A Data-Driven Dynamic State Estimation for Smart Grids under DoS Attack using State Correlations

Md Abul Hasnat and Mahshid Rahnamay-Naeini
Electrical Engineering Department, University of South Florida, Tampa, Florida, USA
hasnat@mail.usf.edu, mahshidr@usf.edu

***Abstract*—The denial-of-service (DoS) attack is a very common type of cyber attack that can affect critical cyber-physical systems, such as smart grids, by hampering the monitoring and control of the system, for example, creating unavailability of data from the attacked zone. While developing countermeasures can help reduce such risks, it is essential to develop techniques to recover from such scenarios if they occur by estimating the state of the system. Considering the continuous data-stream from the PMUs as time series, this work exploits the bus-to-bus cross-correlations to estimate the state of the system's components under attack using the PMU data of the rest of the buses. By applying this technique, the state of the power system can be estimated under various DoS attack sizes with great accuracy. The estimation accuracy in terms of the mean squared error (MSE) has been used to identify the relative vulnerability of the PMUs of the grid and the most vulnerable time for the DoS attack.**

***Index Terms*—Cyber attack, smart grid security, data-driven dynamic state estimation, state correlations, time series.**

I. Introduction

Smart grids are large and complex infrastructures consisting of tightly coupled communication and power systems. The communication system is vital for the flow of information throughout the system, which enables the control mechanisms to monitor and make decisions based on the states of the system. Attacks on the communication system can hinder the control system from taking appropriate decisions and actions, consequently affecting the reliability and efficiency of the system. Communication systems of the power grids are prone to cyber-attacks [1]. One example of the key challenges that can arise due to the cyber attacks is the unavailability of the critical power system's state data (i.e., lack of observability and situational awareness for portions of the power system), for instance, due to denial of service (DoS) attacks on parts of the communication system. In addition to cyber-security measures that can help prevent such scenarios, it is important to develop new complementary mechanisms that can help with dealing with such challenges (i.e., improving the observability of the state of the power system) if such cases occur. Therefore, it is crucial to detect cyber attacks in power grids and estimate the state of the system as accurate as possible to recover from the attacks. Estimation of the smart grid states under cyber attack may assist the control center to work properly even when some part of the system is under cyber attack.

State estimation of the power system has been in use for many years. Particularly, after the renowned blackout of 1965 in the United States, state estimation received significant attention. Since then numerous articles have been published on power system state estimations, it's mathematical modeling, algorithms, numerical aspects, observability, bad data detection, and the implementation issues. However, most of the conventional state estimations rely heavily on power system models and do not exploit the abundant state data available in current power grids. The availability of large volume of data collected and available in today's power systems (due to the large deployment of monitoring sensors such as phasor measurement units-PMUs) has motivated emerging methods for state estimation based on data-driven approaches.

State estimations for power systems can be classified into static state estimation (SSE) and dynamic or forecasting-aided state estimations (DSE or FASE) [2]. The traditional state estimations in power systems are mainly static, which implies that for the estimation of the state of the system at the time instant t, only measurements at the time instant t are used [3]. The SSE was popular in the literature for the past four decades because there were only non-synchronized, low sampling rate (typically one measurement in a few minutes) measurement data available at this period. Although SSE has lower computational complexity, it is not very suitable for real-time monitoring of power grids as the estimation updates in every few minutes [2].

The motivation for evaluating the states of a power system in real-time comes from the insufficiency of the SSE methods to assist the control mechanisms in real-time decision making. The SSE Methods are based on the steady-state assumption of the power system, however, steady-state analysis will not provide an accurate estimate of power system states and operations due to dynamics of the system and random variations in load and generation. Specially in today's grids, distributed energy resources (DERs) can introduce a huge uncertainty in the generation side and thereby causing abrupt changes in the bus voltage phasor [4]. The uncertainty and complexity in the load side have also been increased in recent time due to the use of smart and IOT devices, electrical vehicles, and other modern electrical devices [5]. For the proper operation and control of such stochastic and fast-changing power systems, it is necessary to track the states of the system in real-time. DSE has brought effective changes in the case of oscillation monitoring for system stability and hierarchical decentralized control and enhanced dependability and reliability of the protection systems [5]. Moreover, the increasing threat of different types of cyber-physical attacks on the modern power system demands a real-time assessment of the security issues, which can be implemented with the help of DSE.

