# A Hybrid Attack Model for Cyber-Physical Security Assessment in Electricity Grid

Yu-Cheng Chen, Tim Gieseking, Dustin Campbell, Vincent Mooney and Santiago Grijalva
Georgia Institute of Technology
Atlanta, USA
ychen414@gatech.edu, tgieseking6@gatech.edu, djrox316@gatech.edu, mooney@ece.gatech.edu, sgrijalva@ece.gatech.edu

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

***Keywords*— Bad Data Injection, Attack Graph, Attack Propagation, Markov Chain, PLADD***

## I. INTRODUCTION

The power grid is a critical infrastructure that must continue to function even when under attack. With the characteristics of a large-scale and complex grid, its safety and reliability are easily influenced by external interference. Therefore, the security analysis of power grids is critical and has theoretical and practical significance [1]. The power grid has distinct features that create unique security challenges including a) transmission and distribution circuits over large geographic areas, b) unmanned substations, c) a broad range of modern and legacy components, and d) use of a variety of communications technologies and protocols.

The 2015 Global State Information Security Survey reported that power companies and utilities around the world expressed a six-fold increase in the number of detected cyber incident over the previous year [2]. According to a U.S. Department of Energy report [3], out of 245 total incidents reported across all sectors in FY 2014, roughly 55% involved advanced persistent threats (APT) or sophisticated actors. Cyber-physical security attacks may target individual field cyber-components or the communications network. To ensure a secure and reliable power grid, it is imperative to study the different ways in which the cyber-physical power grid can be compromised and then develop techniques and mechanisms to detect, evaluate and mitigate the propagation and impact of a potential cyber-physical security attack.

The rest of the paper is organized as follows. Section II describes the background and prior work of this research. Section III explains our innovative hybrid attack graph model used for the first time, as best the authors of this paper can ascertain, in modeling the attack propagation. Section IV presents the results. Finally, Section V concludes the paper.

## II. BACKGROUND AND PRIOR WORK

### A. Related Work

Numerous works have investigated the vulnerability of power grids by developing threat and attack models as well as simulating different attack scenarios in a controlled environment. However, developing reasonable approaches and models that can emulate cyber-physical attacks is still a critical challenge. Such models need to incorporate both the human decision-making as well as the power system behavior.

The major approaches for inspecting the effects of cyber-physical attacks on power systems are bad data and bad command injection attacks [4]. To model the power system layer, three popular models are typically adopted: pure topological models [5], pure power flow models [6], and hybrid models [7]. Each approach has its own advantages and disadvantages. However, the attackers might have different knowledge of the cyber-physical power grids, such as power system topological structures, electric features, real-time information, communication network parameters, transmission and listening ports, and access points. Under different levels of knowledge, attackers may adopt different attack strategies.

Game theory has been applied to security analysis in cyber-physical systems in numerous prior works. One such example is Backhaus, et al. [8], which applies game theory to a supervisory control and data acquisition (SCADA) system, specifically, smart grid voltage and power controls. Backhaus et al. propose an imperfect-information, semi net-form game (SNFG) played by an attacker and a defender. In the model, an attacker wishes to compromise the SCADA system while a defender tries to prevent this. The defender does not know if the attacker is present, so they use a statistical representation of memory to infer attacker presence. Backhaus, et al., found that by assuming an attacker to be present more than 20% of the time, the defender is able to prevent an attacker from receiving a large reward. However, the attacker-defender game is modeled in discrete time with each simulation step representing one minute. Another interesting prior work is Hota, et al. [9], which proposes a game involving a group of defenders protecting a cyber-physical system. Hota, et al., propose a static game played by multiple defenders, each of whom is responsible for one or more of the CPS components. Defenders share management of the nodes at the edge of their areas of responsibility. In contrast to Backhaus, et al. and Hota, et al., the hybrid model we proposed is more flexible in terms of

978-1-5386-9284-4/19/$31.00 @2019 IEEE

modeling time, because we consider the time difference between the attacker's action to prepare for an attack in comparison to the attacker's action to execute for an attack.

