Detecting Data Tampering in Synchrophasors using Power Flow Entropy

Anum Rashid‡, Muhammad Naveed Aman†, Mukhtar Ullah‡, and Biplab Sikdar†

‡Department of Electrical Engineering
National University of Computer & Emerging Sciences
Pakistan

†Department of Electrical & Computer Engineering
National University of Singapore
Singapore

***Abstract*—The continuous increase in demand for electric power has resulted in extremely complex power grids. The correct operation of these grids depends on the computerized control and monitoring using a communication network. These modern power grids are equipped with phasor measurement units which play a key role in providing crucial data for the state estimator of an energy management system. The integration of a communication network with the power grid makes it vulnerable to cyber attacks in the form of data tampering. These attacks can disrupt the operation of the state estimator resulting in significant financial as well as infrastructure damage. To solve this issue, this paper proposes a technique to detect tampered data in synchrophasors using the system entropy of a power network. The results show that the proposed technique can be used as an effective tool to detect attacks on synchrophasors.**

I. Introduction

Power grids have experienced continuous expansion over the decades due to the increased demand of consumers and growth if industries. They are spread over large geographical areas and involve multiple operations that need to be monitored and controlled. To maintain generation and facilitate the uninterrupted supply of power to users, modern power systems rely on computer and communication networks. Sensing, control, scheduling, dispatch and billing need a tightly integrated cyber infrastructure. One of the most versatile measurement devices is the Phasor Measurement Unit (PMU) that plays a pivotal role in monitoring and consequent control of a power grid. A synchrophasor is the representation of the complex phasor of an alternating current (AC) power system at the nominal system frequency synchronized to UTC (coordinated universal time) [1]. PMUs measure highly accurate synchrophasors for voltage and current at different buses of the electric power grid. The sampling rates of PMUs are usually sub-multiples of the power-line frequency such as 10, 25 or 50 samples per second for 50Hz systems. Real time monitoring of power grids is a critical process, and creates a mathematical representation of the current conditions of an interconnected power system using PMU measurements. This key process to build the real-time model for the network in energy management systems (EMS) is known as state estimation.

978-1-5386-4291-7/18/$31.00

The main functions of a state estimator include observability analysis, state estimation and bad data processing. The estimator communicates the performance and status of the system to the control center where decisions are taken on the basis of different situations that the network undergoes. The integration of power systems with communication networks make them an attractive target for malicious data injection attacks. As a result, cyber security of the current power grids has become a major concern for the operators. State estimation is a well-established research area, and multiple techniques have been introduced to tackle bad measurements. Most of the conventional approaches are based on residual tests that detect gross errors or noises. However, they are unable to respond if multiple bad measurements are interacting or if the data is intentionally manipulated. Malicious data tampering in synchrophasors can result in significant financial damage as well as damage to civil infrastructure. The authors of [2], [3] discuss the consequences of cyber attacks on power grids. These include increased robustness/resiliency losses, sub-optimal economic dispatch, and blackouts resulting from cascading failures, among others. To solve this issue, in this paper we propose a method based on entropy of the power system measurements.

The concept of entropy was introduced by Rudolf Clausius in 1865 as a measure of the amount of energy in a thermodynamic system [4]. However, later in 1948, it was given a new meaning by Claude Shannon [5]. He defined it as a measure of uncertainty in the context of the communication theory. Since information can reduce uncertainty, the entropy can also be adopted as a measurement of information provided by the discrete probability distributions [4]. Building upon this concept of entropy, this paper describes a method for the detection of malicious data attacks on synchrophasor networks.

The rest of the paper is organized as follows. In Section II we discuss the related work. We present the network model, assumptions, and threat model in Section III. Section IV presents the proposed model for detecting data tampering in synchrophasor networks. while Section V presents the simulation results of the proposed technique. Finally Section VI concludes the paper.

