Analyzing the Effects of Cyberattacks on Distribution System State Estimation

Preprint

Govind Saraswat, Rui Yang, Yajing Liu, and Yingchen Zhang

National Renewable Energy Laboratory

To be presented at the 2021 IEEE Innovative Smart Grid Technologies North America (ISGT NA)
February 15–18, 2021

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-77941
December 2020

Analyzing the Effects of Cyberattacks on Distribution System State Estimation

Preprint

Govind Saraswat, Rui Yang, Yajing Liu, and Yingchen Zhang

National Renewable Energy Laboratory

Suggested Citation
Saraswat, Govind, Rui Yang, Yajing Liu, and Yingchen Zhang. 2020. *Analyzing the Effects of Cyberattacks on Distribution System State Estimation: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5D00-77941. https://www.nrel.gov/docs/fy21osti/77941.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5D00-77941
December 2020

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency Solar Energy Technology Office under Grant DE-EE0008767. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Analyzing the effects of cyberattacks on distribution system state estimation

Govind Saraswat, Rui Yang, Yajing Liu, and Yingchen Zhang
National Renewable Energy Laboratory (NREL), Golden, CO, USA.

***Abstract*—Key components of power systems—such as energy management systems, automatic generation control, and state estimation—are under serious vulnerability from cyberattacks. Cyber threats in electric grids have increased significantly because of the increased interconnectivity of supervisory control and data acquisition systems and public network infrastructure. As the penetration level of distributed energy resources increases, it is imperative to employ system-monitoring techniques such as state estimation for the reliable operation of distribution systems. Recently, multiple methods have been developed that exploit the low rank property of distribution system state matrix and are robust to bad data, such as matrix completion. This paper analyzes the impact of various realistic cyberattack scenarios on matrix completion. Realistic cyberattack scenarios are converted into data corruption models that are used in an extensive simulation of a custom IEEE 123-bus system.**

***Index Terms*—cyberattacks, state estimation, distribution systems, electric grid, security**

I. Introduction

An electric grid comprises transmission and distribution networks that connect different sources of power generation to consumers across a large geographic area. It is a complex system that requires continuous monitoring to maintain reliable operation. It is difficult to obtain reliable and fast measurements of voltage from all nodes, so state estimation is generally used to monitor the system by analyzing available power measurements and the underlying system model; thus, state estimation is critical for reliable electric grid operation. State estimation enables energy management systems to perform crucial control and planning tasks such as optimizing power flows, and bad data detection [1]. In transmission networks, because ample measurements are available, the system is generally fully observable; which roughly means that is it has more observations than unknown variables. For such observable systems, the weighted least-squares (WLS) method is widely used for state estimation [2]. Distribution systems consist of large number of connection points and even with the widespread deployment of sensor units, the system is generally unobservable, so WLS is not effective [3]. Psuedo-measurements that consider past measurements are used with WLS for distribution system state estimation (DSSE), but they can result in significant errors in the estimated state [4]; thus, utilities rarely use state estimation for distribution systems [5], [6]. For distribution system state matrix (see Section II for the matrix structure), all but first few singular values are zero [7]. This leads to the assumption that distribution system state matrices are of low rank. Recently, multiple methods have been developed that exploit this low rank property of distribution system state matrix. These methods include matrix completion [7]–[11] and tensor completion [12], [13]. These methods usually succeed when they augment standard approaches with power flow constraints. Considering matrix completion, it was shown in [14] that it is very accurate with limited measurements as well as robust to bad data. Power flow constraints depend on an underlying impedance model, which is sometimes hard to come by because of aging infrastructure or unrecorded changes in topology. Tensor completion [13] that uses measurements from multiple instants to estimate the unobserved states can be effective when reliable impedance model is not available.

Similar to other systems in the modern grid, state estimation is susceptible to various cyber intrusions [15]. Grid operators rely on accurate information on the current status of the grid, which is provided by state estimation algorithms, to take appropriate control actions. Cyberattacks can cause unforeseen errors in the estimated state [16] that can jeopardize a control center's situational awareness of the grid. This can lead to suboptimal or even harmful control actions. Analyses and impacts of cyber intrusions on state estimation are limited to the WLS algorithm [17]–[19]. Understanding the effects of cyberattacks on new methods—such as matrix and tensor completion — is scarce; thus, there is a great need to first understand the impact of various cyberattacks on the latest state estimation algorithms and then develop mitigation strategies to counter those attacks.