Our prior work uses a Markov model to investigate attack propagation in the power grid [10]. The model includes a state estimation submodule that captures both the changes in the physical system state as well as the impact of bad data. The system can provide additional information to the system operator so that appropriate mitigation strategies can be implemented. However, the attack graph models the attack tasks as sequential, thus the possibility of parallel execution of an attacker's set of tasks is not captured [10]. In addition, the attack graph considers neither the attacker's ability to learn nor the defender's ability to alter the system, which may make the information gained by the attacker useless.

Prior work [11] also models the interaction of a computer system attacker and a defender using game theoretic analysis. PLADD focuses on a game where access to a resource is under attack, e.g., via password credentials to log in to a computer [11]. A strategy is considered where the defender can push a rational and motivated adversary away from attacking the defender's system by making sure adversary's "cost" to successfully execute an attack is higher than the "profit" obtained by the attacker. In the context of a power grid infrastructure, we use PLADD to model the planning stage of an attack where the resource desired by the attacker is the information necessary to execute a successful attack on the power grid.

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

| Node Number | Description |
|---|---|
| 1 | Start |
| 2 | RTU Data Obtained |
| 3 | Vulnerability Report |
| 4 | IP Address Obtained |
| 5 | Substation Breached |
| 6 | Fake Data Injected |
| 7 | Incorrect State |
| 8 | Loss of Load |

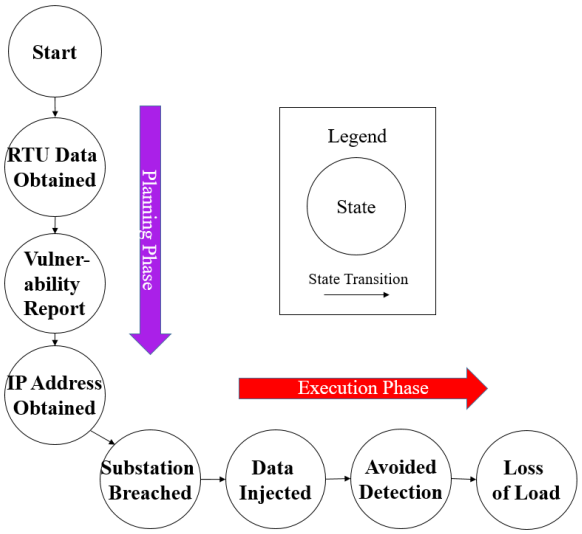



Figure 1. Attack graph capturing attacker's strategy

## B. *Bad Data Injection Attack Surface*

Shown in Figure 1 are actions that an adversary must complete in order to gain the ability to execute a bad data injection attack on a power grid system. In particular, Figure 1 shows that the adversary must gain access to RTU data, a vulnerability report, and IP address information before starting the actual injection of bad data into the power grid. In reality, the adversary may gain access and lose access to RTU data, vulnerability report, and IP information multiple times before actually executing a bad data injection attack on the power grid. Furthermore, these three items (RTU, vulnerability and IP information) may be obtained in any order. For the execution stage of the attack, the adversary must breach the substation, inject fake data, and avoid detection from state estimation. Table 1 shows our mapping of an attacker's tasks to each node in Figure 1.

## C. *Markov Modeling of Bad Data Injection Attack*

In our previous work [10] we have used a Markov approach to model the states shown in Figure 1. The result is shown in Figure 2. The success probabilities are estimated but are intended to represent upper bounds on the probability

