Detecting Malicious Manipulation of Synchrophasor Data

Seemita Pal, Biplab Sikdar and Joe H. Chow
Department of Electrical, Computer and Systems Engineering
Rensselaer Polytechnic Institute, Troy, NY, 12180

***Abstract*—The electrical grid is one of the critical infrastructures of any country whose importance makes them an attractive target for malicious cyber attacks. This paper considers the particular case of data modification attacks in smart grids, where the data generated by Phasor Measurement Units (PMUs) is modified by the adversary in order to introduce errors in the monitoring and control applications that rely on PMU data. The proposed methodology is based on evaluating the equivalent impedance of a transmission line from buses at its either end. The deviations in the magnitude and angle of the equivalent impedances in the presence of a data modification attack are used to detect the attack. Extensive simulations using real PMU data are used to verify the accuracy of the proposed detection mechanism.**

***Index Terms*—Cyber-security, smart grid, synchrophasor network**

I. Introduction

A synchrophasor or a Phasor Measurement Unit is one of the most versatile measurement devices in a power grid and plays a pivotal role in the monitoring and consequent control of the power systems. It provides highly-accurate, real-time measurements of voltage and current phasors from the nodes where they are installed. The measurements are generated at a rate of 30, 50 or 60 samples per second with accuracy better than 1% and precision-timestamped based on a common time-source of the Global Positioning System (GPS). The data from individual PMUs is transferred over a communication network and collected at a Phasor Data Concentrator (PDC) and fed to the control center, where grid-wide time-aligned PMU data are processed to create a single snapshot of the state of the entire system. Thus, the continuous stream of PMU data helps to determine the transient nature of the system and provides dynamic visibility. PMU data is increasingly being used for various power system applications such as state-estimation, real-time congestion management, post-disturbance analysis, economic dispatch, adaptive protection as well as real-time system control and operation.

Given the importance of PMUs in the monitoring, control and operation of a power system and the time-critical nature of the generated data, they are particularly attractive targets for malicious attackers intending to disrupt normal grid operations. Since the PMUs are usually spread over a wide geographical area, the Internet is generally used to transfer these data to the PDCs. Given the public nature of the Internet, a variety of cyber-attacks are thus possible on the data as it transits from the PMUs to the PDCs and the control center. As the power grid is one of the critical infrastructures of any nation, the security and smooth operation of the grid is of great importance.

The data generated by the PMUs is vulnerable to a number of cyber-attacks as it traverses the network to the PDC. In the attack of interest in this paper, we consider the situation where the adversary may exploit network vulnerabilities or cyber-physical dependencies to compromise PMUs, PDCs or the intermediate routers in the network and modify the measurement data in order to bias the estimated system states. Consequently, the attacker may be able to obscure impending problems from the utilities, or mislead the control center into taking erroneous control actions which may prove to be harmful for the grid. For example, it may lead to damage of power system equipment, uneconomic dispatch choices, congestion, or even a cascading sequence of events resulting in blackout. At the very least, it can create a distrust of the system states, thereby hampering system observability. Therefore, development of mechanisms which can perform quick detection of data manipulation attacks is a necessity. Also, if the detection schemes can performed in a distributed manner at the various PDCs, the amount of data handled at any point of time will be lower and detection will be considerably quicker.

This paper addresses the problem of detecting data manipulation attacks on PMU data by using the estimates of the transmission line equivalent impedance. To detect the presence of modified data, at each of the PDCs, the PMU data from both sides of a line are used to estimate the equivalent impedance. The detection mechanism then uses the changes in the equivalent impedance magnitude and angles in the presence of data manipulation attacks as an indicators of the attack. Statistically significant variations between functions based on impedance magnitudes and angles, as calculated from the two end buses of a line are taken as an indication of data manipulation. The proposed detection mechanism is verified using extensive simulations.

The rest of this paper is organized as follow. Section II, provides an overview of the related work, data modification attacks and our system model. Section III presents the proposed mechanism for detecting data modification attacks and Section IV presents the simulation results. Finally, Section V concludes the paper.

