# PAVED: Perturbation Analysis for Verification of Energy Data

Megan Culler
*Electrical Engineering*
*TAMU, College Station*
culmegan@tamu.edu

Katherine Davis
*Electrical Engineering*
*TAMU, College Station*
katedavis@tamu.edu

Abhijeet Sahu
*Electrical Engineering*
*TAMU, College Station*
abhijeet_ntpc@tamu.edu

***Abstract*—Sensor integrity is arguably the most critical feature to protect in cyber-physical systems. Since power systems are cyber-physical systems with ubiquitous sensors that monitor and protect the grid, data must be trustworthy. Process safety and control decisions ultimately depend on data. The focus of this paper is how to design and apply perturbation based detection for sensor verification, under full AC unobservable false data injection (AU-FDI) attacks, by combining an active probing strategy with cyber-side data based on the cyber-physical situational awareness model CyPSA. A case study on a cyber-physical eight substation model is presented, where we construct an AU-FDI attack and introduce our probing-based detection solution and evaluate it with varying probe signals, values, and locations. Results demonstrate how sensor data in power systems can be systematically authenticated using perturbation-based techniques and how different perturbation types and locations affect the results. The case study then demonstrates the improvements to verification by using both physical and cyber data, as CyPSA provides risk prioritization in the form of authenticity weight measure of the sensors, for enhancing the security of power systems from a cyber-physical point of view.**

***Index Terms*—Power systems, security, sensor integrity, control systems, cyber-physical systems**

## I. Introduction

Access to reliable power is essential to modern society, and this ubiquitous dependence on electric power compels understanding and improvement of grid security. The need to consider grid resilience to threats is evidenced by the fact that the energy sector is one of the most targeted critical infrastructure sectors for cyberattacks, and the capabilities of these attacks are growing. Symantec reported that in more than 20 cases during spring and summer 2017, hackers obtained operational access to power systems [1]. The increased prevalence of interconnected devices has improved efficiency, but each additional node is a potential point of entry for a cyberattack. Cyberattacks against power systems have the potential to cause widespread physical damage and can be launched from anywhere from the world [2, 3]. While utilities have significant experience preventing outages due to natural causes, stakeholders are still developing incident response plans for coordinated attacks. Research to close gaps in utility cybersecurity needs, attack detection, and localization technique as an important part of the solution. This work systematically develops and applies perturbation-based sensor verification against AC unobservable false data injection attacks (AU-FDI), building on [4, 5], while combining network connectivity and vulnerability knowledge, from cyber-physical situational awareness (CyPSA) analysis [6].

The paper proceeds as follows. Section II motivates sensor integrity verification and provides a literature review on detection techniques for FDI attacks. Section III presents a case study of an 8-substation cyber-physical model with our perturbation technique and sensitivity analysis. Section IV describes the perturbations and analysis of their detection efficacy and the improvements made when CyPSA is integrated. Section V concludes the paper.

## II. Background

### A. Motivation to Defend Sensor Integrity

The 2017 attack on Ukrainian power distribution companies proved to be a public example of the severe consequences that cyberattacks can have on large scale power systems. The malware was introduced into the system months before it was executed. Seven substations were disconnected by attackers through remotely controlled, false command injection to circuit breakers [7]. The damage could have been worse, but operators responded quickly to the incident and regained control of the system rapidly [8]. Data verification is an important tool in mitigating such situations. Another important type of attack to consider is an insider threat. A power system controlling a waste treatment plant was attacked in Australia in 2001 by a former employee of the company that installed the system [9, 10, 11]. After he accessed and manipulated the SCADA system, millions of liters of raw sewage flooded public areas and rivers [11]. A final noteworthy attack is the Stuxnet virus targeting Iranian nuclear facilities. This malware was developed to target Programmable Logic Controllers (PLCs) to overspeed the centrifuge in the uranium enrichment facility, but it was so aggressive that it spread worldwide [12]. Changes to PLC logic damaged sensitive equipment and forced costly repairs, while injecting false data displayed to the operators to hide the attack [13]. These examples show the importance of having trustworthy data from sensors to inform operators quickly of any abnormalities so they can regain control of their systems.

