Can Predictive Filters Detect Gradually Ramping False Data Injection Attacks Against PMUs?

Zhigang Chu, Andrea Pinceti, Reetam Sen Biswas, Oliver Kosut, Anamitra Pal, and Lalitha Sankar
School of Electrical, Computer and Energy Engineering
Arizona State University

***Abstract*—Intelligently designed false data injection (FDI) attacks have been shown to be able to bypass the χ^2-test based bad data detector (BDD), resulting in physical consequences (such as line overloads) in the power system. In this paper, using synthetic PMU measurements and intelligently designed FDI attacks, it is shown that if an attack is suddenly injected into the system, a predictive filter with sufficient accuracy is able to detect it. However, an attacker can gradually increase the magnitude of the attack to avoid detection, and still cause damage to the system.**

I. Introduction

In the past decade, phasor measurement units (PMUs) have been widely deployed in power systems for monitoring, protection, and control purposes. Since PMUs can directly measure the bus voltage phasor with high sampling rate and accuracy, they have the potential to play a significant role in real-time power system state estimation (SE) [1] and dynamic security assessment [2].

Meanwhile, cyber-attacks against the communication and computing infrastructure of the monitoring and control systems of electric power systems have become a growing concern [3], [4]. As an increasingly important component of this infrastructure, PMUs are also prone to cyber-attacks [5]–[7]. Therefore, it is of great importance to evaluate the vulnerability of PMUs against potential cyber-attacks as well as to develop preemptive countermeasures.

Here, we focus on a broad class of attacks known as false data injection (FDI), wherein an intelligent attacker replaces a subset of measurements with counterfeits. This can be accomplished against PMUs by, for example, spoofing the global positioning system (GPS) signal so as to manipulate a PMU's timestamps [8]. In this paper, we do not limit ourselves to GPS spoofing attacks, but consider FDI attacks accomplished by any means.

The main goals of this paper is to evaluate the effectiveness of countermeasures that use finite impulse response (FIR) predictive filters against sophisticated FDI attacks that are unobservable to current-generation bad data detectors (BDDs) based on χ^2-test. In particular, our contributions are as follows:

1) We create test FDI attacks using a bilevel optimization approach. These attacks are *unobservable* in the sense that they are provably invisible to single-shot BDDs.
2) In order to test these attacks, we generate synthetic PMU data by isolating archetypal data profiles from real data. This technique allows us to create synthetic data to be tested in the context of the IEEE 118-bus system.
3) We investigate whether these attacks can be detected by taking into account temporal correlations. In particular, we use a predictive filtering approach based on the three sample quadratic prediction algorithm (TSQPA) [9], a technique that accurately predicts the next sample of real data based on the previous three. Thus, a large residue of this predictive filter indicates an attack. Moreover, we test an alternative predictive filter learned from real data, that predicts the next sample as a linear combination of the previous five.
4) Finally, we consider two variants of the attack, depending on whether it is applied *suddenly*—i.e., at a single instant—or *ramped*—i.e., gradually increased over a period of time. We demonstrate that predictive filters such as TSQPA can detect sudden attacks with high accuracy, but not ramping attacks.

The first three authors are students ordered by contribution. The last three authors are faculty members ordered alphabetically.

II. Preliminaries

A. PMU-based Linear State Estimation

Throughout our analysis, we assume that the power system is completely observable by PMUs. A PMU placed at a bus measures the complex voltage of that bus, and complex currents on all branches connected to it, typically at a rate of 30 samples per second [10]. These measurements are linear functions of the states, *i.e.,* the complex bus voltages. Let p be the number of buses (states), and n be the number of PMU measurements in the power system, the PMU measurement vector at each time instant, i, is given by

$$w_i = Hx_i + e_i = \begin{bmatrix} I' \\ Y \end{bmatrix} x_i + e_i, \tag{1}$$

where w_i is the $n \times 1$ measurement vector; x_i is the $p \times 1$ vector of true states (complex voltages); e_i is an $n \times 1$ additive Gaussian noise vector whose covariance matrix $R = \text{diag}[\sigma_1^2, \sigma_2^2, \ldots, \sigma_n^2]$; H is the $n \times p$ measurement Jacobian matrix, consisting of I', the reduced identity matrix with only rows corresponding to PMU buses; and Y, the dependency matrix between available current measurements and states. The weighted least squares estimate of x_i, $\hat{x}_i$, is given by [11]

