Undetectable GPS-Spoofing Attack on Time Series Phasor Measurement Unit Data

Imtiaj Khan  
Electrical and Computer Engineering  
Virginia Tech  
Blacksburg, VA, USA  
imtiajkhan@vt.edu

Virgilio Centeno  
Electrical and Computer Engineering  
Virginia Tech

Abstract—The Phasor Measurement Unit (PMU) is an important metering device for smart grid. Like any other Intelligent Electronic Device (IED), PMUs are prone to various types of cyberattacks. However, one form of attack is unique to the PMU, the GPS-spoofing attack, where the time and/or the one second pulse that enables time synchronization are modified and the measurements are computed using the modified time reference. This article exploits the vulnerability of PMUs in their GPS time synchronization signal. At first, the paper proposes an undetectable attack scheme which is able to bypass Bad Data Detection (BDD) algorithms used with PMU data. The attack is applied by solving a convex optimization criterion at regular time intervals, so that after a specific time period the attack vector incurs a significant change in the angle information delivered by the PMU. Secondly, the impact of phase angle shift on the power flow calculation between two adjacent nodes of the transmission line is analyzed with numerical experiment using IEEE 39 bus system. Moreover, the undetectibilities of the proposed attack scheme against conventional \( \chi^2 \), Weighted Least Squares (WLS) and Kalman Filtering test on the estimation residuals are investigated. Finally, the power flow results with the proposed attack are compared with the results using a random GPS-spoofing attack. It can be observed that using the proposed method enables the attacker with more control over the impact against power grid than it is for the random attack. Furthermore, the proposed attack model has demonstrated a very small probability of detection against each of the common detection methods. For WLS and KF, the attack is detected only about 1-20% of the times, whereas for \( \chi^2 \)-test, the attack goes undetected 100% of the times.

Index Terms—PMU, Cyber attack, Undetectable, GPS spoofing, time stamp.

I. INTRODUCTION

Introducing smart metering and protective devices brought a revolution in the traditional power grid. A smart grid comprises of two parts: a physical part which is the conventional power grid and a control center which receive data and takes decision based on the data it received, combination of both part is referred as Cyber-Physical System (CPS). In a typical CPS, a Supervisory Control And Data Acquisition (SCADA) is utilized to gather measurements from meters through Remote Terminal Units (RTUs) [1]. SCADA sends the measurements to the control center to filter out gross measurement noises and errors. The control center also provide economic dispatch, unit commitment and optimal power flow (OPF) [2].

Phasor Measurement Unit (PMU) is relatively newer type of metering device which provides voltage and current magnitudes and phase angles in a time synchronized format [3]. The measurement data provided by PMUs are time-tagged with Universal Time Coordinate (UTC) and the time information include second-of-century (SOC) count, fraction-of-second (FRACSEC) count, and time quality flag. The time information is synchronized with a reliable time-source and the most common time-source is the Global Positioning System (GPS). In addition to the magnitudes and phase angles of voltage and current components, PMUs also provide frequency and Rate of Change of Frequency (ROCOF) data [4]. Installing PMU in the smart grid created a new horizon in terms of accuracy and speed [5] [6]. In conventional SCADA based system, data transfer rate is one sample per second, where in PMU the data transfer rate is 30 to 120 sample per second [7] [8].

Despite being reliable in terms of time-tagged data and accuracy, PMUs are still susceptible to various type of cyber attacks [9] [10] [11]. The most common type of cyber attack against PMU is the malicious data injection attack attack such as false data injection attack (FDIA). Other types of malicious data injection attacks include data modification and replay attacks [12]. In FDIA, the attacker injects data into the system and thereby modifying the power system data fed into the control centre. If the state estimation is performed with falsified data, the System Operator (SO) at control centre may take wrong decision such as taking restorative action or emergency shut down even though the operating condition is not actually violated. Another frequent type of attack that can hamper PMU integrated grid performance is Denial of Service (DoS) attack. In this case the attacker injects large volume of data through the communication channel, therefore the data transfer to destination gets blocked due to the large volume of data traffic [13] [14]. Man In The Middle (MITM) and Side Channel attacks are also critical for PMU [15] [16].

Since PMU relies on GPS signal for time synchronization, it opens the possibility of a new type of attack: GPS-spoofing attack. PMU generally uses public GPS which lacks the sophisticated protection scheme used for military GPS. GPS-spoofing attack poses very serious concern over the cybersecurity of the CPS [17]. It may affect the magnitude and the phase angle, however the phase angle is the most susceptible portion of the synchrophasor, because shift in the GPS 1 PPS, which is used as the common reference for all PMUs, is reflected by the phase angle shift [18]. Slowly changing time reference for an individual PMU slowly shift the phase angle data [19].
provided by the particular PMU from a particular node. Gradual change of phase angle of a particular node with respect to the other nodes in the grid can, in some scenarios, provide incorrect information to a system operator (SO) at control centre that may lead the SO take unnecessary actions. Moreover, the gradual shift in phase angle measurements due to the GPS-spoofing attack has the potential to impact any PMU base transmission line fault detection and identification of event location [17].

The phase angle shift caused by the GPS-spoofing attack can affect a PMU based transmission line differential protection scheme. As soon as the spoofed phase angle crosses the threshold, the relay will trip despite the absence of an actual violation of the operating constraint. In this way the attacker can disrupt the normal operating condition of the grid, without creating any physical change in the cyber-physical model. This phenomenon can be referred as misoperation [21].

Several researchers focused on the protection of PMU integrated smart grid against cyber attacks. Most works are based on detecting FDIA. Detection of FDIA is similar to conventional Bad Data Detection (BDD) method [22] [23]. Conventional BDD algorithms observe the residuals of the measured and expected variables and do statistical test to find the outliers. GPS-spoofing attack can also be considered as a type of BDD, since modification in time reference lead to the shift in phase angles. In GPS-spoofing attack, the voltage and current magnitude may remain unchanged, depending on the algorithm employed by the PMU manufacturer. As a result, it can be considered similar to a FDIA with only the phase angle data modified.

Considering the defense strategy taken by control center, it is possible to create attacks that are undetectable by BDD algorithms [24] [25]. This statement is also true for GPS-spoofing attack if the attack is considered as a variation of FDIA with corrupted phase angle data [26]. These types of undetectable and stealthy attacks can still be prevented by placing PMUs into optimal locations of the grid [27]. The goal of this article is to create an GPS-spoofing attack, which cannot be prevented by optimal PMU placement or by BDD algorithms. The key idea is to inject a shift in the phase angle by creating and maintaining an effective delay in time reference of an individual PMU. Doing so, the attacker will be able to change the phase angle difference between the spoofed PMU and any other monitored PMU in the system. The sample attack used in this article is made in such a way that, its impact on the power flow calculation is insignificant for one instance of attack. The attack is incrementally applied after some interval of time for over a specific time period T.

The attackers’ goal is to eventually cause a significant impact on the SO’s perceived power flow measurement after the time period T. During off-peak hour, the power flow in the line under attack is well below its limit, as indicated by the angle difference of the PMUs at the both ends of the line. The SO will not suspect the power flow to exceed the limit at this time, therefore a significant increase in the calculated power flow will alert the SO about possible cyberattack. The attacker exploits this issue and over the period T, at each time instance s/he creates insignificant increase in the phase angle of a PMU at one end of the line, causing an insignificant increase in the derived power flow through the line. The accumulative effect of the increases grows larger over time, and after T, which can be made to coincide with the peak load, if performed correctly the line power flow as determined by the phase angle difference from PMU measurements exceeds the line’s limit. At peak load-hour, the SO at the control centre is prepared for possible operational limit violations in the physical grid, therefore if the calculated power flow exceeds the line low limit at that time, the SO, considering a physical cause for the event, may then take the protocols required for operational limit violation despite the operational limit is not actually violated. Therefore, the load-shedding or other restorative measures will be taken, which will lead to a hamper in the supply of power to the critical points of the grid.