Most cyberattack studies consider only false data injection (FDI) or random data corruption [20]. This manuscript considers actual physical cyberattack scenarios (based on the National Electric Sector Cybersecurity Organization Resource (NESCOR) report [21]) and relates them to data corruption models that are used to analyze cyber intrusions. We consider strategic as well as local attacks, which could cause significantly more damage than arbitrary random attacks. Analysis reveals that certain corruption models as well as certain locations are much more detrimental to state estimation when used by cyberattackers. This information can be used by utility companies to strengthen the security of critical locations as

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technology Office under Grant DE-EE0008767. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

well as critical measurements to fight cyberattacks.

A. The main contributions of this paper are:

1) This is the first study to analyze the impacts of realistic cyberattack scenarios on DSSE using matrix completion.
2) We present data corruption models that capture cyberattack scenarios that include (i) Measurement loss, (ii) Strategic false data injection, (iii) Neighborhood attack, and (iv) Replay attack.

The rest of this paper is organized as follows. Section II provides a brief background on matrix completion and gives details on the cyber scenarios as well as the data corruption models. Section III presents the results of a cyberattack simulation on a custom IEEE 123-bus system. Section IV concludes the paper and provides some future directions.

II. Approach

A. Matrix Completion

In our recent work, we propose a low-observability state estimation algorithm based on matrix completion, which is a tool for estimating missing values in low-rank matrices. This tool is used to estimate state for a given time step by forming a structured data matrix; whose one axis correspond to measurement types and other correspond to measurement locations. We showed that the matrix completion model augmented with noise-resilient power flow constraints is an effective technique for DSSE under low-observability conditions [7]. Two formulations of the state matrix were proposed in [7]: branch formulation and bus formulation. In this manuscript, we evaluate the effects of cyberattacks on the matrix completion method with bus formulation, which applies to general three-phase distribution systems. For the matrix built using bus formulation, each row represents a bus, and each column represents a quantity relevant to the bus. The quantities we consider for each bus include the real voltage, imaginary voltage, voltage magnitude, active power, and reactive power. The real voltage and imaginary voltage at non-slack buses are considered as variables; and the voltage magnitude, active power, and reactive power are considered as potentially known measurements. The matrix completion model was formulated as a semidefinite program (SDP) and solved using an SDP solver; see [7] for more details.

B. Cyber Scenarios

Here, we analyze the effects of cyberattacks on matrix completion-based state estimation. We consider a custom IEEE 123-bus network as a test system with simulations for 1 week with data sampled each minute. Each phase at a bus has three potential measurements available: voltage magnitude (V), active power (P) and reactive power (Q). Four broad categories of cyberattacks as detailed in the NESCOR report [21] are considered:

1) *Measurement loss*: The accuracy of matrix completion—and similar algorithms that exploit the structure of the measurement data—relies on the amount of data available. For DSSE, because the available data are already scarce, any further loss of data can have a detrimental effect on the algorithm's estimation accuracy. Related scenarios from the NESCOR report include AMI.19, AMI.28, WAMPAC.6, etc.
2) *FDI*: We analyze the effects of randomly corrupting a certain percentage of the measurement data. Along with randomly adding a small corruption value to the measurement, we consider the case when corruption is only in one direction (the corrupted measurements are either all increased or all decreased). Related scenarios from the NESCOR report include AMI.4, AMI.30, WAMPAC.2, WAMPAC.4, DGM.6, etc.
3) *Neighborhood attack*: Under this attack model, all the measurements from a physical neighborhood get compromised. Analysis of this attack leads to the identification of critical locations in the network that are more susceptible to the disruption of the state estimation under a cyberattack. Related scenarios from the NESCOR report include WAMPAC.1, DGM.16, etc.
4) *Replay attack*: Under a replay attack, measurements of previous time steps are passed on as current measurements. We consider time steps with maximum variability in voltage and power to simulate the maximum corruption. Related scenarios from the NESCOR report include AMI.27, WAMPAC.3, etc.

