Bad Data Injection Attack Propagation in Cyber-Physical Power Delivery Systems

Victor Chukwuka, Yu-Cheng Chen, Santiago Grijalva and Vincent Mooney

Georgia Institute of Technology
Atlanta, USA

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

Index-Terms — Bad Data Injection, Attack Propagation, Power System State Estimation, Cyber-Physical Security, State Estimation.

I. INTRODUCTION

The energy delivery system is a critical infrastructure that must continue to function even when under attack. The power grid has distinct features that create unique security challenges: a) transmission and distribution circuits over large geographic areas, b) unmanned substations, c) broad range of modern and legacy components, and d) use of a variety of communications technologies and protocols. In order to maintain secure operation, a centralized control approach supported by Supervisory Control and Data Acquisition (SCADA) systems is used. Sensors distributed across the network transmit system information to the control system, which also affects commands, by sending control messages to field components. The information received from the field is put together into a model and used to perform state estimation. A reliable, trustworthy and secure cyber-physical power delivery system requires continuous and efficient real-time monitoring, assessment of cyber-physical security conditions, and security situational awareness. It should be able to detect various types of cyber-physical attacks and be able to quantify, characterize, and mitigate the impact of such attacks.

There has been an increase in the number of cyber-attacks on cyber-physical power delivery systems with these attacks having severe consequences such as blackouts. Cyber-physical security attacks may target individual field cyber-components or the communications network. Cyber-attacks can modify or affect data or software applications such as demand response, frequency regulation and voltage control. A cyber-physical attack on the other hand can trigger operators to take inappropriate actions, which can lead to instability in the grid and cascading failures with significant consequences. Hence, to ensure a secure and reliable power grid, it is imperative to study the different ways in which the cyber-physical power grid can be compromised and then develop techniques and mechanisms to detect, evaluate and mitigate the propagation and impact of a potential cyber-physical security attack.

The rest of the paper is organized as follows. Section II describes the context and motivation of this research. Section III explains the attack graph semantics used in modeling the attack propagation, while Sections IV and V describes the attack and bad data injections scenarios. Section VI presents the results, and Section VII concludes the paper.

II. BACKGROUND

A. Motivation

Unauthorized access and/or manipulation of cyber-physical power delivery assets by an insider or disgruntled employee is the biggest threat to SCADA, Energy Management Systems (EMS) and bulk electric systems (BES) [1]. Notable cyber-physical attacks on SCADA and EMS systems in recent years include Maroochy Shire sewage spill attack in January 2000 [1], the Davis-Beese Ohio nuclear plant and Slammer Worm attack in January 2003 [1], the Stuxnet malware attack on electrical equipment powering Iran's Nuclear facilities in November 2010 [1], [2], and the cyber-attacks on Ukraine's power grid in December 2015 and February 2016 [3] which caused a blackout affecting 225,000 customers. These attacks have brought more attention to power system threats and vulnerabilities, and the impact of cyber-physical attacks on critical power delivery systems. The consequences and impact of power grid cyber-physical attacks can be worsened by cascading failures. A cascading failure refers to a sequence of dependent events, where the initial failure of one or more components (i.e., substations and transmission lines) triggers the sequential failure of other components [4]. The cause of the initial failures can be a cyber-physical attack, falling of a tree branch, equipment failure, aging equipment, human errors, software, or hardware faults. These cyber-physical attack events stress the need to determine and deploy mechanisms to minimize their risk.

B. Related Work

Much work has been proposed to investigate the vulnerability of power grids by developing threat and attack models as well

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE

as simulating different attack scenarios in a controlled environment. However, important challenges remain. Developing reasonable approaches and models that can mimic cyber-physical attacks in reality is still a critical challenge. Such models need to incorporate both the communications network and the power systems layer. In the current literature, two of the major approaches for investigating the effects of cyber-physical attacks on power systems are bad data and bad command injection attacks [5]. In modeling the power system layer, three popular models are typically adopted: pure topological models [6], pure power flow models [7], and hybrid models [8]. Each category has its own advantages and disadvantages. Finally, 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.

In order to detect and mitigate the effects of cyber-physical attacks, modelling and simulation of how these attacks may propagate through a cyber-physical power system need to be undertaken. The goal of this paper is not to design undetectable bad data injection attacks or to develop better bad data detection tests, but rather the goal is to study how bad data injection attacks propagate in the system before they are identified and contained or mitigated by the operator. Prior work related to attack propagation in networks analyzes honeypot systems [14]. leverages attack graph notation to demonstrate the propagation of malicious measurement injections into the power grid network with the intended result of the System Operator issuing incorrect but legitimate commands with disastrous consequences.