II. Related Work and Assumptions

This section presents brief review of the literature on traditional bad data detection schemes as well as false data injection attack detection. We also present the assumptions and system model used for our analysis.

A. Related Work

One of the key functions of the static state estimator is bad data processing. It uses redundant measurement data to compute measurement residuals in order to detect gross errors caused by sensor problems and/or telemetry failures. In traditional bad data detection techniques, the 2-norm of the difference between the observed measurement vector and the estimated states is compared against a threshold to detect the presence of bad measurements [1], [2]. Although these techniques are effective against random interacting measurement noises, they fail to detect certain structured data manipulation attacks that conform to the network topology. Such vulnerabilities raise serious security concerns and need to be addressed.

The authors of [3] presented a new class of active attacks on a power grid, called false data injection attacks and performed analysis from the attacker's perspective. They showed that an attacker who has complete knowledge of the current grid configuration may successfully inject arbitrary errors into certain state variables without being detected by conventional bad data processing techniques[3]. The authors of [4] introduced indices that quantify the least effort needed by attackers to achieve attack goals while avoiding bad data detection. These indices help to determine and locate power flows which are easier to manipulate. The authors in [5] have investigated the false data injection attacks from an operators point of view in order to determine how to defend against such attacks. They have shown that it is a necessary condition but not a sufficient condition to protect at least a certain number of measurements in order to be able to ensure observability of the system and enable detection of false data injection attacks. In the absence of any verifiable state variables, it is necessary and sufficient to protect a set of basic measurements in order to be able to detect such attacks.

A Bayesian framework that leverages the knowledge of prior distribution on the states to detect false data injection attacks is proposed in [6]. The problem of determining the smallest number of meters that need to be tampered by the attacker has been modeled as an optimization problem satisfying several constraints in [7]. The authors of [8] defined irreducible attacks, their conditions, and proposed an algorithm based on graph theory for finding all irreducible attacks. One of the interesting findings is that if there are p unobservable attack sets, then it is sufficient to place $(p+1)$ PMUs at specific buses to make every attack observable.

Most of the existing work on detection of false data injection attacks are focused on two aspects. Firstly, looking at the problem from the attackers point of view and techniques have been developed for determining the minimum number of PMUs that the attacker needs to corrupt in order to influence the state variables without raising an alarm. The aspect aspect looks at the problem from the defenders point of view and develops schemes for determining the minimum number of secure PMUs required for being able to detect the attacks. In some cases the possible placements of these PMUs have been also suggested. It is quite clear that most of the cases assume that the defenders have some number of absolutely secure PMUs or verifiable states. But in reality, that may not be the case. No PMU can be expected to provide absolutely accurate data and zero possibility of corruption by attackers at all times. Therefore, it is clear that some detection techniques are required which would be able to detect false data injection attacks without making such strong assumptions.

B. Threat Model

Under the threat model considered in this paper, we assume that the adversary has compromised one or more of the entities that generate, transmit or store the PMU data. The compromised entities may be any of the PMUs, PDC, network routers and links or the communication system LAN at the control center. Once a device or link is compromised, the adversary may manipulate the PMU data or inject false PMU data that may bias the power system state estimation. No assumption is made on the presence or absence of data encryption. With data modification attacks, the adversary is implicitly assumed to be capable of breaking the encryption mechanism.

Under the adversary model described above, this paper addresses the following data modification attack. Data generated by the PMUs are sent over a communication network to the PDC. The data is then forwarded to the Super PDC and then ultimately to the control center. During its traversal from the PMU to the control center, the data passes through a number of routers and the communication links that connect them. The attacker is assumed to have compromised one or more of the routers or links and can manipulate the contents of the PMU data packets passing through them. The objective of the attacker is to cause the maximum damage possible by manipulating the PMU data, without being detected. The data manipulated by the attacker changes the estimated system states from their true values and larger deviations are more likely to lead to erroneous actions of greater consequence. Consequently, the attacker aims to manipulate the data to the largest extent possible. The objective of this paper is to develop a mechanism that can accurately detect data manipulation attacks on PMU data.