$$\hat{x}_i = (H^T R^{-1} H)^{-1} H^T R^{-1} w_i. \tag{2}$$

The conventional residue-based BDD performs chi-square test on the residue vector

$$r_{i,S} = w_i - H\hat{x}_i \tag{3}$$

to detect bad measurements. Note that the subscript S denotes state estimation; we introduce this notation in an effort to distinguish measurement residue resulting from state estimation from those resulting from using predictive algorithms that we introduce in Sec. II-C.

B. Unobservable FDI Attacks on PMU Measurements

Suppose an attacker can change measurements in a set $\mathcal{S}$ by controlling a subset of PMUs. At each time instant, i, it can replace w_i with

$$\bar{w}_i = w_i + d_i, \tag{4}$$

where the non-zero entries of the measurement attack vector d_i are all within $\mathcal{S}$. An attack is defined to be unobservable [12] to the conventional residue-based BDD if

$$d_i = Hc_i, \tag{5}$$

where the c_i is the state attack vector. Substituting (4) and (5) into (2) yields the estimated states $\bar{x}_i$ under attack

$$\bar{x}_i = \hat{x}_i + c_i. \tag{6}$$

The residue vector under attack

$$\begin{aligned} \bar{r}_{i,S} &= \bar{w}_i - H\bar{x}_i \\ &= w_i + d_i - H\hat{x}_i - Hc_i = w_i - H\hat{x}_i \end{aligned} \tag{7}$$

is the same as that without attack. Therefore, attacks in the form of (5) cannot be detected by the conventional BDD.

C. Three Sample-based Quadratic Prediction Algorithm (TSQPA)

The residue-based BDD discussed in Sec. II-B does not consider temporal correlations in PMU data to detect an anomaly. To validate the quality of the incoming measurements, Gao *et al.* in [9] investigate temporal correlations in PMU data to find the relationship between the past, present, and future measurements. In particular, they prove that for loads changing at a constant power factor, the complex voltage phasor follows a quadratic trajectory. Applying auto-regressive modeling on a quadratic trajectory, they show that the vector of complex voltages at the next time instant can be predicted using the present and past states as follows:

$$x_{(i|i-1)} = 3x_{i-1} - 3x_{i-2} + x_{i-3}, \tag{8}$$

where $x_{(i|i-1)}$ denotes the predicted value of the complex voltage at time instant i, when the voltages at instants $i-3$ through $i-1$ are known. The authors in [9] also test the performance of TSQPA for detecting dynamic events such as the opening of transmission lines and short-circuit faults. Robustness of TSQPA for analyzing system events for different load models has been demonstrated in [13], while it was used for conditioning and validating real PMU data in [14]. However, the effectiveness of TSQPA in detecting anomalies or cyber-attacks in PMU measurements has not been investigated yet. TSQPA is emerging as a basis for real-time PMU data monitoring by some US power utilities, and therefore, it is important to evaluate its effectiveness in detecting cyber-attacks. To this end, we use TSQPA as a detector to detect anomalies due to cyber-attacks in the following way.

Applying (8) on estimated voltages $\hat{x}_i$ gives the predicted voltage $\hat{x}_{(i|i-1)}$. An observation residue $r_{i,T}$ (where the subscript T stands for TSQPA) at the i^{th} time instant can be obtained as:

$$r_{i,T} = \hat{x}_{(i|i-1)} - \hat{x}_i \tag{9}$$

If the magnitude of the observed residue $r_{i,T}$ exceeds a threshold, then a cyber-attack detection is declared.

Finally, as a point of comparison, we also consider a higher order data-driven predictive filter, for which we similarly calculate residues to detect attacks. Details of such a filter will be given in Sec. V-A.