Regarding prior work related to power grid bad data injection attack analysis, Bad Data Injection (BDI) attacks have drawn wide concerns in cyber-physical power grids and were first proposed by Liu and Ning [9]. Liu showed that attackers can manipulate field measurements and introduce bad data into certain state variables and bypass the existing techniques for bad measurement detection in power systems by exploiting the knowledge of the power system topology. Liu et al. proposed a bad data detection method based on adaptive partitioning state estimation, which can raise the detection sensitivity by dividing the global power system into several subsystems. Bad data then can be located in a small area by multiple rounds of partitioning [10].

The authors in [11] analyze the cyber security of state estimators in SCADA systems operating in power grids by assuming that the attacker only possesses a perturbed model corresponding to a partial model of the true system, or even an outdated model. The attacker is then characterized by a set of objectives, and policies are proposed to synthesize stealthy deceptions attacks, both in the case of linear and nonlinear estimators. Real time online detection of stealthy false data injection attacks in power system state estimation was explored

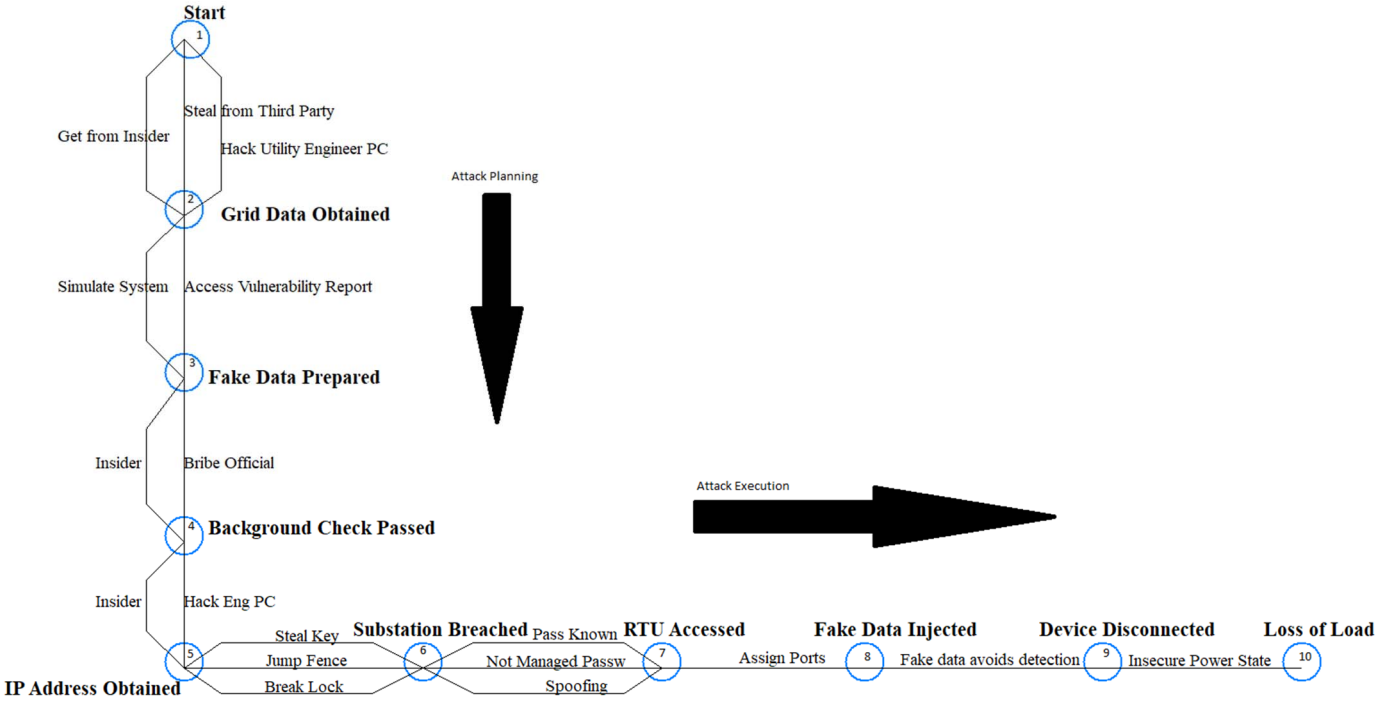

Figure 1. Attack graph capturing attacker's strategy

Our attack propagation model on the other hand, uses contextual information about the attacks by training multiple Markov Chain models. Hence we propose a novel framework that in [12]. An online anomaly detection algorithm is proposed. The algorithm utilizes load forecasts, generation schedules, and synchro-phasor data to detect measurement anomalies and

