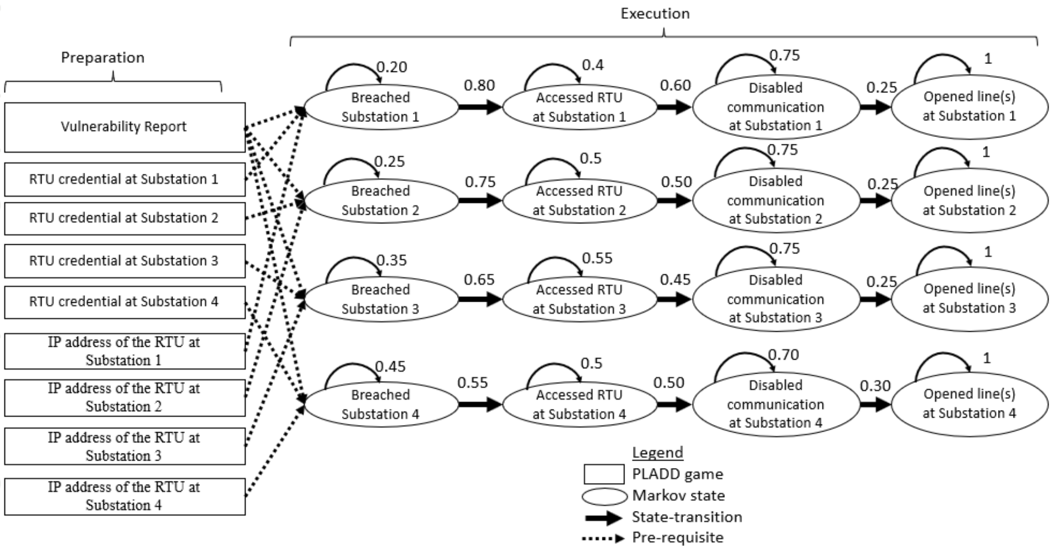


Hybrid Attack Model Of A Single Substation

- We assume that the attacker first gathers all necessary information prior to executing an attack on the substation
- 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
- 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
  4. Opening breaker(s) of transmission lines at a substation



Hybrid Attack Model OF The Four-Bus System



Georgia Tech

Test cases

- Test case 0: Normal power grid operation (base case)
- Test case 1: Attacker attempts to disconnect Substation 1 from the grid.
- Test case 2: Attacker attempts to disconnect Substation 2 from the grid.
- Test case 3: Attacker attempts to disconnect Substation 3 from the grid.
- Test case 4: Attacker attempts to disconnect Substation 4 from the grid
- Test case 5: Attacker attempts to disconnect Substation 1 and Substation 4 from the grid

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

Georgia Tech

Risk calculations of test cases 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

← Lowest
← Highest

- The risk calculation provides a way to compare
  1. The probability of success of different attacks
  2. Risk of individual substations
  3. The risk of a combination of substations
- 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