In this paper, the dynamic states of components under DoS attacks are estimated using a data-driven approach based on the correlations among the state of attacked components and the rest of the components in the system just before the DoS attack. However, this work is not the same as the power system state estimation in a traditional sense rather it can be called 'state estimation' in the sense that we are trying to estimate the states (bus voltage magnitudes and angles) of the power system during DoS attack. Although we have not used any dynamic model of power system explicitly in this work, our technique estimates the states in real-time and can capture any dynamic characteristics of the power system that DSE can capture. In this paper, it has been shown that, by exploiting the correlations among the PMU time-series, it is possible to estimate the time-series data for PMUs under DoS attack even when the attack size is considerably large. The most vulnerable location of the power system and the most vulnerable time in the day for DoS attack have been identified in terms of the mean-squared error (MSE).

II. Literature Review

In this section, we briefly review the data-driven state estimation technique for power systems and discuss them in terms of the accuracy, computational efficiency, and robustness, as well as their variants and modifications to withstand the challenges of the modern smart power systems. We will also discuss some of the recent efforts in the power system's state estimation under cyber attacks with a focus on attacks that can lead to unobservability in the system.

The phrase *state estimation* entered into the power system literature from the control system theory and first introduced by Schweppe [3], [6], [7]. Due to the less complex nature of the power grids back then, the *static state estimation* (SSE) was considered to be sufficient for monitoring and maintenance of the power system. The *dynamic state estimation* (DSE) in the power systems was introduced by Debs [8] in 1970. Since then one of the most prevalent methods for the dynamic state estimation is the Kalman filtering techniques [9], [10], [11] with linear models for the systems and Gaussian assumption for the noise. Filho et al. [12], [13] presented the development and variations of different dynamic and forecasting-aided state estimation techniques along with the implementation issues in power systems. Moreover, the widespread use of PMUs in smart grids added new dimensions in dynamic state estimation. Several authors incorporate the PMU data into state estimation framework to achieve a fast, more accurate and, high-resolution estimate of the states [14], [15], [16]. Recently, the IEEE Task Force on Power System Dynamic State and Parameter Estimation in [5] described the state-of-the-art of the dynamic state estimation and also discussed the future scopes.

Recently, various signal processing and machine learning based approaches are also considered for dynamic state estimations for power systems. Chackhchoukh et al. [17] used the Auto-regressive (AR) model to analyze the time series associated with a single PMU and Vector Auto-regressive (VAR) model to analyze the correlations and inter-dependency of the set of PMUs in the grid. Hassanzadeh et al. [4] used time auto-correlations in the AR model and bus-to-bus correlations in VAR model to estimate the states in different cases: grids with different electrical connectivity, centrality, and node significance patterns, stochastic and intermittent generation patterns and under the loss of observability. This paper also discusses the suitability of the models (AR and VAR) in different situations. Kumari and Bhattacharyya [18] proposed a completely data-driven DSE method using Gaussian Process (GP) for the function approximation. Zhang et al. [19] proposed a real-time state estimation technique using deep unrolled neural network.

Moreover, a considerable amount of work focused on different types of cyber attacks in power systems: their models, effects on the smart grid, detection techniques for different kind of attacks and their countermeasures. For instance, Beasley et al. [20] discussed the popular cyber attacks and their effects on the state estimations along with their countermeasures. Liu et al. [21] provided a details description of the DoS attack. Kurt et al. [22] described two types of DoS attacks: one in the form of the lack of availability of meter measurements and the other in the form of reduction of the signal-to-noise-ratio (SNR) of the PMU signal by jamming the channel with another signal. Although the estimation of the power system dynamic states under the cyber attacks is comparatively a newer topic to address, in the last few years, it has been the focus of many researchers. For instance, Wang et al. [23] proposed a data-driven approach to detect and classify cyber attacks on PMU measurements using density-based spatial clustering and also proposes a data recovery technique for the compromised PMU channels. Mosbah and El-Hawary [24] illustrates a neural network- based method for state estimation under communication failure in which the authors optimized the neural network parameters by stochastic fractal search method. Gu and Jirutitijaroen [25] showed a technique for dynamic state estimation in which the load of the attacked region is forecast at the first step by the time-forward Krigging method using the load profiles outside the attacked region and then the states inside the attack region are estimated using the traditional power flow model. Moreover, a few works address physical failures and attacks along with cyber attacks. For instance, Soltan et al. [26] developed a linear algebra and graph theory-based approach to detect the line failure and to estimate the voltage angle of the buses inside the attack area from the observations outside the attack area. Hossain and Rahnamay-Naeini [27] addressed a similar problem by a data-driven approach with linear Minimum Mean Squared Error (MMSE) estimation and used the estimated state to detect the line failures.