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE

provide some insight into the factors that affect the performance of the proposed algorithm. An empirical method to obtain the minimum attack magnitudes and the detection thresholds for meeting specified false positive and true positive rates is proposed. The work in [12] was extended in [13] by Li et. al. by considering the sequential (online) detection of false data injection attacks which aim to manipulate the state estimation procedure in the smart grid by injecting malicious data to the monitoring meters. The unknown parameters in the system, namely the state vector, injects malicious data and the set of attacked meters pose a significant challenge for designing a robust, computationally efficient, and high-performance detector. A sequential detector based on the generalized likelihood ratio to address this challenge was developed. In order to accurately understand the impact of bad data injection in cyber-physical power delivery systems, we need to go beyond just constructing undetectable bad data injection attacks but also investigate how the attack propagates through the system.

III. TERMINOLOGY & ATTACK GRAPH SEMANTICS

We represent the attacker's strategy in two phases. The first phase is the preparation phase, where the attacker needs to gather information and prepare all the necessary tools to execute an attack. Nodes one through five capture the preparation phase as captured in Figure 1.

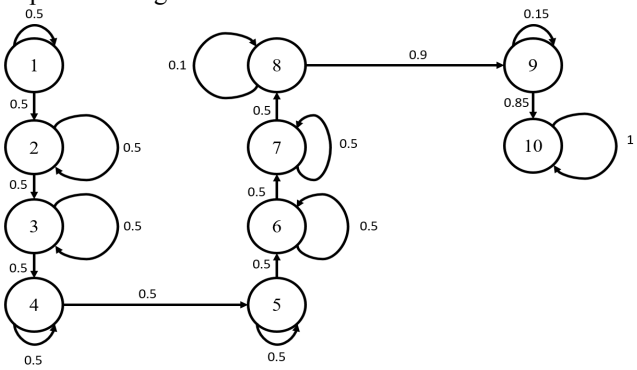

Figure 2. Markov Chain capturing attacker's strategy for compromising the power system under attack assuming no defender

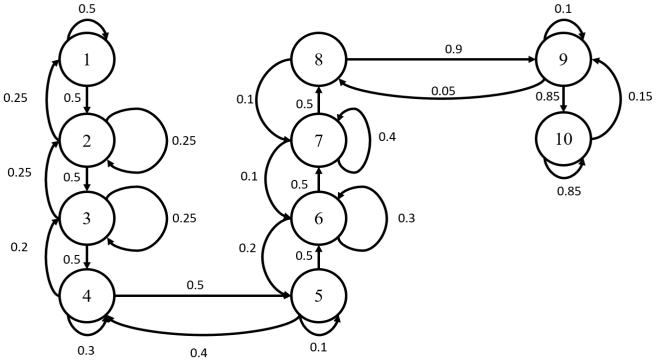

Figure 3. Markov Chain capturing attacker's strategy for compromising the power system under attack assuming defender with no state estimation

The second phase is the execution phase where the attacker executes the attack and interacts with the defender. The success or failure of the attack propagating from the source to the operator at the control center is modelled by a Markov Chain as shown in Figure 2. The Markov Chain encapsulates the attacker's strategy and probabilities of success/failure of the attack propagating from one node to the next.

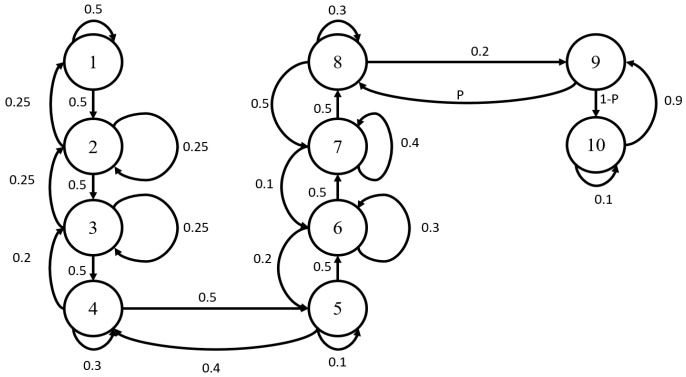

Figure 4. Markov Chain capturing attacker's strategy for compromising the power system under attack assuming defender with state estimation