61

Georgia Tech

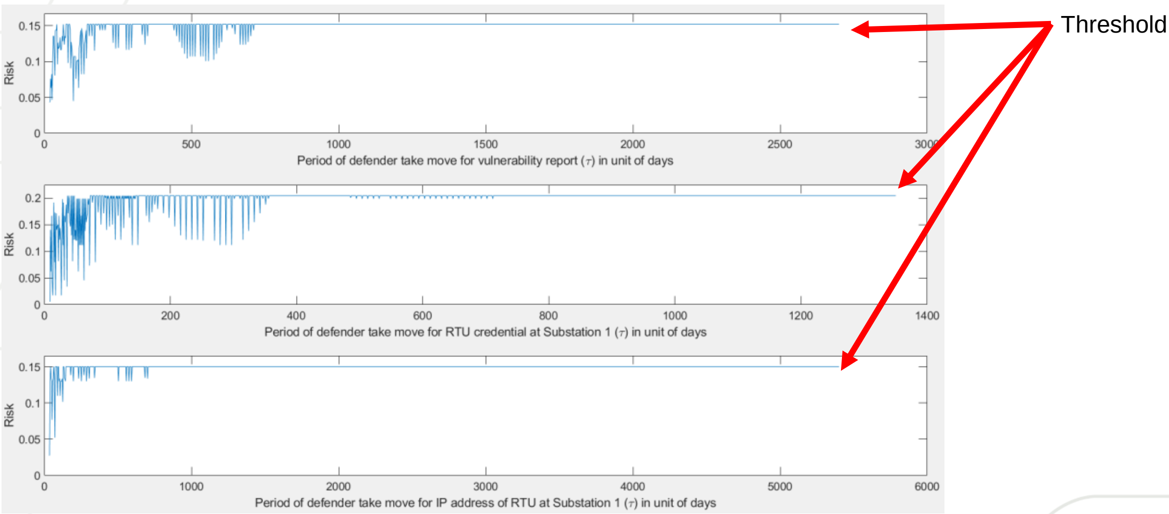
Sensitivity Analysis

- There are three parameters that the defender can control, which are
  - 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
- Assuming the resets above are done periodically, then the defender can only control the periods at which the resets happen, and the initial delay with respect to the start of the simulation.
  - For the purpose of sensitivity analysis, we set the initial delay to 0 for all simulations

