Machine Learning based False Data Injection In Smart Grid

Rehan Nawaz
Department of Electrical and Computer Engineering
Air University
Islamabad, Pakistan
Email: rehan.nawaz@mail.au.edu.pk

Muhammad Awais Shahid
Department of Electrical and Computer Engineering
Air University
Islamabad, Pakistan
Email: awais.shahid@mail.au.edu.pk

Ijaz Mansoor Qureshi
Department of Electrical and Computer Engineering
Air University
Islamabad, Pakistan
Email: imqureshi@mail.au.edu.pk

Muhammad Habib Mehmood
Department of Electrical and Computer Engineering
Air University
Islamabad, Pakistan
Email: habib@mail.au.edu.pk

***Abstract*—Smart grids have two-way power flow, two-way communication system, automated and distributed Energy Network. Communication is the main feature that makes a grid smart but that is the feature, which makes it vulnerable to cyber-attacks. Smart meters are installed to measure the real time data and after measurement this data is sent to control room. In the control room, all the control decisions are based on this received data. In communication lines, this data can be tampered or attacked to mislead the decision-making done in the control room. Load shading, power theft, and delay or blocking of data can be the purpose of an attack. State estimation, support vector machine, and observation of previous patterns are the techniques that can be used to detect the false data injected into the power system.In an effort to devise robust strategies against communication line. we put forth a novel attack strategy, which has not been dealt in the literature earlier. We inject false data into the power system by using Linear regression. We also show that none of the existing defence technique are able to detect the false data.**

***Index Terms*—Smart Grid, Cyber Attacks, Stealthy Attack, Machine Learning, SVM, Linear Regression**

I. Introduction

The Smart grid is a complete infrastructure that ensures the reliable and efficient flow of electricity. Due to increase in population and industries, demand of electricity has increased a lot. Generation of electricity is not a major issue but to manage these huge generated Megawatts and their distribution at the consumer end is a big challenge. A smart grid can provide all of the facility from generation to distribution efficiently. Unlike conventional grids, Smart grids have distributed generation, two way power flow and automation based self healed robust network. By using two way power-flow ability, an electric company can cover a huge area with fewer self generation. Transmission losses are also minimized. The property of self healing requires a complex and wide communication network. Sensors are installed to measure the real time data which can be magnitude of voltage, phase angle of voltage, real power injected to all the buses, forward transmission line real power, forward transmission line reactive power, reverse transmission line real power and reverse transmission line reactive power. On the base of that data decisions are taken to overcome faults and to make efficient flow of electricity possible. Some of the decision can be taken at the level of measurement but not all. Sensors communicate with each other and also to a control room as it is a hierarchical model. Control room is on the top in their hierarchy and has full control of taking any decision at any level. All of the communication is done through cloud. In control room all of the this data is monitored and cross checking of the billing, load shedding or other related decision can be taken.

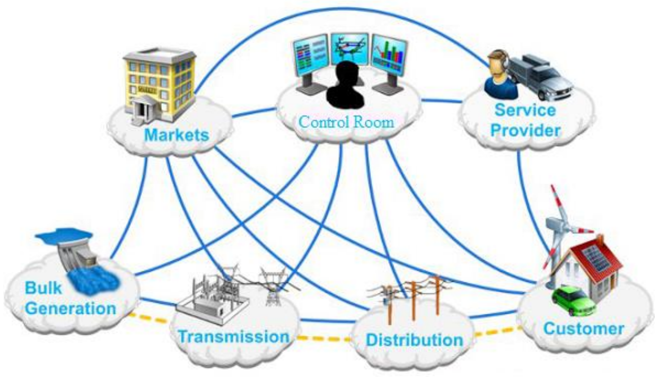

Fig. 1. Communication System of a Smart Grid showing transmission, distribution, customers as well as control room

In Fig. 1 the complex and vast communication system of a smart grid is shown. After measuring the real time data smart meters send their measured data to cloud. In cloud this data can be tempered to mislead the decision making, as all of the decision are taken on the base of that received data. Cyber-attacks in smart grid to mislead the decision-making in control room is known as false data injection. False Data is injected into the smart grid to achieve some purposes. Any person who in trying to temper the data is called as an attacker. These can be the purpose of an attack.

