Revisiting GPS Spoofing in Phasor Measurement: Real-World Exploitation and Practical Detection in Power Grids

CHUNGHYO KIM*, Korea Electric Power Corporation, Republic of Korea
JUHWAN NOH, Korea Advanced Institute of Science and Technology, Republic of Korea
ESMAEIL GHAHREMANI, Hydro-Québec's Research Institute (IREQ), Canada
YONGDAE KIM, Korea Advanced Institute of Science and Technology, Republic of Korea

Phasor Measurement Units (PMUs) are critical devices in modern power grids, providing precise voltage and current phasor measurements (synchrophasors) for real-time monitoring, fault detection, and stability assessment. While previous research suggested that arbitrary time manipulation through GPS spoofing could disrupt grid operations, our study reveals that successful attacks require specific conditions, contrary to earlier assumptions.

Through careful analysis of the synchrophasor data specification (IEEE Standard C37.118.x), we demonstrate that arbitrary time manipulation **does not** directly lead to phase manipulation. Instead, arbitrary manipulations can cause GPS holdover (loss of lock), alert operators with erroneous timing, and ultimately invalidate the received synchrophasors. An experiment with a commercial PMU confirms our specification analysis. We identify the time spoofing conditions to avoid GPS holdover and discover that nanosecond-scale signal alignment (approximately 375 ns error) and gradual time manipulation (around 50 ns/s error) are required.

Experiments on a commercial Wide Area Monitoring System (WAMS) testbed demonstrate that GPS spoofing meeting the identified criteria results in a 500-microsecond time error (10.8-degree phase error) after 12 hours without triggering alarms. Given that a 60-degree phase variation is considered a fault, triggering protection mechanisms, this GPS spoofing technique could potentially induce false faults within 70 hours.

To counter this threat, we propose a practical method to distinguish GPS spoofing-induced false faults from actual faults caused by events like lightning strikes or ground shorts. Analysis of 10 real-world incidents from the past six months demonstrates that genuine faults consistently exhibit instantaneous phase variations within three electrical cycles, providing a basis for differentiation.

CCS Concepts: • **Computer systems organization → Sensors and actuators**; • **Security and privacy → Security in hardware**.

Additional Key Words and Phrases: Phasor Measurement Unit, Synchrophasor, Time Synchronization, GPS Spoofing, Time Manipulation, Wide Area Monitoring, False Protection, Mitigation Method

ACM Reference Format:
Chunghyo Kim, Juhwan Noh, Esmaeil Ghahremani, and Yongdae Kim. 2025. Revisiting GPS Spoofing in Phasor Measurement: Real-World Exploitation and Practical Detection in Power Grids. *ACM Trans. Priv. Sec.* 1, 1, Article 1 (January 2025), 28 pages. https://doi.org/10.1145/3720543

*Also with Korea Advanced Institute of Science and Technology

Authors' addresses: Chunghyo Kim, Korea Electric Power Corporation, Daejeon, Republic of Korea, chunghyo.kim@kepco.co.kr; Juhwan Noh, Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea, juhwan.noh@kaist.ac.kr; Esmaeil Ghahremani, Hydro-Québec's Research Institute (IREQ), Varennes, Canada, esmaeil.ghahremani.1@ulaval.ca; Yongdae Kim, Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea, yongdaek@kaist.ac.kr.

Manuscript submitted to ACM

1 INTRODUCTION

In 2003, a massive power blackout affected eight states in the United States and the province of Ontario in Canada, impacting over 50 million people and disconnecting 61,800 MW of the electricity distribution network. It took more than a week to fully restore power [28]. This event highlighted the urgent need for improved situational awareness in managing electric grids. Following an extensive investigation, the final report recommended the installation of time-synchronized recording devices to capture wide-area snapshots of the electric grid. Phasor Measurement Units (PMUs) emerged as essential tools for this purpose, providing precise, time-synchronized measurements of electrical waves. In response to these recommendations, the Western Electricity Coordinating Council (WECC) successfully demonstrated a situational awareness system based on PMUs through their Wide Area Monitoring System (WAMS) [11]. This system has significantly enhanced the ability to detect and respond to grid anomalies.