III. Detection Mechanism Based on Line Equivalent Impedance

In this section, we propose a data modification attack detection scheme based on verification of the equivalent line impedance in a distributed manner at the regional PDCs. The various line parameters and their significance as well as variations are discussed first.

A. Transmission Line Parameters

Electrical transmission lines are represented by four electrical parameters: resistance (R), inductance (L), capacitance

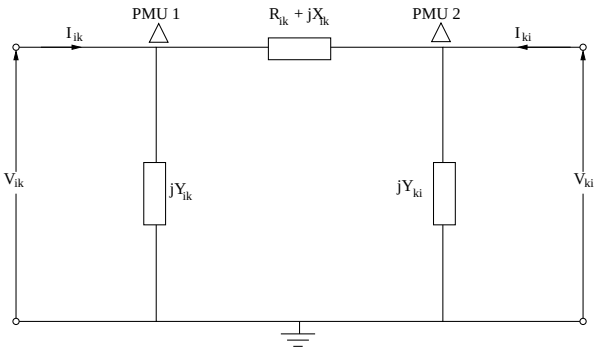

Fig. 1. Example topology.

(C) and conductance (G). The resistance is affected by three factors, namely, temperature, frequency, and spiraling, and accounts for the thermal losses in the line. With increase in conductor temperature, the line resistivity and hence the resistance increases. Between 25°C and 50°C, the variation in resistance is typically about 8%. The inductance is due to the voltage induced by the magnetic flux changes caused by the changing conductor current. It depends on the line geometry, cable size and configuration and is the most dominant line parameter. The capacitance in transmission lines is present due to the potential difference between the conductors. For short transmission lines (length less than 50 miles), the effect of capacitance is negligible. The conductance, is caused by the leakage current over the surface of the insulators. Since it is very small for overhead transmission lines, it can be ignored.

Along any transmission line, the above four parameters are uniformly distributed. However, the lines may be modeled using a lumped parameter configuration in many cases without much loss of accuracy. The resistance and inductance constitute the series impedance, whereas, the capacitance and conductance constitute the shunt impedance. For a short line, the series impedance in the lumped form is a good approximated model for the total line length. Typically, for a medium line (length between 50 miles and 150 miles), along with series impedance, the shunt capacitance is also considered by lumping half the capacitance to neutral of the line at each end of the equivalent circuit. Such a model is also termed as the nominal π-circuit. For long transmission lines (length more than 150 miles), if a high degree of accuracy is required, the parameters are distributed uniformly along the length of the line. However, a nominal π-circuit may represent it sufficiently well in case very high level of accuracy is not necessary [9].

The estimation of the individual parameters of the approximated π-circuit model of a transmission line is an iterative process and the results are not satisfactory when measurement errors or noise are present. Therefore, the final data modification attack detection based on these estimation results are unreliable. Although detectable bad data can be removed using statistics-based filtering methods, small amounts of bias errors and noise in measurements from different PMUs are very hard to eliminate. A detailed analysis of this problem is provided in [10]. When the error is positive in synchrophasor data from one end of the line and negative at the other end, then the resistance estimated may even come out to be negative. Also, when the load is unbalanced or mutual couplings exist on untransposed lines, the estimation can come out to be inaccurate giving rise to false alarms. Therefore, instead of estimating the individual line parameters in an iterative method, the equivalent impedance of the line is directly computed using the voltage measurements and current measurements at the two ends. The computed equivalent impedances are continuously monitored to detect any kind of abnormal deviation. These checks can be done in a distributed manner at the PDCs, thus making the computations simpler and faster.