The work presented in the current paper is also a data-driven method for DSE in power systems under the DoS attacks based on the correlation between states similar to [4] and [17].

Instead of directly using the states, in our method, we have used the state correlations to build a relation among the time derivatives of the observable and unobservable states. Similar to [22], we assume that DoS attacks will cause unobservability of the states in the power system.

III. System and attack models

A. Power System Model

In this paper, the power transmission system has been modeled as the sets of buses, transmission lines (branches) and their interconnections. Let, $\mathcal{B}$ be the set of all the buses in a N bus system; therefore $|\mathcal{B}| = N$, where, $|.|$ denotes the cardinality of the set. We assume that there are PMUs in all the buses. Therefore, the measurements of all the bus voltage phasors are collected by the PMUs in a suitable sampling rate and sent to the control center. This assumption may not be realistic in today's smart grids as the PMUs are generally optimally placed [28] to minimize the cost and maximize the observability. Designing and developing data-driven methods similar to the one discussed in this paper for models with optimally placed PMUs is a prospective future work.

B. DoS Attack Model

In this paper, we assume DoS attacks on the communication system of the power grid result in unavailability of the data (time series of measured parameters) from a subset of the PMUs associated with the buses, $\mathcal{B}$. Let, $\mathcal{A} \subset \mathcal{B}$ be the set of buses, which their associated PMUs are under the DoS attack and $|\mathcal{A}| = M$. Let, $x_k(t)$ denotes any electrical attribute (e.g., voltage or phase angels) from a PMU at time t, where, $k \in \mathcal{B}$. If a DoS attack occurs at time t_a, then, we model the attack by assuming unobservability of $x_k(t)$ for $t > t_a$.

IV. Method

The goal of the estimation method in this paper is to estimate the state of the components, which their PMUs are under attack, from the state of the rest of the components collected by the rest of the PMUs. Specifically, we assume that the time series of the states of electrical attributes $x_i(t)$, where, $i \in \mathcal{B} \backslash \mathcal{A}$ is available except for buses in the attack set, $\mathcal{A}$. In the estimation method, we denote the time series of unknown (unobservable) buses for $t > t_a$ due to DoS attack by $y_j(t)$, where, $j \in \mathcal{A}$.

We define the relation between the known and unknown states as follows:

$$\dot{y_j}(t) = \sum_{i=1}^{N-M} w_{ji}\dot{x_i}(t). \tag{1}$$

For M DoS attacks on M buses, equation (1) will result in a system of equations as follows:

$$\underline{\dot{y}}(t) = W\underline{\dot{x}}(t), \tag{2}$$

where $\underline{\dot{y}}(t)$ and $\underline{\dot{x}}(t)$ are vectors with elements representing the time derivative of the time series corresponding to unknown and known buses, respectively.

Here, the time derivative of a state variable under DoS attack has been estimated as the weighted sum of the time derivatives of the rest of the parameters. The weights come from the correlations between any state outside the attack zone and the attacked state. The rationale behind estimating the time derivative of the state first instead of directly estimating the state is: we observed that although the states vary significantly in terms of the actual values, there exist very strong correlations among several states in their changing pattern with time.