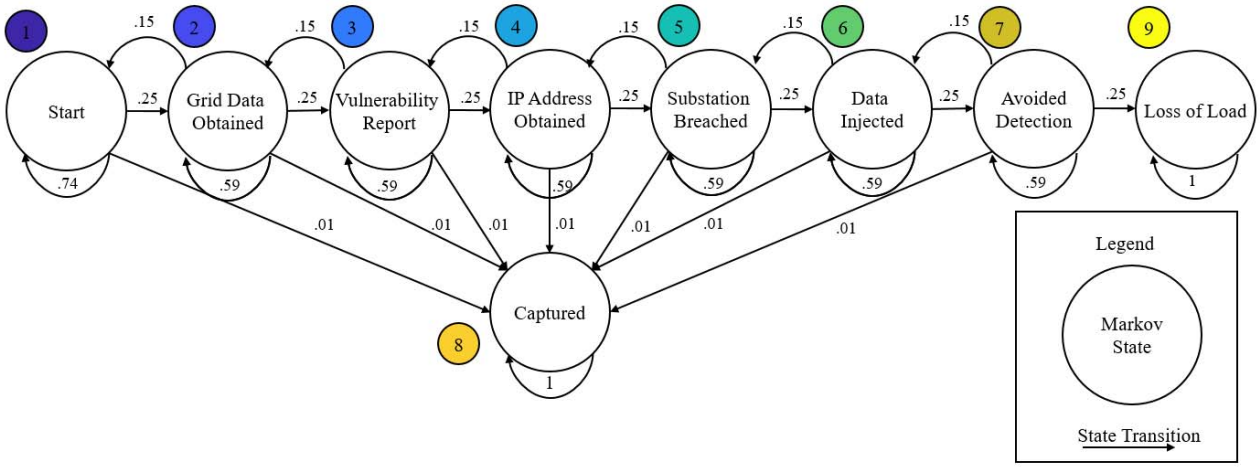



Figure 2. Markov Chain capturing attacker's strategy for compromising the power system under attack assuming defender with state estimation

of success of each attack step [10]. We use the state estimator to identify maliciously injected data. Specifically, for a set of simulation time steps $t \in [1, T]$ the final state is obtained as shown in Equation 1:

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

The $x$ in Equation 1 is a vector representing the state of each node. Therefore, the $x$ in our simulation is a vector of nine elements which represent the nine nodes in our attack graph. The elements in the vector $x$ represent the probability of the attack being located at each node. For example, assuming there is no attack at the start of the simulation, the initial value of the vector $x$ is [1, 0, 0, 0 0 0, 0, 0, 0], because the probability of the attack being located at node 1 is 100%and the probability of the attack being located at node 2 to node 9 is 0%. As the time step $t$ increases, the vector $x$ shows the probability of the attack located at each node. $P$ is the transmission matrix that contains probability values shown in Figures 2 and 3. The row number in $P$ is the node number at the head-end of the edge. If there is no edge connecting two nodes, the corresponding value in the matrix is 0. An example $P$ matrix which is used in Figures 2 and 3 is shown in Equation 2:

$$P = \begin{bmatrix} .74 & .25 & 0 & 0 & 0 & 0 & 0 & .01 & 0 \\ .15 & .59 & .25 & 0 & 0 & 0 & 0 & .01 & 0 \\ 0 & .15 & .59 & .25 & 0 & 0 & 0 & .01 & 0 \\ 0 & 0 & .15 & .59 & .25 & 0 & 0 & .01 & 0 \\ 0 & 0 & 0 & 0.15 & .59 & .25 & 0 & .01 & 0 \\ 0 & 0 & 0 & 0 & .15 & .59 & .25 & .01 & 0 \\ 0 & 0 & 0 & 0 & 0 & .15 & .59 & .01 & .25 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (2)$$

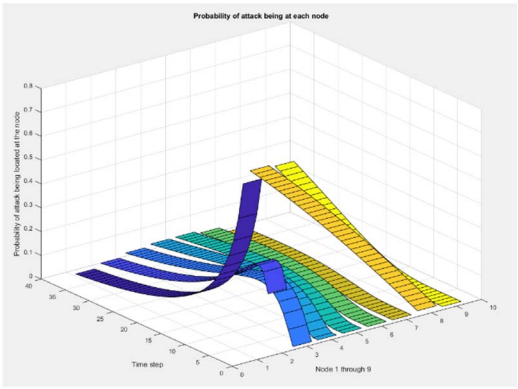



Figure 3. Probability of an attack being at each node with respect to time step for Markov Chain model

## III. HYBRID ATTACK MODEL (HAM)

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

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

### A. PLADD Modeling of the Bad Data Injection Attack

We implement games inspired by PLADD to model the interaction of nodes 2 through 4 between the attacker and the defender [11]. Our PLADD model takes in the following parameters:

- $f_{base}(t)$: The attacker's time-to-success probability distribution
- $\tau$: The period between each defender action; in other word, the gaps between defender moves

Note that the time-to-success probability distribution is simply an exponential distribution. Therefore, $f_{base}(s)$ can be expressed as such in Equation 3:

$$f_{base}(t) = \lambda * e^{-\lambda * t} \quad (3)$$

In Equation 3, $1/\lambda$ is the average time to success given by the probability distribution function, and this is also specified in Figure 4.