PMUs generate synchrophasors, which are precise measurements of electrical waves taken up to 120 times per second and synchronized using a common time source, primarily the Global Positioning System (GPS). These synchrophasors facilitate grid status monitoring by providing time-synchronized measurements of electrical properties such as voltage and current. Currently, over 2,500 PMUs are operational across North America [41]. The data collected by PMUs have a wide range of applications in grid management, including power flow calculation, wide-area monitoring, oscillation detection, load shedding, voltage stability monitoring, event replay, linear state estimation, fault location, and advanced transmission network protection. These applications have been extensively discussed and demonstrated in various studies [6, 10, 13, 18, 22, 23, 25, 27, 30, 32, 45, 48, 51].

Fig. 1 presents a simplified diagram of a WAMS, which consists of three primary components: GPS receivers, PMUs, and grid applications. GPS receivers and PMUs are placed in electrical substations across a wide geographical area. PMUs produce synchrophasors by measuring the magnitude and phase of electrical properties in power grids, and they append the exact timing of these measurements using GPS receivers. These synchrophasors are then transmitted through a wide area network to a central control center, where they are time-aligned for various grid applications. Accurate time synchronization within WAMS is crucial because any discrepancies in the time references of PMUs can lead to incorrect outcomes in grid applications, potentially compromising grid reliability.

Given the critical role of time synchronization in WAMS, it is well known that time manipulation attacks can maliciously alter the time reference of PMUs. This leads to erroneous phasor measurements, which are essential for monitoring and control applications. The red points in Fig. 1 highlight three types of time manipulation attack points targeting one of WAMS components, and Table 1 details the scenarios of time manipulation and their impacts as

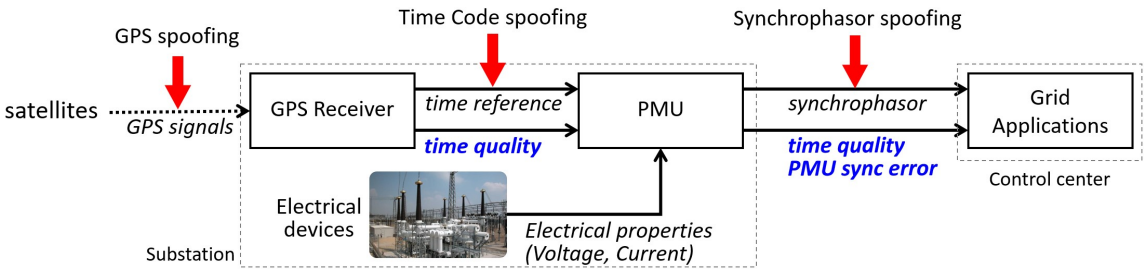


Fig. 1. Simplified diagram of WAMS and its attack points

Table 1. Previous Studies on GPS Time Spoofing in Power Systems

Ref.	Target	Time Manipulation	Grid Application	Impact
[29]	GPS receiver	Arbitrarily 6.8-7.2 ms	Load shedding	False control
[39]	GPS receiver	Gradually up to 3.3 μs	Protection	False control
[1]	PMU	Arbitrarily 10 μs	Anti-islanding	False control
[17]	Synchrophasor	Arbitrarily 2.3 ms	Voltage stability	Monitoring error
[42]	Synchrophasor	Arbitrarily 3.3 ms	Load shedding	Delayed control
[8]	Synchrophasor	Arbitrarily 0.83 ms	State estimation	-
[4]	Synchrophasor	Arbitrarily 1-1000 ms	System stabilizer	Oscillation
[49]	Synchrophasor	Arbitrarily 1 s	Fault detection	False notification
[34]	Synchrophasor	Arbitrarily 200 ms	Damping control	Unstabilized

documented in previous studies. Since time code and synchrophasor spoofing assume the feasibility of the precedent spoofing stage, GPS spoofing [1] becomes the sole attack entry point for WAMS.