Each node represents a malicious task an attacker wants to complete in order to successfully reach the attacker's goal. In Figure 1, we assume that the tasks are sequential, which means that only one task is being executed at any point in time. We also assume that the system has bad data detection capability from the state estimator. This detects and tries to prevent an ongoing attack from succeeding; however, it does not reset the attacker's current progress. Therefore, a successful detection of an attack at any node only pushes the attacker back to the immediate previous node. It is noteworthy to point out that the example scenario of this paper (see Figure1) does not show the possibility that a successful detection by the defender may cause the attacker's progress to be set back by more than one node. The Markov Chain does not restrict how the edges are connected. So the edges do not need to connect with adjacent nodes. Each edge (directed) represents the attacker's attempt to complete the next task given that the current task is completed. The value on each edge represents the probability that the attacker will transition to (amd be in the state of having successfully completed) the next task (i.e., the task pointed to by the edge). The probabilities in Figures 2-4 are chosen as an estimation of the real-world quantity. There are many factors affecting the probability, for instance, that the attacker would jump a fence, e.g., location of substation, type of fence, availability of cameras, etc. Although not discussed in this paper, more detailed models can take some of those factors into account and also must be correlated with actual attempts to physically infiltrate the substation. Similarly, the defense probabilities are reasonable estimates of the defense capabilities of security mechanisms against bad data injection attacks in the power system state estimation process. The probability assigned to each edge only depends on each individual vulnerability, which is similar to many existing metrics, such as Common Vulnerability Scoring System (CVSS) [15]-[16]. Although it is not shown in this paper, we have varied the probabilities for Figures 2-4. As expected, there is a linear relationship between