II. Related Work

The advent of smart grids has made the power system more vulnerable to various cyber-attacks such as data tampering. Smart grids form an attractive target for malicious attacks because of the involvement of critical infrastructure. In the context of data tampering attacks, different research works have proposed multiple techniques for bad data detection. Early power system researchers realized and observed that a bad measurement usually led to a large normalized measurement residual. After the presence of bad measurements is detected, they mark the measurement with the largest normalized residual as the suspect and remove it. Later on, it was found that this largest normalized residual criterion could detect only independent data called non-interacting measurements. Recently, the focus has been on the improvement of robustness using PMUs [6]-[8]. For example, the authors of [8] used PMUs to transform critical measurements into redundant ones so that the presence of bad data can be detected by residual testing. The approaches targeting arbitrary interacting bad data seem to be better at detecting data tampering attacks since such measurements can also be considered arbitrary [9]-[11]. However, despite variations in these approaches, all of them use the same basic method of residual testing. Although researchers have realized the vulnerability of conventional approaches, the study of false data injection attacks is fairly recent. The authors of [12] addressed cyber-attacks on power system state estimation for the first time and showed that by exploiting the knowledge of power system topology, an adversary can introduce arbitrary errors into the state of the system by deceiving a bad data detector. The minimum number of meters required to launch an unobservable attack was first introduced by the authors of [13] as a security index. In [14], the authors proposed a technique based on the security index for categorizing observable and unobservable attacks.

In another work by [15], the problem of defending against data tampering attacks from the perspective of an operator has been investigated. The authors show a minimum set of measurements that needs to be protected in order to ensure observability of the system. Similarly, the authors of [16] propose a greedy algorithm to select a subset of measurements to be protected. Many approaches and applications also use PMUs in order to make the system completely observable. The authors of [17] conducted the analysis of power system observability with PMUs. Placing the PMUs optimally can help maximize the redundancy of measurements thus making the system observable. This placement of PMUs in the power system was further explored in [18] and [19] to enhance power system state estimation, which in turn improves the ability to defend against bad data injection.

In the domain of cyber security, entropy has been used to detect distributed denial of service (DDOS) attacks or to detect anomalies in the Internet traffic [20], [21]. Entropy-based approaches provide the advantage of fine-grained insights for anomaly detection as compared to traditional traffic volume analysis [22]. Similarly, another work by [23] uses the entropy of power measurements to detect theft for the advanced metering infrastructure in smart grids. Common to all these entropy based techniques is that they compare the entropy of two multidimensional data sets to detect attacks. However, given the large size of traffic or power data and the number of variables involved, these techniques result in long convergence times. In this paper we employ power flow entropy which uses a graph representation of the power network to calculate the entropy at every node. The proposed solution uses entropy of one dimensional measurements, i.e., power flow, resulting in a light weight mechanism to detect data tampering attacks on a power grid.

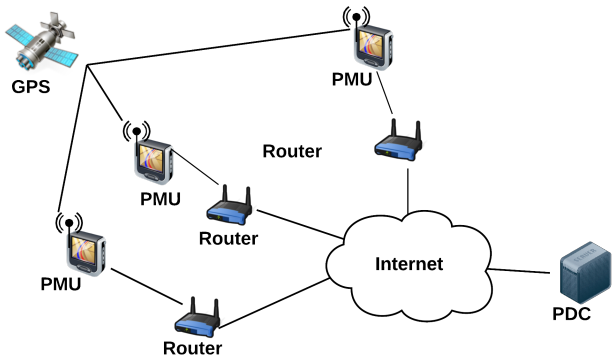

Fig. 1. Network model.

Currently, most of the proposed techniques for detecting data manipulation attacks are based on residual testing or strategic placement of PMUs to protect the system from cyber-attacks. However, this assumption of securing PMUs is not enough in power systems that are spread over a wide area. Therefore, the proposed technique in this paper addresses the problem without making such strong assumptions.

III. Network Model, Assumptions, and Threat Model

A. Network Model

Figure 1 describes our network model. In this model PMUs are connected to the PDC through border routers relaying data over the Internet. The PMUs obtain synchronized clock information through GPS satellites.

B. Assumptions

We make the following assumptions regarding the network model and proposed protocol:

a. The IEEE C37.118.2 [1] packet format is assumed. Table I shows the various fields and their sizes for a typical PMU packet.
b. PMUs unicast their data to a single PDC using the UDP-only method for communication. The encapsulation/decapsulation is done using the normal TCP/IP protocol suite.
c. The adversary can eavesdrop on all the traffic, maliciously modify/inject packets, replay previous packets, and imitate

TABLE I
DATA PACKET FORMAT FOR A PMU [1]

No.	Field	Size (bytes)
1	SYNC	2
2	FRAMESIZE	2
3	IDCODE	2
4	SOC	4
5	FRASEC	4
6	STAT	2
7	PHASORS	4/8 per phasor
8	FREQ	2/4
9	DFREQ	2/4
10	ANALOG	2/4 per value
11	DIGITAL	2 per value
12	CHK	2

other nodes in the network. The PMUs and other network entities including routers and communication links may be compromised. However, the PDC is considered the secure and trusted party.

d. The PMUs connected to the generator buses are assumed to be secure and cannot be tampered with by an adversary.
e. The adversary is capable of breaking the encryption of PMU packets.