However, previous studies have primarily focused on the feasibility of manipulating time references, without providing a comprehensive end-to-end analysis from the reception of GPS signals to their application in grid operations. This limited focus can lead to an incomplete understanding of the potential system-wide impacts of time synchronization attacks. To address these gaps, we conduct a comprehensive analysis of IEEE Standard C37.118.x, which outlines the requirements for synchrophasor measurements that all WAMS components must adhere to. This standard includes provisions for time quality monitoring, specifically through properties such as *time quality* and *PMU sync error*, which are highlighted in blue in Fig. 1. These properties assess the GPS receiver's satellite lock status and determine the validity of the synchrophasor data, ensuring the reliability of time-synchronized measurements across the entire system.

To experimentally validate the impact of time manipulations, as described in previous studies, on WAMS that comply with the IEEE standard, we conducted tests on commercial WAMS setups and devices. Our experiments revealed that time manipulations though GPS spoofing in existing works [29, 39] caused the GPS receiver to lose its lock on GPS signals, resulting in degraded *time quality* and activated *PMU sync errors*. Consequently, the synchrophasors became unsuitable for grid applications. These findings demonstrate that arbitrary time manipulation suggested by previous works did not lead to the anticipated phase manipulation, contradicting previous scenarios that suggested arbitrary phase manipulation could cause cascading failures in WAMS.

However, we found that phase manipulation through GPS spoofing is feasible when *time quality* is maintained, and *PMU sync errors* are not triggered. Successful phase manipulation requires two conditions: seamless takeover and gradual time manipulation. Seamless takeover involves accurately aligning the spoofed signals with authentic satellite signals at a higher strength, allowing the target receiver to lock onto the spoofing signal smoothly without interruption. Gradual time manipulation involves making incremental adjustments to the time, ensuring the GPS lock is not lost. Through experiments in the commercial testbed deployed at Hydro-Québec, we demonstrated that phase measurements and power flow calculations could be manipulated while maintaining good *time quality* and avoiding *PMU sync errors*. This was achieved when the required time alignment accuracy for seamless takeover was less than 375 ns and the time adjustments were less than 50 ns/s. Moreover, our analysis revealed that spoofing can induce false faults on transmission lines, potentially triggering protection controls to disconnect the line, even under normal operating conditions.

[1]According to research conducted by Ioannides et al. [16], other Global Navigation Satellite Systems (GNSS) are, in principle, also vulnerable to spoofing attacks.

To counteract the threat of GPS spoofing, we propose a mitigation strategy that leverages the temporal characteristics of faults. By distinguishing between false faults induced by GPS spoofing and actual faults caused by events such as lightning strikes or ground shorts, we can prevent incorrect control commands. To develop this strategy, we analyzed all faults that occurred on a 345-kV high-voltage transmission line operated by Korea Electric Power Corporation (KEPCO) over a six-month period. Our analysis revealed a significant difference in the temporal patterns of phase variations. Actual faults exhibit a rapid phase variation of nearly 180° within three electrical cycles. In contrast, phase variations induced by GPS spoofing develop gradually, taking several days to reach a comparable degree of change.

By monitoring the rate of phase variation over the specified time frame, operators can differentiate between actual faults and those resulting from GPS spoofing. This significant temporal discrepancy can be exploited to maintain the integrity of the power grid, ensuring that only legitimate faults trigger protection mechanisms and preventing destabilizing incorrect commands. This approach highlights a practical method to safeguard grid operations against sophisticated spoofing attacks.