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE

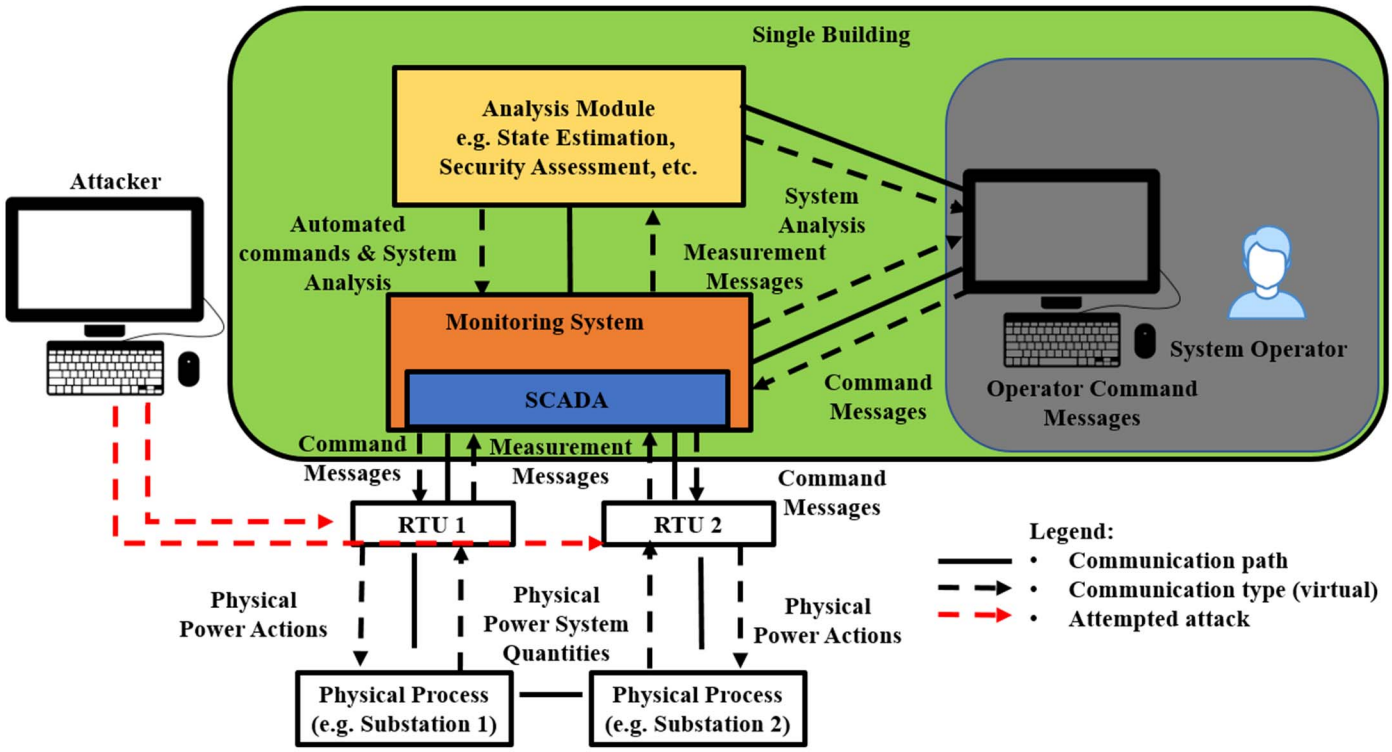

Figure 5. Cyber-Physical System Bad Data Injection Attack Path

how fast the attack propagates and probabilities on edges relating to attack. If the probabilities on an edge relating to defense is high, the probability of an attack going forward to the next edge decreases. Table 1 shows the mapping of an attacker's tasks to each node in Figures 1-4. Figure 1 is the attack graph representation of the Markov Chains shown in Figures 2-4.

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

IV. ATTACK SCENARIO

We assume that the attacker has full knowledge of the power system topology and in the planning state obtains IP addresses/TCP ports of the Monitoring System and the Remote Terminal Units (RTU) at the substations. The attacker breaks into the substation enclosure containing the RTUs and communication radio, connects a malicious computing device to an RTU and is able to access the RTUs. The attacker compromises the measurements polled by the Monitoring System by constructing packets containing fake field readings and transmitting said readings to the Monitoring System as shown in Figure 5 above.

We also assume that the attacker's goal is to cause the System Operator to issue an incorrect command as a result of the fake data injection attack rather than to completely disable the RTUs.

V. ATTACK PROPAGATION MODEL

The attack propagation model is a combined Markovian process and system state estimator model. As shown in Figure 1, we study attack propagation from the substation to the operator using a Markovian process. For a set of simulation time steps $t \in [1, T]$ the final state is obtained as shown in Equation 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 10 elements, which represents the ten nodes in our attack graph. Each element in x is either "0" for uncompromised, or "1" for compromised. P is a matrix that contains probability values shown in Figures 2-4. The row number in P is the node number at the tail-end of the edge. The column number in P is the node number at the head-end of the edge. If there is no edge connecting two nodes, the corresponding value in the matrix is 0. An example P matrix which is used in Figure 3 is shown below.

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE

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

$$\begin{aligned} \boldsymbol{x}^{(T)} &= \boldsymbol{x}^{(T-1)} * \boldsymbol{P} \\ &= \left(\boldsymbol{x}^{(T-2)} * \boldsymbol{P}\right) * \boldsymbol{P} \\ &\;\;\vdots \\ &= \boldsymbol{x}^{(0)} * \boldsymbol{P}^{\boldsymbol{T}} \end{aligned} \tag{1}$$

The model incorporates both the Markov Chain that captures attack propagation and a state estimation with bad data detection capabilities. The bad data detection algorithm is implemented at node nine of Figure 4. We investigate three cases – no defender, defender without state estimation, and defender with state estimation. In the attack graph shown in Figure 1, nodes one through five represent the attacker's preparation process, which is described in Table 1. Nodes six through ten represent the tasks executed by the attacker on to the power grid. Without defense, the Markov Chain representation of the attack graph is shown in Figure 2. There is no edge that shows an attacker's attack is pushed back to the previous node. In Figure 3, the Markov Chain representation of the attack graph shows the existence of a defender, but without a state estimation. Node eight represents an attacker injecting fake data from the RTU. Node nine represents the Analysis Module and Monitoring System in Figure 5. Without state estimation, there is a 0.9 (90%) chance that the fake data injected may cause the Analysis Module to reach an incorrect system state, and then the Monitoring System displays the incorrect system state to the system operator. Furthermore, there is a 0.05 (5%) chance that the attack may be identified by the system operator, in which case the attacker's progress is pushed back to node eight. Finally, there is also a 0.05 (5%) chance that the attack stays in node eight, because the fake data has not reached the Analysis Module yet. The probabilities are chosen to reflect the attacker's chances of successfully carrying out a bad data injection attack in the real world. Without a state estimator, the operator would have to rely on experience and intuition in analyzing the massive amounts of data received at the control center which means the chance of detecting bad data injection is low. In Figure 4, the Markov Chain representation of the attack graph assumes the existence of a defender with state estimation in node nine. In this case, the state estimator can detect and eliminate the bad data. The bad data detection of the state estimation enhances the detection capabilities of the power system, therefore, the edge from node nine to node eight in Figure 4 has the probability **P**. **P** is a variable probability of detection which is calculated by the state estimator using Chi-square cumulative distribution function. The existence of a state estimator provides a means to mitigate the attack by attempting to prevent the attack from propagating to the next node.