B. Detection Mechanism

We consider a power system with N buses and let these buses be labeled as $i = 1, 2, \cdots, N$. In order to analyze the interaction of the measurement errors in the data and the effects on the estimates of the equivalent impedance, we assume that all the buses are equipped with PMUs so that estimates can be compared to the measured values. As shown in Figure 1, let us first consider any one specific transmission line which has PMUs at its two end buses (say bus 1 and bus 2). The measured bus voltage magnitudes and their corresponding voltage phase angles are represented by $|V_i|$ and θ_i respectively where $i = 1, 2$. The PMUs also measure the line current at both ends and the magnitudes and the phase angles of the currents flowing from bus i to bus k is denoted by $|I_{ik}|$ and δ_{ik} respectively, where $i, k = 1, 2$ and $i \neq k$. In order to compute the equivalent impedances, we first arbitrarily pick one of the buses as the reference bus. The phase angle of the selected reference bus is then subtracted from all the phase angle measurements to obtain their phase angles with respect to the reference bus. The equivalent impedance of the line, z_{ik}, as seen from bus i, is then calculated using the measurement data as follows:

$$V_i = |V_i|(\cos\theta_i + i\sin\theta_i) \tag{1}$$

$$I_{ik} = |I_{ik}|(\cos\delta_{ik} + i\sin\delta_{ik}) \tag{2}$$

$$z_{ik} = (V_i - V_k)/I_{ik} \tag{3}$$

Similarly, z_{ki} can also be computed using both the voltages and the current as measured at bus k. Although the magnitudes of the two computed equivalent impedances may be slightly different due to instrumentation errors in the current transformers, potential transformers or PMUs, the trend observed in both should be the same. If the impedance values and their trend show significant variation, data modification may be suspected with a certain level of confidence. This observation is the key to the proposed data modification attack detection mechanism. A sample of the magnitudes of the equivalent impedances calculated at both ends of a transmission line as well as their ratio and difference are provided in Figure 2. These impedances were calculated from real PMU measurements. It can be clearly seen that both their ratio and difference have minimal variation in the normal case.

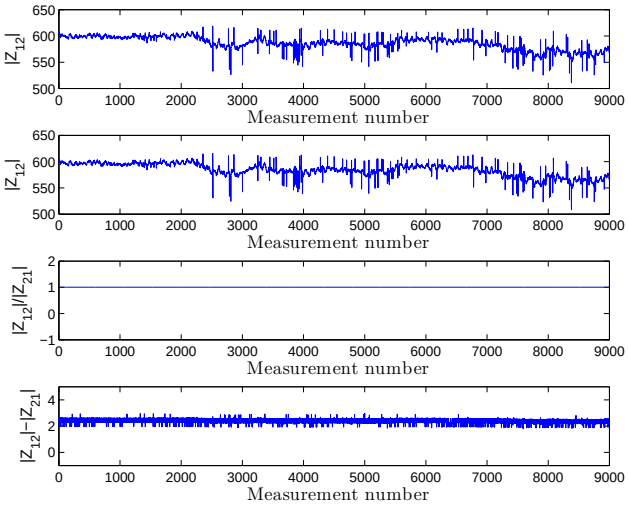

Fig. 2. Magnitude of equivalent impedances calculated from both ends.

Similarly, although the angles of the equivalent impedances computed at both ends are not exactly the same, they too follow a similar pattern and their difference is also observed to be nearly constant.

Therefore, the ratio and difference of the magnitudes and the difference of the angles of the equivalent impedances computed using the voltage and current measurements at both ends of a transmission line provide a viable means of detecting modification of PMU data. In the proposed detection scheme, if there is a sudden and/or sustained change in one or more of their values, it is taken as an indication of modification of measurement data by malicious attackers.

During a data modification attack on PMU data, the attacker may modify any or all of the following three quantities:

1) Current Magnitude: The current magnitude may vary widely even in normal situations due to change in load, generation, routes, or any combination of these causes. Thus in case of current magnitude, the level of difficulty in distinguishing between normal system variations and variations caused by an attacker's manipulation is the greatest. Therefore, modification of the current magnitude is the most likely target of the attacker for biasing the system states without being detected. Let us assume that the attacker changes one of the current magnitudes by a factor p, that is,

$$|I'_{ik}| = p|I_{ik}|. \tag{4}$$

Due to the modification in the current magnitude, the ratio of the magnitudes of the equivalent impedance will then deviate from 1 and become