62

Georgia Tech

Sensitivity Analysis of Risk for Substation 1

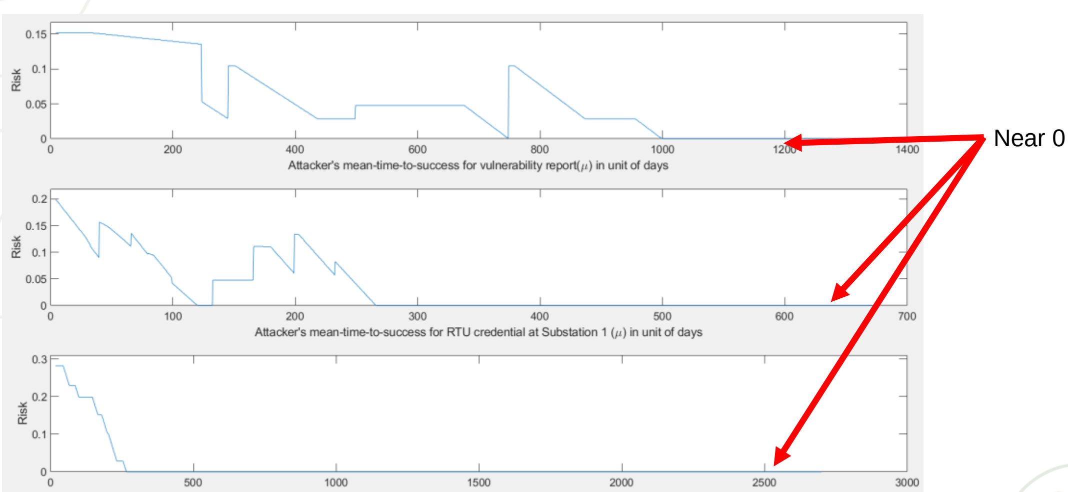


63

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

Georgia Tech

Sensitivity Analysis of Risk for Substation 1

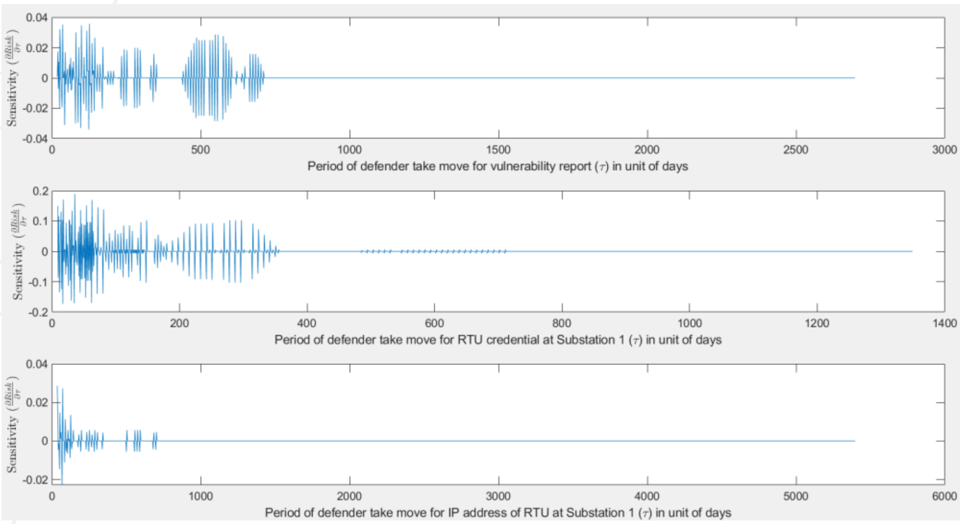


64

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

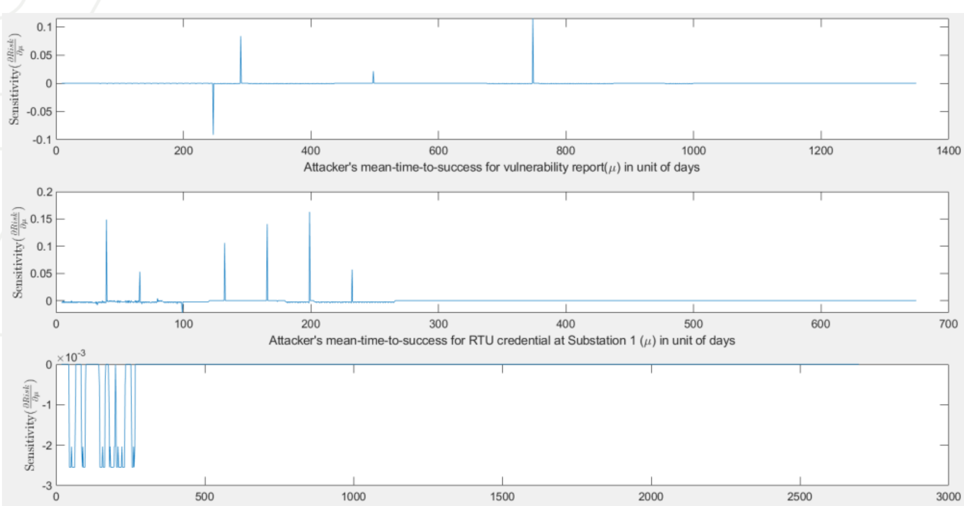
Georgia Tech

Sensitivity Analysis of Risk for Substation 1



Sensitivity of Risk for Substation 1 to be successfully attacked as the period of resets increases.

Sensitivity Analysis of Risk for Substation 1



Sensitivity for Substation 1 to be successfully attacked as the attacker's mean-time-to-success increases.

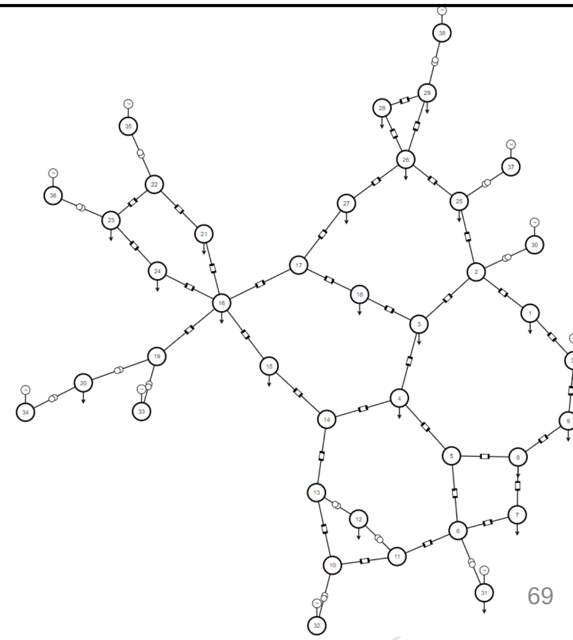
Outline

39-bus Risk Assessment

- The 4-bus power system simulation 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 New England IEEE 39-bus system [11]

39-Bus Power System

- A graphical view of a 39-bus system
- In reality, sometimes, taking down a substation (and then disconnects 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

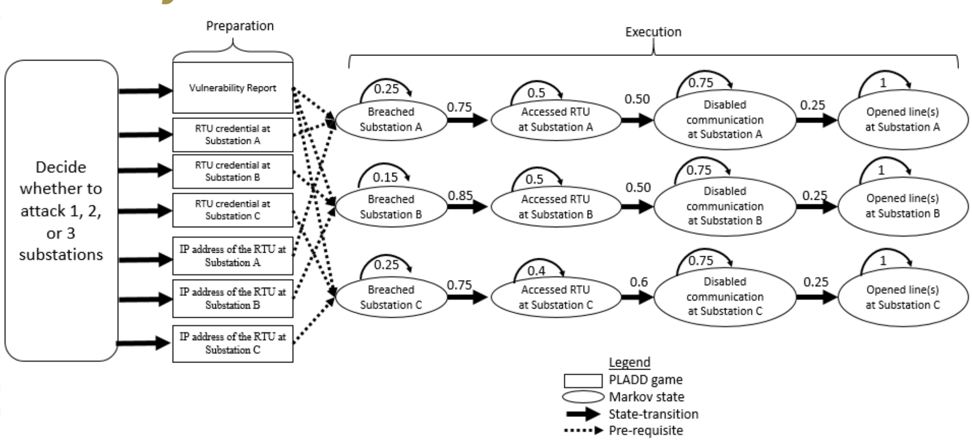


Network Visualization tool [12]