### B. Current State-of-the-Art and Literature Review

Research of cybersecurity for power systems has historically focused on keeping intruders out of a network. Now, given adversary success in accessing systems unobserved, detection and remediation of cyber-events in a system are also included.

Power systems need to be resilient under cyber compromise, detecting the source of intrusions. State estimation can be useful when reconstructing the actual state of the system with injected or noisy data. Methods to improve the accuracy and observability of a system are discussed in [14] and [15]. Correct system state estimation is not always possible under attack [11], hence secure state estimation for power systems under attack is discussed in [11, 16, 17]. An adversary can



978-1-5386-8099-5/19/$31.00 ©2019 IEEE

perform random and targeted FDI attacks to modify measurements to mislead the state estimator to predict incorrect states without triggering alerts from residual-based bad data detector [17, 18]. In [19], an attack strategy is proposed that can generate an attack with partial system information. Attackers can also launch reinforcement learning-based FDI attacks as proposed in [20]. Designing a defense mechanism for such intelligent attacks is challenging. Advanced signal processing techniques are used [16] to defend against both stealthy and non-stealthy attacks. Additionally, intrusion tolerance techniques for general cyber-physical systems are developed [21].

Perturbation methods can be used to detect errors in communication systems and FDI attacks. These methods *strike* the system, and observe how it responds. In power systems, such a strike can be implemented by changing a control signal [22, 23], physical parameters [24], or controller outputs. Research in [4] develops the generic concept of probing of power systems, and explains why it can be used for detection. Building on that, [5] shows how the attacker only needs a limited set of information about the system to execute a successful AC unobservable FDI attack (AU-FDI). A reactance perturbation technique has been incorporated in [24] to maximize the likelihood of FDI attack detection by minimizing the operation cost but considers a DC model for validating their perturbation method. Authors in [23] proposed an input control signal perturbation for replay attack detection in a linear control system with Linear Quadratic Gaussian (LQG) controller. A dynamic watermarking technique is proposed in [22] for detection of cyberattacks in Automatic Generation Control (AGC). PAVED improves upon previous works [4, 5] by exploring various probing strategies and the combination of perturbation defense validated by cyber-physical modeling proposed in [25] to detect and localize AU-FDI attacks. Our technique is independent of the measuring devices used in the system. The use of perturbations in combination with cyber-physical modeling extends the use for such models in situation awareness, and improves on the ability of perturbation methods to detect cyberattacks.

### C. AU-FDI Attack Model

AC unobservable false data injection attacks (AU-FDI) are characterized as attacks where an adversary modifies the data to achieve some objective for the observed system values, where measurements are changed such that the AC power flow equations are still satisfied [5]. Because power flow equations are nonlinear, there can be multiple solutions for the same set of constraints. The attack succeeds in staying unobservable by finding a different feasible AC power flow solution, and the problem formulation is such that it requires only local knowledge by the adversary, as described in [5]. In our scenario, we assume an adversary has gained access to a particular substation and executes a Man-in-the-Middle attack such that the data received at the control center is different from sensor data. PAVED is independent of attack strategy or mechanism.

## III. System Model

Power system operational reliability requires correct decision making by both human operators and automated systems. An operator must be able to trust the data displayed at a console and be able to make intelligent operational decisions based on trustworthy data. A synthetic 8-substation cyber-physical model of the grid, originally developed and presented in [26], is the case study used for PAVED. This model is unique in the cyber-physical dependencies that are modeled, allowing unified analyses of the control network, protection systems, and the electrical power network.