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

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

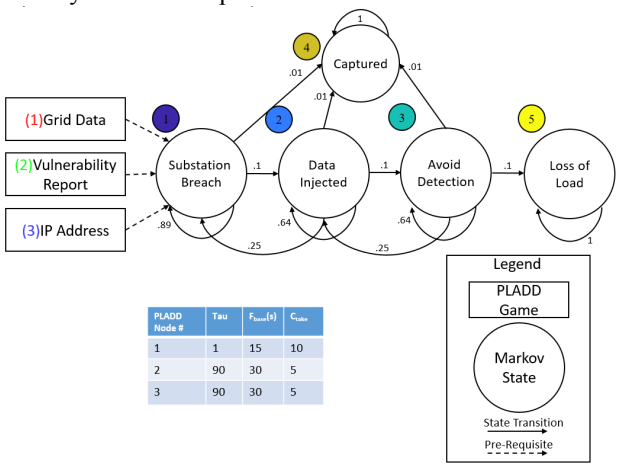
A further refinement to our scenario is that the fence may have cameras to monitor the surroundings of the fence and the substation may have alarms that can alert the defender. However, even in these cases we still consider "jumping a fence" to not match the PLADD model because cameras and alarms are detection techniques that PLADD does not support.

As a result of the aforementioned considerations, we do not consider modeling our scenario completely in PLADD.

### B. Hybrid Model Characteristics

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

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




| PLADD Node # | Tau | $F_{base}(s)$ | $C_{take}$ |
|---|---|---|---|
| 1 | 1 | 15 | 10 |
| 2 | 90 | 30 | 5 |
| 3 | 90 | 30 | 5 |

Figure 4. Hybrid model attack graph, where the table shows the parameters used for each PLADD node

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

### C. *Hybrid Model of the Bad Data Injection Attack*

In the scenario shown in Figure 4, the attacker/adversary needs access to RTU data, Vulnerability Report and IP address to be able to carry out a bad data injection attack on the power grid. Each of these attempts by the adversary to gain necessary information is modeled as a PLADD node. For simplicity, we assume that the RTU data is stored in a cloud drive and the adversary must run a password cracking program to gain access. We also assume that the vulnerability report is stored in a utility engineer's computer, so the adversary must gain access by cracking the engineer's password. Lastly, we assume that the IP address is stored in a computer located at the control center, and the adversary must gain access by password cracking. Once the adversary has gained access to all the nodes in the preparation stage, this means the adversary is ready to execute the attack, and then the adversary immediately starts to attack the power grid by moving through the Markov states in Figure 4. Finally, as specified in Section III.C, to interface the PLADD model and the Markov Chain model, the number of time steps in the

