Line Failure Detection from PMU Data after a Joint Cyber-Physical Attack

MD Jakir Hossain and Mahshid Rahnamy-Naeini
Electrical Engineering Department, University of South Florida, Tampa, Florida, USA
mdjakir@mail.usf.edu, mahshidr@usf.edu

***Abstract*—The joint cyber and physical attacks propose new threats to many cyber-physical systems including smart grids. Due to the critical interdependency of power grids on the cyber components, modern power grids exhibit new vulnerabilities to cyber and physical attacks. In this paper, a joint cyber-physical attack is considered in which an adversary damages some lines physically (physical attack) and prevents the information flow from the attacked zone to the control center to tamper the observability of the grid and mask the physical failure (cyber attack). The goal of the presented work is to evaluate if the PMU data available from outside of the attacked zone can be used to estimate the state of the components in the attacked zone and how various scenarios of attacks will affect the state estimation. In this regard, a linear Minimum Mean Square Error (MMSE) estimation is applied to simulated PMU data. The MMSE is further extended to an iterative process with feedback to improve the performance of estimation. In this paper, the state estimation to recover the status of the components after the joint cyber physical attack is a data-driven approach and does not use system models. The IEEE 118 test case is used to show scenarios that the state of the lines can be estimated with minimum error as well as the lines that are difficult to estimate their state and thus may require more protection.**

***Index Terms*—Line Outages, PMU Data, Cyber-Physical Attack, State Estimation, Smart Grid Security.**

I. Introduction

Modern power grids are becoming more and more equipped with cyber elements for sensing, monitoring, communication, computation, and control, which make them exemplary complex cyber-physical systems. Due to such increased dependency on cyber components, these systems exhibit new vulnerabilities to cyber threats. When cyber attacks occur jointly with physical attacks or failures in the power grid, they could have even more serious impacts and cause large-scale blackouts with severe societal and economic consequences [1]. In the case of physical attacks or failures, the system's stability can be maintained if the Supervisory Control and Data Acquisition (SCADA) receives precise information about the status of the components and take proper action accordingly. If however, the flow of information is obstructed by a cyber attack, the status of the components will be unobservable to the SCADA, which prevents the control center from taking necessary and appropriate actions in a timely manner. Figure 1 presents the historical timeline of reported cyber-physical attacks, which is a clear indication of ever-increasing threats and concerns on cyber-physical systems security, such as the smart grid security.

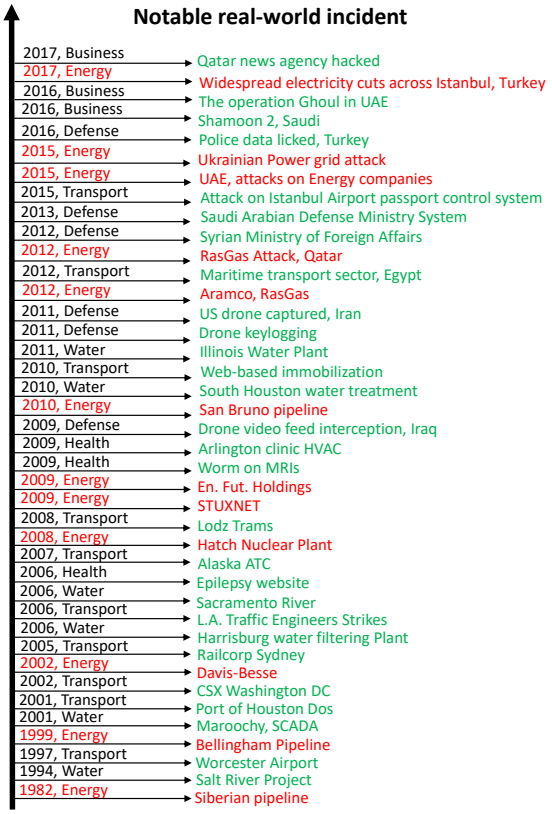


Fig. 1: Historical time-line of reported cyber-physical attacks on various infrastructures (energy infrastrcture is indicated by red) [7,16].