C. Threat Model

As a power network is distributed over a large area, multiple buses are present that contribute to the data collected at the PDC. The attacker may manipulate the data of these buses in order to change the state of power system so that false data is communicated to the control center. The PMU data generated traverses through a multi-hop network and reaches the control center through different routes. The attacker is assumed to have introduced an attack vector in the measurements of state estimators installed on buses. He/she aims to cause the maximum possible damage to the system without being detected. Large deviation from the true state can lead to erroneous actions of greater consequence. The objective of this paper is to detect tampered data accurately in order to secure the power grid from damage.

IV. PROPOSED TECHNIQUE TO DETECT DATA TAMPERING USING ENTROPY

In this section we describe the proposed mechanism for detecting data tampering in synchrophasor networks.

Consider the AC power flow equations for a power system, given as follows [24]:

$$P_k = \sum_{j=1}^{N_B} |V_k||V_j| \left(G_{kj}\cos(\theta_k - \theta_j) + B_{kj}\sin(\theta_k - \theta_j)\right) \quad (1)$$

$$Q_k = \sum_{j=1}^{N_B} |V_k||V_j| \left(G_{kj}\sin(\theta_k - \theta_j) - B_{kj}\cos(\theta_k - \theta_j)\right) \quad (2)$$

where P_k and Q_k are the real and reactive powers of bus k, N_B is the total number of buses, V_k and V_j are the voltage magnitudes at buses k and j, respectively, G_{kj} and B_{kj} are the real and imaginary parts of the kj-th element in the bus admittance matrix, and θ_k and θ_j denote the voltage phase at bus k and j, respectively.

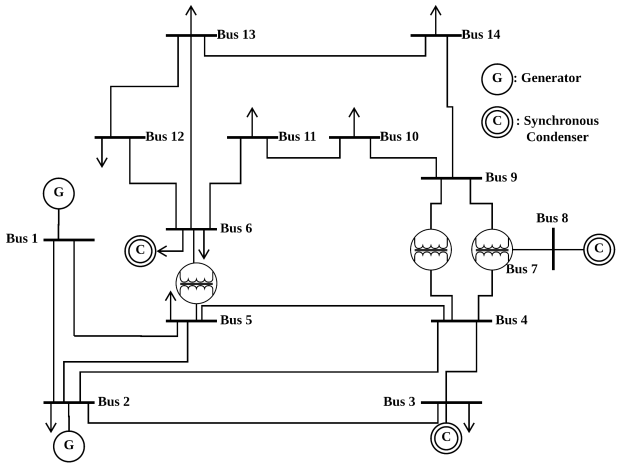

Fig. 2. IEEE 14-bus test system.

In this paper, we model a power grid as a complex network of interconnected generation, transmission, and distribution elements. Figure 2 shows the single-line diagram while Figure 3 shows the graph representation of the IEEE 14 bus test system. The buses are labeled with the corresponding bus number, the generators and synchronous condensers are symbolized as G and C (encircled), and the arrow heads represent loads connected to different buses. Generators provide power for the grid while a synchronous condenser is used to generate or absorb reactive power through a voltage regulator needed to adjust the grids voltage or improve the power factor. Unlike capacitor banks, the reactive power from the synchronous condenser can be adjusted continuously. In the graph representation the substations, transformers, and generation, transmission, and distributions buses are represented by nodes. Similarly, the transmission lines make up the links or arcs connecting the nodes. We observe that the AC power flow Equations (1) and (2) are non-linear equations used to model both the active and reactive powers. However, AC power flow analysis introduces long convergence times due to the inherent complexity [26]. Therefore, we use DC power flow analysis and introduce the following assumptions [24]

1) The resistance of transmission circuits is significantly less that the reactance, i.e., we can neglect the G_{kj} terms in Equations (1) and (2).
2) Angular separation across any transmission circuit is very small, i.e., $\sin(\theta_k - \theta_j) \approx (\theta_k - \theta_j)$.
3) Voltage magnitudes in a per-unit system are very close to 1.0, i.e., $|V_k| \approx |V_j| \approx 1.0$.
4) It is reasonable to neglect reactive power flows when assessing circuit overload.