For simplicity, we model the bad data injection attack propagation using a two-bus system with a generator and load as shown in Figure 6. The field measurements from each bus are polled by two separate RTUs. The attacker compromises RTU1 measurements before compromising RTU2 measurements. RTU2 also acts as a Master Terminal Unit (MTU). An MTU can be an RTU that accepts different inputs such as field measurements from several RTUs and then transmits the measurements over the network to the analysis module for computational analysis.

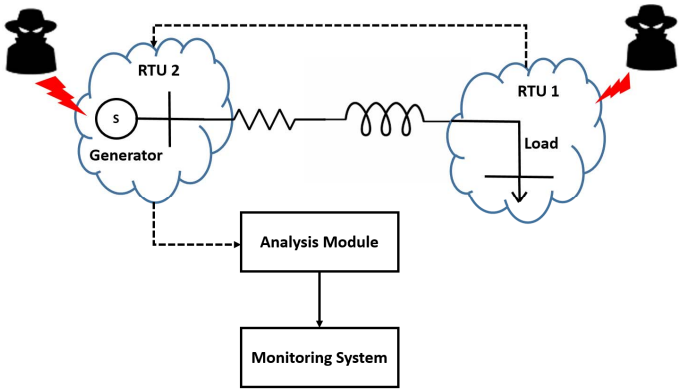

Figure 6. Two-Bus Case under Bad Data Injection Attack

The monitoring system collates the measurements by concatenating the measurements into a single measurement vector as shown in Equation 2.

$$\boldsymbol{z} = \left[\boldsymbol{z}_{\boldsymbol{RTU_1}}; \boldsymbol{z}_{\boldsymbol{RTU_2}}\right] \tag{2}$$
$$\boldsymbol{z} = \boldsymbol{h}(\boldsymbol{x}) + \boldsymbol{e} \tag{3}$$
$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{e} \tag{4}$$
$$\hat{\boldsymbol{x}} = (\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{H})^{-\boldsymbol{1}}\boldsymbol{H}^{\boldsymbol{T}}\boldsymbol{R}^{-\boldsymbol{1}}\boldsymbol{z} \tag{5}$$
$$\boldsymbol{r} = \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}} \tag{6}$$
$$\left|\left|\boldsymbol{r} = \boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}}\right|\right| \leq \boldsymbol{\tau} \tag{7}$$
$$\boldsymbol{z}_{\boldsymbol{attack}} = \boldsymbol{z} + \boldsymbol{a} \tag{8}$$
$$\left|\left|\boldsymbol{z}_{\boldsymbol{attack}} - \boldsymbol{H}\hat{\boldsymbol{x}}\right|\right| \leq \boldsymbol{\tau} \tag{9}$$

Using an standardized weighted least-squares state estimation model, Equation (3) shows how the various field measurements denoted by $\boldsymbol{z}$ are related to the state variables $\boldsymbol{x}$ (i.e. the voltages and phase angles) and the measurement error $\boldsymbol{e}$. $\boldsymbol{h}(\cdot)$ is a non-linear vector function expression of the measurements in terms of the state variables. Equation (4) shows the linear relationship between $\boldsymbol{z}$ and $\boldsymbol{x}$ under DC power flow model assumptions. Equation (5) denotes the state estimates, where $\boldsymbol{z}$ is the vector of measurements, **H** is the measurement Jacobian matrix, **R** is the error covariance matrix, $\boldsymbol{x}$ and $\hat{\boldsymbol{x}}$ are the vectors of state variables and state estimates respectively, and $\boldsymbol{e}$ is the vector measurement error. The state estimates are considered valid only if the measurement residuals $\boldsymbol{r}$ are less than

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE

a threshold (τ) as shown in equation (6) and (7). The threshold is set based on state estimation residual information obtained from historical data when the system is operating normally. The attacker compromises measurements in the measurement vector z by changing measurement values as shown in Equation (8) thus corrupting existing legitimate measurements.