On the other hand, cyber components provide invaluable opportunities for a more secure and reliable operation of smart grids. For instance, the immense volume of energy data collected by various sensors, such as Phasor Measurement Units (PMUs), provide new opportunities for detecting, estimating and predicting various events in the system using big data analytics techniques. In this paper, we consider a scenario of joint cyber and physical attack on the smart grid and discuss how a data-driven method based on PMU data can help in recovering the status information of the components. Similar to the work in [1-3], we consider the scenario in which an attacker conducts a physical attack on the power system by disconnecting few transmission lines and simultaneously launches a cyber attack on the communication system and prevents the flow of information from the region around the

physically attacked area or other regions of the system to the control center. This joint cyber attack leads to unobservability on a portion of the power system, which has experienced line outages. The goal of the presented work is to use the PMU data from outside the attacked zone (observable parts of the system) to estimate the state of the lines in the attacked zone using a data-driven technique. The availability of large volumes of PMU data in future smart grids and limitations of the traditional power system state estimation due to dependency on accurate power system models, make the data-driven approaches more appealing than before as a complement to the traditional state estimation or separately. In this work, we have specifically used a linear minimum mean square error (MMSE) estimator for recovering the status information of components in the attacked zone. We have evaluated various scenarios and observed that recovering the status information of certain power components are more difficult than others and thus, we have proposed an extension to the linear MMSE estimator by adding iterative feedback to the estimator, which has improved the estimation performance. We have evaluated these data-driven estimation methods on various scenarios of joint-cyber attacks on the IEEE 118 test bus system including scattered and localized attacks. The results show that the data-driven approaches can be promising approaches for state estimation, particularly during cyber-physical attacks.

II. Related works

Security of the cyber physical systems (CPSs) including smart grids has been the focus of many researches. Studying and mitigation the effects of joint cyber and physical attacks in CPSs are categories of such researches that have gained lots of attention recently [1]-[5]. For instance, Sultan et. al in [1]-[3] exploited a joint graph-based and power analysis approach for state estimation and line failure detection. In [4], the authors considered coordinated cyber physical attacks that can lead to line outages. In the latter work, the goal is to identify the most damaging and undetectable line outages using power system analysis and an optimization framework. In [5], an in-depth review of the smart grid security from a CPS perspective is presented and prominent cyber physical attack schemes with significant impact on the smart grid operation and corresponding defense solutions have also been discussed.

Other than the power-based and graph-based analyses of the security threats, many researchers have used PMU data for detecting the line outage in power grids in case of failures or attacks. For instance, in [6] the authors use PMU data along with the topology information to detect line outages. State estimation of power system using PMU data have also been extensively studied [8-12]. For instance, in [9] a two-step hybrid state estimation combining both conventional WLS method and linear estimation that utilizes PMU measurements. In [12], a real-time fault detection and faulted line identification functionality is proposed based on computing parallel synchrophasor-based state estimators.

In addition to new techniques based on graph and PMU data analyses, power system security has been extensively studied using traditional state estimation methods [13-15] in which accurate knowledge of the system model is required. The work in [13] provides a survey discussing the state of the art in electric power system state estimation. A review of power system dynamic state estimation techniques using conventional methods have also discussed in [14,15]. Although many powerful techniques has been developed in state estimation for power systems, availability of large volume of data and data analytics techniques can provide new opportunities to help with state estimation in special situations, for example, when the system model is not available or accurate (such as in the cases of joint cyber attacks). The presented work in the current paper, is focused on a data-driven approach for state estimation using PMU data for transmission line state estimation and fault detection during joint cyber physical attacks.

III. System and attack model

A. Power System Model

We consider a power transmission system with a set of buses (including generation, transmission and substation buses) denoted by N and a set of transmission lines denoted by L. We also assume that the system is fully equipped with PMUs, which although may not be realistic based on current real-world systems, it will allow us to evaluate the proposed methodology for the case of complete information on the system. Similar study can be performed with limited number of PMUs as the future work. Moreover, we assume that the real and reactive power flow through transmission lines and phase angels of the components are being sampled by PMUs and sent to the control center (SCADA). Finally, we assume that the loads at substations vary in time and cause change in the flow distribution.