The attacker starts the attack at the initial time $t_0$. The phase angle shift $\theta_0$ generated by the spoofed signal will be derived by solving optimization equation which aims at enabling the attack undetectable by commonly used detection techniques that are discussed in section III. The attacker creates a spoofed GPS signal to the PMU at bus i and/or j at $t_0$, introducing a time shift $\Delta t_0 = \frac{a_0}{2\pi f}$ [28], corresponding to the optimal phase angle measurement shift $a_0$ caused by spoofing and system frequency $f$. All the sampled measurements of PMU following the timestamp $t_0$ will carry on this time shift in their measurements and the corresponding phase angle measurements will be phase shifted by $\Delta \theta_0 = 2\pi f \Delta t_0 = a_0$. The next attack is initiated at time $t_1$, after S number of samples. At time $t_1$ the attacker solves the optimization equation to compute the new attack value $a_1$. The corresponding time shift that the attacker needs to introduce by GPS-spoofing will be $\Delta t_1 = \frac{a_1}{2\pi f}$. The overall phase angle shift in the PMU measurement for the next S number of samples becomes $\Delta \theta_1 = 2\pi f \Delta t_1 + \Delta \theta_0$. The power flow through the branch $i \rightarrow j$ will also deviate accordingly. The attacker keeps instigating the spoofing attack for the following timestamps $t_2, t_3, \ldots$, until T, at which the power flow through the branch $i \rightarrow j$ reaches the peak value. The tempered power flow, which kept increasing from the actual power flow in the previous timestamps, suffers from maximum deviation and crosses the power flow limit of the line $i \rightarrow j$.

The contribution of this work has two aspects: firstly, for each 1 PPS of the GPS receiver, the attacker calculates the phase angle shifts using optimization equation with a goal of keeping the small individual change in phase angle measurement undetectable by most bad data detection algorithms. This optimization method is similar to stealthy FDIA methods discussed in previous literature. However, existing stealthy FDIA algorithms considered the attack vector to be greater than a significance threshold $\zeta$, whereas the proposed method in this article consider the attack vector to be less than $\zeta$ to create insignificant variation in the phase angle measurements at each time instance. Secondly, our proposed model creates an attack that has the objective of slowly shifting a PMU angle to achieve a maximum impact at the peak loading time of a line monitored by two PMUs. In conventional FDIA, attack values at each timestamp are discrete from the previous ones; however, in the proposed GPS-spoofing model the phase shift
The undetectability of the proposed GPS-spoofing attack scheme is outside of the cyber-physical system of the smart grid. In this work, the attacker doesn’t inject any falsified measurement, rather s/he forces the PMU algorithm to introduce a phase shift in the computed phasor by disrupting GPS signal received by the PMU’s GPS receiver. Instead of altering the phase angle measurement directly, the GPS spoofing attack shifts the 1 Pulse-Per-Second (PPS) signal used by the PMU for time reference, and this shift in 1 PPS reference signal is reflected by a small change in phase angles for the phasors computing until the next 1 PPS is received. The overall topological structure of the GPS-spoofing attack considered in this work can be depicted in fig. 1.

The paper is organized as follows: Section II briefly discusses the previous literature on the cyberattack on PMU and necessary countermeasures. Section III explains the proposed undetectable attack scheme. Section IV validates the undetectability criteria of the proposed method. The test setup for the proposed stealthy attack is discussed in section V. Section VI provides the results depicting the impact of the proposed GPS-spoofing attack on the power flow calculations as well as analyzes the undetectability of the proposed model. Section VII discusses the limitations and future research scope.

The main contribution of this article can be summarized as follows:

- An optimization criterion is modeled to create undetectable phase angle shift at evenly spaced consecutive timestamps until the peak load hour is reached;
- The proposed optimization criterion for undetectable attack is extended to incur a significant impact on the perceived power flow between two nodes during peak load-hour by assuming an angle stability limit in the constraint, even though the actual flow through the same branch remain unchanged;
- The undetectability of the proposed GPS-spoofing attack at each affected timestamp is tested against multiple BDD algorithms such as $\chi^2$, Weighted Least Square (WLS) and Kalman Filtering (KF). Measurements with noise from the IEEE 39 bus system model in SIMULINK are used to test the undetectability;
- The effectiveness of the proposed attack scheme is demonstrated with dynamic simulation of IEEE 39 bus system;
- The effectiveness of the proposed optimization criterion is validated for the IEEE 39 bus system using simulation in SIMULINK.

II. PREVIOUS WORKS

The works on cyber-attack on PMU can be classified as two parts: 1) detection and mitigation of attack and 2) creating undetectable attack.

A. GPS-Spoofing Attack

Global Positioning System (GPS) is one of Global Navigation Satellite Systems (GNSS) and provides position, navigation and time information using four or more GPS satellites. GPS provides accurate locations and time references, is widely used in time synchronization of Phasor Measurement Units (PMUs). PMUs require precise time reference to keep the timing error within the limit of 26μs, standardized by IEEE C37.118.2 protocol.

Despite being accurate in time reference and locations, GPS signals are prone to jamming and spoofing. Jamming is accomplished by using a jammer device that creates a Radio Frequency (RF) signal to deny the signal from satellite being transmitted to the GPS receiver. The GPS-spoofing refers to providing a fake GPS signal of stronger transmission power to the receiver. The fake signal can be implemented using one of the three methods: open-loop simulator, repeater or hardware injection. Once the receiver is locked with the fake GPS-signal, it estimates the location and time reference at a altered position.

Since PMUs use GPS signal for time synchronization, the PMU as well as the whole power grid operation relies on the authenticity of GPS signal. GPS-Spoofing Attack (GSA) on PMU integrated smart grid can either be performed by manipulating the GPS timestamp or modifying GPS propagation time. In [34], researchers performed a GPS-spoofing field test on PMUs and it has been demonstrated that the attacker can cause a time error more than tens of microseconds, which exceeds the limit prescribed in the IEEE standard. Time synchronization error due to GSA can impact the transmission line fault detection, voltage stability monitoring and identification of event location.
Detection mechanism of GSA can be performed by implementing cryptographic authentication methods such as public key infrastructure, signal authentication sequence, navigation message authentication etc. [37] [38]. Y. Fan et al. [39] proposed a GPS carrier-to-noise ratio (C/No) based GSA detection mechanism for PMUs, which are installed in the physical layer of the cyber-physical system. The suspicious PMUs are identified by calculating a priori probability of spoofing. The autocorrelation among multiple GPS-signals can also be a useful tool for the detection of GSA. The p-score thresholds of statistical runs test are used to classify the GPS signal as safe or unsafe. Supervised machine learning techniques can be applied to train the signals based on their classifications [40].

PMUs in power grid uses civilian GNSS and the sophisticated GSA detection methods are not utilized in the current smart grid infrastructure. This limitations have made the PMUs vulnerable to GSAs. However, as GSA creates a modifications in the timestamps of PMU, it leads to a phase angle shift in the PMUs. Therefore, GSA can be analyzed similarly as the part of the cyber-physical system. The suspicious PMUs are identified by calculating a priori probability of spoofing. The autocorrelation among multiple GPS-signals can also be a useful tool for the detection of GSA. The p-score thresholds of statistical runs test are used to classify the GPS signal as safe or unsafe. Supervised machine learning techniques can be applied to train the signals based on their classifications [40].