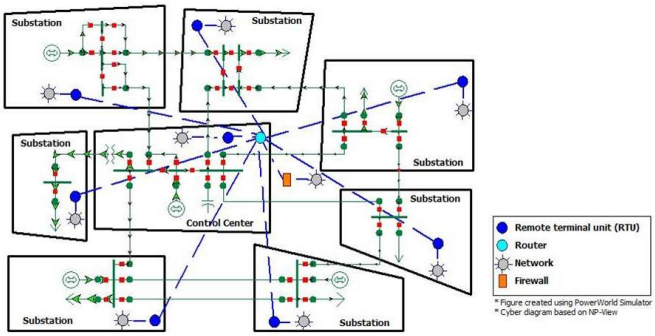


Fig. 1: Cyber-physical 8-substation model [26]

### A. Case Study: Cyber-Physical 8-Substation Model

The model has eight substations, five of which have generators. There are a total of 52 buses across the eight substations, each with voltage, angle, real power, and reactive power measurements. Internal substation nodes, relays, breakers, firewalls, and routers are modeled as shown in Figure 1. This model additionally contains cyber information unlike most of the other models, and it is exactly this enhanced detail developed in [26] that made it an appropriate case study for PAVED's detection method. The relays and breakers represented in the substations are crucial for cyber-physical modeling because the relays detect faults and trip breakers to prevent physical damage to the system. Protective relays and a control network were added to the original model later based on real utility setups. Protection schemes were based on Schweitzer Engineering Laboratories published best practices [26].

### B. Perturbation Development

Test cases were set up so that probes of different measurements could be analyzed. The data from the 8-substation case was initially set up in PowerWorld, and the AC power flow was solved in MATLAB as the base case before any perturbations, labeled $m_0$. Although useful for setting up the scenario, this unattacked case was not used in testing as it was neither the expected nor observed state of the system under perturbations.

Then, the attacked case was created where an adversary had access to one particular substation. It was shown in [5] that an attacker would need knowledge of neighboring nodes in addition to the target node to create a successful AU-FDI attack, but only values from within the substation could be modified. To achieve this, all buses outside of the attacked substation and buses inside the substation that were directly connected to external nodes were designated as *protected buses*. This was considered the observed state as seen by the operator, $\tilde{m}_0$, as detailed in [5].

After the initial attacked case was created, a perturbation was generated at a node that propagated throughout the system.

We observed how the system responded to the perturbation based on the size, origin, and type of the perturbation. After perturbing the system, a normal power flow analysis was performed. The real state of the system after the perturbation is a function of $m_0$ as defined in [5],

$$m_1 = d_1(m_0) \tag{1}$$

where $d_1$ is change to the system in response to the perturbation. This is useful to know, but it is not the expected case because the operator expects to see changes based on $\tilde{m}_0$, not $m_0$. It is not the fully observed case because the attacker will still be influencing some of the measurements. The state that the operator will expect is

$$\tilde{m}_{exp} = d_1(\tilde{m}_0) \tag{2}$$

To prevent the system state to be disturbed, a small perturbation is incorporated, which even the attacker cannot distinguish from other disturbances. Even if the attacker did recognize the change, it is unlikely that they would be able to respond in real time. Thus, we assume that the adversary does not know about the perturbation, and he does not subsequently alter the measurements for the nodes under his control. The final set of observed values is the perturbed values of the attacked case at the *protected buses*, and the perturbed values of the attacked case at the *non-protected buses* as shown below.

$$\tilde{m}_{obs} = \begin{cases} d_1(m_0) & for\ \ protected\ \ bus \\ \tilde{m}_0 & for\ \ non\, protected\ \ bus \end{cases} \tag{3}$$

We would expect $d_1(m_0)$ to be almost same as $d_1(\tilde{m}_0)$ for the *protected buses* since the attacker is not modifying values outside of the compromised substation, and the attack construction is designed for us to perceive these changes. For this experiment, we only looked at one time iteration of the probing. Three types of probes were used to test the perturbation method. A *voltage probe* simulated a small change in voltage level at a bus. A *real power probe* simulated a small change in real power output at the generator. A *reactive power probe* simulated a small change in reactive power output at the generator. At each bus, real power, reactive power, voltage, and angle were measured after each probe. A flowchart of this algorithm is shown in Figure 2. Finally, we perform sensitivity analysis and use our CyPSA engine [6] to validate our detection technique.