- **Power Theft:** To make power theft, attackers try to show less power consumption to control room as compare to the original one so, billing will be based on low power consumption.
- **Load Shedding:** To cause load shedding, attackers try to show more power consumption to the control room as compared to the original power. When an authenticated person in control room observes that power consumption is increased than my rated generation, they may switch off some load to avoid the heat up of generators and turbines.
- **Delay or blocking of data:** By adding delay or blocking in communication line attacker can make sure that control room has not prior knowledge of updated change in load.[1]

Measured Data from communication lines or cloud can be collected by hacking. This data is unlabelled and to make it labelled all the system connectivity must be known. sometimes all the power system network connectivity is not observable. Information about the unobservable part of the power system network can be collected with the help of pseudo measurements and data exchange(CIM) techniques.

$$M = h(x) + \eta \tag{1}$$

Here M is the Measurement Vector, $h(\cdot)$ is the system Jacobian matrix, which shows the non-linear relationship between the measurement vector and states and η is the Measurement Noise.

DC approximation is a technique widely used by researchers to approximate or linearise this non-linear system as it reduces complexity and computational cost but with very accurate results. DC assumptions are the voltage magnitude of all the buses equal to one, difference of phase angles of two connected buses is less than fifteen degrees, all the transmission lines have zero resistance and all the reactive powers are zero.

$$P_i = \sum_{k=1}^{N} B_{ik}(\varphi_i - \varphi_k) \qquad Q_i = 0$$
$$P_{ik} = -B_{ik}(\varphi_i - \varphi_k) \qquad Q_{ik} = 0$$

Where P_i is the Total Real power injected to bus i, Q_i is the total Reactive power injected to bus i, φ_i is the Phase angle of bus i, P_{ik} is the Real power flows from bus i to bus k, Q_{ik} is the Reactive power flows from bus i to bus k and B_{ik} is the Susceptance of transmission line that is between bus i and bus k. Now,

$$M = [P_1 \quad P_2 \quad P_3 \ldots P_m]^T$$
$$M = Hx + \eta \tag{2}$$

Where H is the Jacobian Matrix and x is the State Vector. Therefore, we only left with total real power injected to all the buses and forward transmission line powers. Any type of attack can be constructed by attacking in this reduced and simplified system in Equation (2) instead of system defined in Equation (1).

In this paper, we will construct an attack that will be undetectable by the state of art defence techniques. We will inject false data in the smart grid that will be able to Bypass BDD, SVM classifier. We also qualitatively show that our attack bypasses the defence strategies.

II. Literature Review

Any person trying to detect the false data is knows as defender. Relationship between attacker and defender is like cat and mouse play. Simple attacks can be constructed by just adding any non zero column in the measurement vector. There are some techniques that are used to detect the attacks.

A. Bad Data Detection

Bad data detection is a technique used to detect false data in power system[1, 2, 3, 17]. In Equation 2, Measurement vector *M* and Jacobian matrix *H* is known, and state vector *x* is unknown. As *m*>*n* so, we have an over determined system as number of unknowns are less than the number of equations. There are three techniques that can be used to estimate the states in such case minimum variance, maximum likelihood, and weighted least square (WLS). If measurement noise is Gaussian with zero mean, then all three techniques lead to the same estimator

$$\hat{x}_r = \left({H_r}^T W H_r\right)^{-1} {H_r}^T W M \tag{3}$$
$$R \ = \ diag\left\{{\sigma_1}^2, {\sigma_2}^2\ , {\sigma_3}^2 \ldots\ldots {\sigma_m}^2\right\} = Cov\left(\eta\right))$$
$$W = R^{-1}$$

where n is the Number of buses, m is the Number of Measurements, $\hat{x}_r$ is the Estimated state vector of dimension $(n-1)\times 1$, H_r is the Jacobian matrix without the column of the reference bus so having dimensions $m \times (n-1)$, W is the Diagonal covariance Matrix having weights of the meters on the diagonals and σ_i is the variance of i_{th} measurement. By adjusting the weights of the meters, we can rely more on the trust worthy measurements while estimating the states and if attack is detected then by re-adjusting the weights attacked measurements can be eliminated. Here, States are the phase angles of the voltage of all the buses. One bus is the reference bus. Reference bus always have zero phase angle that is why total number of states that should be estimated are one less than the total number of states. Residue is calculated after estimation of the states.

$$r = M - H\hat{x} \tag{4}$$

$r > \gamma$ Measurements are Attacked
$r < \gamma$ Measurements are Secured
Where r is the Residue and γ is the Maximum residue of the secured measurements

Under normal conditions x and $\hat{x}$ are very close to each other, Therefore Euclidean norm of the residue is less than a certain threshold and the measurements are marked as secured. Residue calculation in case of attack:

$$\begin{aligned} M_a &= M + F \\ r_a = M_a &- H\hat{x}_a \\ r_a = r + &\ F - Hc \end{aligned} \tag{5}$$

where M_a is the Attacked measurement vector, F is the False Data and r_a is the Residue in case of Attack. This is called as Bad data detection (BDD).