B. Creating Undetectable Attack

For an n bus system, the state variable can be represented as the vector $\mathbf{x} = [x_1, x_2, \ldots, x_n]$ and the measurement variables can be represented with the vector $\mathbf{z} = [z_1, z_2, \ldots, z_m]$. Here m is the number of meters (m >> n). The relation between $\mathbf{z}$ and $\mathbf{x}$ can be expressed as

$$\mathbf{z} = \mathbf{Hx} + \epsilon$$

$\mathbf{H}$ is the jacobian matrix that represents the non-linear relation between the state variable and the measurement variable. $\epsilon = [\epsilon_1, \epsilon_2, \ldots, \epsilon_m]$ is the measurement error vector. An FDIA will go undetected if $\|z - H\hat{x}\|_2$ is less than threshold $\tau$, where $\hat{x}$ is the estimated state variable which can be calculated from the Weighted Least Square (WLS) method $\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z$. $\mathbf{R}$ is the measurement error covariance matrix. If the attack $\mathbf{a}$ is applied, the measurement vector under attack will be $\tilde{x}_a = z + a$ and the estimated state variables under attack will be $\hat{x}_a = \hat{x} + c$. The estimated attack vector is $c = (H^T H)^{-1} H^T a$. After attack, $\|z_a - H\hat{x}_a\|_2 = \|z + a - H\hat{x} - Hc\|_2 \leq \|z - H\hat{x}\|_2 + ||a - Hc||_2$. If $a = Hc$, then $\|z_a - H\hat{x}_a\|_2 \leq \tau$. Therefore, the attack goes undetected.

To defend against this type of undetectable attack, the defender’s goal is to make attack infeasible. Assume S is the set of measurement that are protected and $\bar{S}$ is the set of unprotected measurements. When PMU is installed at a particular node, the measurements from that node and the connected branches and nodes become observable, making those measurements protected. The matrix $H^S$ reflects the part of H matrix that corresponds to the protected measurements and $H^S$ is the complementary matrix of $H^S$. The part of measurements being protected poses a new constraint to attacker, which is

$$H^S c = 0$$ (4)

For sufficiently large number of protected measurements, the rank of $H^S$ becomes n. The only solution for eqn 4 becomes $c = 0$. It implies that the attacker cannot create non-zero attack vector.

For the case when rank($H^S$) < n, the attacker can create a non-zero c. To make a significant effect on the system, the vector $c$ needs to be greater than a threshold $\gamma$. Therefore, the attacker can create an undetectable attack which impacts the system using the following minimizer [41]:

$$\min_c \|H^S \|_0$$

s.t. $H^S c = 0$

$$||c||_\infty > \gamma,$$ (5)

The goal is to find a sparse solution from the eqn 5 which is NP-hard. Thus, a naive $\ell_1$ relaxation can be used to increase the sparsity. Another approach to bypass the non-convexity of the optimization criteria of eqn 5 is to create a random attack that will be considered as a random noise by the control center. To achieve that, the $\mathbf{a}$ must be within the null space of $F = H(H^T H)^{-1} H^T - I$. If a standard basis matrix $\mathbf{B}$ is created from Null($\mathbf{F}$) and a vector $\mathbf{b}$ is chosen from the column of $\mathbf{B}$ with variance, a random attack vector $\mathbf{a}$ can be created by adjusting the $\mathbf{b}$ vector by a scaling factor $\epsilon_0$ and shrinking the $\mathbf{b}$ vector using the shrinkage function $S_\epsilon(b)$. [44]

Attack vector $\mathbf{a}$ can be constructed by $\mathbf{a} = S_\epsilon(b)$. Since the attack needs to be considered as a random Gaussian noise by the control center, the threshold $\tau$ can be estimated by keeping within the range $[-3\sigma, 3\sigma]$.

Attackers’ target is to create an low cost undetectable attack by minimizing $h(x + c) - h(x)$ [45], while keeping...
the $Hc = 0$ to evade the detection by residual based attack detection techniques \cite{27}. Another approach of creating low cost and least effort undetectable FDIA is applying Particle Swarm Optimization (PSO) technique. The affected PMUs are considered as particles, and sparse attack vector $a$ is regarded as swarm. The attacker chooses only a few PMUs to attack, rather than attacking all of the vulnerable PMUs. The attacker calculates each PMUs’ personal best position, thereby creating the sparse attack vector by solving the following optimization algorithm \cite{46}:

$$\begin{align*}
\min_{a_p} & \quad ||a_p||_0 \\
\text{s.t.} & \quad H_p c_p = a_p \\
& ||c||_{\infty} > \gamma, \\
& b = 1,
\end{align*} \quad (6)$$

In eqn \ref{eqn:6}, the minimizer $||a_p||_0$ ensures the undetectability. $H_p$ refers to the portion of the Jacobian matrix; corresponding to the positions where the PMUs are installed. The sparsity of the attack vector can further be improved by applying the sparse imperfect strategy proposed in \cite{47}. In this method, the measurements are selected by solving subset selection problem; for which the Locally Regularized Fast Recursive (LRFR) can be a useful tool \cite{47}.

The observability space of the cyber-physical system can be a useful tool for creating undetectable FDIA for PMU integrated smart grid. The attack is tested with the $\chi^2$-test using the $\ell_2$-norm of the residual $r = z - H \hat{x}$, and the measurements under proposed attack model doesn’t reject the null hypothesis, thereby making the attack undetectable. In \cite{48}, undetectable attacks are constructed for flight vehicles by utilizing the Singular Value Decomposition (SVD)-based subspace identification and solving an optimization problem with state estimation error being the attack objective.

Despite being undetectable by conventional residual based detection methods, these attacks can be detected by Low-Rank Decomposition (LRD) technique proposed in \cite{49}. A class of multiplicative attacks that doesn’t change the rank of measurement matrix can bypass LRD based detection scheme \cite{50}.

In all the FDIA schemes discussed above, the attacker is assumed to have the sufficient knowledge of the whole network topology of the cyber-physical system. If the complete topology of the grid is unknown, there exists incomplete information in the H matrix. To tackle this issue, a Kernel Independent Component Analysis (ICA) based attack construction model has been developed \cite{51}. The ICA is a process of separating a multivariate data into the linear combination of all data components \cite{52}, whereas Kernel ICA is a special type of analysis where the separation is performed using optimization of canonical correlation \cite{53}. The H matrix will be replaced by $H_p$ which corresponds to the portion of the bus connection which is known. The attackers dont need the complete information of H matrix to create undetectable FDIA \cite{51}.

According to the linear Independent Component Analysis (ICA), the steady state measurement $z$ of few consecutive sequence is required to construct the attack vector $a$. The H matrix can be expressed as $Hx = HA\nu$, $A$ is the unknown impurity matrix and $\nu$ represents the independent components. The new matrix $H_p = HA$ refers to the Jacobian matrix of the partial known topology. The attack vector is computed by maximizing the undetectability of the attack.

X. Liu and Z. Li \cite{54} proposed a optimal attack vector using the partial knowledge about network topology. The attack vector is obtained by solving the optimization equation which minimizes an introduced non-negative slack variable. The constraints are real and reactive power flow limits throughout the branches.