The matrix W, contains the bus-to-bus correlation of the electrical attributes among the buses under DoS attack and the buses that are not under the attack. Any element of W is represented as:

$$w_{ji} = e^{ar_{ji}}, \tag{3}$$

where r_{ji} is the correlation coefficient between $y_j(t)$ and $x_i(t)$ for the last t_c moments before the DoS attack:

$$r_{ji} = \int_{t_a - t_c}^{t_a} x_i(t)y_j(t)dt. \tag{4}$$

Since we have considered the DoS attack to be on the communication layer of the smart grid, therefore, we are assuming no physical attack or topology changes. Moreover, we consider the correlation among the PMUs just before the DoS attack happens. As a result, the correlation among the PMUs before the attack and after the attack can be considered unchanged. It is true that if the DoS attack continues for a long period, the estimation accuracy decreases because the correlation among the PMUs changes within this period due to the change in loads. Besides, if any physical attack is masked by the DoS attack, our technique may not perform well because the correlation among the PMUs will be changed due to the physical attack.

The reason behind taking the exponential of the correlation coefficients is to emphasize the highly correlated buses and to de-emphasize the barely correlated buses. However, the set of the weights also depends on the scalar parameter, a. In this paper, the value of a is empirically selected and the effect of choosing different values for parameter a has been illustrated in the simulation and result section. However, the determination of the value of a from the topology of the grid and system properties directly or indirectly can be prospective future work.

For the discrete-time realization of the continuous-time time series, the derivative of a time series at t, can be considered as the backward difference system: $\dot{f}(t) = f_t - f_{t-1}$, where, f_t is the sampled value of the time series f at time t, and f_{t-1} is the previous sampled value. According to this notion, the equation (2) can be written in the following form:

$$\underline{y}_t - \underline{y}_{t-1} = W(\underline{x}_t - \underline{x}_{t-1}). \tag{5}$$

The sampled value of the attacked states at the moment of the attack (t_a), denoted by $\underline{y}_{t_a}$ can be considered as the initial value and assumed to be known. During the attack interval the values are updated by:

$$\underline{y}_t = \underline{y}_{t-1} + W(\underline{x}_t - \underline{x}_{t-1}),\ t > t_a. \tag{6}$$

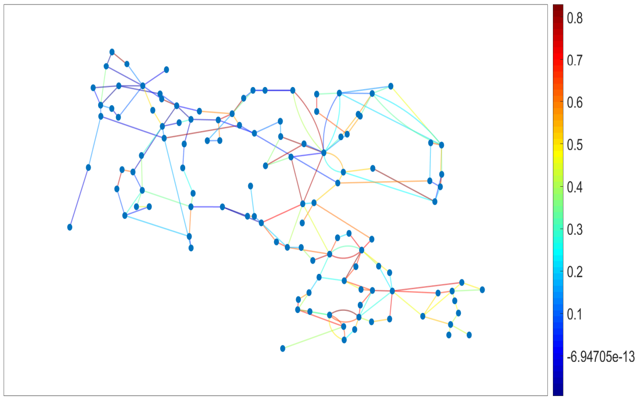


Fig. 1: Relative correlations among the PMUs of the physically connected buses in terms of voltage angles for IEEE 118 bus case.