B. Stealthy Attack

Y. Liu proposed that if, Injected false data is $F = Hc$ then, $r_a = r$. Therefore, BDD fails to detect that attack. This attack is called as stealthy attack or undetectable attack [1, 2, 3, 17, 19]. To make a stealthy attack, Jacobian matrix must be known.

$$H = \left. \frac{\partial P(\varphi)}{\partial \varphi} \right|_{\varphi=0} \tag{6}$$

Different scenarios were discussed to construct Jacobian matrix [12, 13, 17, 18, 19]. There are four scenarios to construct the Jacobian matrix:

- when attacker was able to get all the susceptances then it was very easy to make Jacobian matrix[1, 2, 3].
- X. Liu proposed that a stealthy attack can be constructed by using only partial susceptances [10, 11].
- J. Kim [7] and Z.H [8] proposed that if an attacker was not able to get the susceptances but he is receiving the measurements then stealthy attack can be constructed by applying PCA on the measurement matrix over time.
- M. Esmalifalak[15], M. Rahman [4] and A. Anwar [5] proposed that attacker doesn't need the whole measurements to construct Jacobian matrix. If attacker has access over just partial measurements, still stealthy attack can be constructed. By using Independent component analysis, sparse optimization and Lagrange multiplier Jacobian matrix can be constructed.

Mohammad Esmalifalak used SVM classifier to detect the FDI and results are shown in Fig 2. By looking at the results it can be seen clearly that by using SVM classifier simple attacks as well as stealthy attacks both can be detected with accuracy of up to 99%.

Remaining paper is organised as follows. Proposed attack is given in section III. Simulations and the results are described in section IV, Discussion is given in section V and the final section concludes the paper.

III. PROPOSED ATTACK

Measured Data is collected over time, after receiving a significant amount of measurements then a measurement matrix over time is constructed. Then By using M_t(measurement matrix over time) attack vector is constructed with the help of linear regression and we name it as FDI using Linear regression.

$$M_t = \begin{bmatrix} P_{1,t} & P_{2,t} & P_{3,t} & \dots & P_{m,t} \end{bmatrix}$$

Where $t = 1, 2, 3, \dots, t_n$

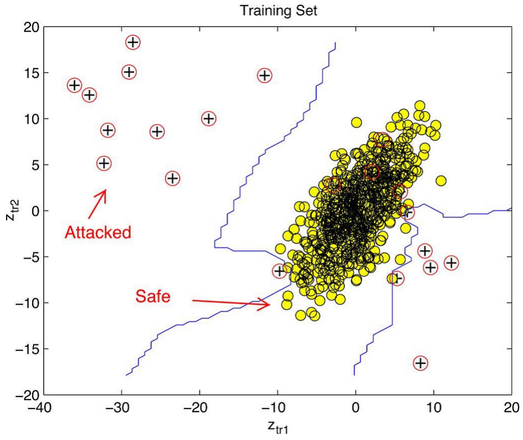

Fig. 2. SVM Classifier to detect the False Data in which there is a no linear boundary to separate attacked measurements from the safe measurements

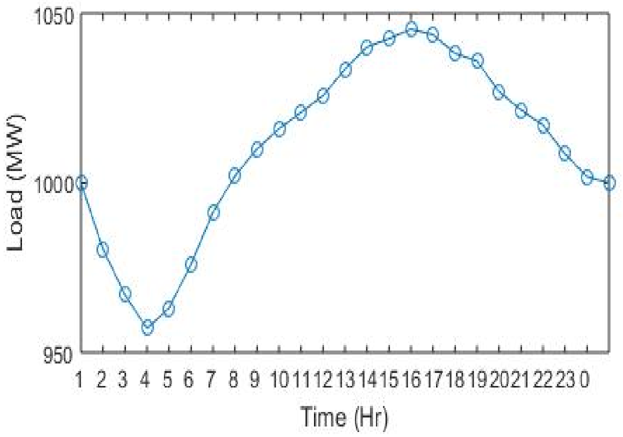

Fig. 3. Demand Curve For One Day in which Time in hours is given on independent axis and the total load of the system in Megawatts is given on dependent axis

A. FDI using Linear Regression

Our data was not normalized as some of the load are consuming more power and some feeders are consuming very less power.So, Mean normalization is applied on the data M_t. Then Linear regression is applied by taking one feature of M_t as input in which you want to attack and all other parameters as output one by one.

$$h_\theta(P_j) = \theta_{0(j,i)} + \theta_{1(j,i)} P_j \qquad i = 1, 2, 3, \dots, (m)$$

where P_j is the power injected to bus j, P_i is the power injected to bus i, $\theta_{0(j,i)}$ is the Learned best fit coefficient when input is P_j and output is P_i, $\theta_{1(j,i)}$ is the Learned θ_1 for input P_j and output P_i.