Since the GPS-spoofing attack (GSA), also referred as the timing attack, can be considered as a special type of FDIA with a modification in the phase angle values only, it can be created as a stealthy attack utilizing the stealthy FDIA algorithms discussed above. If $\alpha_i$ is the difference between the original and modified values of $i_{th}$ phase angle, then the measurement $z$ deviates by $\Delta z = z_m(cos\alpha_i + jsin\alpha_i - 1)$. Similar to the work for FDIA in \cite{43}, the timing attack will be undetectable if and only if $||(H(H^T H)^{-1}H^T - I)\Delta z||_2 = ||F\Delta z||_2 = 0$.

If $A$ is the set of the index of the measurements under attack, $A_i \in M; i = 1,2,..,p$ and $M = \{1,2,...,m\}$, $p$ is the total number of measurements being modified. For total measurement $m$, $\psi$ is the $m \times 1$ attack measurement indicator matrix with

$$\psi_j = 1; \text{for } j \in A$$
$$\psi_j = 0; \text{for } j \notin A$$

An attack vector matrix W can be created, where $W = \psi^T diag(z) F^T diag(z) \psi$. As a result, the condition for undetectable attack can be formulated as follows \cite{26}:

$$W(\overrightarrow{u} - \overrightarrow{1}) = 0 \quad (7)$$

Where $u_i = cos\alpha_i + jsin\alpha_i$. For a single attack ($p = 1$), it is not possible to find an attack value $\alpha_i$ other than 0 \cite{26}. However, for two attack ($p=2$), there exists an undetectable attack vector $\alpha = \{\alpha_1, \alpha_2\}$. This attack model can be extended for three attacks ($p=3$). Observing the measurements $z'$ at time $t$, which are already attacked with $p = 2$, the attacker compute the unaffected measurements $z_i = z'_i e^{-js\alpha_i}$ and the angles $\alpha_1, \alpha_2, \alpha_3$ by maximizing the power flow error on a particular branch \cite{28}.

C. Detection of Attack and Countermeasure

Mousavian et. al. \cite{55} proposed a Mixed-Integer Linear Programming (MILP) based attack prevention scheme where threat level of various PMUs connected to the grid is assessed. The objective function minimizes the maximum threat level of existing PMUs in the system. If the threat level is still higher after first minimization step, the corresponding PMU is disconnected from the system.

Vulnerability due to cyber-attack was analyzed for conventional measurements and data-format of PMUs \cite{55}. Independent Component Analysis (ICA) based signal separation model is utilized to create attack on PMU measurements. The authors also proposed a Cognitive Radio (CR) based network topology to ensure secure PMU data transmission, where the network is not directly connected to the backbone network \cite{56}.

Cyberattack can cause cascading failure by triggering the failure in the interconnected parts of the physical power
system. Rui Ma et al. [57] proposed a Recovery-based Model Predictive Control scheme (RMPC) to tackle the cascading failure caused by cyber attack. This model takes into account the modified operating conditions and tempered measurements after attack. The control action is determined by solving an optimization algorithm over finite time horizon. The state variables at state k is computed with the historical state variable data in the event of attack. If the power system has been compromised for consecutive N states, the RMPC will predict the k-th state variables using the state variable from k-N state. The incorrect state data are then replaced by the predicted state data.

Detection of successive observable cyberattacks can be considered as a matrix decomposition problem of a low-rank matrix plus a transformed column-sparse matrix [58] [59]. For the measurement model in eqn 3, the attack can be identified if the low rank approximation of z and the column-spars matrix c can be separated [59]. An optimization problem is solved to obtain the optimal z" and c".

For timing attack, risk assessment and mitigation algorithm for power grid Automatic Generation Control (AGC) under attack has been developed [60] [27]. The stability assessment is done first, if the system is considered unstable, which implies the system is unsafe, the mitigation scheme is initiated. If the system is stable, the safety assessment is done. The mitigation scheme is initiated if the system is found to be unsafe.

One of the most widely used method to counter malicious attack is to secure the measurements by placing the PMUs to critical locations. A greedy based PMU placement has been developed [43] where a new PMU is added in the location that can protect the most number of vulnerable measurements. $H^S$ refers to the measurements which are already secured. Adding a new PMU will add a new row $H^{PMU}$ to this matrix. Therefore new condition for attack is:

\[
\begin{bmatrix}
H^S \\
H^{PMU}
\end{bmatrix} c = 0
\]

If $H^{PMU}c = 0$, then adding a new PMU doesn’t provide any additional security. However, for the case of $H^{PMU}c \neq 0$, the attacker has to find alternate solution to create stealthy attack. The greedy algorithm is modified for specific attack vector created by least effort Reduced Row Echelon (RRE) method [61]. RRE form of a matrix refers to the case when the leading entry in each nonzero row is a 1 and all other entries in the column with leading 1 are zeros. A predelployment based greedy algorithm can be used for further protection against more stealthy attack where the measurements of the edge buses are moved to the secured measurement matrix in the first step [27].

The most common attack detection method relies on state estimation based Bad Data Detection (BDD) method as discussed in the subsection 11-B. Since the affect of GPS-spoofing attack can be reflected by the shift in phase angle data, the bad data detection techniques that are used to identify FDIA can also be used to detect GPS-spoofing attack. The most common BDD technique is the residual based detection method [62], where the control center receives the measurements from the physical power system and calculates the residuals between the actual measurement $z$ and the estimated measurement $H \hat{x}$. The notation $z$, $H$ and $x$ are same as discussed in 11-B. The development of stealthy attacks as described in 11-B engendered the need of using more sophisticated detection schemes.

Kalman Filtering (KF) [63] is an effective tool to detect bad data caused by electrical events and FDIA. For a system, if the state variable is $x(t)$ and the measurement variable is $y(t)$, the state variable at time $t+1$ can be estimated from the previous state $x(t)$ using the following relation:

\[
x(t+1) = Ax(t) + w(t)
\]

A is the state transition matrix and w is the system noise. The relation between state variable and measurement is as follows:

\[
z(t) = Hx(t) + e
\]

$H$ is defines the relation between the state variables and measurements, similar to eqn [3] and e is the measurement noise. $w$ and $e$ are zero-mean Gaussian signals and the corresponding covariance matrices are Q and R respectively. KF estimates the state variables $\hat{x}(t)$ at time t using the state variables and measurements upto t-1. P(t) is the covariance of estimates at time t. The time updates of state variables and covariance matrix are expressed as:

\[
x(t+1|t) = Ax(t) + w(t)
\]

\[
P(t+1|t-1) = AP(t-1|t-1)A^T + Q
\]

Consequently, the measurements are updated using the following relations:

\[
K(t) = P(t|t-1)H^T[H P(t|t-1)H^T + R]^{-1}
\]

\[
P(t|t) = P(t|t-1) - K(t)H P(t|t-1)
\]

\[
\hat{x}(t) = \hat{x}(t-1) + K(t)[z(t) - H\hat{x}(t-1)]
\]

\[
P(t) = [I - K(t)H]P(t|t-1)
\]

$K(t)$ is the Kalman gain at time t. Starting from an initial condition $x(0) = 0$ and $P(0) = \text{covariance matrix of: } x(0)$, KF provides a recursive calculation of state variables using minimized mean-squared error. The residuals between the measurement $z(t + 1)$ and the estimation $H\hat{x}(t + 1)$ is tested against predefined threshold. If the residual exceeds the predetermined threshold, it is perceived as a bad data. The KF estimator generates better estimations of state variables than conventional weighted least square based estimator [63]; however when a FDIA is initiated, the injected attack impacts the estimation performance [64]. This effect can be avoided by updating measurement weighting function $W(t) = R^{-1}$ using the following equation [65]:

\[
(W_{\text{new}}(t))^{-1} = (W(t))^{-1} \times e^{[z(t)-H\hat{x}(t-1)]}
\]

The updated weighting function in eqn [17] increases the FDIA detection probability for the deviation based KF approach compared to the conventional KF estimator [66].