69

Georgia Tech

39-Bus Hybrid Attack Model



- In this section, we analyze the difference between
    1. Immediately attack one substation when the preparations are complete
    2. Wait until the preparations for attacking two substations are complete
    3. Wait until the preparations for attacking three substations are complete

70

Georgia Tech

39-Bus Power System Risk Calculation

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

- As the number of simultaneously attacked substations 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 two substations being simultaneously attacked, has the highest worst case and average case risk

71

Georgia Tech

39-Bus Power System Risk Calculation

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

- As the number of simultaneously attacked substations 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 two substations being simultaneously attacked, has the highest worst case and average case risk

72

Georgia Tech

39-Bus Power System Risk Calculation

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

- As the number of simultaneously attacked substations 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 two substations being simultaneously attacked, has the highest worst case and average case risk

Georgia Tech

Outline

- Introduction
- Research Overview
- Background and Prior Work
- Attack Propagation Model for Cyber-Physical System
- Mathematical Analysis of Parallel PLADD System
- Attack Model Driven Mitigation Strategies
- **Conclusions**
- List of Publications
- Reference

Georgia Tech

Conclusion

- We introduced a hybrid attack model that combines the advantages of the PLADD and Markov chain models
- 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 proved that for both AND configuration 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 Theorems 1 and 2

Conclusion

- 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 39-bus system
- Given the risk calculation for the 39-bus system we found that Substation 6 may be a critical substation for attacks involving more than one substations

Future work

- The techniques presented in this dissertation can be further expanded for larger cyber-physical systems because each PLADD node is of linear complexity
- 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, reconnecting disconnected substation back to the grid should be considered

77

Georgia Tech

Future work

- 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.
- 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

78

Georgia Tech

List of Publications

1. V. Chukwuka, Y. Chen, S. Grijalva and V. Mooney, "Bad Data Injection Attack Propagation in Cyber-Physical Power Delivery Systems," *2018 Clemson University Power Systems Conference (PSC)*, Charleston, SC, USA, 2018, pp. 1-8, doi: 10.1109/PSC.2018.8664024.
2. Y. Chen, T. Gieseking, D. Campbell, V. Mooney and S. Grijalva, "A Hybrid Attack Model for Cyber-Physical Security Assessment in Electricity Grid," *2019 IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, USA, 2019, pp. 1-6, doi: 10.1109/TPEC.2019.8662138.
3. Y. Chen, V. Mooney and S. Grijalva, "A Survey of Attack Models for Cyber-Physical Security Assessment in Electricity Grid," *2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*, Cuzco, Peru, 2019, pp. 242-243, doi: 10.1109/VLSI-SoC.2019.8920326.
4. Y. Chen, D. Campbell, V. Mooney, S. Grijalva, B. eames, A. Outkin, E. Vugrin, R. Helinski, and B. Anthony, "Power Grid Bad Data Injection Attack Modeling in PRESTIGE," *2019 Government Microcircuit Applications and Critical Technology Conference (GOMACTech)*, Albuquerque, New Mexico, USA, 2019, pp. 1-6.
5. Y. Chen, V. Mooney and S. Grijalva, "Grid Cyber-Security Strategy in an Attacker-Defender Model," *2020 Clemson University Power Systems Conference (PSC)*, Clemson, SC, USA, 2020, pp. 1-8, doi: 10.1109/PSC50246.2020.9131230.
6. Y. -C. Chen, V. Mooney and S. Grijalva, "Electricity Grid Cyber-Physical Security Risk Assessment Using Simulation of Attack Stages and Physical Impact," *2020 IEEE Kansas Power and Energy Conference (KPEC)*, Manhattan, KS, USA, 2020, pp. 1-6, doi: 10.1109/KPEC47870.2020.9167679.
7. Chen Y-C, Mooney VJ III, Grijalva S. Grid Cyber-Security Strategy in an Attacker-Defender Model. *Cryptography*. 2021; 5(2):12. https://doi.org/10.3390/cryptography5020012

Ongoing:

1. "Risk Assessment and Sensitivity Analysis of the Electricity Grid Using Simulation of Attack Stages and Physical Impact,", 2022 IEEE Transactions on Smart Grid.