B. Attack Model

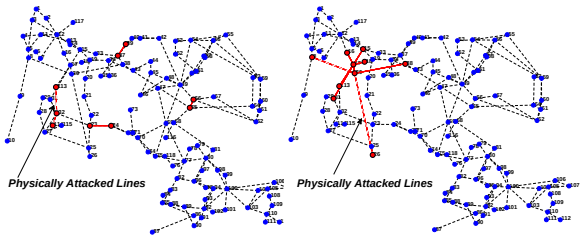
In this paper, we consider joint cyber and physical attacks and thus the attack definition has two parts. Specifically, to model the *cyber attack*, we assume that the attacker randomly selects a subset A_c of transmission lines (i.e., $A_c \in L$) and masks the flow of information from them to the control center. We call the set A_c the *cyber attack zone* or *attack zone* for short. Further, to model the *physical attack*, we assume that a subset A_p of lines from the attack zone (i.e., $A_p \in A_c$) experiences physical attack or failure.

Further, we consider two scenarios for the attack zone:
(1) Randomly scattered attacks, where the set A_c of transmission lines is geographically scattered on the system. Figure 2-a depicts one example of a scattered attack on the IEEE 118 test case topology.

(2) Localized attacks, where the set A_c of transmission lines are all adjacent to each other (i.e., have physical connection in the topology of the system). Figure 2-b represents an example of a localized attack scenario on IEEE 118 test case.

IV. Estimating the state of components

After a joint cyber and physical attack occurs in the system, we use the collected PMU dataset and apply a "Minimum



(a) (b)

Fig. 2: Example of a) scattered attack scenario, and b) a localized attack scenario. The red marked branches have experienced cyber attack and became unobservable and the red dashed lines indicate branches, which are physically attacked.

Mean Square Error Estimator" to estimate the status of the branches in the unobservable portion of the grid. We specifically use a linear MMSE estimation model, where the unobservable portion of the grid is the estimation target and is denoted by $\mathbf{Y}$. The size of vector $\mathbf{Y}$ is equal to $|A_c|$, where $|.|$ represents the cardinality of the set. The elements Y_is of $\mathbf{Y}$ represent the power flow through the unobservable transmission lines in the attack zone. In this work, we use the real power flow through the lines to identify the physically attacked/failed lines. The rest of the information outside the attacked zone provided by the PMUs are considered as the estimation features $\mathbf{X}$, where the size of vector $\mathbf{X}$ is given by $(|L| - |A_c|) * f$ and f is the number of feature parameters to be used. Specifically, in this work we consider three possible feature parameters including real and reactive power flow and the phase angel. We can use a single feature parameter or a combination of them as well as certain lines or all the lines as a part of our estimation features.

The linear MMSE model suggests that our estimation of $\mathbf{Y}$ is related to features through $\hat{\mathbf{Y}} = \mathbf{AX} + \mathbf{B}$, where matrix $\mathbf{A}$ and vector $\mathbf{B}$ can be characterized based on the data such that estimation error is minimized. Specifically, the matrix $\mathbf{A} = R_{\mathbf{XY}} R_{\mathbf{X}}^{-1}$, where the matrix $R_{\mathbf{XY}}$ and $R_{\mathbf{X}}$ are the cross-correlation and auto-correlation matrices and $\mathbf{B} = \bar{\mathbf{Y}} - \mathbf{A}\bar{\mathbf{X}}$, where $\bar{\mathbf{X}}$ and $\bar{\mathbf{Y}}$ are the mean of the variables $\mathbf{X}$ and $\mathbf{Y}$.

An important observation based on our simulations is that when a subset of the grid branches changes their status (fail or the change the power flow), not all other lines will be effected equally due to such changes. For example in Figure 2-b, changes inside the red portion of the grid (e.g., failure in the attack zone) does not equally affect the other branches outside the attack zone. Figure 3 shows a heatmap of the real power flow changes in all transmission lines due to the changes in the status of components inside the attack zone. This result is obtained based on 250 different scenarios with multiple combinations of failed transmission lines inside the attack zone. Based on this observation we can conclude that to determine the status of the unobservable components, one does not need data on all other branches outside this zone. Thus we can introduced a feature selection mechanism based on such analyses, which will allow selecting feature with most information to ease the computational complexity.