To evaluate the undetectability of proposed phase angle shift caused by GPS-spoofing attack, we have utilized three aforementioned BDD methods: conventional weighted least square residual test, Deviation based Kalman Filtering based
residual test and conventional $\chi^2$-test. The residuals between the actual measurement and estimation using each method is tested with a predetermined threshold. The outcome is categorized as four types: True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The detector algorithm flags "Positive" if the residual is crossed the threshold, and "Negative" otherwise. An attack is undetectable by a specific type of detector if the detector’s response is "FN" after performing estimation.

III. FORMULATION OF UNDETECTABLE TIMING ATTACK

During GPS-spoofing attack, the time synchronization with GPS signal is distorted. Therefore, only the phase angle will be shifted, keeping the magnitude same. The control center needs to apply bad data detection algorithm in the time-axis and phase angle data, rather than looking at the magnitudes. This requirement can be exploited by the attacker. The key idea is that attacker needs to shift the time reference by a very small degree, which goes undetected by the control center. If the attacker keeps shifting the time reference by this small amount over a period of time, it will be a significant amount of shift in time reference after the whole period. From the control center, it is not possible to detect the shift since the change in synchronization is done while satisfying all the undetectibility constraints.

A. Optimizing Attack Vector

For conventional FDIA detection, control center needs to check the residual: $||z-H\hat{x}||_2$. After the attack the corresponding measurement $z_a$ and estimated state variables $\hat{x}_a$. The residuals become $||z_a-H\hat{x}_a||_2 = ||z+a-H(\hat{x}+c)||_2 = ||z-H\hat{x}+a-Hc||_2$. $c$ is the estimated attack vector. The attacker goal is to make the term $||a-Hc||_2$ as small as possible so that $||z_a-H\hat{x}_a||_2$ remains less than the threshold $\tau$. The attack vector satisfying undetectibility constraint can be written as $Fa$, where the term $F=(H(H^TH)^{-1}H^TH-I)$. The attacker needs to satisfy the following criterion:

$$\min_a ||Fa||_2 \quad (18)$$

To avoid getting detected, the term $||Fa||_2$ needs to be between $\tau$ and $||z-H\hat{x}||_2$. The attacker must be able to satisfy the following optimizer:

$$\min_a \quad ||Fa||_2 \quad \text{s.t.} \quad ||Fa||_2 \leq \tau - ||z-H\hat{x}||_2 \quad (19)$$

Assume the impact threshold of attack vector is $\zeta$, which implies that if the attack vector is greater than this value, there will be a significant impact on the system. The attack vector a will be created in such way that it is less than impact threshold during each time instance, but the total impact will be significant after the total time period. For each time instance, the attacker has to satisfy the following:

$$\min_a \quad ||Fa||_2 \quad \text{s.t.} \quad ||Fa||_2 \leq \tau - ||z-H\hat{x}||_2 \quad ||a||_1 < \zeta \quad (20)$$

Each time instance can be depicted as index $i$; $i = 1,2, ... , T$. $T$ = total time period. Therefore for the whole time period the optimization criteria becomes:

$$\min_{a_i} \quad ||Fa_{i}||_2 \quad \text{s.t.} \quad ||Fa_{i}||_2 \leq \tau - ||z_{i,1}-H\hat{x}_{i,1}||_2 \quad ||a_{i,1}||_1 < \zeta \quad (21)$$

The next challenge is to find the impact threshold $\zeta$. The $\zeta$ must be greater than the $\ell_1$ norm of the attack vector for single time instance, but it must be less than the sum of the $\ell_1$ norm of the attack vector over the total $T$ period of time. Since the $||a||_1$ can takes the value between $0$ to $\zeta$ at each time instance, it should be between $\zeta/T$ to $\zeta$ so that the $\sum_{i=1}^{T} ||a_i||_1 > \zeta$ condition is satisfied.

The optimizer $21$ becomes:

$$\min_{a_i} \quad ||Fa_{i}||_2 \quad \text{s.t.} \quad ||Fa_{i}||_2 \leq \tau - ||z_{i,1}-H\hat{x}_{i,1}||_2 \quad \zeta/T < ||a_{i,1}||_1 < \zeta \quad (22)$$

In the optimization criteria $22$ mentioning the suffix $i$ is redundant, since if the attack vector at each time instance satisfies $\zeta/T < ||a_{i,1}||_1 < \zeta$, the impact will be automatically greater than threshold over the whole time period $T$. Additionally, $\zeta/T$ can be replaced as $\zeta'$. Since the eqn $22$ is a convex, there exists a global minima that corresponds to the attack vector satisfying undetectibility constraint. For the second inequality constraint, the solver needs to search the point in a wide range of values between $\zeta'$ and $\zeta$, depending on the size of time period $T$. The second inequality constraint can be computationally simplified by making the attack vector within the range $\zeta'$ to $\zeta'+\epsilon$, where $\epsilon$ is a small positive integer. In this case, the solver needs to find the optimum attack vector within small range of constraints.

B. Determining Impact Threshold

The next challenge is to find the impact threshold $\zeta'$. The impact must not exceeds the operating limit of the power system. For an instance, if the operating constraint is violated, the control center will be aware of the situation earlier than the expected and will take restorative action before the target is achieved by the attacker. The operating limits of the power system are:

Branch current limit between the bus i and bus j,

$$-I_{lim} \leq I \leq I_{lim}$$

Power flow limit between the bus i and bus j,

$$-P_{lim} \leq P \leq P_{lim}$$

The power flow between two buses generally depends on the voltage magnitudes of the two nodes, the phase angles of two nodes and the line admittance between the nodes. In AC power flow model, real power flow between the bus i and bus
\[ P_{ij} = V_i^2 (g_{si} + g_{ij}) - V_i V_j [g_{ij} \cos(\theta_i - \theta_j) + \theta_i \sin(\theta_i - \theta_j)] \]  

(23)

\( g_{si} \) is the shunt conductance at bus i, \( g_{ij} \) is the line conductance between bus and bus j, and \( b_{ij} \) is the line susceptance between bus i and bus j. \( V_i \) and \( V_j \) are the voltages at bus i and j respectively. For simplicity, the DC power flow model has been considered in this work. In the DC power flow model the voltage phase difference are very small (\( \theta_i \approx \theta_j \)) and the voltage magnitudes at buses i and j are normalized to \( r \approx b \).