Georgia Tech

References

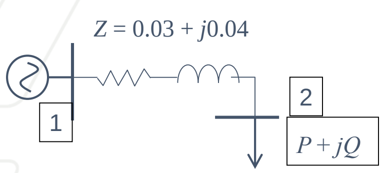
1. R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
2. P. Donghui, M. Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks", 2017. [Online]. Available: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
3. "Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015," PWC, 2015. [Online]. Available: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf. [Accessed 15 November 2018].
4. L. Simonovich, "Are utilities doing enough to protect themselves from cyberattack?," ed: World Economic Forum, 2020.
5. L. Simonovich, "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?," Siemens, Houston, Texas, 2020.
6. Federal Energy Regulatory Commission, "Supply Chain Risk Management Reliability Standard". [Online]. Available: https://www.federalregister.gov/documents/2018/10/26/2018-23201/supply-chain-risk-management-reliability-standards
7. 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).
8. 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.
9. 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
10. P. A. Gagniuc, *Markov Chains: From Theory to Implementation and Experimentation*. John Wiley & Sons, 2017.
11. T. Athay, R. Podmore, and S. Virmani, "A Practical Method for the Direct Analysis of Transient Stability," *IEEE Transactions on Power Apparatus and Systems,* vol. PAS-98, no. 2, pp. 573-584, 1979, doi: 10.1109/TPAS.1979.319407.
12. Monash University. https://immersive.erc.monash.edu/stac/ (accessed February 16th, 2022)

Georgia Tech

Backup Slides

Georgia Tech

State Estimation – Power Flow Example



$$\mathbf{Y}_{bus} = \begin{bmatrix} 12 - j16 & -12 + j16 \\ -12 + j16 & 12 - j16 \end{bmatrix}$$

Measurements are:

$$\mathbf{z} = \begin{bmatrix} V_1 \\ V_2 \\ P_{12} \\ Q_{21} \\ P_2 \end{bmatrix} = \begin{bmatrix} 144.7 \text{ kV} \\ 119.0 \text{ kV} \\ 463.1 \text{ MW} \\ -105.0 \text{ Mvar} \\ 404.5 \text{ MW} \end{bmatrix} \underset{\substack{\text{Base } 100\text{MVA} \\ 138\text{kV}}}{=} \begin{bmatrix} 1.0485 \\ 0.8623 \\ 4.631 \\ -1.050 \\ -4.045 \end{bmatrix} \text{pu}$$

Available measurements:
V_1, V_2, P_{12}, Q_{21}, P_2

$$\mathbf{x} = \begin{bmatrix} \theta_2 \\ V_1 \\ V_2 \end{bmatrix}$$

Assume σ is 0.02 for voltages and 0.04 for power measurements.

$$\mathbf{R} = diag(\begin{bmatrix} 0.02^2 & 0.02^2 & 0.04^2 & 0.04^2 & 0.04^2 \end{bmatrix})$$

$$J(\hat{\mathbf{x}}) = \sum_{i=1}^{m} \frac{\left(z_i - h_i(\hat{\mathbf{x}})\right)^2}{\sigma_i^2} \qquad p = \Pr\left\{ J\left(\hat{\mathbf{x}}\right) \le \chi^2_{(m-n),p} \right\}$$

Georgia Tech

Simulation (Matlab)

• Attack starts at time step = 2
• To model state estimation in the simulation we introduce a scale factor to distort the measurement vector z

- z = [1.0485, 0.8623, P12*scale, -1.05, P2*scale]
- When scale = 1, the measurement vector is "correct" or not tampered with.
- When the measurement vector is tampered with, the scale factor becomes:

$$scale = 1.25 - 0.25 * rand()$$

where $rand()$ varies between 0 and 1

• For each time step, state estimation calculates the residual vector $z_i - h_i(\hat{x})$, and uses the Chi-Square test to calculate the probability of current set of measurements indicates bad data
• This probability value is used as the parameter "P" in Figure 4 (slide 16)

• Finally, for each time step, the probability (of attack) occurring at each node is calculated using the Markov Chain equation

Georgia Tech

Tradeoffs of Hybrid Attack Model

- Disadvantage
  - More effort needed to input more information (planning phase)
  - Relatively more complex than simply simulating the attack execution phase
- Advantage
  - Design and policy recommendations that takes account of attacker's planning phase

Georgia Tech

Mathematical Model Basics

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 $\lim_{t \to t^-} P_k(t)$.
$R(t)$	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.