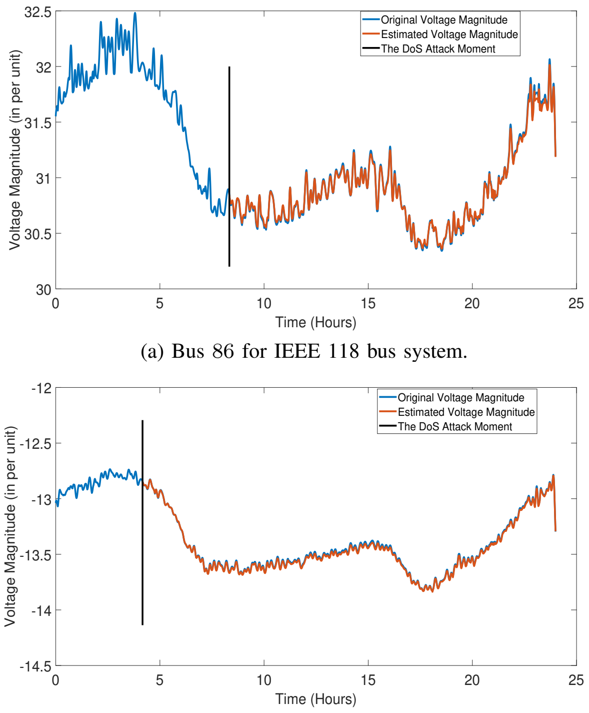
V. Simulations and Results

In this paper, the simulations have been run on the IEEE 14 bus system [29] and IEEE 118 bus system [30]. The load patterns are collected from the New York Independent System Operator (NYISO) [31]. The NYISO consists of eleven regions. The load profiles are normalized and added with the default constant loads of the eleven load buses of the IEEE 14 bus case to generate the load profile time series. For the IEEE 118 bus case, we do not have enough load data since there are 91 load buses in this system. Therefore, the available data for the different regions are combined to synthesize load profiles for those 91 load buses similar to [25]. By combining three different regions to synthesize one new load profile by taking the average, it is possible to create $\binom{11}{3} = 165$ such combinations. Out of the 165 profiles, the first 91 are considered as the load profile of the 91 load buses of IEEE 118 bus system. In the NYISO data, the load is measured in every five minutes. However, these data are linearly interpolated to generate time series of $0.033Hz$ sampling rate. MATPOWER 6.0 [32] has been used to simulate the power flow for both of the IEEE 14 bus and 118 bus case. The details of the simulation have been discussed in the following subsections:

A. *Correlation among PMU time series*

As discussed in Section IV, the time-series data from the PMUs under DoS attack are estimated from the correlations among the PMU data, which arises from the physical dynamics of the power system. Fig. 1 illustrates the correlations among the voltage angle PMU data for the IEEE 118 bus case. From the figure, it is clear that some of the PMU data have very strong correlations among them. In this figure, correlations have been shown only for the buses, which have physical connections among themselves. However, PMUs installed in the buses having no connections may still have correlations due to the physics of the electricity and power flows.

B. *Estimation of PMU time series under single and multiple DoS Attack*



(a) Bus 86 for IEEE 118 bus system.

(b) Bus 7 for IEEE 14 bus system.

Fig. 2: Estimation of bus voltage angle under single DoS attack.

Fig. 2a illustrates the estimation of the voltage angle time series of bus 86 of IEEE 118 bus system when only the PMU associated with that bus is under DoS attack. The red curve represents the estimated time series based on the method presented in Section IV and the blue line represents the ground truth, while the DoS attack occurred at t_a, is represented by the black vertical line. The estimated time series seems to track the ground truth quite accurately. The mean squared error, in this case, is 8.8631×10^{-4} degree. The value of a is empirically selected as 300. However, the accuracy of the estimation depends on the proper choice of a, which has been discussed later in this section. Fig. 2b shows similar results for bus 7 for IEEE 14 bus system. The estimation of voltage magnitude time series has been shown in Fig. 3.

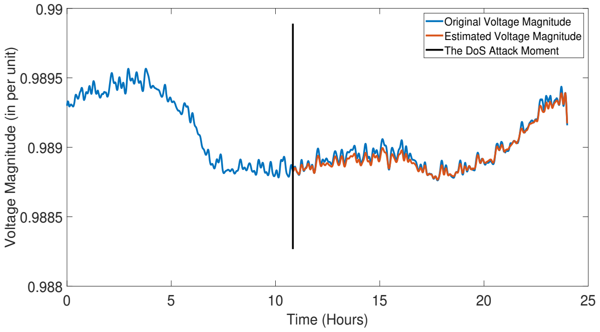


Fig. 3: Estimation of bus voltage magnitude under DoS attack at Bus 86 for IEEE 118 bus system.

The accuracy of the estimation of a PMU data deteriorates when a larger number of nearby PMUs go under DoS attack.

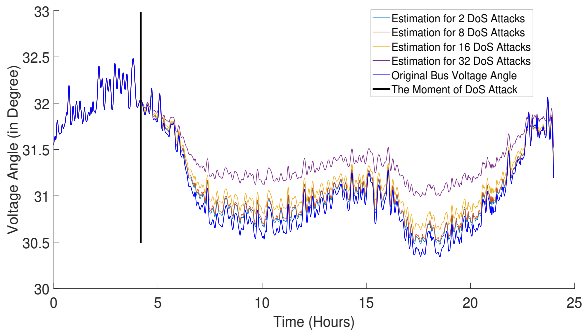


Fig. 4: Estimation of bus voltage angle under DoS attack at Bus 86 for IEEE 118 bus system for multiple attacks.