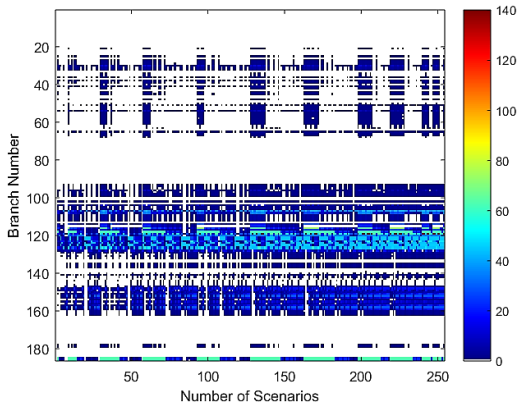


Fig. 3: Effect on all other branches due to changes in red marked zone (Figure 2-b.) for different combination of changes inside the zone.

A. *Iterative MMSE with feedback*

As we will show in Section V, when multiple lines becomes unobservable, it gets more difficult to estimate the status of the line with an acceptable confidence level. To improve the performance of the estimation, we can use a feedback mechanism in the linear MMSE to use the components that are easier to estimate the states as features for the rest of the components. Note that this requires a pre-assessment of estimation capabilities for various components of the system, which can be a cumbersome task. In this subsection, we assume such information is available and has been pre-evaluated for the components and thus the focus is on the concept of the feedback MMSE.

In this approach, we assume that if the status of a subset of unobservable branches can be estimated with 90% confidence level (this level can be adjusted) then this subset will be used in the next iteration of the estimation as additional estimation feature (as a part of vector $\mathbf{X}$). This means that the estimated components's states with a predefined confidence level will no longer be a part of the attack zone and thus the attack zone shrinks to a small size, which we again we assume that we know the estimation capability for the components inside the new attack zone. This feedback process can continue until the status of the whole unobservable portion is estimated.

An example of this process applied to attack zone $[B21, B22, B23, B36, B37, B38, B39, B54, B178]$ is as following. In the first step, the estimator predicted a subset of the branches $[B36, B37, B38, B54]$ with $\geq 90\%$ confidence level. In the next step, the status of the latter components used as additional features in the linear MMSE, which helped in estimating the status of three more components including $[B21, B22, B23]$ and the process continues until the status of all except one component ($[B178]$) has been identified with $\geq 90\%$ confidence level.

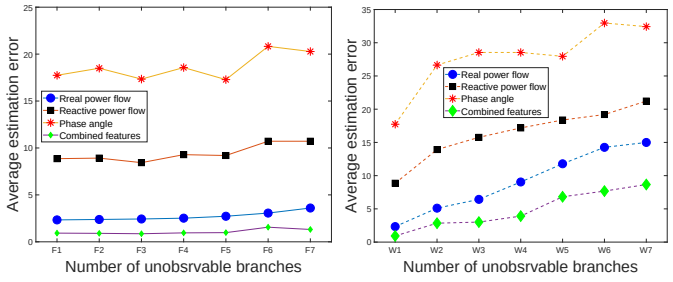
V. Case Study and Results

In this paper, the IEEE 118 bus system has been selected for our study. We have simulated a large PMU dataset in both normal and also under various physical attack scenarios using our IEEE 118 simulations in MATPOWER [17]. In addition

to various physical attack scenarios, we have considered load variations at different substations in time. The load variations on the buses are performed by adding/subtracting a random percentage of the original load at the bus (with a uniform distribution) to its load. To simulate a PMU dataset, the real and reactive power and the phase angel of all the branches have been recorded. We use this dataset to identify (train) our linear MMSE parameters **A** and **B** as discussed in Section IV.