### C. Sensitivity Analysis of Perturbation on the States

The perturbation amount that prevents the system from reaching an unsafe state can be estimated by performing sensitivity analysis. This analysis would help the operator to select a range of feasible probes. Sensitivities analysis is used to validate the results of our perturbation method. For each probe introduced, the negative inverse of the AC power flow Jacobian reveals how the states change during power flow solution due to small change in mismatch,

$$\begin{bmatrix} \Delta\boldsymbol{\theta}^{(v)} \\ \Delta\left|\boldsymbol{V}\right|^{(v)} \end{bmatrix} = -\boldsymbol{J}^{(v)} * \begin{bmatrix} \Delta\mathbf{P}\left(\mathbf{x}^{(v)}\right) \\ \Delta\mathbf{Q}\left(\mathbf{x}^{(v)}\right) \end{bmatrix} \tag{4}$$

where Jacobian $\boldsymbol{J}$ is given by

$$\begin{bmatrix} \frac{\partial\mathbf{P}^{(v)}}{\partial\boldsymbol{\theta}} & \frac{\partial\mathbf{P}}{\partial\mathbf{V}}^{(v)} \\ \frac{\partial\mathbf{Q}^{(v)}}{\partial\boldsymbol{\theta}} & \frac{\partial\mathbf{Q}}{\partial\mathbf{V}}^{(v)} \end{bmatrix} \tag{5}$$

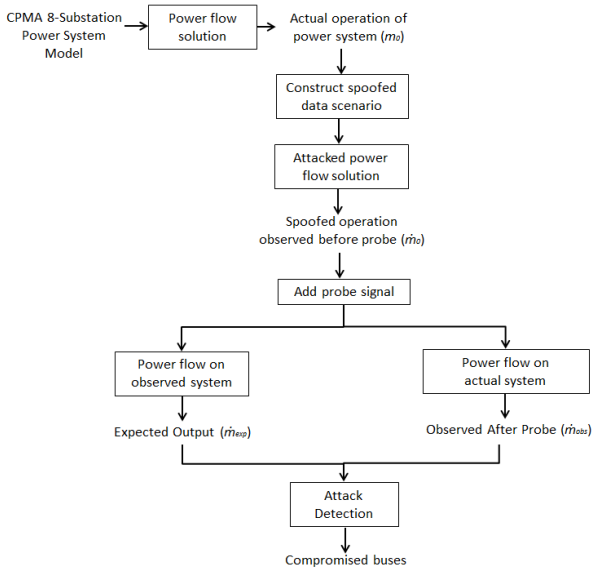


Fig. 2: Attack Detection Algorithm.

and $\Delta P(\mathbf{x}^{(v)})$ is given by

$$\Delta\mathbf{P}\left(\mathbf{x}^{(v)}\right) = \begin{bmatrix} P_2\left(\mathbf{x}^{(v)}\right) + P_{D2} - (P_{G2} + P_{probe}) \\ \vdots \\ P_n\left(\mathbf{x}^{(v)}\right) + P_{Dn} - (P_{Gn} + P_{probe}) \end{bmatrix} \tag{6}$$

In Eq. 6, $P_{probe}$ and $Q_{probe}$ are the vectors of real and reactive power probe introduced in the generator and load buses respectively. In our simulations, we consider one non-zero value to be perturbed. Our objective was to observe the impact of probe on the state variables, hence we analyze $\frac{\partial\theta}{\partial P_{probe}}$ and $\frac{\partial\mathbf{V}}{\partial P_{probe}}$. The state variables are changed as per Eq. 4. Usually, the resistance of the transmission lines are less than the impedance and the phase difference between the buses is small and the 8-substation case also follows the same approximation. Hence, the off diagonal terms in $\mathbf{J}$ are usually small and we find that $\boldsymbol{\theta}$ is more sensitive to $P_{probe}$ than $Q_{probe}$. Similarly, $|\boldsymbol{V}|$ is more sensitive to $Q_{probe}$ than $P_{probe}$.