The remainder of this paper is organized as follows. Section 2 discusses the basic principles of GPS receiver functions, including holdover, also known as loss of lock, and the process of generating timing signals. Section 3 presents an analysis of the specifications and demonstrates the feasibility and implications of the spoofing attacks examined in previous studies. Section 4 investigates the two requirements for time manipulation that avoid loss of lock, resulting in successful phase manipulation of synchrophasors. Section 5 describes the end-to-end configuration of WAMS with a commercial setup. This section also presents test results and discusses the consequences for power grids. Section 6 analyzes the principles of line differential current protection and the occurrence of false faults due to spoofing attacks. Section 7 proposes a mitigation method that utilizes the characteristics of phase variation patterns observed in both false and actual faults. Section 8 evaluates the false negatives and performance overhead associated with the proposed mitigation method. Section 9 summarizes related work, providing context and background for the current study. Finally, Section 10 offers concluding remarks, summarizing the key findings and contributions of this paper.

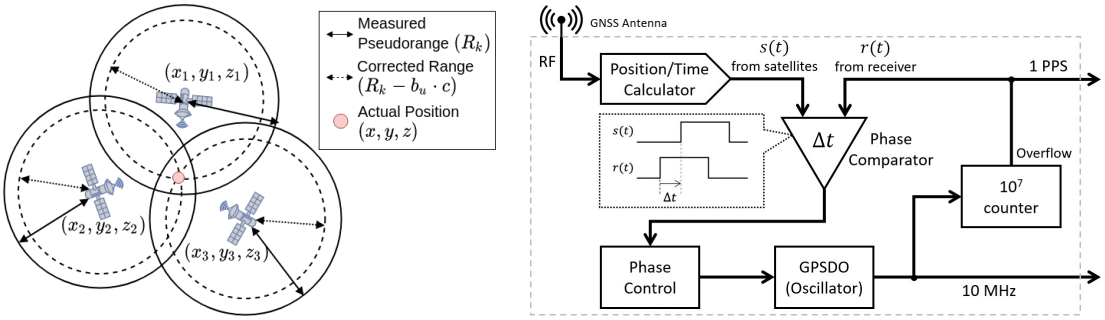
2 BACKGROUND

2.1 Global Positioning System (GPS)

The GPS provides accurate location and time information using satellites. GPS satellites broadcast signals that contain navigation data, and a GPS receiver calculates its location coordinates and clock offset using at least four satellite signals. In detail, navigation data include 1) orbital data called *ephemeris data*, which allows receivers to estimate satellite locations, and 2) *time-of-week (TOW) count*, namely timestamps indicating when the signal is generated [43]. As a GPS receiver can determine a propagation delay of the received signal using the TOW count, it can measure the pseudorange R_k from satellite k to itself by multiplying the delay by the speed of light. (R_k is called *pseudorange* because it is the coarse range from the satellite to the receiver; it contains the error caused by clock offset, which is the difference between the receiver's system time and the GPS time.) As a receiver can estimate the satellite's coordinates with ephemeris data, its location coordinates $r = (x, y, z)$ can be computed by solving the following navigation equations.

$$R_k = \sqrt{(x - x_k)^2 + (y - y_k)^2 + (z - z_k)^2} + b_u \cdot c \tag{1}$$

where x_k, y_k, and z_k are the coordinates of satellite k's geographic location, b_u is the clock offset of a receiver, R_k is the pseudorange, and c is the speed of light. Eq. (1) represents a sphere whose center is (x_k, y_k, z_k) and radius is



(a) GPS trilateration (b) Timing signal generation in a GPS receiver

Fig. 2. Two-dimensional representation of a GPS trilateration and GPS Timing Signal

$(R_k - b_u \cdot c)$. Thus, solving the navigation equations involves finding the intersection of multiple spheres, as illustrated in Fig. 2a. Since there are four unknowns, x, y, z, and b_u, at least four visible satellites are required to determine them.

2.2 GPS Receiver Operation and Holdover State

A GPS receiver calculates its clock offset, denoted as b_u, in addition to determining its location coordinates. This enables the receiver to deliver precise time information to grid applications via a network-based time protocol (e.g., Network Time Protocol or Precision Time Protocol) or a direct timing signal (e.g., IRIG time code). To stably generate these signals, a GPS receiver uses a GPS disciplined oscillator (GPSDO), whose output frequency is continuously steered to match the satellite timing signal $s(t)$, as illustrated in Fig. 2b. Internally, the GPSDO compares the difference of 1 PPS between satellite signals $s(t)$ and the internal oscillator signal $r(t)$, and compensates for the time gap Δt by steering the oscillator to align with $s(t)$.