A. Randomly scattered attacks

To evaluate the performance of our trained estimator under the scattered attack scenarios, we create randomly scattered attacked zones (where the lines under cyber attack are geographically distant). We specifically create attack zones of size one to seven (while larger attack zones are possible but we assume that attackers have limited resources and the size of the attack zones are relatively small compare to the size of the grid.) We represent the attack zones with size i by F_i, representing the unobservable components under cyber attack. In each of the randomly generated attack zones, there might be any number ($\leq i$) of physically failed lines. For each size of attack zone, we have generated 250 random attack zones. The average estimation error for each size of attack zone is presented in Figure 4-a when different features are used in the estimation. We observe that the estimation error increases with block size and combined features gives the best estimate for the power flow status of branches.



(a) (b)

Fig. 4: Average estimation error using different features a) randomly scattered attack, b) localized attack.

B. Localized attacks

To evaluate the performance of our trained estimator under the localized attack scenarios, we generate attack zones with topologically adjacent lines under cyber attack. We call these attack zones, windows and consider sizes of one to seven for the attack zone. In this case, we represent the attack zones with size i by W_i. Similar to the scattered attacks, we generated 250 random scenarios of localized attacks for each window size. The average estimation error for the localized attacks is shown in Figure 4-b when different features are used in the estimation. From the results, we observe that the estimation error increase with the attack size and the combined features give the best estimate for the power flow of the branches.

To evaluate the performance of the estimator in detecting the failed or physically attacked components in the attack zone, we have evaluated the average detection rate for both scattered and localized scenarios, where the failure is identified when the power flow through the line is estimated to be below certain threshold. The results are shown in Figure 5. From the results, we observe that the detection rate is lower for localized attacks (dashed lines) than the scattered attacks (solid lines). This is because when a transmission line is affected by a physical attack or failure, usually the adjacent lines will bear the most impact and thus the most information to help with the estimation. In the localized attack scenarios, since information from a portion of the locally adjacent lines are unavailable (due to cyber attack), estimating the state of components in the attack zone is more difficult.

Note that one of the key observations that we obtained from our estimation results is that the estimation performance is different for various transmission lines. The results in Figures 4 and 5 show the average performance, while Figure 7 shows the average performance of estimation for the individual lines in an attack zone F_{ij} & W_{ij} (**j** is the position of the branch in block/window).

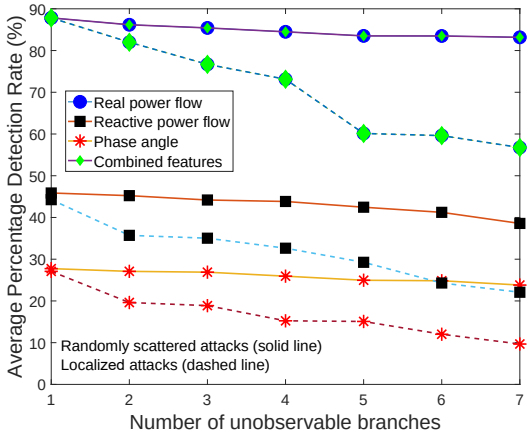


Fig. 5: Percentage detection rate for different window size using different features.

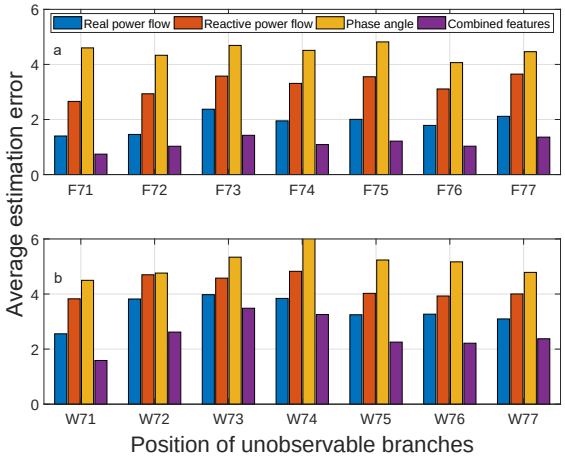


Fig. 6: Average estimation error for a) randomly scattered attack (F7), b) localized attack (W7) using different features.