### D. CyPSA Topology Scores

The final step is to compare the expected and observed results. Because the system responds normally at the *protected buses*, we believe that the expected and observed values will match, but at the adversary-controlled nodes, the data received will not match the expected case. This type of mismatch can indicate that certain buses have been compromised.

$$m_{result} = m_{exp} - m_{obs} \tag{7}$$

The mismatch can sometimes be caused due to a fault in the sensors as well. To facilitate interpretation of the results, such as distinguishing a fault from a compromise, and also identifying the relationship among the compromised measurements, we used a topology analysis tool, CyPSA [6], to determine the feasibility of the perturbation results given the cyber connections in the system. CyPSA is a tool that analyzes physical and cyber connections in a power system to determine nodes vulnerability level. CyPSA provides two scores, the performance index ($PI$) and the cyber cost($CI$),

which combine into a single security index ($SI$) for each bus computed using Eq 8. $PI$ indicates the severity if a bus is compromised and $CI$ indicates the difficulty to reach a bus through cyber connections along the path $p(i)$, given a cyber entry point. The list of the hosts in the access path $p(i)$ provides us the set of measurements that can result in higher $m_{result}$, asserting our detection using perturbation based technique.

$$SI(p(i)) = \frac{PI(p(i))}{CI(p(i))} \tag{8}$$

A higher CyPSA score indicates that a host is easier to reach and has a higher impact on grid performance if compromised, and is, therefore, more vulnerable. This analysis is time-independent; it measures the vulnerability of the configuration of the system. The tool uniquely integrates the cyber paths, physical devices and power flows in a way that is difficult to perform with other power flow modeling software, and thus serves as the best tool to verify a potential attack detected by perturbations, and decide if a certain bus is under attack. For this experiment, we started the CyPSA analysis from a random bus within the compromised substation. Buses that were considered *unreachable* on a cyber path from the entry node was given a cyber cost of infinity.

## IV. Results

### A. 8-substation AU-FDI Attack Scenario

A simulated data injection attack scenario is launched at the compromised substation which corresponds to buses 15-25. The attack is designed to cause the generator to appear to have 50 MVAr less reactive power that what is actually injected and to make another substation bus appear to be at 80% of its actual voltage. Normally, voltage limits are between 0.95 and 1.10 p.u., so 0.8 p.u. would alert to a potential issue. An operator might then increase reactive power generation to fix the perceived low voltages that are actually high.

### B. Voltage Perturbation

The first probe tested is a voltage magnitude perturbation, which is only valid at PV buses. There are five generators (PV buses) in the original system, and one of these is reserved as a slack bus, and cannot be perturbed. Each generator is individually probed. The results from a perturbation of 0.01 p.u. did not clearly identify any substation as different from the others. The per-unit voltage results were largest at the compromised substation, but the magnitude was still so small that it would not have been detected on a larger, more dynamic system. The magnitude of the angle, real power, and reactive power measurements are similarly too small in size to be detectable. A larger probe of 0.1 p.u. was also tested. This test produced larger magnitudes of differences between expected and observed values, but the patterns did not identify the compromised substation clearly. Additionally, a probe size of 0.1 p.u. is large and could be capable of causing other effects in the system.

### C. Real Power Perturbation

The next perturbation tested is a real power perturbation, which is also a generator probe, because real power at a generator is a controlled value. As long as the generator is not at full capacity, a small real power probe will not cause problems in the system. The first perturbation has a magnitude of 1 MW and is tested at all generators except the slack bus.

Although the measurement of voltage magnitude is noisy, measurement of real power and voltage angle correctly identify bus 20, which is one of the compromised buses at the compromised substation. The fact that this perturbation type gives consistently accurate results no matter which generator the perturbation was launched from, increases our confidence that this probe would reliably identify the compromised substation. Additionally, we can see that the difference between expected and observed voltage angle very clearly identifies the compromised substation. Although the magnitude is different depending on where the probe was launched from, in all cases, the only place where the expected and observed values differ is at the compromised substation.

Testing different sizes of real power perturbations reveal that the results change proportionally with the perturbation size. The relative relation between measurements at each substation is the same for all perturbation magnitudes. The larger perturbation more obviously reveals the compromised substation, but we do not want to perturb too much.