Applying these assumptions we get the simplified equation for

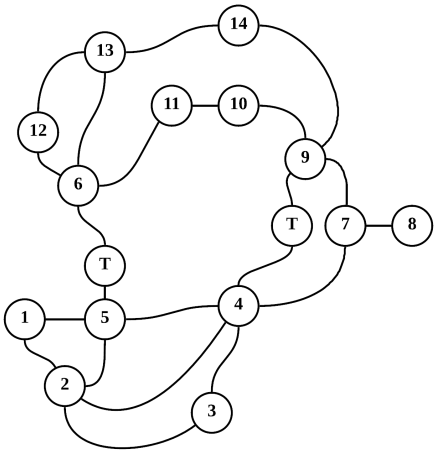

Fig. 3. Graph representation of the IEEE 14-bus test system.

active power flow as follows:

$$P_k = \sum_{j=1}^{N_B} B_{kj}(\theta_k - \theta_j). \tag{3}$$

We can re-write Equation (3) in the form of matrices as follows:

$$\boldsymbol{P} = \boldsymbol{B\theta} \tag{4}$$

where $\boldsymbol{P}$ represents the vector of real power injections, $\boldsymbol{\theta}$ represents the vector of voltage angles at each node, and $\boldsymbol{B}$ is the bus susceptance matrix with $B_{kj} = -\frac{1}{x_{kj}}$ and $B_{kk} = \sum_{j=1}^{L_k} -B_{kj}$ (x_{kj} is the reactance of the transmission line l_{kj} and L_k is the out degree of node k). Thus, we can use DC power flow analysis to calculate the nodal voltage angles as follows:

$$\boldsymbol{\theta} = \boldsymbol{B}^{-1}\boldsymbol{P}. \tag{5}$$

The entropy of a system is defined as follows [4]:

$$H = -\sum_{i=1}^{N} p_i \log p_i \tag{6}$$

where p_i is the distribution value or probability of occupying a state i out of a total of N states. Translating Equation (6) to the entropy of a node in an electrical power system we get [27]:

$$E_k = -\sum_{i=1}^{L_k} p_{ki} \log p_{ki} \tag{7}$$

where p_{ki} is the normalized active power flow injected into the transmission line l_{ki} connecting node k to node i and is given by:

$$p_{ki} = \frac{f_{ki}}{\sum_{j=1}^{L_k} f_{kj}} \tag{8}$$

where f_{kj} is the active power flow injected into line j from node k. For example, Figure 4 shows a node A with an outdegree of 3. In this case, $p_{AB} = \frac{30}{100} = 0.3$, similarly,

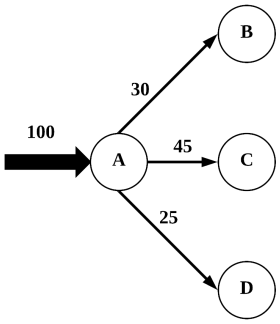

Fig. 4. Example of a node with outdegree 3.

$p_{AC} = 0.45$ and $p_{AD} = 0.25$. Therefore, the entropy for node A is given by:

$$\begin{aligned} E_A &= -p_{AB}\log p_{AB} - p_{AC}\log p_{AC} - p_{AD}\log p_{AD} \\ &= -0.3\ \log\ 0.3 - 0.45\ \log\ 0.45 - 0.25\ \log\ 0.25 \\ &= 0.4634. \end{aligned} \tag{9}$$