C. Iterative Estimator with Feedback

The results in Figure 7, suggests that due to the power system attributes and topological location of the lines, it is

easier to recover the lost information on the state of some lines. Identifying such components using similar studies can help in the iterative estimator with feedback discussed in Section IV. In this section, we are presenting two examples of attack zones with such components that can help improving the estimation on the rest of the components in the attack zone. Although the results for the iterative estimator with feedback are very dependent on the attack zone and the pre-existing information on our estimation capability for lines, these examples show how the approach can help the recovery with such information in an iterative process. In these examples, we use the estimator to find the status of the lines that we know they can be estimated with 90% confidence rate. We will the update the attack zone size and use the estimated states in the previous step as new features for estimation. The iterative process will go on until all components are estimated with 90% confidence rate or we cannot improve the estimation confidence for the remaining components. The steps of the process for a scattered and localized attack are presented in Table 1. In addition, feature selection using maximum variance in the data (as shown in Figure 3) is also applied to eliminate the unnecessary PMU data for the lines that were not impacted by the changes in the state of the attack zone to ease the computational complexity.

Table 1: Examples from localized attack and a scattered attack scenario with and without the iterative estimation with feedback. The data pairs shown in each column represent the line number and their detection rate. Bold-underlined values show the components with low detection rate in each iteration.

	Feedback	Unobservable Lines	1st Iteration	2nd Iteration	3rd Iteration	4th Iteration
Randomly Scattered Attacks	Before	F7 – [B28, B49, B102, B171, B175, B177, B183]	(B28, 100%), ***(B49, 1.75%)***, (B102, 100%), ***(B171, 0%)***, ***(B175, 0%)***, ***(B177, 0%)***, (B183, 100%)			
		F6 – [B26, B74, B92, B145, B149, B166]	(B26, 100%), ***(B74, 60%)***, (B92, 100%), (B145, 100%), (B149, 100%), ***(B166, 74%)***			
	After	F7 – [B28, B49, B102, B171, B175, B177, B183]	(B28, 100%), ***(B49, 1.75%)***, (B102, 100%), ***(B171, 0%)***, ***(B175, 0%)***, ***(B177, 0%)***, (B183, 100%)	***(B49, 1.75%)***, ***(B171, 0%)***, ***(B175, 0%)***, (B177, 95.75%)	(B49, 100%), (B171, 100%), (B175, 100%)	0
		F6 – [B26, B74, B92, B145, B149, B166]	(B26, 100%), ***(B74, 60%)***, (B92, 100%), (B145, 100%), (B149, 100%), ***(B166, 74%)***	(B74, 100%), (B166, 100%)	0	0
Localized Attacks	Before	W7 - [B21, B22, B23, B36, B39, B40, B42]	***(B21, 0%)***, ***(B22, 0%)***, ***(B23, 0%)***, (B36, 100%), ***(B39, 0%)***, ***(B40, 0%)***, ***(B42, 0%)***			
		W6 – [B45, B47, B48, B49, B50, B51]	***(B45, 25%)***, ***(B47, 0%)***, ***(B48, 0%)***, ***(B49, 0%)***, ***(B50, 0%)***, (B51, 100%)			
	After	W7 - [B21, B22, B23, B36, B39, B40, B42]	***(B21, 0%)***, ***(B22, 0%)***, ***(B23, 0%)***, (B36, 100%), ***(B39, 0%)***, ***(B40, 0%)***, ***(B42, 0%)***	(B21, 100%), ***(B22, 0%)***, (B23, 100%), ***(B39, 0%)***, ***(B40, 0%)***, ***(B42, 0%)***	(B22, 100%), ***(B39, 74%)***, ***(B40, 87%)***, ***(B42, 49%)***	(B39, 100%), ***(B40, 87%)***, ***(B42, 54%)***
		W6 – [B45, B47, B48, B49, B50, B51]	***(B45, 25%)***, ***(B47, 0%)***, ***(B48, 0%)***, ***(B49, 0%)***, ***(B50, 0%)***, (B51, 100%)	***(B45, 25%)***, ***(B47, 0%)***, ***(B48, 0%)***, ***(B49, 0%)***, (B50, 100%)	***(B45, 25%)***, (B47, 100%), (B48, 98%), (B49, 100%)	***(B45, 25%)***

VI. Conclusion and Future Work

In this paper, a joint cyber and physical attack on smart grids is considered, which results in unobservablity of a portion of the grid while causing transmission lines failures. We used a data-driven approach to estimate the state of the unobservable portion of the grid under cyber attack from the PMU data available outside the attack area. Specifically, a linear MMSE approach was used and was trained based on the simulated PMU data. We also proposed the idea of iterative estimation with feedback to improve the estimation performance. Further, we considered two different types of attack scenarios including localized and scattered attacks and showed that estimating the state of components in a scattered attack is easier compared to localized attacks. This work shows the importance and the power of data and data analytics methods in addressing joint cyber and physical attacks on smart grids.