Only power that comes into consideration is the real power \( P_{ij} \leq r x \) be negligible in DC power flow model, which implies \( r \ll x \). The line resistance is considered to be negligible in DC power flow model, which implies \( r < x \). Hence the susceptance can be approximated as \( b_{ij} \approx 1/x_{ij} \). The power flow between the bus i and j in DC model can be expressed as follows:

\[ P_{ij} = -V_i V_j \sin(\theta_i - \theta_j) b_{ij} \approx \sin(\theta_i - \theta_j)/x_{ij} \]

(24)

In the attack model described in the previous subsection, attack vector a consists of two elements (since two phase angles are required to be shifted in order to create meaningful attack vector)\(^{[25]}\). The \( \ell_0 \) norm of vector a is 2. Elements of attack vector a represents the shift in voltage phase angle at different buses. Assuming two attack targets bus i and bus j, the corresponding shift in phase angles are represented by \( a_i \) and \( a_j \). After the attack, the new power flow will be:

\[ P_{ij}' = \frac{\theta_i + a_i - \theta_j - a_j}{x_{ij}} \]

\[ = \frac{\theta_i - a_i}{x_{ij}} + \frac{a_i - a_j}{x_{ij}} \]

\[ = P_{ij} + \frac{a_i - a_j}{x_{ij}} \]

(25)

To make the power flow between bus i and bus j within the power flow limit, \( P_{ij}' \) must be less than \( |P_{lim}| \). The second constraint of the eqn \(^{[20]}\) can be rewritten as:

\[ \frac{a_i - a_j}{x_{ij}} < \frac{-|P_{lim}|}{x_{ij}} - \frac{\theta_i - \theta_j}{x_{ij}} \]

(26)

The right hand term of the eqn \(^{[25]}\) can be approximated as the impact threshold \( \zeta' \). The optimization criterion from eqn \(^{[22]}\) is modified to the following form:

\[ \min_{a_i} \{ \text{subject to} \}
\]

\[ \|F a_{i,t}\|_2 \leq \tau - \|z_{i,t} - H x_{i,t}\|_2 \]

\[ \zeta' < \|a_{i,t}\|_1 < \zeta' + \epsilon \]

\[ \epsilon > 0 \]

(27)

where, \( \zeta' = x_{ij} \left[ |P_{lim}| - \frac{\theta_i - \theta_j}{x_{ij}} \right] / T \)

IV. ROBUSTNESS OF PROPOSED ATTACK

We consider three important criteria that the proposed attack needs to satisfy in order to create an fully undetectable attack.

**Criterion I:** The power flow after attack must follow the power flow trend over time. Since during off peak period the flow is expected to be smaller, if the power flow during off peak period rises sharply, the control center can suspect about the abnormality and may take mitigation scheme. Therefore, the attacker needs to ensure the attack doesn’t create such anomaly, the power flow should be low during off peak period and high during peak period. The attack must cause the power flow exceed the flow limit during peak period, since the control center will not consider the rise in power flow as a abnormal scenario.

**Criterion II:** The attacker must have control over the impact of the undetectable attack. The attack must cause a significant impact only at the exact predetermined time instance.

**Criterion III:** The attack cannot be defended using optimal placement of the PMUs.

A. Proposed Method’s Validity for Criterion I

In order to satisfy the criterion 1, the power flow vs time curve must show similar trend for both of with attack and without attack conditions. This can be explained mathematically by comparing the slope of power flow after attack \( P_{ij}' \) curve with the power flow without attack \( P_{ij} \) curve. The slope of power flow after attack can be expressed as:

\[ \frac{\Delta P_{ij,t}}{\Delta t} = \frac{\Delta (\theta_{i,t} + a_{i,t} - \theta_{j,t} - a_{j,t})}{\Delta t} \times \frac{1}{x_{ij}} \]

\[ = \frac{1}{x_{ij}} \left[ \frac{\Delta (\theta_{i,t} - \theta_{j,t})}{\Delta t} + \frac{\Delta (a_{i,t} - a_{j,t})}{\Delta t} \right] \]

(28)

As the attack vector of the bus k at time instance t, \( a_{k,t} \) is the result from the optimal value by satisfying the condition of \( ||F a_{k,t}||_2 \leq ||z_{k,t} - H x_{k,t}||_2 \); the attack value at any given time make the \( ||F a_{k,t}||_2 \) term take any value between \( \tau \) and \( ||z_{k,t} - H x_{k,t}||_2 \). Thus the attack vectors at time t are not the functions of t. The second term of the eqn \(^{[28]}\) becomes zero, making \( \frac{\Delta P_{ij,t}}{\Delta t} \approx \frac{\Delta P_{ij,t}}{\Delta t} \).

From the aforementioned discussion, it can be concluded that the power flow after the proposed optimal attack will follow the actual power flow curve, and will exceeds the power flow limit during the peak-period.
B. Proposed Method’s Validity for Criterion II

Another feature of GPS-spoofing attack for consecutive time instance, is that at a given time instance the shift of the phase angle reference will be from the phase angle reference in the previous time instance. Since the phase angle is already shifted by an amount \( \alpha_t \) at the time instance \( t \), the shift in phase angle for the next time instance \( t+1 \) will be \( \alpha_t + \Delta_\alpha \). The modified phase angle at time \( t \) becomes:

\[
\theta'_t = \theta_t + \alpha_t
\]

(29)

For the next time instance \( t+1 \), the new modified phase angle \( \theta'_{t+1} \) will be shifted by a total \( \Delta_\alpha \). For the phase angle \( \theta_{t+1} \) during normal condition, the phase angle during GPS-spoofing attack condition becomes:

\[
\theta'_{t+1} = \theta_{t+1} + \alpha_t + \Delta_\alpha
\]

(30)

\[
\theta'_{t+1} = \theta'_{t+1} + \alpha_t + \Delta_\alpha
\]

(31)

This scenario affects the power flow calculation at each time instance. The corrected power flow after considering the phase angle shift from previous time instance can be represented as \( P'_{ij,t} \):

\[
P'_{ij,t} = \frac{\theta'_{ij,t} + \alpha_{i,t-1} + \alpha_{j,t} - \theta_{j,t}}{x_{ij}}
\]

(32)

Assuming the attack is initiated at time instance 1, and the attacker continues to create GPS-spoofing attack with time shift \( \alpha_t \), where \( t = 1,2,3,...,T \). At any time instance \( t \), the modified due to attack becomes:

\[
P'_{ij,t} = P_{ij,t} + \frac{\alpha_{i,t} - \alpha_{j,t}}{x_{ij}} + \sum_{k=1}^{t-1} \left( \frac{\alpha_{i,t} - \alpha_{j,t}}{x_{ij}} \right)
\]

(33)

At any time instance \( t \), the second constraint of optimizer \( 27 \) is satisfied and the power flow becomes:

\[
P'_{ij,t} = P_{ij,t} + \alpha_{ij,t} + \alpha_{jt} + t \times A
\]

(34)

The vector \( A \) corresponds to the attack vector, which satisfies \( \zeta' < A < \zeta' + \epsilon \). The term \( \epsilon \) is very small positive real number \( \epsilon < (\left| P_{lim} - (\theta_t - \theta_j) \right|/x_{ij})/T \). A can be approximated as \( [P_{lim} - (\theta_t - \theta_j)/x_{ij}]/T + \mu \). The modified power flow becomes:

\[
P'_{ij,t} = P_{ij,t} + \alpha_{ij,t} + \alpha_{jt} + t \times [P_{lim} - (\theta_t - \theta_j)/x_{ij}]\frac{T}{T + \mu}
\]

(35)

Since in eqn \( 35 \), \( t < T \), therefore \( M \) is negative and the term \( v < \epsilon < (t - T) \times (\left| P_{lim} - (\theta_t - \theta_j) \right|)/T \). The modified power in eqn \( 35 \) is less than \( P_{lim} \). For each time instance \( t < T \), the power flow after attack doesn’t exceed the flow limit of the line, therefore creating insignificant impact. However, after the time period \( T \), the modified power becomes:

\[
P'_{ij,t} = P_{ij,t} + \alpha_{ij,t} + \alpha_{jt} + T \times [P_{lim} - (\theta_t - \theta_j)/x_{ij}] + \mu
\]

(36)

Eqn \( 36 \) shows that the power flow after the time period \( T \) exceeds the flow limit. As a result, the attacker can create significant impact after exactly \( T \) time instance, without causing any significant damage for the time instance \( t < T \). This enables the attacker a complete control over the attack’s impact on power grid.