### D. Reactive Power Perturbation

The final set of probes that were tested is reactive power perturbations at PQ buses. Specifically, we increase reactive power produced at a load bus. We assume that the load is constant for a short period time, which isolates the effects of the reactive power perturbation. The perturbation is individually sent from different locations, from load buses rather than generators. There are six substations with loads in our model, and no load at the compromised substation. The results are similar to the results obtained with a real power perturbation. In both cases, the reactive power results are small, and likely would not be detectable in real systems. The magnitude of the other types of results is also very small for a reactive power probe of 1.0 MVAr. Testing different magnitudes of perturbations reveal that the results depend heavily on the source of the perturbation, which is different from other perturbations. The operator would not know before generating perturbations where the attacked substation was, so all probe sources should be tested. We can observe from Figure 4 that the real power perturbations produce greater differences between expected and observed voltage angles. This suggests that a real power perturbation will be more efficient at identifying the compromised substation. Measurable results are obtained for reasonably small-sized perturbations. It is also clear that voltage angle measurements are less noisy that voltage magnitude. However, the magnitude measurements still appear noisiest at the compromised substation, suggesting this measurement could be used to detect anomalies.

The comparison of the effect of real power and reactive power perturbations on voltage angle and voltage magnitude measurements is shown in Figure 3. These comparisons show that the voltage angle is more sensitive to real power, and the voltage magnitude is more sensitive to the reactive power, validating the sensitivity analysis of perturbation.

### E. CyPSA Topology Analysis

The CyPSA analysis is performed considering each hardware device with an IP address. There is not a one-to-one correlation between devices and buses, but each component belongs to a substation, and each relay controls particular