Fig. 4 illustrates the estimation of voltage angle at the PMU associated with bus number 86, respectively, for the failure of 2, 8, 16 and 32 number of PMUs including the PMU associated with bus 86. It is clear that although the accuracy of the estimation decreases with the increase in the number of DoS attacks, this method can estimate the PMU data even for a large number of DoS attacks. Fig. 5 illustrates the relation between the Mean squared error and the number of PMUs under the DoS attack for three types of distribution of attacks: uniform, clustered and inhibition.

C. Most vulnerable Combination of Attack

The most vulnerable PMU for the initial DoS attack from the attackers' point of view can be identified on the basis of the largest mean squared error (MSE) of estimation of the voltage angle under the single DoS attack. The relative vulnerability of the PMUs of IEEE 118 bus system has been represented in Fig. 6 by the node colors. For example, from the attackers perspective, it is possible to create more unobservability in the power system by launching a DoS attack on a red node (e.g. node 82) in Fig. 6.

D. Parameter a values

The choice of the parameter a has a significant impact on the accuracy of the estimator. Fig. 7 illustrates the effect of parameter a on the estimation. In this paper, we have kept the value of the parameter a fixed for all buses. From Fig. 7 it can be inferred that a value between 200 and 500 can be a good choice. When the bus voltage to be estimated has strong correlations with only a few numbers of bus voltages, then larger values of a work better (the weights for the barely-correlated buses would be negligible compared to the weights for the strongly correlated buses). However, a small value of parameter a would work better, when that bus has significant correlations with many buses.

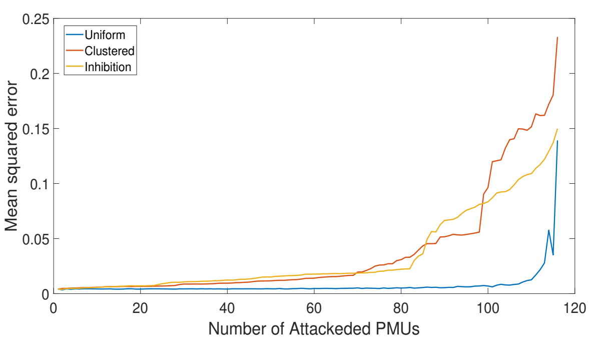


Fig. 5: Mean squared error vs. number of DoS Attacks (average over all possibilities).

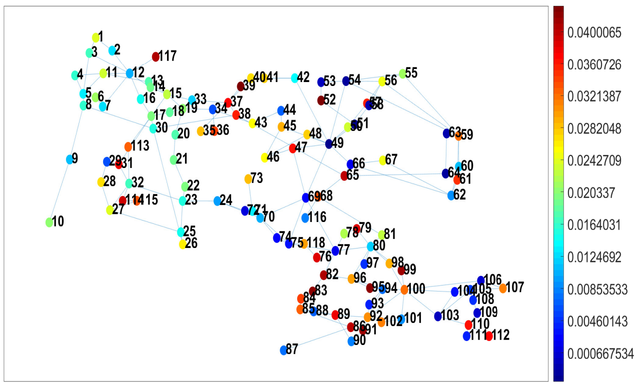


Fig. 6: Relative vulnerability of the PMU locations for initial DoS attack on the basis of MSE for IEEE 118 bus system.

E. Most vulnerable time for the DoS attack

The moment when the DoS attack initiates also impacts the estimation accuracy. This is because the correlations among the bus parameters vary in time. This variation comes from the variation in the load profile at the load buses throughout the day. Fig. 8 represents the MSE in the cases of DoS attacks at different times of the day. The two profiles are from two different days, however, show the same pattern. It can be inferred from the two figures that in terms of the MSE, the most vulnerable time for the initiation of the attack is during the end of the office hours when the load fluctuation is very high. From the attackers perspective, the highest amount of unobservability can be created by initiating DoS attack during this period.