Useful Definitions

- 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*

$$R_{AND}(t) = P_1(t) \times P_2(t) \times \cdots P_N(t)$$

- 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*

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

- 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*

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

- 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*

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

Georgia Tech

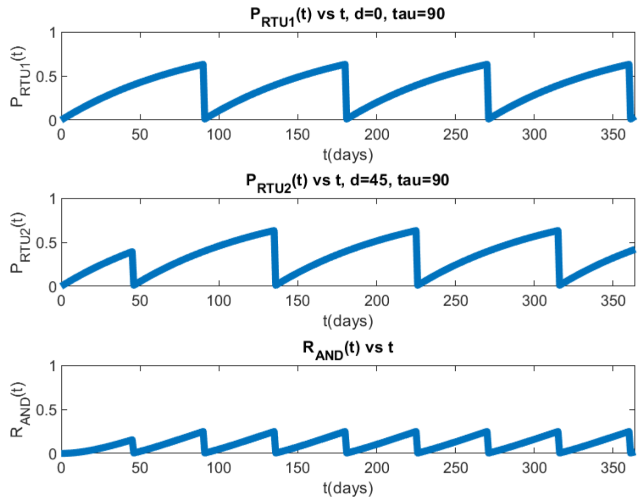
Simulation Result Of Two PLADD Nodes In AND Configuration

Simulation 1.c with the following parameters:

$d_{RTU1} = 0, d_{RTU2} = 45$

$\mu_{RTU1} = \mu_{RTU2} = 90$

$\tau_{RTU1} = \tau_{RTU2} = 90$



87

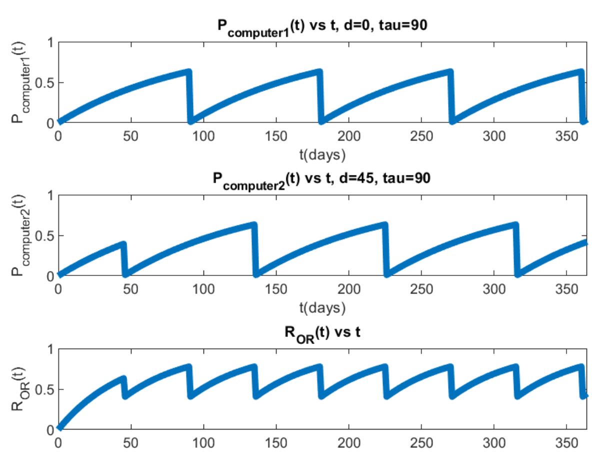
Simulation Result Of Two PLADD Nodes In OR Configuration

Simulation 1.c with the following parameters:

$d_{computer1} = 0, d_{computer2} = 45$

$\mu_{computer1} = \mu_{computer2} = 90$

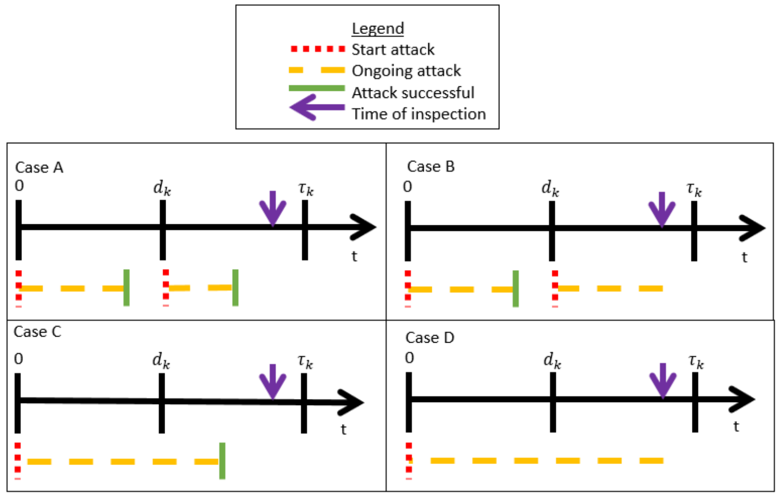
$\tau_{computer1} = \tau_{computer2} = 90$