These scenarios are used to create detailed data corruption models. Two aspects of corrupting measurements are 'which measurements get corrupted' and 'how much do they get corrupted'; we call them 'which' and 'how'. For the FDI attack, these aspects are given as:

a) *Which:* Corrupt a certain percentage of all available or either V, P, or Q measurements. Here, the effect of the corruption in different measurement channels will be quantified.
b) *How:* Let the true value of a measurement i be defined as x_i and the corrupted value as $\hat{x}_i$. The extent of the corruption is defined as r which is chosen from a uniform probability distribution between 0 and 1. Then for all available measurements i, the corruption is chosen to be either multiplicative:

$$\hat{x}_i = (1 \pm 0.1r)x_i \tag{1}$$

or additive:

$$\hat{x}_i = x_i \pm 0.1r\bar{x} \tag{2}$$

where $\bar{x}$ is the mean of all the similar measurements—that is, if x_i is a voltage measurement, then $\bar{x}$ is the mean of all available voltage measurements, and so on. When the corruption is only in one direction, two cases are considered. First is an over attack, where $\hat{x}_i = (1 + 0.1r)x_i$ (multiplicative) or $\hat{x}_i = x_i + 0.1r\bar{x}$ (additive). Second is an under attack, where $\hat{x}_i = (1 - 0.1r)x_i$ (multiplicative) or $\hat{x}_i = x_i - 0.1r\bar{x}$ (additive). With the model of equations (1) or (2) and choosing r between 0 and 1 implies a corruption of up to $\pm 10\%$.

Over/under attacks provide strategic ways to spoof sensor data. For the measurement loss scenario, a certain percentage of available data is randomly removed from the available measurement data. Determining *which* measurements to remove is

similar to the FDI scenario—all available or either V, P, or Q measurements are assumed to be lost. For the neighborhood attack, all available measurements corresponding to a single neighborhood are assumed to be corrupt using equations (1) or (2). Neighborhoods are chosen based on different switches in the IEEE 123-bus system and are shown in Fig. 1. Here, Neighborhood 1 is the smallest in terms of total number of node phases, and 5 is the biggest, in that order. For the replay attack, measured values from one of the previous time steps are used as the corruption. Determining *which* measurements to corrupt is similar to the FDI and measurement loss scenarios. The next section presents representative results of simulations based on these models.

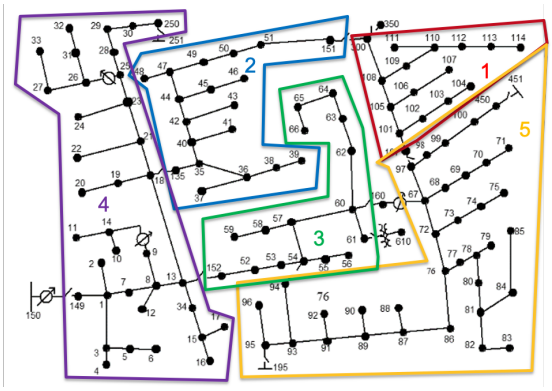

Fig. 1: Chosen neighborhoods. Neighborhood 1 (in red) is the smallest in terms of total number of node phases and 5 (in yellow) is the largest (in that order).

III. Results

Realistic cyberattack scenarios described in Section II are simulated in detail here. We plot mean average percentage error (MAPE) of the voltage magnitude and mean angle error (MAE) of the voltage angle for each scenario. Matrix completion based SE usually have the acceptable accuracy of MAPE $\leq$ 1% and MAE $\leq 1^\circ$ [14]. Measurement data for this study are taken from a week long simulation of a custom IEEE 123-bus model with high photovoltaic (PV) penetration. Number of node phases in the model is 260 (excluding the slack bus), with 3 measurements on each node; voltage magnitude, active and reactive power. Thus, the total number of measurements at each time instant is 780. Matrix completion is used for state estimation. For all simulations, the total available measurements for matrix completion are fixed to be 20% of all possible measurements in the system ($= 0.2 * 780 = 156$), which are randomly selected for each scenario.