D. Attack Design Optimization

In this paper, we focus on a class of unobservable FDI attacks that aim to maximize the physical power flow on a target line subsequent to a generation re-dispatch, and possibly cause overflow [15]. The attacker injects false measurements in the form of (4), leading to false estimated states as in (6). For a known generation commitment and dispatch plan, these false estimated states lead to false load estimations. The generation re-dispatch caused by the false loads will maximize the physical power flow on the target line. The worst-case attack can be found using an attacker-defender bi-level linear program (ADBLP) [15], wherein the first level models the attacker's objective and limitations, while the second level models the system response via DC-optimal power flow (DCOPF). The formulation of the ADBLP is given by

$$\underset{c,P_G^*}{\text{maximize}} \;\; f(P_G^*) \tag{10a}$$

subject to

$$A_1 c \leq b_1 \tag{10b}$$

$$\{P_G^*\} = \arg\left\{\min_{P_G} g(P_G)\right\} \tag{10c}$$

subject to

$$A_2 P_G \leq b_2 \tag{10d}$$

where P_G and P_G^* are vectors of generation dispatch variables and optimal generation dispatch solved by DCOPF, respectively. The objective function (10a) maximizes the physical power flow on a target line, which is a function of generation dispatch given fixed topology and branch parameters. The attacker is constrained by (10b), which include the resource limitation characterized by the l_1-norm of c, and the detection limitation characterized by the load shift caused by the attack. In each case, A_1 and b_1 are the appropriate parameters. For example, for the load shift constraint, $A_1 = [H; -H]$

and $b_1 = [\lambda \cdot P_D; \lambda \cdot P_D]$, where λ is the max load shift in percentage, and P_D is the vector of loads at all buses. The system DCOPF objective (10c) is to minimize the total generation cost. The DCOPF constraints are represented by (10d) that includes node balance, line limit constraints, and generation limit constraints, where A_2 and b_2 indicate the appropriate system parameters for these constraints.

This ADBLP can be solved by replacing the second level problem by its Karush-Kuhn-Tucker (KKT) conditions and introducing binary variables to convert the non-convex complementary slackness conditions into mixed-integer constraints [15]. The problem then becomes a single level mixed-integer linear program, and can be efficiently solved by the algorithms described in [16]. Alternatively, one can use a Benders' decomposition based algorithm to solve the ADBLP as introduced in [17].

III. Attack Implementation

A. False Measurement Creation

We assume that the system performs DCOPF based on the measurements obtained at every five minutes [18]. After the system re-dispatches at time instant $i = 0$, the attacker solves the ADBLP (10) to obtain the state attack vector c, and then uses c to create false measurements. Although the loads at time instant $i = 0$ may be different than those at the fifth minute when the system re-dispatches again, it is reasonable to assume that they will not change dramatically. Hence, the attack vector solved at $i = 0$ is expected to have similar consequences to the one solved using loads at the fifth minute. Once the state attack vector c is obtained, the attacker can form a measurement attack vector d to create false measurements $\bar{w}$. However, it is unrealistic for the attacker to be omniscient and omnipotent. Thus, as mentioned in Sec. II-B, we assume the attacker only controls a subset of PMUs, whose measurements are in $\mathcal{S}$. Given c, an attack subgraph can be constructed as in [19], consisting only of PMUs under the attacker's control. Note that here c is the outcome of the ADBLP (10), and hence is an attack vector on voltage angles. The measurement attack vector directly formed as $d = Hc$ will cause loads appearing at non-load buses, and possibly raise alarm at the control center. Therefore, the attacker has to solve for the final state attack vector $\tilde{c}$ that ensures the power injections at non-load buses remain unchanged, using the Newton-Raphson method as described in [20]. Once $\tilde{c}$ is obtained, the measurement attack vector can be constructed as $d = H\tilde{c}$.

B. Attack Strategies

We consider the following two strategies for the attacker to inject false measurements:

(1) Sudden attack. At any time instant on or before the fifth minute, the attacker injects d, the measurement attack vector computed at $i = 0^+$, and keeps injecting d afterwards. Without loss of generality, we focus on the situation where d is injected at the fifth minute. Denoting i as the sample number, the fifth minute is $i = 9000$ assuming PMU outputs at 30 samples/sec. The false measurements in a sudden attack are given by

$$\bar{w}_i = \begin{cases} w_i, & i < 9000 \\ w_i + d, & i \geq 9000 \end{cases} . \tag{11}$$

A sudden attack will cause the system to re-dispatch according to the false loads, and maximize the physical power flow on the target branch. However, as we will demonstrate in Sec. V, sudden attacks can be detected by predictive filters such as TSQPA.