C. Proposed Method’s Validity for Criterion III

The optimal placement algorithm relies on using residual based attack detection and place the PMUs at specific locations which can make the system most observable. The proposed method doesn’t need the information of the whole grid topology, rather it only requires the topological information of two connected buses, both equipped with PMUs. Therefore the conventional optimal placement methods will not be useful against the proposed undetectable attack.

Moreover, at every time instance, the attacker ensures that the attack will go undetected by conventional BDD. The optimal placement methods based on residual based test will not be able to anticipate this type of attack.

V. EXPERIMENT METHOD

The proposed undetectable attack has been tested on IEEE \( 39 \) bus 10-machine New England Power System [67]. The physical power system is simulated in MATLAB SIMULINK. To simulate Phasor Measurement Unit (PMU), default PMU model in SIMULINK is used. The PMU is considered to be transmitting \( 60 \) fps data rate.

The attack vector \( a \) corresponds to the phase angle of voltage. For simplicity, only the DC power flow model has been considered. The attacker calculates the phase angle shift required to instigate undetectable attack, and then creates the corresponding time shift by spoofing the GPS signal and thereby causing loss of synchronization in the PMU. The relation between the time shift \( t_d \) and corresponding specific angle variation \( \Delta \theta \) can be written as:

\[
\Delta \theta = 2\pi f_0 t_d
\]

(37)

The optimization criterion described in eqn \( 27 \) is solved using MATLAB Yalmip tool box. For each time instance, the phase angle shift required to satisfy all the constraint in eqn \( 27 \) is computed by using the Yalmip solver. The attack vector \( a \) represents the required phase angle shift \( \Delta \theta \) to incur successful attack, which is done by applying the time delay from eqn \( 37 \) at bus i and bus j in the SIMULINK model. The simulated voltage angle and impedance data from the power system model is then fed into MATLAB to compute the power flow between bus i and bus j.

The detectibility of the proposed attack model is tested using two robust residual based state estimation methods: Weighted Least Square (WLS) \( 27 \) and Deviation based Kalman Filtering (DKF) \( 66 \) method. The general Kalman
The Probability of Detection (PD) over time period T can be defined as:

\[ PD = \frac{\text{Total : } TP}{\text{Total : } TP + \text{Total : } FN} \]  

The threshold is predetermined by taking the mean of \( \| r \|_2 \) over a specific time period during a normal condition (with no attack). As there are measurement and process noises in the system, a standard deviation \( \sigma \) of the \( \| r \|_2 \) values over the same time period is added to the mean. The threshold can be expressed as \( \mu + n\sigma \), where \( \mu \) is the mean of the \( \| r \|_2 \) values over time T and \( \sigma \) is the corresponding standard deviation. The \( n \) is an integer, and the PD over T is calculated with varying \( n = 1, 2, 3, \ldots \).

For both of the WLS and DKF, a random Gaussian measurement noise \( \nu \) with a mean 0 and variance \( \sigma^2 \) is added to the voltage and current measurements. The \( \sigma^2 \) is calculated with the voltage measurements under pre-attack condition. For DKF, the initial state vector \( x(0) \) is assumed to be 0, and the initial covariance matrix \( P \) is assumed to be an identity matrix.

For IEEE 39 bus system used for this work, load at bus 18 is increased by 50% at 13 sec. and again another 50% at 18 sec. In this way, a dynamic load varying condition is considered which reflects the increase in the load at the peak hour. The attacker instigate a small shift in GPS 1 PPS over time period T, such that the perceived power flow through the branch 3-18, which is calculated using the shifted phase angle measurements at each end of the branch, increases. The target is to make a significant impact on the calculated power flow during the peak load at 18 sec. At this time, the calculated power flow through the branch 3-18 will cross the MVA limit of the branch, even though the actual power flow is within the limit. The MVA rating of the line 3-18 of IEEE 39 bus system is 500 [67].

\[ z_{16 \times 1} = H_{46 \times 38} x_{38 \times 1} + \nu_{46 \times 1} \]  

\( H \) represents the relation between the state vector and measurement vector, which is therefore the impedance matrix \( Y \) of the system. \( \nu \) represents the measurement noise which is a Gaussian noise as discussed in the section V.

A. Impact on Power Flow measurement

At first, starting at 5 sec., the proposed optimization algorithm for each time instance is executed and the corresponding optimal attack vector \( a_{op} = \theta_0 \), which is the phase angle shift required to achieve the target of misleading the power flow calculation, is determined. In the rest of the paper, the term attack vector and phase angle shift will be used interchangeably. Time-shifts (as in eqn. [37]) are applied to the GPS 1 PPS signal of the corresponding PMUs located at the buses 3 and 18. The power flow through the branch connecting the buses 3 and 18 is calculated using DC power flow equation. Since there is a presence of time shift in the GPS 1 PPS into the corresponding PMUs at the both ends of the branch For random attack, the perceived power flow through the branch will be different from the actual value.

In the second case, two random time shifts are applied to GPS signals received by the corresponding PMUs located at buses 3 and 18 and the corresponding power flow is calculated at each time instance, starting from 5 sec. The attack vector in this case is \( a_{rand} \).

VI. RESULT

The goal of this proposed model is to create undetectable GPS-spoofing attack (GSA). There are two evaluation criteria: 1) The attack must be undetected by conventional detection tests and 2) the attack must create significant impact over the time period T, however after a single time instance the impact cannot be significant.

As the IEEE 39 bus system has been considered for this work, there are 38 state variables and 46 measurement variables. The vector \( x \) consists of the voltage phasors with a total of 38 elements and the vector \( z \) consists of the current phasors of the branches with a total of 46 elements.

Fig. 2 and 3 demonstrates the results obtained from applying GPS-spoofing attack using proposed attack model and using random attack values, respectively. From fig. 2 we can observe that the perceived power flow calculated using the shifted phase angle measurement is higher than the actual power flow through the branch 3-18. for each time instance after initiating attack at 5 sec. When the power flow through the branch increases, the calculated power flow is also increased by a small amount, keeping the calculated power flow within the line flow limit. At 18 sec, when the maximum power flows...
through the branch at peak hour, the calculated power flow exceeds the line flow limit, which is 500 MVA. Therefore the control center will be forced to take contingency actions despite the actual power flow is within the limit, and the branch 3-18 will be tripped.

For the random attack vector in fig. 3, the calculated power flow can both increase or decrease from the actual power flow. Another observation is that, the perceived power flow can cross the line flow limit even before the peak hour is reached, thereby alerting the control center about possible cyberattack, since the SO at control center will not expect power flow increase significantly at the off peak hour. Moreover, for random attack vector, the attacker doesn’t have control over the magnitude of the calculated power flow and the time when the calculated flow exceeds the limit. Even at peak hour, the perceived power flow can go both above and below the actual power flow, which impedes the attackers goal of instigating controlled attack.

B. Undetectibility Analysis

Fig. 4 and 5 depict the measurement residuals $||r||_2$ using Deviation based Kalman Filtering (DKF) method. The residuals $r$ is computed by taking the difference between estimated measurement $Hx$ and the measurement under attack $Z_a = Z + a$ [16]. Here $a$ is the optimum attack vector and the phase angle shift at each time instance. In the fig. 4 and 5 the $\ell_2$-norm of the residuals is very small, to the order of $10^{-2}$. Three horizontal axes represents the predetermined threshold. During most of the time instances, the residuals is less than the threshold, therefore making the attack undetectable in most of the time instances. When the threshold is $\mu + 3 \times \sigma$, only a very small portion of time instances crosses the threshold and get detected. For smaller threshold $\mu + 2 \times \sigma$, the probability of attacks getting detected (PD) increases, since more residuals crosses the threshold. The PD is further increased for the threshold $\mu + 1 \times \sigma$.