We first present the results of Scenario 1, measurement loss. Here, out of 20% available data, from 10% to 95% of available data is removed. For each percentage removal, 10 different simulation runs are performed while randomly removing that percentage of data in each run. MAPE for the case when the voltage measurements are lost is plotted in Fig. 2(a). Similarly for the cases when the P or Q measurements are lost, MAPEs are plotted in Fig. 2(b) and Fig. 2(c), respectively. As the percentage of measurement loss increases, initially it has a negligible effect on state estimation, which points to good robustness of the matrix completion to the measurement loss. As the measurement loss increases up to 80 and higher, matrix completion suffers (with average MAPE$>$ 5 and MAE$>$ 2) when the voltage measurements are lost. The loss of the P measurements does not have any effect on the state estimation, with average MAPE$\leq$ 1% and average MAE $\leq 1^\circ$. Angle error for the same two cases is plotted in Fig. 3(a) and Fig. 3(b) respectively. As in the case of MAPE, results clearly show that the effect of the P measurement loss has a negligible effect on voltage angle estimation, whereas the loss of the V measurement has a significant effect when the loss is 80% or more. The effects of loss of the Q measurements is similar to the P measurements and is omitted because of space constraints.

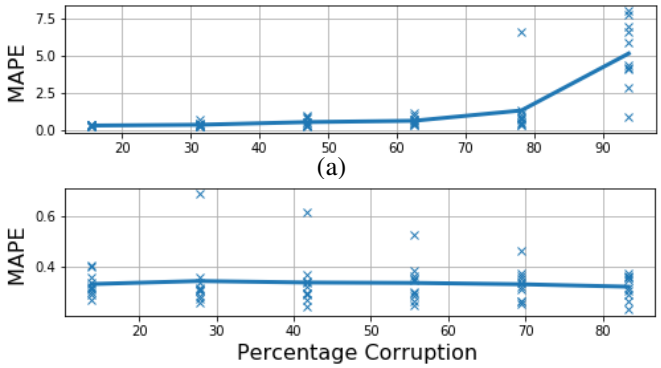

Fig. 2: MAPE of voltage magnitude estimation when (a) voltage and (b) P measurements are lost.

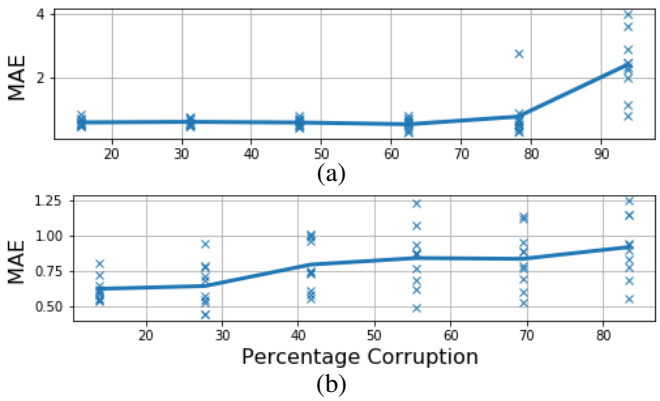

Fig. 3: MAE of voltage angle estimation when (a) voltage and (b) P measurements are lost.

Next, we present the results of Scenario 2, FDI. Here, out of 20% available data, from 10% to 95% of available data is randomly corrupted. As discussed earlier, for each percentage, 10 different runs are simulated with randomly corrupting data in each run for both multiplicative and additive corruption. MAPE for the case when the voltage and P measurements are corrupted is plotted in Fig. 4(a) and Fig. 4(b) respectively. As in Scenario 1, corruption in the V measurements has a significant effect on MAPE (with average MAPE$>$ 2 and MAE$>$ 1), whereas corruption in the P measurements has a negligible effect. The effects of corruption on the Q

measurements is similar to the P measurements and is omitted because of space constraints. Note that the matrix completion formulation used in this paper employs the linearized power flow constraints [22]. We chose the appropriate tolerance that the optimization problem has to satisfy, thus, voltage estimates are less sensitive to the small changes in power injections as their effect may be within the tolerance, whereas voltage magnitude measurements directly impact how the voltages will be estimated and thus leading to a larger impact. Angle errors for the same two cases are plotted in Fig. 5(a) and Fig. 5(b) respectively, and the results are similar.