By minimizing the cost of linear regression iteratively

$$J = \frac{1}{2s} \sum_{k=1}^{s} (h(P_k) - P_k)^2 \tag{7}$$

Where s is the total number of Training examples and J is the cost that will be minimized at the best fit hypothesis.

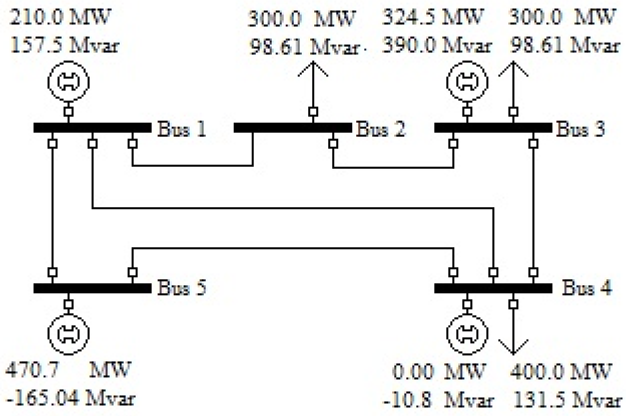

Fig. 4. Modified IEEE Case-5 Bus System having 5 buses 6 Transmission lines, 4 Generators as well as the Load

Best fit coefficients are obtained by minimising the cost and updating the learning coefficients(thetas) iteratively. After successful learning of all the thetas attack vector is constructed.

$$P_{ia} = \theta_{0(j,i)} + \theta_{1(j,i)} P_{ja} \qquad i = 1, 2, 3, \ldots\ldots, m$$

Now, P_{ja} is the power of j^{th} bus that we mainly want to attack. P_{ia} is the remaining i^{th} power required to complete the whole attack vector.

IV. SIMULATIONS

In simulations, a toolbox of MATLAB matpower 6.0 is used to generate the data. All the simulations are done on the Modified IEEE Case-5 bus system. In case-5 bus system, there are 5 buses and 6 transmission lines.

In Fig 4, there are three loads that are connected to bus 2, bus 3 and bus 5. Four generators are connected at bus-1, bus-3, bus-4 and bus-5. Demand curve of one day shown in Figure 3.

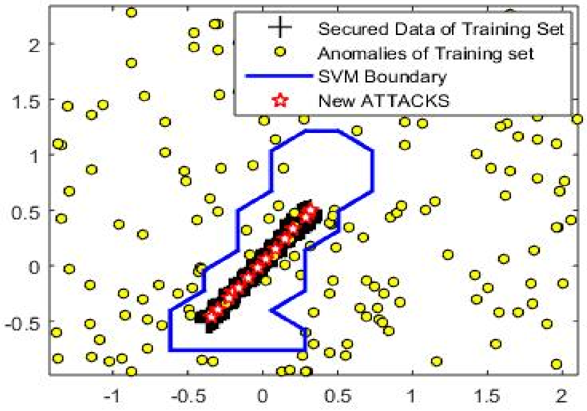

Fig. 5. Testing of Attack Vector using SVM in which Gaussian Kernel is applied to classify the anomalies and an accuracy of 99% is achieved

TABLE I
THETAS BY KEEPING P_2 AS INPUT AND P_i AS OUTPUT, P_i CAN BE ANY POWER FROM MEASUREMENT VECTOR

	θ_0	θ_1
$\theta_{(2,1)}$	210	0
$\theta_{(2,2)}$	0	1
$\theta_{(2,3)}$	-814.253	-2.796
$\theta_{(2,4)}$	-3.476	1.322
$\theta_{(2,5)}$	614.669	0.480
$\theta_{(2,12)}$	426.683	0.581
$\theta_{(2,14)}$	157.224	-0.102
$\theta_{(2,15)}$	-373.907	-0.479
$\theta_{(2,23)}$	423.066	1.574
$\theta_{(2,34)}$	-390.909	-1.22
$\theta_{(2,45)}$	-238.523	0