88

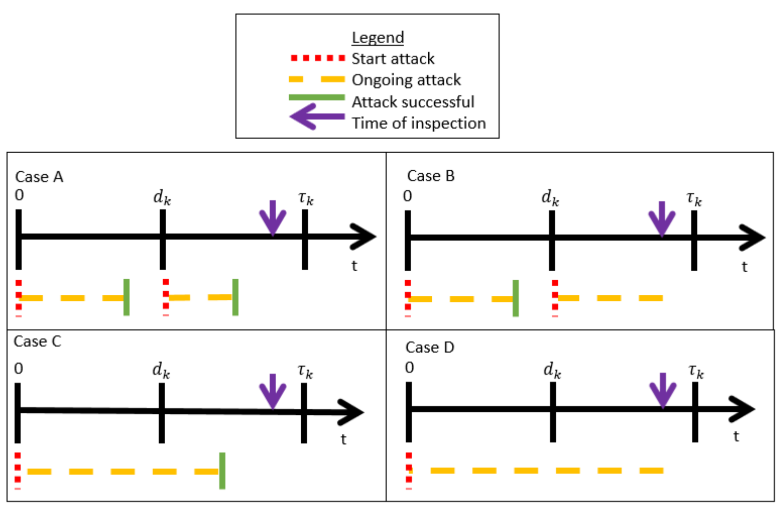
PLADD game (Mathematical Representation) cont.

- 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, $d_k < t < \tau_k$.



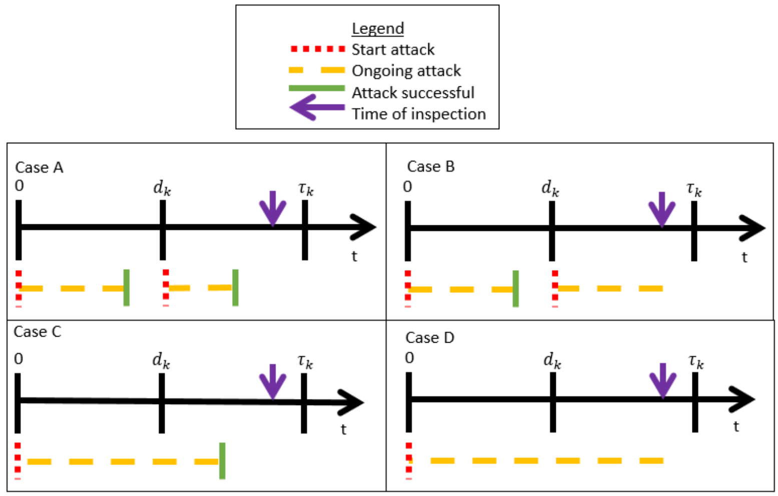
PLADD game (Mathematical Representation) cont.

- 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



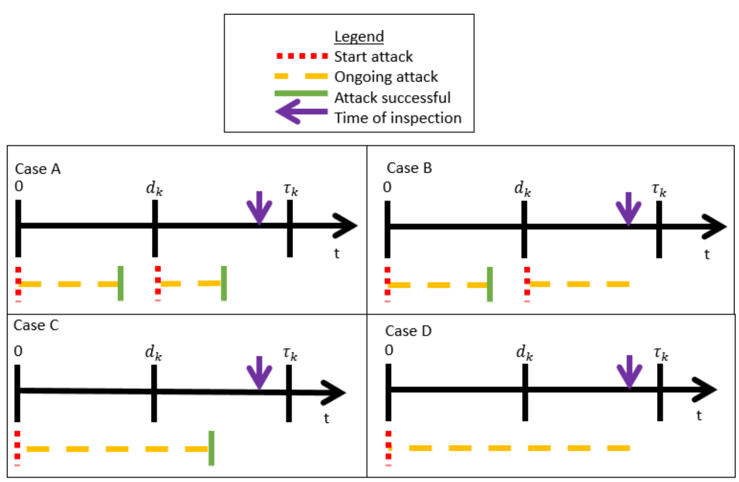
PLADD game (Mathematical Representation) cont.

- In Case A, 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 $t_k{}'$ ($t_k{}'$is the time since the last defender take move).
- In Case C, 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 $(d_k, t]$.



PLADD game (Mathematical Representation) cont.

- 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



$P_k(t) = F_k(t) - F_k(d_k) + P_k(d_k) * F_k(t_k')$, where $d_k < t < \tau_k$