VI. Conclusion

This paper describes a simple, easy-to-implement, and efficient algorithm to estimate the dynamic states of a power system's components inside the DoS attack zone from the dynamic states of components outside the attack zone by

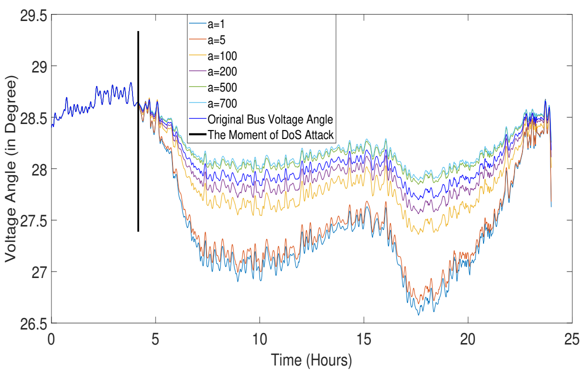


Fig. 7: The effect of the parameter a on the estimation of bus voltage angles in IEEE 118 bus system.

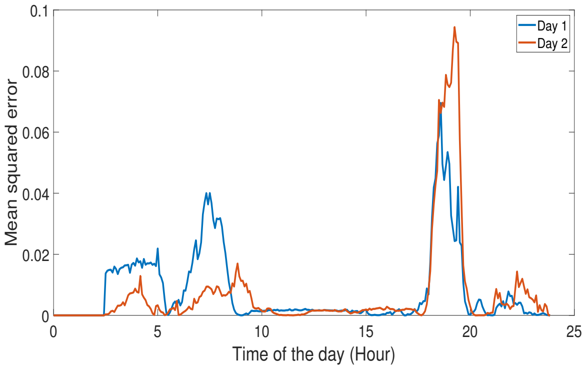


Fig. 8: The effect of the attack time on the estimation of bus voltage angles in IEEE 118 bus system.

using the correlations among the states. The accuracy of the estimation is compared by means of the mean squared error (MSE) between the estimated time series and the ground truth for the DoS duration. The MSEs for the different number of DoS attacks have been compared. The relative vulnerability of the locations of the PMUs and the relative vulnerability of the time of the day from the attackers' perspective have been analyzed on the basis of the calculated MSEs. Extending this technique for estimating the states of the grid under topology change and cyber-physical attack under optimum PMU placement can be considered as a prospective future work.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1761471. Also, this work is partially supported by the Defense Threat Reduction Agencys Basic Research Program under grant No. HDTRA1-13-1-0020.

References

[1] J. Wang, L. Huia, S. Yiu, E. Wang, and J. Fang, "A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities", Pervasive and Mobile Computing 39 (2017) 5264.

[2] Y. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid", IEEE Signal Processing Magazine, Volume: 29, Issue: 5, Sept. 2012.

[3] F. Schweppe and J. Wildes, "Power System Static State Estimation, Part I: Exact Model", IEEE Transactions on Power Apparatus and Systems, IEEE Transactions on Power Apparatus and Systems, Volume: PAS-89, Issue: 1, Jan. 1970.

[4] M. Hassanzadeh, C. Evrenosoglu, and L. Mili, "A short-term nodal voltage phasor forecasting method using temporal and spatial correlation", IEEE Transactions on Power Systems, Volume: 31 , Issue: 5, Sept. 2016.

[5] J. Zhao, A. Gomez-Exposito, L. Mili, A. Abur, V. Terzija, I. Kamwa, B. Pal, A. Singh, J. Qi, Z. Huang, A. Meliopoulos (IEEE Task Force on Power System Dynamic State and Parameter Estimation), "Power System Dynamic State Estimation: Motivations, Definitions, Methodologies and Future Work", IEEE TRANSACTIONS ON POWER SYSTEMS, Volume: , No: , 2019.

[6] A. Gomez-Exposito, A. Conejo, and C. Canizares, *"Electric Energy Systems, Analysis and Operation"*, CRC Press, 2004.

[7] A. Wood, B. Wollenberg, and G. Shebl, "*Power Generation, Operation, and Control*", 3rd Edition, Wiley, November 2013. (Chapter 9).

[8] A. Debs, and R. Larson, "A Dynamic Estimator for Tracking the State of a Power System", IEEE Transactions on Power Apparatus and Systems, Volume: PAS-89, Issue: 7, Sept. 1970.

[9] A. Silva, M. Filho, and J. Queiroz, "State forecasting in electric power systems", IEE Proceedings, Volume: 130, Issue: 5, September 1983, p.237244.

[10] H. Beides and G. Heydt. "Dynamic state estimation of power system harmonics using kalman filter methodology". IEEE Transactions on Power Delivery, Volume: 6, Issue: 4, Oct 1991.