Measurement vector is

$$M = \begin{bmatrix} P_1 & P_2 & P_3 & P_4 & P_5 & P_{12} & P_{14} & P_{15} & P_{23} & P_{34} & P_{45} \end{bmatrix}^T$$

By Following the standardized demand curve of one day shown in Figure 3, data is generated for one year by keeping Load variance of 95% to 105%.

$$M_t = \begin{bmatrix} P_{1,1} & P_{2,1} & P_{3,1} & \ldots & P_{45,1} \\ P_{1,2} & P_{2,2} & P_{3,2} & \ldots & P_{45,2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ P_{1,8760} & P_{2,8760} & P_{3,8760} & \ldots & P_{45,8760} \end{bmatrix}$$

False data is injected by using linear regression. If we want to attack in $\mathbf{P_2}$, thetas are calculated by keeping $\mathbf{P_2}$ as input and all other powers as output one by one. shown in Figure 6

By using the value of thetas given in Table I and power P_{2a} in Equation 8, whole attack vector can be constructed

$$P_{ia} = \theta_{0(2,i)} + \theta_{1(2,i)} P_{2a} \tag{8}$$

Where $i = 1, 2, 3, \ldots\ldots, m$
This vector is injected into the power system. This vector is tested on the BDD, SVM and Violation of previous patterns. when BDD is applied,

$$\parallel r \parallel = 4.79, \quad \gamma = 4.85$$

Therefore $r < \gamma$
So, BDD has failed to detect this FDI.
SVM is applied on that vector after reducing the number of dimensions using PCA. Results are shown in Figure **??**SVM has completely failed to detect that attack as all the attacks lies inside the secured boundary of SVM.

So, FDI using Linear regression has been able to make an attack that can bypass BDD and SVM based defence mechanisms.

V. DISCUSSION

Thinking like an attacker and making such kind of algorithms, we can see how attackers can attack in future. Therefore, we can make our defence mechanism strong to detect false data. By controlling attacks in smart grid, we can

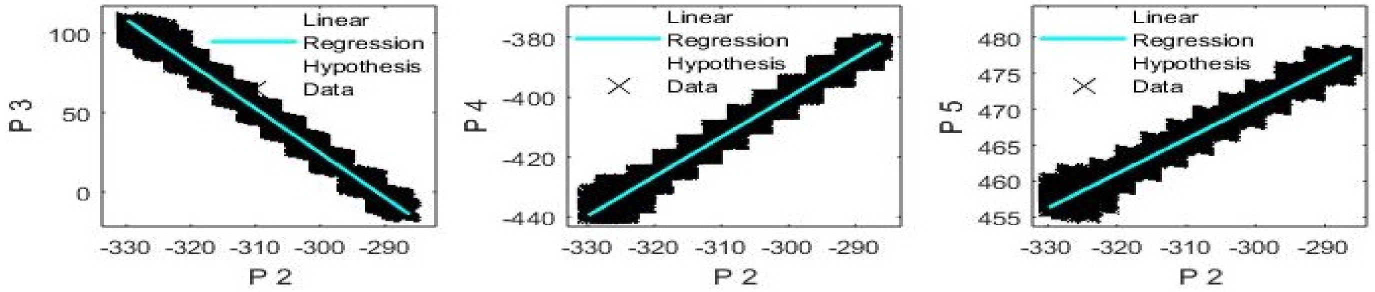

Fig. 6. Plotting of Training Data and Linear Regression Hypothesis in which the left most figure shows the training data and the linear regression hypothesis by using power injected to bus-2 and power injected to bus-3, middle figure shows the training data and the linear regression hypothesis by using power injected to bus-2 and power injected to bus-4 and the right most figure shows the training data and the linear regression hypothesis by using power injected to bus-2 and power injected to bus-5

make sure that control decisions in control room are based on the secured measurements and misleading can be avoided. Our data has non-linear dependencies. In future we can make a non-linear predictor to make an attack that will be more powerful.

VI. Conclusion

Communication is the main feature of smart grid and also the vulnerable one. By attacking in communication line any load shading power theft or any other purpose can be achieved. In FDI using Linear Regression, we assumed that our data is linear and applied linear regression. Attack vector is constructed and we showed that our attack vector has bypassed BDD and SVM.

References

[1] Y. Liu, P. Ning, and M. K. Reiter, ”False data injection attacks against state estimation in electric power grids” Proceedings of the 16th ACM Conference on Computer and Communications Security pages 21—32, 2009.