$$\frac{z'_{ik}}{z_{ki}} = \frac{1}{p}. \tag{5}$$

Therefore, if the current magnitude is modified by a factor p, there will be a corresponding change in the computed equivalent impedance magnitude, causing the ratio to deviate. In general (and in Figure 2), variations of less than 1% in the ratio occur naturally and frequently. Hence, a current magnitude modification of less than 1% would be difficult to detect without causing false positives. However, a modification of such low value is not expected to cause significant biasing of the states or any kind of damage. The impact of current magnitude modification on the impedance magnitude ratio is shown in Figure 3. The current magnitude has been gradually increased upto 5% between measurement numbers 6000 and 6500 and then gradually decreased between 6500 and 7000. The other measurements are not manipulated. It can be seen that between measurements 6000 and 7000, there is a deviation in the impedance ratio conforming to the modification.

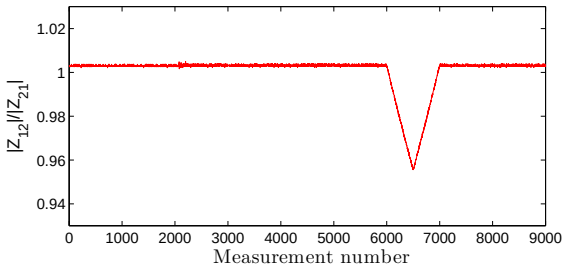

Fig. 3. Change in ratio of impedance magnitudes when current magnitude is modified.

2) Current Angle: In the second option, the attacker may change the current angle in order to mislead the control center regarding the power factor of the load. Let one of the current angles (e.g. δ_{ik}) be changed by a factor of q:

$$\delta'_{ik} = q\delta_{ik}. \tag{6}$$

Let γ be the angle of phasor $V_i - V_k$. That is,

$$arg(z_{ik}) = \gamma - \delta_{ik} \tag{7}$$

$$arg(z_{ki}) = 180 + \gamma - \delta_{ki} \tag{8}$$

In the normal case, the difference of the impedance angles will be,

$$arg(z_{ik}) - arg(z_{ki}) = \delta_{ki} - \delta_{ik} - 180 \tag{9}$$

When there is current angle modification, the ratio of the equivalent impedance magnitude stays the same. However,the difference of the angles changes as shown below,

$$arg(z'_{ik}) - arg(z_{ki}) = \delta_{ki} - q\delta_{ik} - 180 \tag{10}$$

Thus, after the manipulation in the current angle, the impedance angle difference changes. Therefore, any change in the current angle is accompanied by a change in the corresponding equivalent impedance angle making the difference of the angles deviate from the normal value. The impact of current angle modification on the equivalent impedance angle difference is shown in

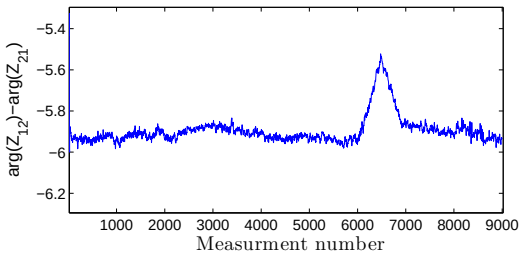

Fig. 4. Change in the ratio of impedance angles when current angle is modified.

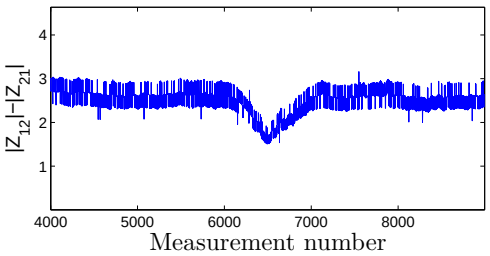

Fig. 5. Change in the difference between equivalent impedance magnitudes when voltage angle is modified.

Figure 4. For the results in this figure, the current angle was gradually increased upto 10% (the maximum modification being -0.74°) between measurement numbers 6000 and 6500 and then gradually decreased between 6500 and 7000. The other measurements are not manipulated. It can be seen that between measurements 6000 and 7000, there is a corresponding deviation in the ratio of the impedance angle.