Note that the power flow values f_{kj} through each line can be calculated using the right hand side of Equation (3), i.e.,

$$f_{kj} = B_{kj}(\theta_k - \theta_j). \tag{10}$$

Thus, after solving Equation (5) for voltage angles at all the nodes, we can find the power flows, i.e., f_{kj} for all the lines. Thus, we can obtain the entropy for the entire system as follows:

$$H = -\sum_{k=1}^{N_B}\sum_{i=1}^{L_k} p_{ki}\ \log\ p_{ki}. \tag{11}$$

Let us assume that the attacker attacks the power flow measurements on a subset of the lines denoted by S_a. Then Equation (8) can be re-written for a system under attack as follows:

$$p_{ki} = \frac{f_{ki}(1 - \mathbb{1}_{S_a}(i)) + f_{ki}\mathbb{1}_{S_a}(i)L_A}{\sum_{j=1}^{n_{B_i}} f_{kj}(1 - \mathbb{1}_{S_a}(j)) + f_{kj}\mathbb{1}_{S_a}(j)L_A} \tag{12}$$

where L_A denotes the attack vector and $\mathbb{1}_{S_a}$ denotes the indicator function given as follows:

$$\mathbb{1}_{S_a}(i) = \begin{cases} 1 & \text{if } i \in S_a \\ 0 & \text{otherwise} \end{cases}. \tag{13}$$

When a fault occurs, the load of the failing line is distributed among the rest of the system. This is equivalent to multiplying the power flow value of each of the remaining functioning lines with a loading factor. Thus, during a fault in the absence of an attack, $p_{l_{ki}}$ is given as follows:

$$\begin{aligned} p_{ki} &= \frac{L_F \times f_{ki}}{L_F \times \sum_{j=1}^{n_{B_i}} f_{kj}} \\ &\approx \frac{f_{ki}}{\sum_{j=1}^{n_{B_i}} f_{kj}} \end{aligned} \tag{14}$$

where L_F represents the loading factor during a fault. Comparing Equations (12) and (14) shows that the system entropy in Equation (11) may change negligibly during normal or fault conditions. However, if at least one bus is kept safe from the attacker, H will change when the system is under an attack. This shows that the proposed data tampering detection technique will work as long as one of the system buses is protected. Therefore, the entropy is monitored for a given system, and any change in the entropy results in sounding an alarm and alerting the operator for suspicious activity.

Algorithm 1 shows the proposed data tampering detection mechanism. In this algorithm $z_1, z_2, \cdots, z_{n_B}$ are the active power injections obtained through the system state estimator [25], H_n is the most recent value of system entropy, and $\boldsymbol{n_{B_i}}$ is a vector containing the information of the number of lines connected to each node. This algorithm uses a threshold of 0.3% to check if the system is under attack, i.e., if the system entropy changes by more than 0.3% as compared to the previous value recorded then the system will raise an alarm indicating a possible attack. The value of 0.3% was selected after simulating the system under different attack scenarios. We observed that if a fault occurs, then the entropy value usually changes by less than 0.1%. However, under an attack the entropy value changes by at least 0.3%.

Input : $z_1, z_2, \cdots, z_{n_B}$,$H_n$, $\boldsymbol{n_{B_i}}$
Output: Sound Alarm if Attack Detected
while *Session Active* **do**
  `// Apply DC power flow to compute power flow values through each line`
  $\boldsymbol{f}$ = DC_Power_Flow($z_1, z_2, \cdots, z_{n_B}$)
  `// Calculate System Entropy using Equation (11)`
  H_i = Entropy($\boldsymbol{f}$,$\boldsymbol{n_{B_i}}$)
  if $\frac{|H_n - H_i|}{H_n} \times 100 > 0.3$ **then**
    Sound Alarm
    else
      `// Update the current entropy value`
      $H_n = H_i$
    end
  end
end

Algorithm 1: Proposed Data Tampering Detection Algorithm

V. Simulation Results

In this section we present the results after simulating the proposed data tampering mechanism in MATLAB using the matpower toolbox [29].

The proposed mechanism was simulated on the IEEE 14 bus system shown in Figure 2. The data required for the calculation and analysis of system entropy includes the information of power flows of each individual bus. We consider three scenarios for our analysis. In the first scenario we study the entropy of the system under normal load conditions, and in the second scenario we consider a system under stress, i.e., we assume a fault has occurred causing the system to be overloaded. This scenario is created by applying different loading factors ranging from 1.2 to 1.6 to our test system. Finally, in the third scenario we consider the case when the attacker is introducing various attack vectors into the system.