For this simulation, the available measurements are taken to be

$$\boldsymbol{z} = \begin{bmatrix} V_1\,(kV) \\ V_2\,(kV) \\ P_{12}(MW) \\ Q_{12}(MVAr) \\ P_2(MW) \end{bmatrix}$$

and the quantities being estimated are $\boldsymbol{x} = [\theta_2, V_1, V_2]$. $RTU1$ measurements are relayed to $RTU2$ which collates those measurements with its own and send the collated measurements over the backbone communication network to the monitoring center. A synthetic load profile with peak load at mid-day is adopted to drive the simulation. Equation (8) is adopted in the formulation for minimizing the weighted least squares state estimator objective function shown in Equation (10) where $\boldsymbol{h_i(x)}$ are components of the measurement Jacobian, and R_{ii} is the diagonal matrix element representing the standard deviation of each measurement i.

$$J(\boldsymbol{x}) = \sum_{i=1}^{m} \frac{\left[z_{attack,i} - h_i(\boldsymbol{x})\right]^2}{R_{ii}} = [\boldsymbol{z_{attack}} - \boldsymbol{h(x)}]^T \boldsymbol{R^{-1}} [\boldsymbol{z_{attack}} - \boldsymbol{h(x)}] \quad (10)$$

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

$$\boldsymbol{g(x)} = \frac{\partial J(\boldsymbol{x})}{\partial \boldsymbol{x}} = [\boldsymbol{H(x)}]^T \boldsymbol{R^{-1}} [\boldsymbol{z_{attack}} - \boldsymbol{h(x)}] \quad (11)$$

where $\boldsymbol{H(x)} = \left[\frac{\partial h_i(x)}{\partial x_j}\right]$ is the measurement Jacobian.

Expanding the nonlinear function $g(x)$ around a guess state vector $\boldsymbol{x^k}$ and dropping the higher order of terms leads to a Newton iterative solution:

$$\boldsymbol{x^{k+1}} = \boldsymbol{x^k} - [\boldsymbol{G(x^k)}]^{-1} \boldsymbol{g(x^k)} \quad (12)$$

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

VI. Simulation Results and Discussions

As described in the previous sections, the attacker's strategy to compromise the power grid is broken down into multiple tasks that the attacker has to complete in order to reach a certain outcome. In the example attack graph shown in Figure 1, the attacker's goal is to inject bad data into the power grid in order to fool the system operator into issuing an incorrect command which can damage the power grid itself. The attacker manipulates field measurements to be telemetered from the RTUs to the Analysis module for execution of important grid functions such as state estimation as illustrated in Figure 5. The attacker compromises measurements from both RTUs. For detecting bad data, the Chi-squared distribution is used to identify the presence of bad data followed by the largest normalized residual test that identifies the actual measurements to be removed. The operator at the monitoring center is notified when the residual is higher than normal.

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

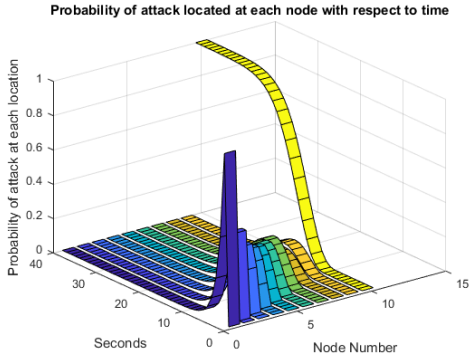

Figure 7. Probability of an attack being located at each node with respect to time for the case assuming no defender

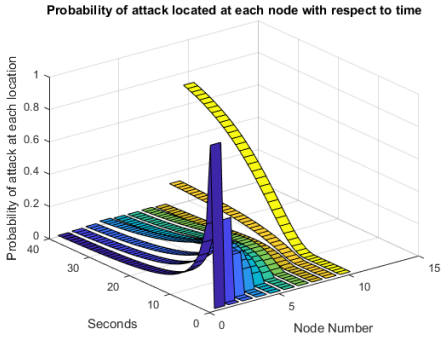

Figure 8. Probability of an attack being located at each with respect to time for the case assuming defender exists, but not using state estimation

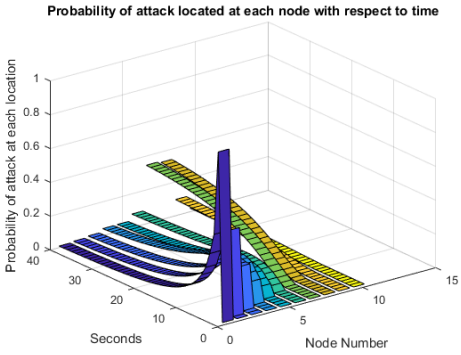

Figure 9. Probability of an attack being located at each node with respect to time for the case assuming defender exists, and uses state estimation.