3) Voltage Angle: Similarly, if the attacker changes any of the voltage angles, the difference in the equivalent impedance magnitudes changes and aids in detecting the data modification. Let one of the voltage angles be changed as follows:

$$\theta_i' = r\theta_i. \tag{11}$$

Let $|V_d|$ be the magnitude of the phasor $V_i - V_k$. That is,

$$|z_{ik}| = \frac{|V_d|}{|I_{ik}|} \tag{12}$$

Similarly, we can compute $|z_{ki}|$. Therefore, in the normal case, the difference of their magnitudes will be given by,

$$|z_{ik}| - |z_{ki}| = |V_d|(\frac{1}{|I_{ik}|} - \frac{1}{|I_{ki}|}) \tag{13}$$

However, when the voltage angle θ_i is changed, the corresponding voltage phasor, that is, V_i changes. Let it be denoted by V_i^{prime}. Therefore, the difference of the voltage phasors become:

$$|V_d'| = |V_i' - V_k| \neq |V_d| \tag{14}$$

Hence, the difference of the impedance magnitudes changes to:

$$|z_{ik}'| - |z_{ki}'| = |V_d'|(\frac{1}{|I_{ik}|} - \frac{1}{|I_{ki}|}) \tag{15}$$

Thus, when there is voltage angle modification, the difference of the equivalent impedance magnitude changes. The effect of modifying any of the voltage angles on the difference of the computed equivalent impedance magnitudes is shown in Figure 5. The voltage angle has been gradually increased upto 5% (the maximum modification being 1.13°) between measurement numbers 6000 and 6500 and then gradually decreased between 6500 and 7000. A corresponding deviation in the difference of the impedance magnitudes is observed between measurements 6000 and 7000.

Since the voltage magnitude is always expected to stay near 1 p.u. value, the attacker is not expected to modify it. If the attacker modifies the voltage magnitude, it can be readily detected.

The proposed data modification attack detection scheme is as follows. On receiving data from the PMUs, the PDCs calculate the equivalent impedances for each of the lines. The ratio and difference of the impedance magnitudes and as well as the difference of the impedance angles are computed. Any change in the current magnitude, current angle and/or voltage angle will cause one of the above three variables to deviate in the manner discussed above. Let x_i be the current estimated value of any the three variables for the i^{th} measurement and let μ_i be the mean and σ_i) be the standard deviation as observed over a window of n measurements preceding the current one, i.e.,

$$\mu_i = \sum_{j=i-1}^{i-n} x_j \tag{16}$$

$$\sigma_i^2 = \sum_{j=i-1}^{i-n} (x_j - \mu_{i-1})^2 \tag{17}$$

If the difference between the current estimated value and the current mean is more than thrice the current standard deviation, i.e.,

$$|x_i - \mu_i| > |3\sigma| \tag{18}$$

then the system enters the "alert" mode.

In order to minimize false alarms, alarm clustering is done. When the detection mechanism enters the alert mode, it initiates a timer of t seconds. In the alert mode, the system keeps track of the deviations observed. If the cumulative sum of the deviations exceeds a certain threshold (η) before the expiry of the timer, then the "attack" alarm is generated. The proposed data manipulation detection algorithm is shown in Algorithm 1.

IV. Simulation Results

In this section we present simulation results to verify the proposed detection mechanism. Real PMU data collected from various locations in New York have been used to verify the