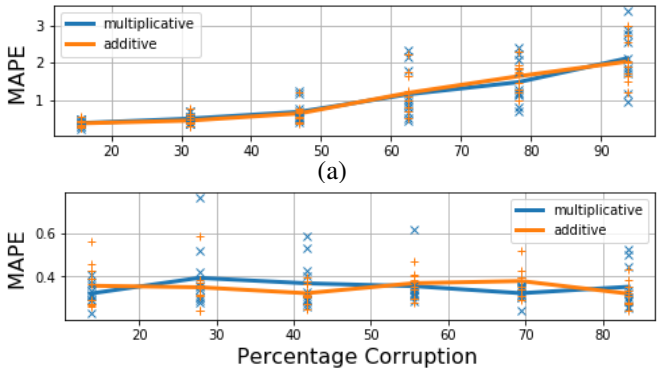

Fig. 4: MAPE of voltage magnitude estimation when (a) voltage and (b) P measurements are randomly corrupted. Results from both multiplicative and additive corruptions are shown.

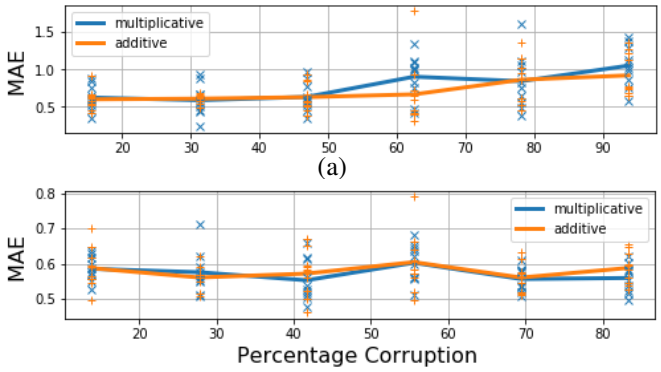

Fig. 5: MAE of Voltage angle estimation when (a) voltage and (b) P measurements are randomly corrupted. Results from both multiplicative and additive corruptions are shown.

For the over/under attacks, MAPE and MAE when the voltage measurements are corrupted are plotted in Fig. 6(a) and Fig. 6(b), respectively. Here, only the case of multiplicative corruption is presented; additive corruption showed similar results, but it is omitted. Compared to the random corruption results shown in Fig. 4 and Fig. 5, for the same percentage of corruption in the voltage measurements, the error in estimation is almost twice when the corruption is in one direction (average MAPE> 4). The effects of corruption on the P and Q measurements are negligible (similar to the random corruption), and they are omitted because of space constraints. Even when only 30% of the measurements are corrupted in this attack, MAPE is more than double (≈ 1.0) the baseline (≈ 0.5). Clearly, when corruption is strategic, as in the over/under attacks, the effect on state estimation is much more detrimental than random corruption.

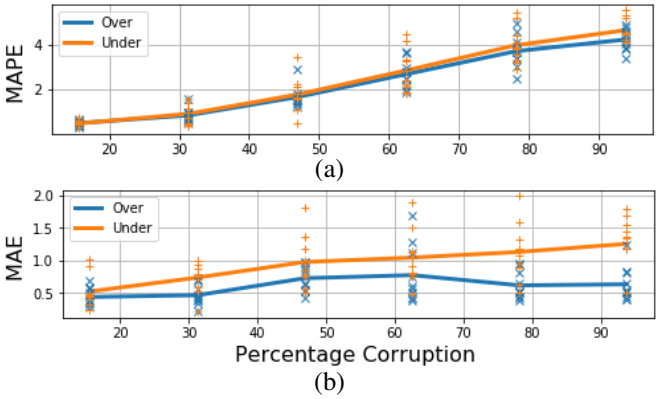

Fig. 6: (a) MAPE of voltage magnitude and (b) MAE of voltage angle estimation when the voltage measurements are corrupted in one direction with multiplicative corruption. Results from both over and under attacks are shown.