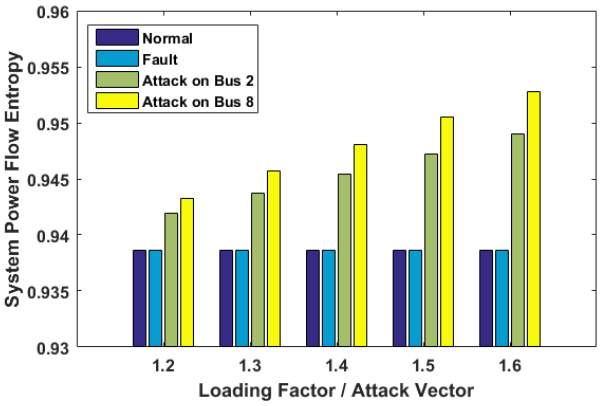

Fig. 5. System entropy.

Figure 5 shows the entropy values under the three scenarios. When a fault occurs the power system enters a contingency condition, i.e., the system is stressed and overloaded. To get the same effect in our simulations, we simulated the test system for different values of the loading factor ranging from 1.2 to 1.6. Figure 5 shows the value of entropy corresponding to each loading factor. As expected the entropy value during normal operation and fault remains approximately the same. However, Figure 5 shows that when the attacker introduces an attack vector to the state vector of bus 2 or bus 8, the system entropy is significantly increased as compared to the normal condition or the contingency conditions.

Different schemes for detection of data modification attacks have been introduced in existing literature with multiple assumptions. In order to analyze the effectiveness of the proposed scheme, a comparison is done with a recent technique that is based on calculation of line impedance. The authors of [28] use the ratio of impedance magnitudes of transmission lines in order to identify an attack. The attack on the system is modeled by changing voltage or current magnitudes and phase angles from both the ends of a transmission line. Under normal system conditions, the ratio remains 1 while if there is a sudden or sustained change in the ratio, it is considered as attack. The same scheme was applied to our attack scenario where bus 2 is considered to be under attack and accordingly overloaded with a loading factor of 1.2. The simulation results for the impedance ratio of bus 2 are shown in Figure 6. Figure 6 shows that the impedance ratio of bus 2 remains unchanged during this type of attacks. This shows that the technique proposed in this paper is effective in detecting data tampering attacking in synchrophasor networks and can even detect attacks on a single bus.

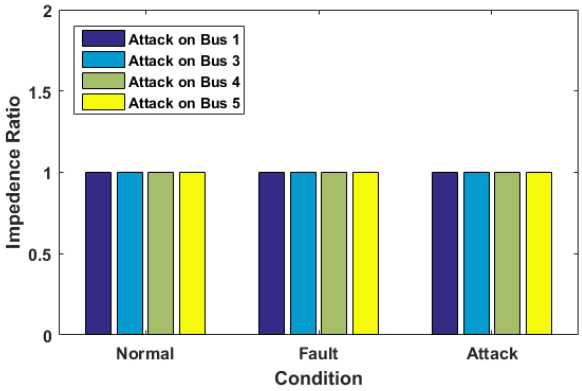

Fig. 6. Impedence Ratio of Bus 2 [28].

VI. Conclusions

This paper presented a technique to detect data tampering in synchrophasor networks. The proposed technique uses the graph representation of a power network and calculates the system entropy. An attack can be detected by monitoring any change in the system entropy value. The results show that the proposed technique can successfully identify attacks on the IEEE 14 bus test system.

References

[1] *Synchrophasor Data Transfer for Power Systems,* IEEE Standard C37.118.2, 2011.

[2] A. Giani, R. Bent, M. Hinrichs, M. McQueen, and K. Poolla, "Metrics for assessment of smart grid data integrity attacks," *IEEE Power and Energy Society General Meeting,* pp.1-8, July 2012.

[3] Y. Deng, and S. Shukla. "Vulnerabilities and Countermeasures: A Survey on the Cyber Security Issues in the Transmission Subsystem of a Smart Grid," *J. Cyber Security and Mobility,* vol. 1, no. 2, pp. 251-276, 2012.

[4] Li, Zhimin et. al., "Applications of Entropy Principles in Power Systems: A Survey". *Proc. of the IEEE Power Engineering Society Transmission and Distribution Conference,* 2005.

[5] C. E. Shannon, "A Mathematical Theory of Communication". *Bell System Technical Journal.*, vol. 27, no. 3, pp. 379423, JulyOctober 1948.

[6] Zhao, L. and Abur, A., "Multi area state estimation using synchronized phasor measurements." *IEEE Trans. Power Syst.* 20, 2, 611617,2005.