(2) Ramping attack. In this strategy, the attacker gradually increases the attack magnitude during the first five-minute interval, starting at $i = 1$, ensuring d is injected at the fifth minute, and keeps injecting d afterwards. The false measurements in a ramping attack are given by

$$\bar{w}_i = \begin{cases} w_i + \frac{i}{9000} \cdot d, & i < 9000 \\ w_i + d, & i \geq 9000 \end{cases} . \tag{12}$$

At $t = 5$ mins, the false measurements in ramping attack are identical to those in sudden attack, and hence, have the same consequences. Sec. V will illustrate that predictive filters have more difficulty detecting ramping attacks due to the slow change across the 5 minute interval.

IV. Generation of Synthetic Load Profile at PMU Time Scale

To verify the proposed FDI attacks against PMU-based system operations, a realistic testbed is required; specifically, the PMU measurements used to test the BDDs must reflect realistic operating conditions. In our tests, we achieve this by simulating the dynamics of the IEEE 118 bus system with time varying loads and primary generation control. The bus-level time-series load data for this test system is generated based on a real PMU dataset that was provided by a large utility company in the southwest of the US. The approach we adopted to create realistic load profiles is mainly based on the work described in [21]. The authors present a data-driven algorithm to learn from a real dataset the spatial and temporal correlation between system loads and use the learnt model to generate new synthetic data that retains the same characteristics. In [21], the approach is demonstrated on SCADA-based, hourly load data. In this section, we detail how this technique was adapted to the learning and generation of load profiles at PMU data speeds.

The utility company provided us with one week worth of PMU data for a group of neighboring substations. From the voltage and current measurements of each bus and line, we compute the loads of two substations, one at the 500kV level and one at 230kV level. Each time-series is 168 hours long, sampled at 30 samples/sec. From these two data streams we can learn the behavior of loads at different voltage levels and subsequently map them to the loads of the IEEE 118 bus system according to their voltage levels. The procedure described in the remainder of this section is followed independently for each of the two loads.

For our simulations, we are interested in generating load data at each bus for 10 minutes. For this reason, the time-series

load data for one consecutive week is broken into segments of length of 10 minutes; this results in 1008 segments, each containing 18,000 samples. The segments are then stacked to form a load matrix $P \in \mathbb{R}^{1008\times 18000}$. As shown in [21], it is possible to learn the behavior of the loads over time by factorizing the load matrix P using singular value decomposition (SVD) as $P = U\Sigma V^T$. The rows of V^T, which are vectors of size 1×18000, constitute the basis of the load matrix and they correspond to archetypal *temporal profiles*. The synthetic loads will be generated by taking linear combinations of a subset of the first load basis (first rows of V^T). To determine the number of basis vectors to be used in the generative model it is useful to look at approximations of P, defined as $\hat{P} = U^f \times \Sigma^f \times V^{f^T}$, where U^f indicates the first f columns of U, Σ^f the first f columns and rows of Σ, and V^f the f first columns of V. By varying the value of f (corresponding to the number of basis vectors to be used) and measuring the root mean squared error (RMSE) between P and $\hat{P}$ we can determine an appropriate number of base temporal profiles to be used in the generative model. In Fig. 1, the error is plotted as a function of the number of basis vectors used. It can be seen that the error decreases rapidly up to $f = 10$ and then it slowly reaches zero when all the basis vectors are used. For this reason, the first 10 temporal profiles are used in the generation of the synthetic load profiles.