All of the simulation cases have the attacker starting to attack at time equals to 2 seconds. We assume one second as the time

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE

unit for evaluation where an edge may be traversed with the probability associated with the edge. This time unit may of course be made to be longer, e.g., one minute or one day; for simplicity in showing our results, we use one second as the time unit.

In Figure 7, the simulation shows that the attack quickly propagates through nodes one through ten, and so the probability of the attack being in node ten is 1 after only a few seconds. In this case, the attack propagates all the way through with the operator being presented with the incorrect state of the system thus causing the operator to take an incorrect action. In Figure 8, the simulation shows that the attack takes longer to reach node ten, and after the simulation ends, the probability of attack reaching node ten is less than 1. This means that with consideration of defender in the power grid, the attacker does not always reach the goal with certainty. In Figure 9, the simulation shows that the attack still propagates through nodes one through five, but due to an increase in detection capability, the probability that the attacker's attack stays at node seven and eight is very high. In this case, the state estimation provides a viable means of increasing the defender's capabilities through the bad data detection functionality of the system state estimator. As a result, it is highly unlikely that the bad data propagates all the way to the control center forcing the operator to make a decision based on inaccurate data.

VII. Conclusion

The use of attack graph to model attack propagation in a power grid scenario that combines the use of state estimation is the novel contribution of this paper. Currently, the attack graph models only sequential tasks, so parallel execution of an attacker's set of tasks is not modeled. In addition, the attack graph does not take into account the attacker's ability to learn nor the defender's ability to take away the knowledge gained by the attacker. Other types of state estimation, such as the dishonest Gauss Newton method in [17] may also be implemented in our simulation. The combination of attack propagation model and state estimation provides additional information for the system operator, so appropriate mitigation strategies can be implemented. For example, if the simulation result shows that there is a high chance a RTU's being attacked, then the system operator may take actions such as password reset, disconnect access point of an RTU or increase the priority to send out substation crews to check on the compromised RTU. Results and insights from this paper can inform designing better incidence response plan for operators at the control center. Operators can use the information provided from visualization of the attack propagation and abnormal residuals to filter through information and pin-point the most vulnerable sectors of the cyber-physical power system under attack and thus trip the necessary alarms and/or issue the appropriate control commands to contain the attack and mitigate its effects.

References

[1] R. Tsang, "Cyberthreats, vulnerabilities and attacks on SCADA networks," *Univ. California, Berkeley, Work. Pap. ...*, pp. 1–23, 2010.

[2] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electr. Power Syst. Res.*, vol. 149, pp. 210–219, 2017.

[3] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *SANS Ind. Control Syst.*, p. 23, 2016.

[4] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li, J. Li, Z. Li, C. C. Liu, L. Mili, S. Miller, R. Podmore, K. Schneider, K. Sun, D. Wang, Z. Wu, P. Zhang, W. Zhang, and X. Zhang, "Initial review of methods for cascading failure analysis in electric power transmission systems," *IEEE Power Eng. Soc. Gen. Meet.*, pp. 1–8, 2008.

[5] 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.

[6] 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.

[7] 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.

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

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Ccs*, vol. 14, no. 1, pp. 1–33, 2009.

[10] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, "A novel method to detect bad data injection attack in smart grid," *2013 Proc. IEEE INFOCOM*, pp. 3423–3428, 2013.

[11] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," *Proc. 49th IEEE Conf. Decis. Control*, pp. 5991–5998, 2010.

[12] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1–1, 2016.

[13] S. Li, Y. Yilmaz, and X. Wang, "Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, 2015.

[14] A. Bar, B. Shapira, L. Rokach and M. Unger, "Scalable attack propagation model and algorithms for honeypot systems," *2016 IEEE International Conference on Big Data (Big Data)*, Washington, DC, 2016, pp. 1130-1135.

[15] L. Wang, T. Islam, T. Long, A. Singhal and S. Jajodia, "An Attack Graph-Based Probabilistic Security Metric," in IFIP Annual Conference on Data and Applications Security and Privacy, Berlin, Heidelberg, 2008.

[16] P. Mell, K. Scarfone, and S. Romanosky. Common vulnerability scoring system. IEEE Security & Privacy Magazine, 4(6):85–89, 2006.

[17] M. A. Rahman and G. K. Venayagamoorthy, "Dishonest Gauss Newton method based power system state estimation on a GPU," *2016 Clemson University Power*

Systems Conference (PSC), Clemson, SC, 2016, pp. 1-6.

978-1-7281-0316-7/18/$31.00 (c)2018 IEEE