Next, we present the results with neighborhood attacks in Fig. 7. As mentioned in the previous section, neighborhoods are selected based on switches, and the size of a neighborhood is determined in terms of the available measurements. Here, Neighborhood 1 is the smallest, and 5 is the biggest (in that order). For each subplot, all measurements corresponding to one of the neighborhoods are corrupted, and MAPE/MAE corresponding to the measurements from each neighborhood are plotted. For example, the orange plot corresponds to when the second neighborhood is attacked; each point on the plot is the MAPE/MAE of the measurements from the specific neighborhood. As evident from the plots, even though Neighborhood 2 is second smallest in size, it has the second

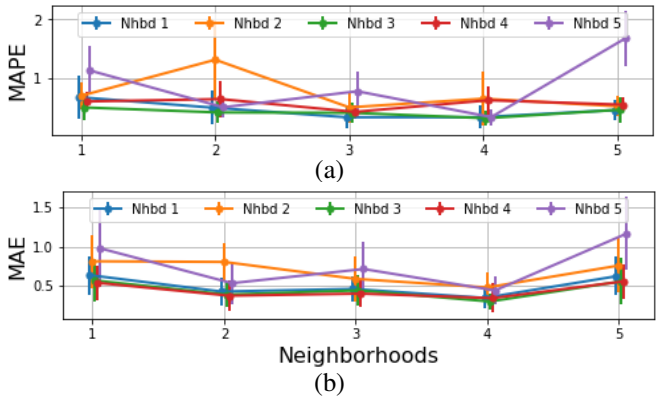

Fig. 7: (a) MAPE of voltage magnitude and (b) MAE of voltage angle estimation when a single neighborhood is attacked. The x-axis shows the effect on the specific neighborhood. Each subplot shows the effects of attacks on five different neighborhoods. Points are the mean, and error bars are the standard deviation.

highest impact on the state estimation accuracy. Clearly, it is the critical neighborhood, and it should be given extra preference in security.

Next, we present the replay attack when measurements from previous time steps are camouflaged as current measurements. For this result, we used measurements from two time steps that are the most different, and we plot the voltage magnitude and angle estimation accuracy in Fig. 8(a) and Fig. 8(b), respectively. For this simulation, even with a high PV penetration, variations in voltage and power are not enough to have any detrimental effects on DSSE using matrix completion. This might not be the case for other distribution systems; thus, this attack scenario needs to be explored further.

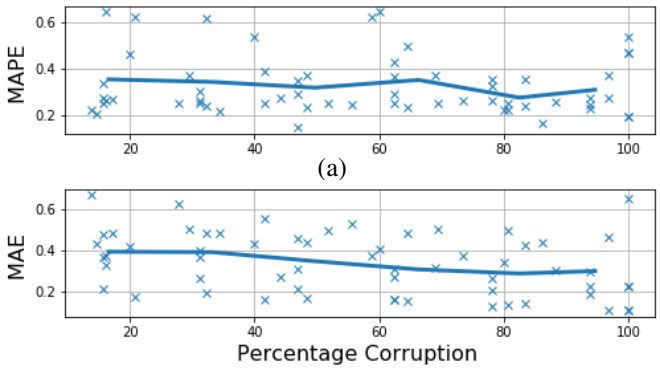

Fig. 8: (a) MAPE of voltage magnitude and (b) MAE of voltage angle estimation during a replay attack.

IV. Conclusions and Future Work

Simulations reveal that corruption in voltage measurements has a much greater impact on state estimation than corruption in active or reactive power measurements. Further, strategic attacks, such as over/under attacks, cause higher errors in voltage estimation than random attacks with similar corruptions. Simulations on the neighborhood attack reveal a critical neighborhood that when attacked has a much greater impact on state estimation accuracy. In normal operations, voltage magnitude does not vary much between measurements, and a replay attack is not very effective to cause any significant errors in state estimation using matrix completion. Thus, the state estimation algorithm using matrix completion is more susceptible to cyberattacks when:

1) Corruption happens in the voltage measurements
2) Values are changed toward one direction (over/under attack)
3) Critical neighborhoods are attacked.