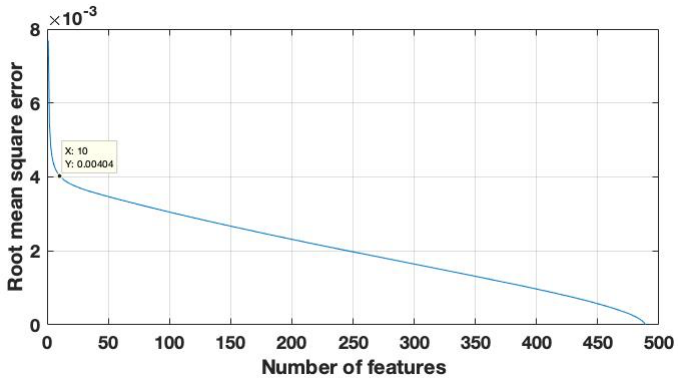

Figure 1. Root mean squared error between P and $\hat{P}$ as a function of the number of basis used.

Having identified some typical temporal load patterns, a new load profile can be created by generating a vector of coefficients and multiplying it by the set of base profiles contained in V. To compute these new coefficients we need to learn the distribution of the coefficients in the original data (e.g. the first 10 columns of U). Using MATLAB, it is observed that each vector of coefficients follows a different Gaussian distribution. At this point, a new matrix of load profiles for n buses can be generated as:

$$P_{\text{new}} = U^{10}_{\text{new}}\Sigma^{10}V^{10^T} \tag{13}$$

where $P_{\text{new}} \in \mathbb{R}^{n\times 18000}$, $U^{10}_{\text{new}} \in \mathbb{R}^{n\times 10}$ is a matrix of coefficients randomly sampled from the distributions learnt from the columns of U, and Σ^{10} and V^{10^T} represent the first 10 singular values and first 10 temporal profiles obtained from the original PMU load data. To account for the spatial correlation which exists between neighboring loads, the model is modified as follows:

$$P_{\text{new}} = (DU^{10}_{\text{new}})\Sigma^{10}V^{10^T} = U'^{10}_{\text{new}}\Sigma^{10}V^{10^T} \tag{14}$$

where $D \in \mathbb{R}^{n\times n}$, and each entry $d_{i,j}$ of D is given by:

$$d_{i,j} = \begin{cases} 1, & \text{if } i = j \\ e^{-2\text{dist}_{i,j}}, & \text{if } \text{dist}_{i,j} \leq 3 \text{ and } i \neq j \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

and $\text{dist}_{i,j}$ is the minimum number of branches between buses i and j. Overall, this relation was experimentally derived in [21] and was adapted to the system for which we designed the synthetic loads.

V. Numerical Results

A. Experiment Setup

We use the IEEE 118-bus system in our simulations. The PMU placement scheme is obtained from [22]. The following steps are required before we can test the performance of predictive filters for attack detection:

1) Synthetic load profile generation: Using the model in (14) on the 500kV and 230kV loads, we generate individual load profiles for 10 minutes for the loads in the IEEE 118 bus system according to their nominal voltage. Fig. 2 shows the synthetic load profiles generated for two adjacent loads. As expected, they show a similar pattern over 10 minutes.

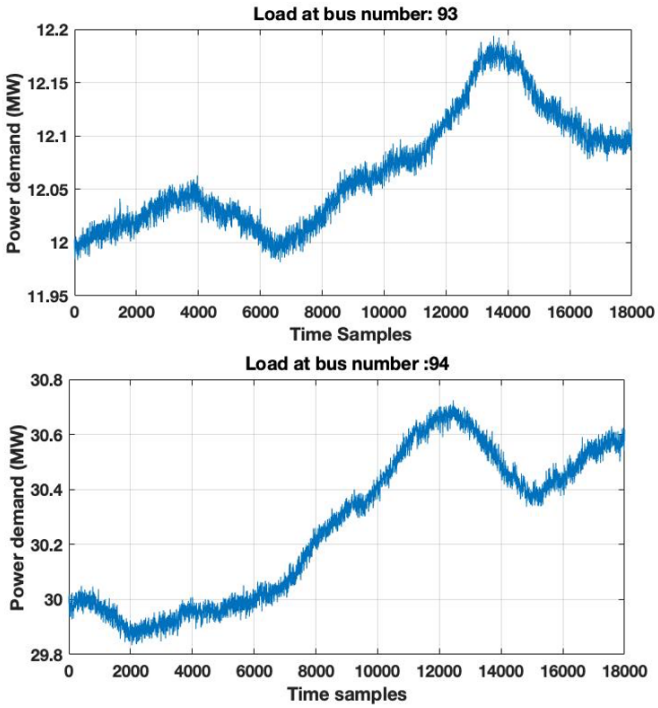

Figure 2. Synthetic load profiles generated for two neighboring buses.