Acknowledgement

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] S. Soltan and G. Zussman, "Power grid state estimation after a cyber-physical attack under the AC power flow model," 2017 IEEE Power and Energy Society General Meeting, Chicago, IL, 2017, pp. 1-5.

[2] S. Soltan, M. Yannakakis and G. Zussman, "Power Grid State Estimation Following a Joint Cyber and Physical Attack," in IEEE2 Transactions on Control of Network Systems, vol. 5, no. 1, pp. 499-512, March 2018.

[3] S. Soltan, A. Loh and G. Zussman, "Analyzing and Quantifying the Effect of *k*-line Failures in Power Grids," in IEEE Transactions on Control of Network Systems, vol. 5, no. 3, pp. 1424-1433, June 2017.

[4] Z. Li, M. Shahidehpour, A. Alabdulwahab and A. Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems," in IEEE Transactions on Smart Grid, vol. 7, no. 5, pp. 2260-2272, Sept. 2016.

[5] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," in IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13-27, 12 2016.

[6] J. E. Tate and T. J. Overbye, "Line Outage Detection Using Phasor Angle Measurements," in IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1644-1652, Nov. 2008.

[7] George Loukas, "Cyber-physical attacks: A History of Cyber-Physical Security Incidents", Butterworth-Heinemann, vol. 1, ch. 2, Pages 21-57, June 2015, ISBN 9780128012901.

[8] H. Zhao, "A New State Estimation Model of Utilizing PMU Measurements," 2006 International Conference on Power System Technology, Chongqing, 2006, pp. 1-5.

[9] J. James and Bindu S., "Hybrid State Estimation including PMU measurements," 2015 International Conference on Control Communication and Computing India(ICCC),Trivandrum, 2015, pp. 309-313.

[10] I. Kolosok, E. Korkina and E. Buchinsky, "The test equation method for linear state estimation based on PMU data," 2014 Power Systems Computation Conference, Wroclaw, 2014, pp. 1-7.

[11] S. Hou, Z. Xu, H. Lv, Z. Jiang and W. Lingyi, "Research into Harmonic State Estimation in Power System Based on PMU and SVD," 2006 International Conference on Power System Technology, Chongqing, 2006, pp. 1-6.

[12] M. Pignati, L. Zanni, P. Romano, R. Cherkaoui and M. Paolone, "Fault Detection and Faulted Line Identification in Active Distribution Networks Using Synchrophasors-Based Real-Time State Estimation," in IEEE Transactions on Power Delivery, vol. 32, no. 1, pp. 381-392, Feb. 2017.

[13] A. Monticelli, "Electric power system state estimation," in Proceedings of the IEEE, vol. 88, no. 2, pp. 262-282, Feb. 2000.

[14] N. R. Shivakumar and A. Jain, "A Review of Power System Dynamic State Estimation Techniques," 2008 Joint International Conference on Power System Technology and IEEE Power India Conference, New Delhi, 2008, pp. 1-6.

[15] M. R. Karamta and J. G. Jamnani, "A review of power system state estimation: Techniques, state-of-the-art and inclusion of FACTS controllers," 2016 International Conference on Electrical Power and Energy Systems (ICEPES), Bhopal, 2016, pp. 533-538.

[16] Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Warusia Yassin, Aslinda Hassan, Zaheera Zainal Abidin, Nabeel Salih Ali and Karrar Hameed Abdulkareem, "Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems", International Journal of Advanced Computer Science and Applications(IJACSA), vol. 9, no. 1, 2018.

[17] 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," Power Systems, IEEE Transactions on, vol. 26, no. 1, pp. 12-19, Feb. 2011.