Algorithm 1 Detection based on equivalent impedance

loop
  for Arrival of measurement number 'j' **do**
    Update the measurement set $|V|$, θ, $|I|$, δ;
    $V_i = |V_i|(cos\theta_i + i \sin\theta_i)$;
    $I_{ik} = |I_{ik}|(cos\delta_{ik} + i \sin\delta_{ik})$;
    Determine equivalent impedance $z_{ik}(j) = (V_i(j) - V_k(j))/I_{ik}(j)$;
    Calculate $z_{ki}(j)$ similarly;
    Impedance magnitudes $|z_{ik}(j)|$ and $|z_{ki}(j)|$;
    Impedance angles $arg(z_{ik}(j))$ and $arg(z_{ki}(j))$;
    Calculate $x_1(j) = |z_{ik}(j)|/|z_{ki}(j)|$;
    Calculate $x_2(j) = z_{ik}(j) - z_{ki}(j)$;
    Calculate $x_3(j) = arg(z_{ik}(j)) - arg(z_{ki}(j))$;
    Calculate $\mu_k(j) = \sum_{m=i-1}^{i-n} x_k(m), k = 1, 2, 3$;
    Calculate $\sigma_k(j) = \sum_{m=i-1}^{i-n} x_m - \mu_k(j-1)$;
    if $|x_k(j) - \mu_k(j)| > |3\sigma_k(j)|$ **then**
      ALERT(j);
    else
      Continue monitoring;
    end if
  end for
end loop when session is terminated

function ALERT(j)
  if $a = 0$ **then**
    Start timer for value t;
    $Sum = 0$;
  end if
  Update $a = a + 1$;
  Calculate $Sum = Sum + |x_k(j) - \mu_k(j)|$;
  if Timer has Expired **then**
    if $Sum > \eta$ **then**
      Generate alarm for "Data manipulation attack";
    end if
    Update $a = 0$;
  end if
end function

mechanism. Five sets of PMU data containing 9000 measurement samples each, and taken on different days were used for evaluating the proposed detection method. To simulate an attack, the values of the PMU measurements were altered. Three sets of simulations have been performed: first with modification in current magnitude, second with modification in current angle and third with modification in voltage angle. For each set, three levels of modifications have been simulated, that is, 0% or no change, 5% change and 10% change. Also, both step and ramp modifications have been simulated to determine the performance of the detector in two different types of modification scenarios. For each of the simulations, the accuracy, false positive and false negative have been computed in the form of percentages. The results are shown in Table I.

The accuracy of the detection scheme is above 80% with lower than 20% false alarms when there is no attack. The accuracy increases with increase in the modification level or if the modification is in the form of step-change. The maximum possible detection delay is 30 seconds, since it is the timer value used for the simulations. However, in most cases the threshold is exceeded much before the timer expiry, making the detection delay much smaller. We note that further tuning of the timer setting and the threshold may be possible leading to improvement of the results.

TABLE I
OVERALL DETECTION RESULTS USING PROPOSED DATA MODIFICATION ATTACK DETECTION ALGORITHM. A: ACCURACY, FP: FALSE POSITIVE, FN: FALSE NEGATIVE

Modification percentage	Step change			Ramp change		
	A	FP	FN	A	FP	FN
5	93.33	0	6.67	86.67	0	13.33
10	100	0	0	100	0	0

V. CONCLUSIONS

In this paper, we proposed a mechanism for detecting data manipulation attacks on PMU data. The method is reliable even in the presence of instrumentation errors and noise. It does not require any iterative computations and hence is comparatively fast. The effectiveness of the detection mechanism has been verified using simulations. The accuracy of the proposed mechanism is above 85% for even modifications in measurements as small as 5%. Also, unlike many existing mechanisms for detecting bad data, it does not require the assumption that either some of the PMUs are absolutely secure or that some of the states are verifiable.

REFERENCES

[1] 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.

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

[3] Y. Liu, P. Ning and M. Reiter, "False data injection attacks against state estimation in electric power grids", *Proceedings of ACM CCS,* Chicago, IL, November 2009.

[4] 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.

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

[6] Kosut, O.; Liyan Jia; Thomas, R.J.; Lang Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on* , vol., no., pp.220,225, 4-6 Oct. 2010.

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

[8] Giani, A.; Bent, R.; Hinrichs, M.; McQueen, M.; Poolla, K., "Metrics for assessment of smart grid data integrity attacks,"*Power and Energy Society General Meeting, 2012 IEEE*, pp.1,8, 22-26 July 2012.

[9] J. Grainger and W. Stevenson, Power System Analysis. New York: McGraw-Hill, 1994.

[10] D. Shi, "Utilizing Sunchrophasor Technology to Determine Transmission Line Impedance Parameters", Master's thesis, Arizona State University, December 2009.