2) Synthetic PMU measurements generation: Based on the synthetic loads, dynamic simulations are run in PSLF [23]

and voltage and current data are sampled 30 times per second to represent the PMU measurements. For adding noise to the synthetic PMU measurements we investigate the observation residues computed by TSQPA in the real PMU data obtained from the utility. The noise in the synthetic measurements are added in proportion to the noise in real data such that it results in similar observation residue for a no-attack scenario. The noise in magnitude and angle are selected from a Gaussian distribution of zero mean and 0.01% standard deviation, which ensures the total vector error (TVE) to be within 1% [24].

3) False measurements creation: A state attack vector c is obtained by solving the attack design ADBLP in Sec. II-D with 10% load shift constraint. We then follow the procedure described in Sec. III to create the measurement attack vector d, and subsequently the false measurements $\bar{w}$ for both sudden attack and ramping attack. The generation re-dispatch caused by the false measurements will lead to 30% overflow on branch 54 (bus 30-38) and 22% overflow on branch 37 (bus 8-30).
4) Data-driven five-sample predictive (FSP) filter: Based on the real PMU measurements that we received from the utility, we perform a moving window linear regression to learn the best coefficients of a five-sample predictive filter. This predictive filter is given by

$$\begin{aligned} x_{(i|i-1)} =& 0.9186x_{i-1} + 0.0196x_{i-2} + 0.0438x_{i-3} \\ &+ 0.0058x_{i-4} + 0.0122x_{i-5}. \end{aligned} \tag{16}$$

B. Attack Detection using Predictive Filters

We now investigate whether intelligently designed FDI attacks can be detected by predictive filters. The hypothesis of detecting an attack is that the observation residue in the presence of an attack would increase. Note that these attacks cannot be detected by the χ^2-based BDD currently employed in the power systems. False measurements resulting from sudden and ramping attack, as well as attack-free measurements at two buses of the IEEE 118 bus system are illustrated in Fig. 3. It can be seen that the measurements of both attack strategies are identical after 5 minutes (9,000 samples). Fig. 3(a) shows a relatively large attack, where the attack magnitude on the real part of the voltage at bus 8 at the fifth minute is 0.0141 per unit, while Fig. 3(b) shows a small attack at bus 40 where the attack magnitude to the real part of the voltage is merely 0.0017 per unit.

Fig. 4 demonstrates the observation residues when applying the predictive filters on measurements with sudden attack. Both TSQPA and FSP give a large residue at the fifth minute when the attack is injected, indicating that they are both able to detect sudden attacks. Moreover, they can detect both the attacks at bus 8 and bus 40, even though the attack magnitude at bus 40 is much smaller.

Fig. 5 illustrates the observation residues obtained by applying predictive filters on measurements with ramping attack. The residues do not increase because the attack magnitude at each time instant is too small. These observations indicate that