In future work, we will consider the effects of the cyber scenarios presented here on utility-scale distribution systems. We will analyze the effects of these cyberattack scenarios on other DSSE algorithms, such as Tensor completion and 1D/2D compressive sensing [23]. We will also develop intrusion detection strategies for these algorithms to make them robust to such cyberattacks. Initial idea is to take traditional residue-based mitigation strategies used for WLS algorithms and adapt them for matrix and tensor completion based DSSE.

References

[1] F. F. Wu, "Power system state estimation: a survey," *International Journal of Electrical Power & Energy Systems*, vol. 12, no. 2, pp. 80–87, 1990.

[2] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[3] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, "A survey on state estimation techniques and challenges in smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2312–2322, 2018.

[4] K. A. Clements, "The impact of pseudo-measurements on state estimator accuracy," in *2011 IEEE Power and Energy Society General Meeting*. IEEE, 2011, pp. 1–4.

[5] N. Katic, L. Fei, G. Svenda, and Z. Yongji, "Field testing of distribution state estimator," 2013.

[6] D. Atanackovic and V. Dabic, "Deployment of real-time state estimator and load flow in bc hydro dms-challenges and opportunities," in *2013 IEEE Power & Energy Society General Meeting*. IEEE, 2013, pp. 1–5.

[7] P. L. Donti, Y. Liu, A. J. Schmitt, A. Bernstein, R. Yang, and Y. Zhang, "Matrix completion for low-observability voltage estimation," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2520–2530, 2019.

[8] E. J. Candès and B. Recht, "Exact matrix completion via convex optimization," *Foundations of Computational mathematics*, vol. 9, no. 6, p. 717, 2009.

[9] Y. Zhang, A. Bernstein, A. Schmitt, and R. Yang, "State estimation in low-observable distribution systems using matrix completion," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep. NREL/CP-5D00-73540, 2019.

[10] A. Sagan, Y. Liu, and A. Bernstein, "Decentralized low-rank state estimation for power distribution systems," *arXiv:1910.04831*, 2019.

[11] Y. Liu, A. Sagan, A. Bernstein, R. Yang, X. Zhou, and Y. Zhang, "Matrix completion using alternating minimization for distribution system state estimation," in *2020 IEEE SmartGridComm*. IEEE, 2020, pp. 1–6.

[12] R. Madbhavi, H. S. Karimi, B. Natarajan, and B. Srinivasan, "Tensor completion based state estimation in distribution systems," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2020, pp. 1–5.

[13] A. Zamzam, Y. Liu, and A. Bernstein, "Model-free state estimation using low-rank canonical polyadic decomposition," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 605–610, 2021.

[14] B. Liu, H. Wu, Y. Zhang, R. Yang, and A. Bernstein, "Robust matrix completion state estimation in distribution systems," in *2019 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2019, pp. 1–5.

[15] J. Wang, L. C. Hui, S.-M. Yiu, E. K. Wang, and J. Fang, "A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities," *Pervasive and Mobile Computing*, vol. 39, pp. 52–64, 2017.

[16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[17] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *2010 first IEEE international conference on smart grid communications*. IEEE, 2010, pp. 220–225.

[18] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *49th IEEE conference on decision and control (CDC)*. IEEE, 2010, pp. 5991–5998.

[19] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[20] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—attacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2016.

[21] A. Lee, "Electric sector failure scenarios and impact analyses," *National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group*, vol. 1, 2013.

[22] A. Bernstein, C. Wang, E. Dall'Anese, J.-Y. Le Boudec, and C. Zhao, "Load flow in multiphase distribution networks: Existence, uniqueness, non-singularity and linear models," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 5832–5843, 2018.

[23] H. S. Karimi and B. Natarajan, "Compressive sensing based state estimation for three phase unbalanced distribution grid," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.