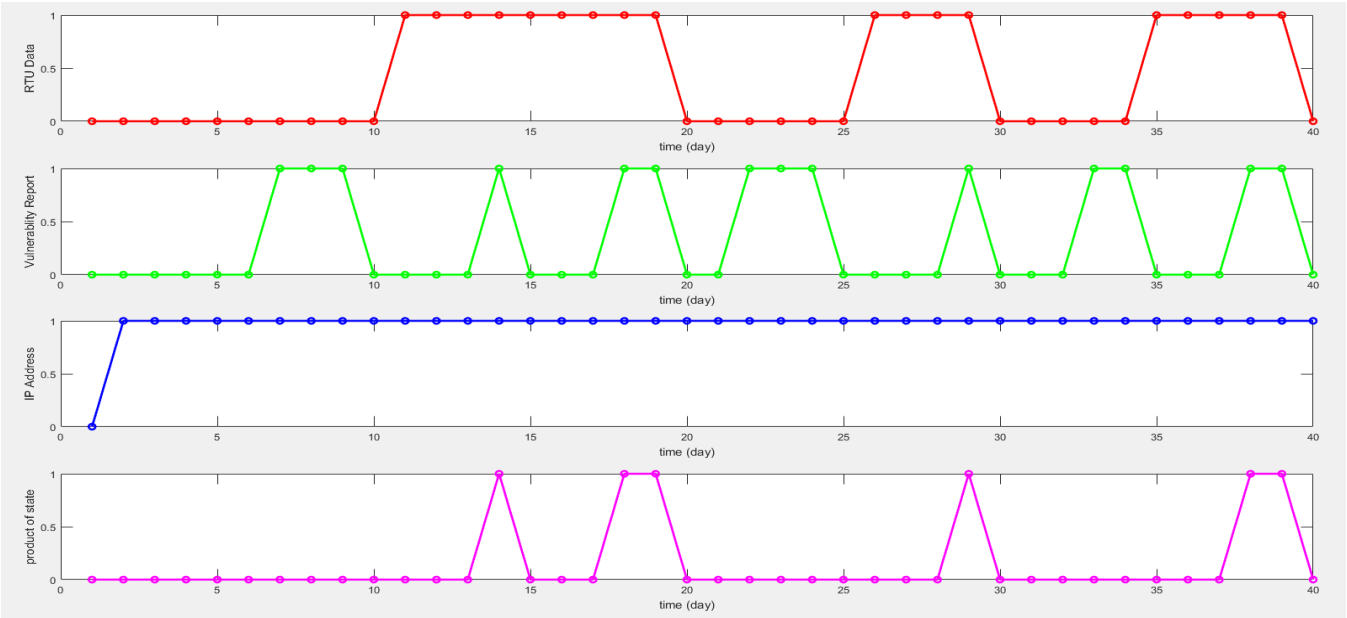



Figure 5. State of each PLADD nodes with respect to time are shown from top to bottom, where the top plot represents the state of PLADD node 1 in Figure 4. The second plot from the top represents the state of PLADD node 2 in Figure 4. The third plot from the top represents the state of PLADD node 3 in Figure 4. The bottom plot represents the result of doing a logical AND on PLADD node 1-3's state.

Markov Chain model occurs within a time unit specified by the PLADD model. For the bad data injection attack scenario, the PLADD model uses one day as the smallest unit of time. If we assume that each step of the Markov Chain is estimated to require, on average, four hours, this would mean that six time steps in the Markov Chain model would occur within a day of PLADD model. Each time step of traversal of the Markov Chain is done using Equation 1.

## IV. EXPERIMENTAL RESULTS

We implemented HAM for our scenario shown in Figure 4 using MATLAB. As described in Section III.C, each PLADD node requires the parameters shown in Figure 4. HAM simulation starts by having the attacker attempt all PLADD nodes simultaneously on the first day. Note that attacks are not instantaneous; the time-to-successful attack is generated by using a well-known technique called Inverse Transform Sampling. The purpose of inverse transform sampling is to generate pseudo-random number samplings from any probability distribution given its cumulative distribution function [11]. For the purpose of this simulation, this pseudo-random number represents the amount of time needed to successfully take over a PLADD node as the attacker. The defender in the simulation takes the control of each PLADD node at a periodic period with respect to the $\tau$ shown in Figure 4. Note that the defender's action to take the control of PLADD node is instantaneous.