Similar behavior can be observed for the residuals computed from Weighted Lease Square (WLS) method (fig. 6 and 7).

Table I and II summarize the PD of both DKF and WLS methods for the residuals between the real and imaginary components of observed measurements and the real and imaginary components of estimated measurements. From the above
results, we can conclude that the proposed attack model goes undetected most of the time instances (> 50%). However, the thresholds \( \mu + 1 \times \sigma \) and \( \mu + 2 \times \sigma \) can provide the best performance in terms of PD. Nevertheless, there are measurement noises that can also be mistakenly perceived as attack in these cases. The threshold \( \mu + 3 \times \sigma \) is the most optimal one, which provides higher probability of attack detection using DKF method than using WLS method.

The next part is to perform the undetectability against \( \chi^2 \) test. For 45 Degree of Freedom (DF) and significance level of 95%, the threshold is \( \approx 28 \). The residuals \( ||r||_2 \) from both of the KF and WLS from fig. 4 to 7 are much less than the threshold. Table I summarizes the probability of detection against \( \chi^2 \)-test using varying significance level and DF. From the table, it can be concluded that the proposed attack is undetected against \( \chi^2 \)-test.

| Threshold          | DKF (%) | WLS(%) |
|-------------------|---------|--------|
| \( \mu + 3 \times \sigma \) | 3       | 0.5    |
| \( \mu + 2 \times \sigma \) | 12.5    | 18     |
| \( \mu + 1 \times \sigma \) | 29.5    | 31.5   |

VII. LIMITATIONS OF PROPOSED MODEL

The key idea of the proposed attack model is the phase angle shift required to be undetectable is calculated using optimization technique. The optimization equation considers the commonly used state estimation based Bad Data Detection (BDD) techniques in the constraints, therefore the attack created using spoofing remains undetectable for conventional state estimation based BDD techniques such as weighted least squares and Kalman Filtering. The undetectability of the attack against BDD techniques is ensured by applying stealthy FDIA attack models developed in the previous literature to bypass state estimation-based detection schemes. Since most detection schemes utilize either of WLS or KF based estimation techniques, the proposed attack model in this work remains stealthy in the current cyber-physical infrastructure. However, if a detection model using an approach different from any form of KF, WLS or any other robust state estimation techniques can be developed, our proposed attack can be detected by that.

Nevertheless, the detector can use a smaller threshold so that a small change in the estimated measurement can be detected; however, reducing the threshold to a small value has the risk of producing False Positive (FP) flag. For instance, a measurement noise can exceed the threshold if the threshold is kept very small, therefore a random noise is going to be detected as an attack.

Another approach of detecting small phase angle shifts caused by spoofing is using time-series data and monitoring any deviation based on the estimation using the dataset of the previous time window. A possible solution is the Hankel matrix based data estimation [68]. However, testing the undetectability of the proposed algorithm against Hankel matrix based approach and creating an optimization algorithm based on Hankel matrix based estimator is beyond the scope of this paper. We are planning to extend our work to the Hankel matrix based approach in future.

VIII. CONCLUSION

Despite providing efficient and accurate time-synchronized data, the Phasor Measurement Unit (PMU) is prone to various types of cyberattacks. One of the most critical cyber attacks against PMU is the GPS-spoofing attack, where the reference signal for time-tagging is modified. This paper aims at developing a stealthy GPS-spoofing attack, where the attacker inject very small scale shift in the GPS 1 PPS signal at each timestamp, and gradually increases the deviation. Since the effect of timestamp shift is reflected by a shift in phase angle, the perceived power flow through a branch calculated using the phase angle at the both ends of the branch is changed, even
though the actual power flow through the same branch remains unchanged. The attacker’s goal is to increase the perceived power flow, and make the perceived power flow exceeds the line flow limit at the peak hour.

At first, the paper proposes an undetectable attack scheme which is able to bypass the Bad Data Detection (BDD) algorithm. The attack is applied by solving a convex optimization criterion at regular time interval, so that after a specific time period the attack vector incurs a significant change in the perceived power flow calculated with shifted phase angles, hence forcing the control centre take contingency actions. Secondly, the proposed attack model is tested on the IEEE 39 bus system in SIMULINK and the corresponding impact on the calculated power flow through the branch connecting buses 3 and 18 is observed. Load at bus 18 is varied to reflect the peak power demand. Thirdly, the undetectability of the proposed algorithm is tested against WLS, DKF and $\chi^2$-test. The result shows that the attacker can modify the perceived power flow through the branch 3-18 and make it cross the line flow limit at the peak hour (18 sec.). Moreover, it can be observed that the proposed attack remains mostly undetected against all three detection scheme. For WLS, the probability of detection is less than 30% for the predetermined thresholds. For DKF, the probability is also less than 30%, whereas for the largest predetermined threshold it can detect between 3 – 8% of the time. For the same threshold, the WLS can detect only 0.5 – 1% of the times. The proposed attack is completely undetected against $\chi^2$ test.

REFERENCES

[1] M. M. Ahmed and W. L. S.，“Supervisory control and data acquisition system (SCADA) based customized remote terminal unit (RTU) for distribution automation system,” PECCon 2008 - 2008 IEEE 2nd International Power and Energy Conference, pp. 1655–1660, 2008.

[2] A. Abur and A. Gomez Exposito, “Power system state estimation: theory and implementation,” p. 327, 2004.

[3] A. G. Phadke and J. S. Thorp, "Synchronized Phasor Measurements and Their Applications," 2017.

[4] IEEE Power & Energy Society, “IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005) - IEEE Standard for Synchronized Phasor Data Transfer for Power Systems,” IEEE Standards, 2011.

[5] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, “Wide-area monitoring, protection, and control of future electric power networks,” Proceedings of the IEEE, vol. 99, no. 1, pp. 80–93, 2011.

[6] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, “Synchronized phasor measurement applications in power systems,” IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 20–27, 2010.

[7] M. Kuzunovic, S. Meliopoulos, V. Venkatasubramanian, and V. Vittal, “Application of Time-Synchronized Measurements in Power System Transmission Networks,” 2014.

[8] G. B. Giannakis, V. Kekatos, N. Gatsis, S. J. Kim, H. Zhu, and B. F. Wollenberg, “Monitoring and optimization for power grids: A signal processing perspective,” IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 107–128, 2013.

[9] C. Tu, X. He, Z. Shuai, and F. Jiang, “Big data issues in smart grid – A review,” Renewable and Sustainable Energy Reviews, vol. 79, pp. 1099–1107, 2017.

[10] W. Li, L. Vanfretti, and J. H. Chow, “Pseudo-Dynamic Network Modeling for PMU-Based State Estimation of Hybrid AC/DC Grids,” IEEE Access, vol. 6, pp. 4006–4016, 2017.

[11] Z. Shuai, W. Huang, C. Shen, J. Ge, and Z. J. Shen, “Characteristics and Restraining Method of Fast Transient Inrush Fault Currents in Synchronverters,” IEEE Transactions on Industrial Electronics, vol. 64, pp. 7478–7497, 2017.

[12] M. N. Aman, K. Javed, B. Sikdar, and K. C. Chua, “Detecting data tampering attacks in synchrophasor networks using time hopping,” IEEE PES Innovative Smart Grid Technologies Conference Europe, 2016.