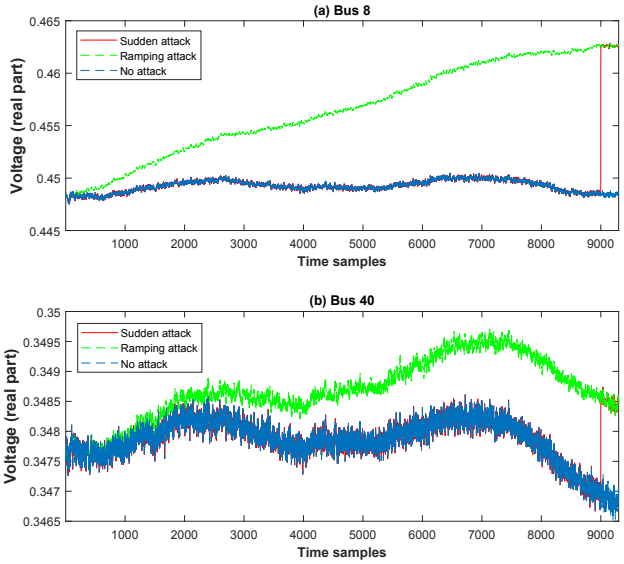

Figure 3. Examples of false measurements at (a) bus 8; and (b) bus 40

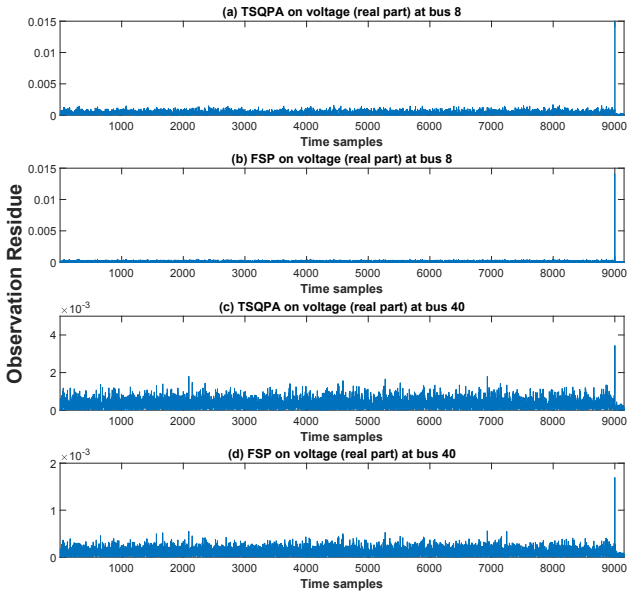

Figure 4. Sudden attack detected by predictive filters

gradually ramping attacks can avoid detection by the selected predictive filters.

VI. Concluding Remarks

In this paper, we applied two predictive filters to detect FDI attacks against PMU measurements that are unobservable by the conventional measurement residue-based bad data detector. We first created synthetic load profiles at PMU time scale that capture both temporal and spatial correlations. Using these synthetic load profiles, we then generated synthetic PMU measurements by running dynamic simulations. Subsequently, we designed test FDI attacks via a bilevel optimization approach, and created two sets of unobservable false measurements, one

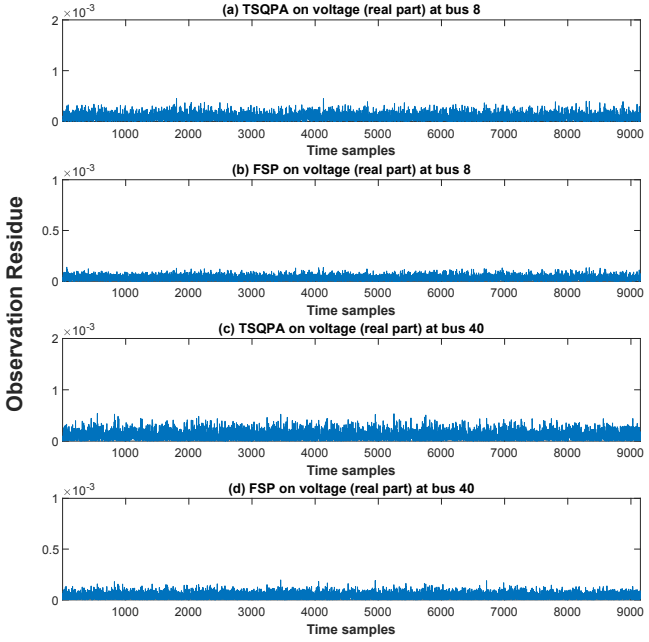

Figure 5. Ramping attack undetected by predictive filters

for sudden attack and the other for ramping attack. Finally, the false measurements are tested through a theoretically derived and a data-driven predictive filter, to see whether they can detect the attacks.