Shown in Figure 5 are the PLADD nodes in the preparation stage. Each PLADD node can be represented as a state where "0" means the defender has the control of the node and "1" means the attacker has the control of the node. The result in Figure 5 shows that the attacker's efforts do not always provide the attacker with any benefit. For example, in Figure 5, the attacker gained control of PLADD node 2 on the 7$^{th}$ day and continues to hold control of PLADD node 2 until the 9$^{th}$ day. However, the defender was able to take back the control of PLADD node 2 on the 10$^{th}$ day. It is noteworthy to point out that during the time from the 7$^{th}$ day to 9$^{th}$ day, the attacker was not able to continue to do the execution stage of the attack because PLADD node 1 is still controlled by the defender for the duration of the 7$^{th}$ to the 9$^{th}$ day. Therefore, it can be concluded that the attacker may have to attack the same PLADD node multiple times before being able to carry out the actual execution of the attack on the power grid. The bottom plot in Figure 5 shows the days where the attacker is able to execute attack on the power grid because the bottom plot shows the product of all three PLADD states. Figure 6 shows the result of the hybrid model where on the left of Figure 6, the bottom plot of Figure 5 is reproduced for comparison. On the right side of Figure 6 is shown the attack propagation on Markov nodes 1-5 of Figure 4 for the duration of one attack, which happens to be one day long. As described in Section III. B, the reason that the duration of attack is one day long for the first effort to carry out the execution stage of the attack (on the 14$^{th}$ day) is because the defender takes back control of PLADD node 2 (the vulnerability report) on the next day (the 15$^{th}$ day). Figure 6(b) also shows that at the end of the day, the probability that the attacker has reached node 5 in Figure 4 is 32.38%, and the probability that the attacker is captured by the defender is 5.36%.

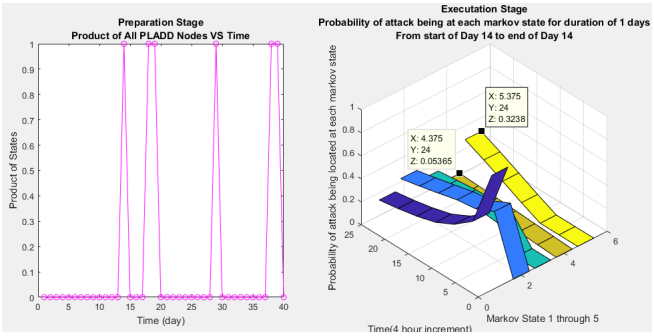



Figure 6. (a) The preparation stage for day 1 through 40 is shown on the left. (b) The first execution stage happens on the 14$^{th}$ day and the corresponding attack propagation is shown on the right.

Figure 7(a) shows the state of the nodes in the preparation stage for reference and Figure 7(b) shows the attack propagation on node 1-5 in Figure 4 for the duration of 40 days. To explain Figure 7(b) we have to first explain Figure 7(a): the attacker is in the preparation stage for the first 13 days of the simulation. On the 14$^{th}$ day, the attacker gains control of all the nodes in the preparation stage and then immediately starts to attack the power grid. This result is previously shown in Figure 6. Note that the attacker's progress is removed at the end of an attack as described in the previous sections. The next attack happens for a duration of 2 days, from the 18$^{th}$ to 19$^{th}$ day, as shown in Figure 7(a).

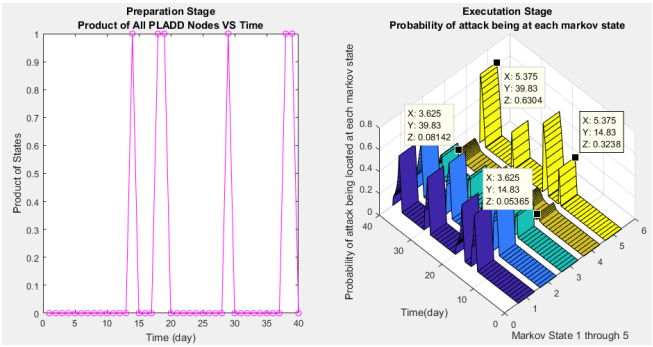



Figure 7. (a) The preparation stage for days 1 through 40 is shown on the left. (b) On the right, the execution stage for days 1 through 40 is shown on the right. Note that attacker's progress is reset at the end of each attack-frame.

As shown in Figure 7(b), we see that because the 2$^{nd}$ attack allows the adversary more time to attack the power grid, the probability that the attacker has reached node 5 (which is the "load loss" node which is very bad) at the end of the attack is 63.04%, which is significantly higher than the first attack, which happened on the 14$^{th}$ day.

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

## V. DISCUSSSION

Our experimental results clearly show the advantages of the hybrid model with respect to the handling of time. Specifically, HAM is capable of running simulations where the attacker takes significantly longer time to prepare for an attack in comparison to the actual execution of the attack (i.e., injection of bad data).