[7] Chen, J. and Abur, A., "Placement of PMUs to enable bad data detection in state estimation". *IEEE Trans. Power Syst.* 21, 4, 16081615,2006.

[8] Zhu, J. and Abur, A. "Bad data identification when using phasor measurements". *In Proceedings of the IEEE Power Tech Conference.*, Los Alamitos, CA, 16761681, 2007.

[9] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Transactions on Power Apparatus and Systems,* vol. 94, no.2, pp. 329-337, March 1975.

[14] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on the smart grid," *IEEE Transactions on Smart Grid,* vol. 2, no. 4, pp.645-658, 2011.

[10] Gastoni, S., Granelli, G. P., and Montagna, M., "Multiple bad data processing by genetic algorithms". *In Proceedings of the IEEE Power Tech Conference.*, Los Alamitos, CA, 16,2003.

[11] Asada, E. N. et. al., "Identifying multiple interacting bad data in power system state estimation". *In Proceedings of the IEEE Power Engineering Society General Meeting.* Los Alamitos, CA, 571577, 2005.

[12] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Proceedings of ACM Conference on Computer and Communications Security,* pp.21-32, Chicago, IL, November 2009.

[13] H. Sandberg, A. Teixeira, and K. Johansson, "On Security Indices for State Estimators in Power Networks," *First Workshop on Secure Control Systems,* Stockholm, Sweden, 2010.

[15] R. B. Bobba, K. M. Rogers, Q. Wang, and H. Khurana, "Detecting false data injection attacks on DC state estimation," *Proceedings of the First Workshop on Secure Control Systems,* 2010.

[16] T. T. Kim, and H. V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," *IEEE Transactions on Smart Grid,* vol.2, no.2, pp.326,333, June 2011.

[17] B. Xu and A. Abur, "Observability analysis and measurement placement for systems with PMUS," *in Proc. IEEE PES Power Systems Conf. Exposition*, New York, NY, Oct. 2004, vol. 2, pp. 943946.

[18] F. Chen et. al., "State estimation model and algorithm including PMU," *in Proc. 3rd Int. Conf. Electric Utility Deregulation and Restructuring and Power Technol. (DRPT 2008),* Nanjing, China, Apr. 2008, pp. 10971102.

[19] M. J. Rice and G. T. Heydt, "Power systems state estimation accuracy enhancement through the use of PMU measurements," *in Proc. PES TD 2005/2006*, Dallas, TX, May 2006, pp. 161165.

[20] S. Yu and W. Zhou, "Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks," *in Proc. 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom),* Hong Kong, 2008, pp. 566-571.

[21] X. Qin, T. Xu and C. Wang, "DDoS Attack Detection Using Flow Entropy and Clustering Technique," *in Proc. 2015 11th International Conference on Computational Intelligence and Security (CIS),* Shenzhen, 2015, pp. 412-415.

[22] G. Nychis et al., "An empirical evaluation of entropy-based traffic anomaly detection," *in Proc. 8th ACM SIGCOMM conference on Internet measurement,* Vouliagmeni, Greece, October 2008, pp. 151-156.

[23] S. K. Singh, R. Bose, and A. Joshi, "Entropy-based electricity theft detection in AMI network," *IET Cyber-Physical Systems: Theory & Applications*, 2017, Digital Library, http://digital-library.theiet.org/content/journals/10.1049/iet-cps.2017.0063.

[24] A. P. Meliopoulos, *Power System Modeling, Analysis, and Control*, Marcel Dekker Inc., 2004.

[25] M. Baran, and A. Abur, "Power System State Estimation," *Wiley Encyclopedia of Electrical and Electronics Engineering,* 1999.

[26] Z. J. Bao et al., "Analysis of cascading failure in electric grid based on power flow entropy", *Physics Letters A*, vol. 373, pp. 3032-3040, 2009.

[27] Y. Koc et al., "An entropy-based metric to quantify the robustness of power grids against cascading failures", *Safety Science*, vol. 59, pp. 126-134, November 2013.

[28] Pal, Seemita et. al., "Detecting malicious manipulation of synchrophasor data". *IEEE Smart Grid Communications (SmartGridComm), 2015*.

[29] 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*, vol. 26, no. 1, pp. 12-19, Feb. 2011.