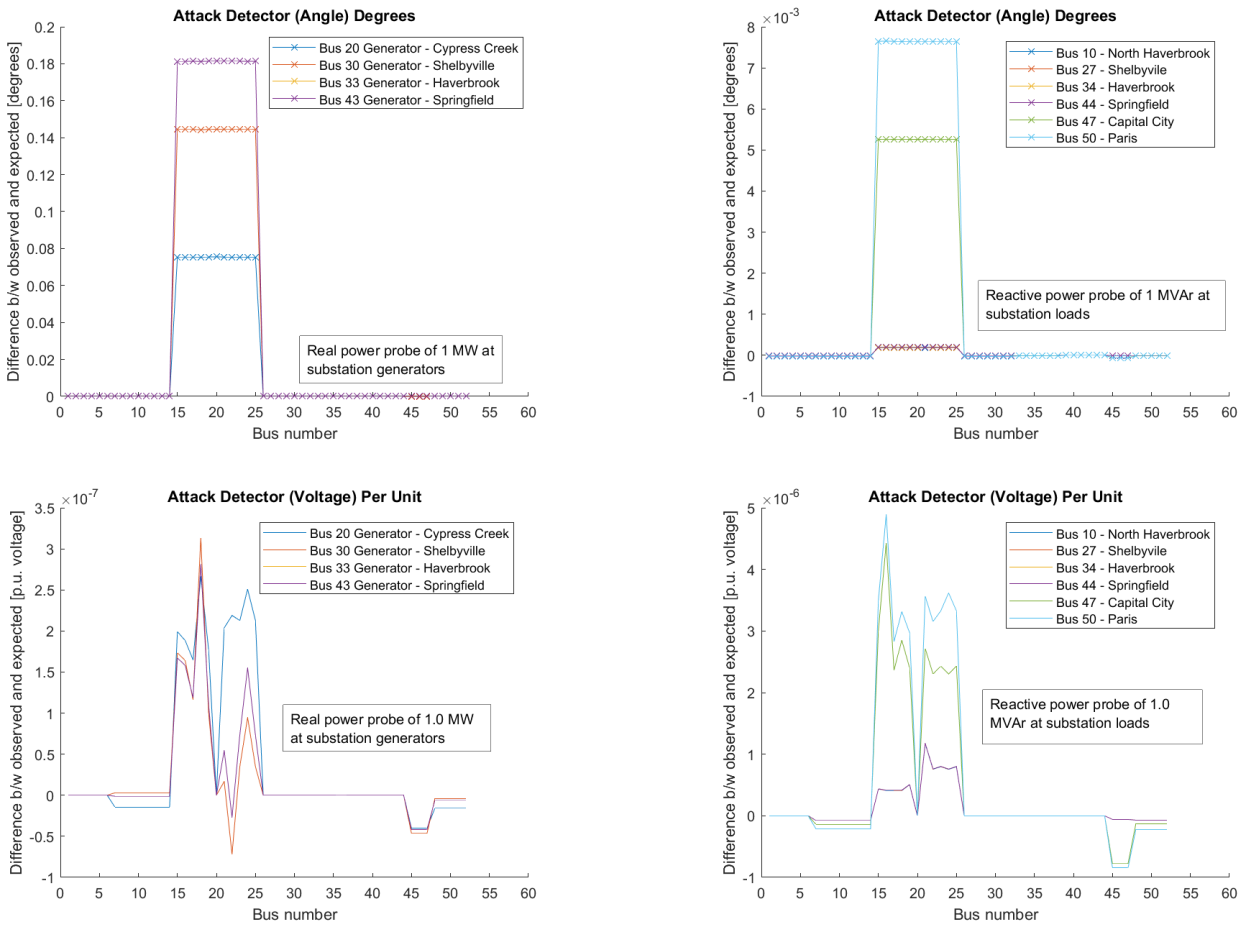


Fig. 3: Voltage angle and magnitude from real power perturbation of 1.0 MW and reactive power perturbation of 1.0 MVAr.

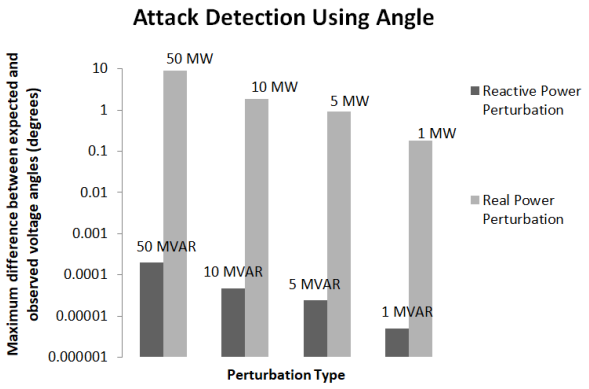


Fig. 4: Voltage angle results from real and reactive power perturbations.

breakers and measurements. The CyPSA analysis can verify if the results from the perturbation experiment can be attributed to a cyber event. Table I shows the CyPSA scores from the cyber entry point in the compromised substation. All six of the reachable hardware components belong to the compromised substation. All other devices not listed had a security index of 0. Given the connections and firewalls in this system, if an attacker gains entry to the compromised substation, he will be unable to modify values at any other substation.

TABLE I: CyPSA scores for cyber entry at 10.31.1.201.

| IP Address | PI | CC | SI |
|---|---|---|---|
| 10.31.1.101 | 1.38 | 8.95 | 0.15 |
| 10.31.1.102 | 2.23 | 8.95 | 0.25 |
| 10.31.1.103 | 3.89 | 8.95 | 0.43 |
| 10.31.1.104 | 1.38 | 8.95 | 0.15 |
| 10.31.1.105 | 1.57 | 8.95 | 0.18 |
| 10.31.1.201 | 10.45 | 44.76 | 1.17 |

### *F. Sensor Trustworthiness Scores*

The final step of PAVED was to combine the CyPSA topology analysis with the real-time probing results. This allows us to determine if the perturbation results make sense in the context of cyber-physical security, which makes this approach more comprehensive compared to other perturbation techniques. We should ensure that the compromised substation identified by the perturbation analysis is something that could be feasibly reached by the cyber connections. We weight the perturbation results with the CyPSA security index scores, and find that the weighted results eliminate the noise at other

substations (since the security index at those nodes is zero), and places a higher value on the compromised substation. The results from the perturbation analysis are refined by the CyPSA integration. The integrated results support the conclusion that the compromised substation has experienced a cyberattack, and improve the detection rate over a regular perturbation method. Thus, this could help identify the compromised substation where the perturbation results are less pronounced, and maybe more valuable in a system with fewer cyber defenses between substations.