The observation residues obtained from the two predictive filters for both attack strategies indicate that sudden attacks can be detected by predictive filters, while ramping attacks cannot, because the ramping attack magnitudes between time instants are smaller than those of the sudden attack. Future work will include designing more dynamic detection schemes beyond FIR filters, such as Kalman filters, to detect ramping attacks, as well as machine learning-based countermeasures to mitigate FDI attacks.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1449080 and the Power System Engineering Research Center (PSERC) under project S-74.

References

[1] J. Zhao, G. Zhang, K. Das, G. N. Korres, N. M. Manousakis, A. K. Sinha, and Z. He, "Power system real-time monitoring by using PMU-based robust state estimation method," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 300–309, Jan 2016.

[2] Y. Zhang, Y. Xu, S. Bu, Z. Y. Dong, and R. Zhang, "Online power system dynamic security assessment with incomplete pmu measurements: a robust white-box model," *IET Generation, Transmission Distribution*, vol. 13, no. 5, pp. 662–668, 2019.

[3] K. Zetter, "An unprecedented look at Stuxnet, the world's first digital weapon," Nov. 2014. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[4] B. Ibelle, "Russian cyberattack on US power grid meant to be show of power, researchers working to thwart the next one," Mar. 2018. [Online]. Available: http://news.northeastern.edu/2018/03/21/northeastern-researchers-address-russian-power-grid-attack/

[5] S. Paudel, P. Smith, and T. Zseby, "Stealthy attacks on smart grid PMU state estimation," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018.

[6] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "False data injection attacks on phasor measurements that bypass low-rank decomposition," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2017.

[7] Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "Unobservable false data injection attacks against PMUs: Feasible conditions and multiplicative attacks," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*, 2018.

[8] S. Barreto, M. Pignati, G. Dán, J. Le Boudec, and M. Paolone, "Undetectable timing-attack on linear state-estimation by using rank-1 approximation," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3530–3542, July 2018.

[9] F. Gao, J. S. Thorp, A. Pal, and S. Gao, "Dynamic state prediction based on auto-regressive (AR) model using PMU data," in *2012 IEEE Power and Energy Conference at Illinois*, Feb 2012, pp. 1–5.

[10] A. G. Phadke, J. S. Thorp, R. F. Nuqui, and M. Zhou, "Recent developments in state estimation with phasor measurements," in *IEEE/PES Power Systems Conference and Exposition*, March 2009, pp. 1–7.

[11] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: CRC Press, 2004.

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

[13] A. Pal, "Effect of different load models on the three-sample based quadratic prediction algorithm," in *2015 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2015, pp. 1–5.

[14] K. D. Jones, A. Pal, and J. S. Thorp, "Methodology for performing synchrophasor data conditioning and validation," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1121–1130, May 2015.

[15] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, Sept 2016.

[16] Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "Evaluating power system vulnerability to false data injection attacks via scalable optimization," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov 2016, pp. 260–265.

[17] ——, "Vulnerability assessment of $N-1$ reliable power systems to false data injection attacks," 2019. [Online]. Available: https://arxiv.org/abs/1903.07781

[18] L. Zhang, A. Bose, A. Jampala, V. Madani, and J. Giri, "Design, testing, and implementation of a linear state estimator in a real power system," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1782–1789, July 2017.

[19] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[20] J. Liang, O. Kosut, and L. Sankar, "Cyber-attacks on AC state estimation: Unobservability and physical consequences," in *IEEE PES General Meeting*, Washington, DC, July 2014.

[21] A. Pinceti, O. Kosut, and L. Sankar, "Data-Driven Generation of Synthetic Load Datasets Preserving Spatio-Temporal Features," in *IEEE Power and Energy Society General Meeting*, 2019 Accepted.

[22] A. Pal, A. K. S. Vullikanti, and S. S. Ravi, "A PMU placement scheme considering realistic costs and modern trends in relaying," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 552–561, Jan 2017.

[23] "GE energy consulting: Positive Sequence Load Flow (PSLF)." [Online]. Available: https://www.geenergyconsulting.com/practice-area/software-products/pslf

[24] "IEEE standard for synchrophasor measurements for power systems – amendment 1: Modification of selected performance requirements," *IEEE Std C37.118.1a-2014 (Amendment to IEEE Std C37.118.1-2011)*, pp. 1–25, April 2014.