[11] H. Karimipour and V. Dinavahi, "Extended Kalman Filter-Based Parallel Dynamic State Estimation", IEEE Transactions on Smart Grid, Volume: 6, Issue: 3, May 2015.

[12] M. Filho and J. Souza, "Forecasting-Aided State Estimation Part I: Panorama", IEEE Transactions on Power Systems, Volume: 24, Issue: 4, Nov. 2009.

[13] M. Filho, J. Souza, and R. Freund, "Forecasting-Aided State Estimation-Part II:Implementation", IEEE Transactions on Power Systems, Volume: 24, Issue: 4, Nov. 2009.

[14] G. Korres and N. Manousakis, "State estimation and bad data processing for systems including PMU and SCADA measurements", Electric Power Systems Research, Volume: 81, Issue: 7, July 2011, p.1514-1524.

[15] A. Phadke, J. Thorp, R. Nuqui, and M. Zhou, "Recent Developments in State Estimation with Phasor Measurements", 2009 IEEE/PES Power Systems Conference and Exposition.

[16] N. Zhou, D. Meng, Z. Huang, and Greg Welch, "Dynamic State Estimation of a Synchronous Machine Using PMU Data: A Comparative Study", IEEE Transactions on Smart Grid, Volume: 6, Issue: 1, Jan. 2015.

[17] Y. Chakhchoukh, V. Vittal, and G. Heydt, "PMU Based State Estimation by Integrating Correlation", IEEE Transactions on Power System, Volume: 29, Issue: 2, March 2014.

[18] D. Kumari and S. Bhattacharyya, "A Data-driven Approach to Power System Dynamic State Estimation", 19th International Conference on Intelligent System Application to Power Systems (ISAP), 2017.

[19] L. Zhang, G. Wang, and G. Giannakis, "Real-Time Power System State Estimation via Deep Unrolled Neural Networks", 2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP).

[20] C. Beasley, X. Zhong, J. Deng, R. Brooks, and G. Venayagamoorthy, "A Survey of Electric Power Synchrophasor Network Cyber Security", 5th IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), October 12-15, 2014, Istanbul.

[21] S. Liu, X. Liu, and A. Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids", 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT).

[22] M. Kurt, Y. Yilmaz, and X. Wang, "Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid", IEEE Transactions on Information Forensics and Security, Volume: 14, Issue: 2, Feb. 2019.

[23] X. Wang, D. Shi, J. Wang, Z. Yu, and Z. Wang, "Online Identification and Data Recovery for PMU Data Manipulation Attack", IEEE Transactions on Smart Grid, 2019.

[24] H. Mosbah and M.E. El-Hawary, "Optimization of neural network parameters by Stochastic Fractal Search for dynamic state estimation under communication failure", Electric Power Systems Research 147 (2017) 288301.

[25] C. Gu, and P. Jirutitijaroen, "Dynamic State Estimation Under Communication Failure Using Kriging Based Bus Load Forecasting", IEEE Transactions on Power Systems. Volume: 30, Issue: 6, Nov. 2015.

[26] S. Soltan, M. Yannakakis, and Gil Zussman, "Power Grid State Estimation Following a Joint Cyber and Physical Attack", IEEE Transactions on Control of Network Systems, Volume: 5, Issue: 1, March 2018.

[27] M. Hossain and M. Rahnamay-Naeini, "Line Failure Detection from PMU Data after a Joint Cyber-Physical Attack", Accepted in IEEE PES General Meeting, 2019.

[28] W. Yuill, A. Edwards, and S. Chowdhury, "Optimal PMU placement: A comprehensive literature review", IEEE Power and Energy Society General Meeting, 2011.

[29] R. D. Christie, Power Systems Test Case Archive, University of Washington, Aug. 1993.

[30] Electrical and Computer Engineering Department, IEEE 118-Bus,54 Unit, 24-Hour System Unit and Network Data, Illinois Institute of Technology.

[31] The New York Independent System Operator, Inc[US], https://www.nyiso.com/.

[32] R. D. Zimmerman, C. E. Murillo-Snchez, and R. J. Thomas, MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education, IEEE Transactions on Power Systems, Volume: 26, Issue:1 , Feb. 2011.