### *A. Hybrid Model Choices for PLADD Nodes*

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

### *B. Hybrid Model Choices for Markov Nodes*

The motivation behind HAM is to show that if the difference between the time spent in preparing for an attack is significantly longer than the time spent in executing the said attack, then the behavior of the attacker may become less straightforward than one might think. Therefore, we use PLADD to model the preparation stage and Markov Chain to model the execution stage. The challenge of using a hybrid model is how to come up with a good interface between the PLADD and Markov Chain model. Both PLADD and Markov Chain model have a notion of "time", although the "time" in PLADD may not necessarily be the same "time" in the Markov Chain. In order to simulate the hybrid model, we must define how many Markov Chain model time-step is equivalent to a time-step in PLADD model. In the simulation result shown in Figure 6-7, we assumed that six Markov Chain model time-steps are equivalent to one time-step in PLADD model. This is because we choose preparation stage's time-step to be equivalent to one day based on our estimate that each action in the preparation stage would need at least one day to complete, hence the smallest unit is one day. We also estimated the average time of an action in the execution stage to be four hours, which means there are six Markov Chain time-step in one day. Note that using four hours to represent one time-step in execution stage may be appropriate for bad data injection attack scenario, but this is not true for all attack scenarios. Our hybrid model can be applied to model attacks such as botnets in a network, however, the appropriate time-step in the execution stage should be seconds or minutes, rather than four hours.

## VI. CONCLUSION

HAM combines the advantages of PLADD model's timing information to improve the Markov Chain model's ability to assess the security risk in the power grid. In this paper, we show that even though PLADD is good at modeling interactions between the attacker and defender for a long period of time, actions such as "jumping a fence" is not a good fit in PLADD because PLADD does not support detection done by the defender. We also show that even though Markov Chain model is good at modeling attack propagation, the Markov Chain model is not good at modeling scenarios where the actions in the preparation stage of an attack take significantly longer time than the actions in the execution stage. Finally, we show that the hybrid model is capable of modeling long time-to-completion actions in the preparation stage and short time-to-completion actions in the execution stage. One possible future work is to take advantage of game theoretical property of the PLADD model to investigate the security properties of a power grid system.

## REFERENCES


[1] He, H., Yan, J.: 'Cyber-physical attacks and defenses in the smart grid: a survey', IET Cyber-Phys. Syst.: Theory Appl., 2016, 1, (1), pp. 13–27

[2] "Managing Cyber Risks in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015," PWC, September 30, 2014, accessed November 15, 2018.

[3] Glenn, Colleen, Sterbentz, Dane, and Wright, Aaron. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*. United States: N. p., 2016

[4] N. Saxena, V. Chukwuka, L. Xiong, and S. Grijalva, "CPSA : A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid," pp. 69–79, 2017.

[5] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," *Eur. Phys. J. B*, vol. 46, no. 1, pp. 101–107, 2005.

[6] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 631–641, 2012.

[7] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grids vulnerability: a complex network approach," pp. 1–16, 2008.

[8] Scott Backhaus, Russell Bent, James Bono, Ritchie Lee, Brendan Tracey, David Wolpert, Dongping Xie, and Yildiray Yildiz. Cyber-physical security: A game theory model of humans interacting over control systems. IEEE Transactions on Smart Grid, 4(4):2320–2327, 2013.

[9] Ashish R Hota, Abraham A Clements, Shreyas Sundaram, and Saurabh Bagchi. Optimal and Game-Theoretic Deployment of Security Investments in Interdependent Assets. In International Conference on Decision and Game Theory for Security, pages 101–113, New York, NY, USA, November 2016. Springer

[10] Chukwuka, Cheng, Grijalva and Mooney, "Bad Data Injection Attack Propagation in Cyber-Physical Power Delivery Systems," Power System Conference, Sep. 2018

[11] S. Jones, A. Outkin, J. Gearhart, J. Hobbs, J. Siirola, C. Phillips, S. Verzi, D. Tauritz, S. Mulder, and A. Naugle. Evaluating moving target defense with pladd. Technical report, Sandia National Labs-NM, Albuquerque, 2015.