## V. Discussion and Conclusion

Combining the results from the real-time probing and the CyPSA analysis, PAVED showed successful identification of AU-FDI attacks. Different types of probes are examined and found to have varying levels of accuracy in identifying the compromised substation. The most accurate results were obtained by measuring voltage angle response to real and reactive power perturbations. On average, the response from a real power perturbation was ten thousand times larger than the response from a reactive power perturbation. Our technique identifies the compromised substation with a probe sized such that it would not disrupt normal operation while producing detectable results. The most promising results from PAVED were from real power probes, together with the CyPSA scores, to prune the feasibly attacked substations. This work can be used to help operators determine the trustworthiness of sensors in a system. If an operator suspects that data is being manipulated, they can use the probing technique to test their theory before taking actions that might negatively disrupt the system. PAVED provides a cyber-physical foundation for continued real-system work on topology and real-time probing attack detection methods for cyber-physical power systems. To build on PAVED, future work includes exploring how to consider the dynamic response of attackers to probing, whether and how an adversary could detect the probe, and how they might respond while remaining unobserved.

## VI. Acknowledgements

This work was supported by the National Science Foundation under Award #1446471 and #1808064. The authors would like to thank the Texas A&M LAUNCH Undergraduate Research Scholars Program for supporting the undergraduate thesis research that led to the results reported in this paper.

## References

[1] A. Greenburg, "Hackers Gain Direct Access to US Power Grid Controls," https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

[2] M. E. Beatty, S. Phelps, C. Rohner, and I. Weisfuse, "Blackout of 2003: Public health effects and emergency response," *Public Health Reports*, 2006.

[3] W. Boyer and S. A. McBride, "Study of security attributes of smart grid systems current cyber security issues," 04 2019.

[4] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *2012 45th Hawaii International Conference on System Sciences*, Jan 2012.

[5] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation-based defense," in *2012 IEEE Third International Conference on Smart Grid Communications*, Nov 2012, pp. 342–347.

[6] K. R. Davis, R. Berthier, S. Zonouz, G. Weaver, R. B. Bobba, E. Rogers, and D. M. N. P. W. Sauer, "Cyber-physical security assessment for electric power systems," in *IEEE-HKN: The Bridge*, 2017.

[7] D. Case, "Analysis of the Cyber Attack on the Ukrainian Power Grid," https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, 2016.

[8] J. Wirfs-Brock, "The Realities Of Cybersecurity At A Rural Utility," https://grid.insideenergy.org/cybersecurity, 2015.

[9] J. Zubairi and M. A, *Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies*, 01 2011.

[10] T. Smith, "Hacker jailed for revenge sewage attacks," 01 2001.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.

[12] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, March 2013.

[13] Y. Han, S. Etigowni, H. Liu, S. Zonouz, and A. Petropulu, "Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. NY, USA: ACM, 2017.

[14] S. Hossain-McKenzie, S. Etigowni, K. Davis, and S. Zonouz, "Augmented dc power flow method with real-time measurements," in *2016 Power Systems Computation Conference (PSCC)*, June 2016, pp. 1–7.

[15] J. Johnson, S. Hossain-McKenzie, U. Bui, S. Etigowni, K. Davis, and S. Zonouz, "Improving power system neural network construction using modal analysis," in *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*, Sep. 2017, pp. 1–6.

[16] J. Jiang and Y. Qian, "Defense mechanisms against data injection attacks in smart grid networks," *IEEE Communications Magazine*, Oct 2017.

[17] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[18] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, pp. 717–729, 03 2014.

[19] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference*.

[20] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, 2019.

[21] S. Hossain, S. Etigowni, K. Davis, and S. Zonouz, "Towards cyber-physical intrusion tolerance," in *2015 IEEE International Conference on Smart Grid Communications*, Nov 2015.

[22] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Transactions on Power Systems*, 2018.

[23] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sep. 2009, pp. 911–918.

[24] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying fdi attacks in power system state estimation," *IEEE Journal of Selected Topics in Signal Processing*, Aug 2018.

[25] M. Culler and K. R. Davis, "Toward a sensor trustworthiness measure for gridconnected iot-enabled smart cities," in *2018 IEEE Green Technologies Conference*, Apr 2018, pp. 168–171.

[26] G. A. Weaver, K. Davis, C. M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and D. M. Nicol, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications*, Nov 2016, pp. 140–146.