[2] Y. Liu, P. Ning, and M. K. Reiter, ”False data injection attacks against state estimation in electric power grids” ACM Trans. Information System Security 2011.

[3] L. Xie, Y. Mo, and B. Sinopoli, ”False data injection attacks in electricity markets” in IEEE International Conference on Smart Grid Communications, pages 226-–231, 2010.

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

[5] A. Anwar, A. Mahmood, and M. Pickering, ”Data-driven stealthy injection attacks on smart grid with incomplete measurements”, in Intelligence and Security Informatics, 2016.

[6] Mohammad Esmalifalak, Lanchao Liu, Nam Nguyen, Rong Zheng, and Zhu Han, ”Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid” in IEEE Systems Journal, 2014.

[7] J. Kim, L. Tong, and R. Thomas, ”Subspace methods for data attack on state estimation: A data driven approach” in IEEE Transactions on Signal Processing, 1102-–1114, 2015.

[8] Z.-H. Yu and W.-L. Chin. ”Blind false data injection attack using pca approximation method in smart grid” in IEEE Transactions on Smart Grid, 1219—1226, 2015.

[9] Jun Yan, Bo Tang, and Haibo He, ”Detection of False Data Attacks in Smart Grid with Supervised Learning” in International Joint Conference on Neural Networks, 2016.

[10] X. Liu and Z. Li, ”Local load redistribution attacks ” in power systems with incomplete network information IEEE Trans 1665–1676, 2014.

[11] X. Liu, Z. Bao, D. Lu and Z. Li, ”Modeling of local false data injection attacks with reduced requirement on network Information”, in IEEE Trans. Smart Grid, vol.6, no. 4, pp. 1686–1696, 2015.

[12] A. Ipakchi and F. Albuyeh, ”Grid of the future”, IEEE Power and Energy Magazine, pp. 52—62, 2009.

[13] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, ”Towards a framework for cyber-attack impact analysis of the electric smart grid”, in IEEE Smart Grid Comm, Gaithersburg, 2010.

[14] M. Esmalifalak, Z. Han, and L. Song, ”Effect of stealthy bad data injection on network congestion in market based power system”, in Proc. IEEE WCNC, Paris, France, pp. 2468-–2472, 2010.

[15] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, ”Stealth false data injection using independent component analysis in smart grid”, in Proc. IEEE 2nd Conf. Smart Grid Commun., Brussels, Belgium, pp. 244—248, 2011.

[16] M. Ozay, I. Esnaola, F. Yarman Vural, S. Kulkarni, and H. Poor, ”Machine learning methods for attack detection in the smart grid”, in Neural Networks and Learning Systems, IEEE Transactions, in press, 2015.

[17] Yi Huang, Mohammad Esmalifalak, Huy Nguyen, Rong Zheng, and Zhu Han, Husheng Li, Lingyang Song, ”Bad Data Injection in Smart Grid: Attack and Defense Mechanisms”, in IEEE Communications Magazine, 2013.

[18] Oliver Kosut, Liyan Jia, Robert J. Thomas, and Lang Tong, ”Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures”, In Smart Grid Communications, First IEEE International Conference on Smart Grid Communications, 2010.

[19] Kebina Manandhar, Xiaojun Cao, Fei Hu, Yao Liu, ”Detection of Faults and Attacks Including FalseData Injection Attack in Smart Grid Using Kalman Filter” in IEEE Transactions on Control of Network Systems 2014.

[20] Meng Wu, Le Xie, ”Online Detection of False Data Injection Attacks to Synchrophasor Measurements: A Data-Driven Approach” in 50th Hawaii International Conference on System Sciences, 2017.

[21] Mete Ozay, Iñaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor, ”Machine Learning Methods for Attack Detection in the Smart Grid” in IEEE Transaction on Neural Networks

and Learning Systems, 2016.

[22] Yacine Chakhchoukh, Song Liu, Masashi Sugiyama, and Hideaki Ishii, ”Statistical Outlier Detection for Diagnosis of Cyber Attacks in Power State Estimation” in Power and Energy Society General Meeting, 2016.

[23] Panos M. Pardalos, Vijay Pappu and Marco Carvalho ”Optimization and Security Challenges in Smart Power Grids” ”Smart Grid Tamper Detection Using Learned Event Patterns” pp. 99–115 2013

[24] Michael G. Kallitsis, George Michailidis and Samir Tout ”Correlative Monitoring for Detection of False Data Injection Attacks in Smart Grids” in Smart Grid Communications, IEEE International Conference, 2015.