However, this operation can fail because weak GPS signals can easily be corrupted. Factors such as antenna failure, natural signal interference, and intentional jamming can prevent receivers from receiving GPS signals and cause loss-of-lock onto the signals. Additionally, multi-path errors and spoofing signals can degrade the time accuracy of the signals. To continue providing accurate timing even in these situations, GPS receivers activate the holdover mode, which relies on the internal clock only and stops tracking the external signals. From the adversary's perspective, a time spoofing attack might not succeed if the holdover mode is activated, because the receiver will ignore the external spoofing signals.

3 CAN ARBITRARY TIME MANIPULATION CAUSE PHASE MANIPULATION?

If the spoofing pattern of arbitrary time manipulation, as presented in previous studies, triggers holdover, the attacker's intention to induce false protection fails for two reasons. First, the receiver distrusts the external spoofing signals and relies on the internal clock instead, thus preventing it from being controlled by the adversary's intention. Second, a PMU detects poor *time quality*, leading to a *PMU sync error*. As a result, the synchrophasor data generated by the PMU becomes invalid and unusable for grid applications.

Therefore, it is necessary to confirm whether the arbitrary time manipulation [29, 39] presented in Table 1 actually triggers holdover. To check this, we analyzed the specifications, and examined the results and implications using commercial devices.

3.1 Specification Analysis

The Inter-Range Instrument Group (IRIG) time code, commonly used in industrial applications, is generated by a GPS receiver and fed to timing applications. IEEE Standard C37.118.1 enhances this time code with an additional feature, *time quality*, for the synchronization of Phasor Measurement Units (PMUs). This *time quality* is represented by four bits at IRIG positions 71 to 74 and is set to all zeros when the receiver locks onto a traceable UTC source, such as GPS satellites.

IEEE Standard C37.118.2 further specifies that the PMU data format incorporates the four-bit *time quality* value generated by the GPS receiver, along with an additional one-bit *PMU sync error*. The sync error bit indicates the validity of the synchrophasors and is set when the time quality is non-zero.

As described in Section 2.2, any arbitrary time manipulation that causes the receiver to lose lock on GPS satellites will switch the receiver to holdover mode. This transition to holdover mode would degrade the *time quality*, resulting in a non-zero value. Consequently, this would activate the *PMU sync error* and invalidate the synchrophasors. To validate these theoretical implications, we conducted experiments using a commercial PMU, which are described in the following sections.

3.2 Experimental Setup and Results

Fig. 3 illustrates the experimental setup used to test the feasibility of GPS spoofing attacks on Phasor Measurement Units (PMUs). The spoofing signal is generated using a custom spoofer built on the GPS-SDR-SIM platform [7]. This spoofing signal was then mixed with the authentic satellite signal before being introduced to the target GPS receiver.

The GPS receiver employed in our experiments, provided by a leading manufacturer for PMUs in operational power systems [2], includes front-panel indicators that display the current operational status, alternating between satellite lock and holdover modes. Initially, the green indicators confirmed active GPS satellite locks, indicating that the receivers were functioning correctly. Following this, we injected spoofing signals designed to manipulate the time, as outlined in Table 1, to observe the response of the receivers.

The results consistently demonstrated that in each scenario listed in Table 1, the injection of spoofing signals caused the receivers to switch into holdover mode. This outcome signifies that arbitrary time manipulation is ineffective within a commercial setup. The receivers detected the spoofing signals and subsequently entered holdover mode. This resulted in poor *time quality* and a *PMU sync error*, rendering the synchrophasor data invalid and alerting the grid operator to a time synchronization issue.

[2]To prevent potential exploitation of live systems, we anonymize the specific manufacturer and model name.

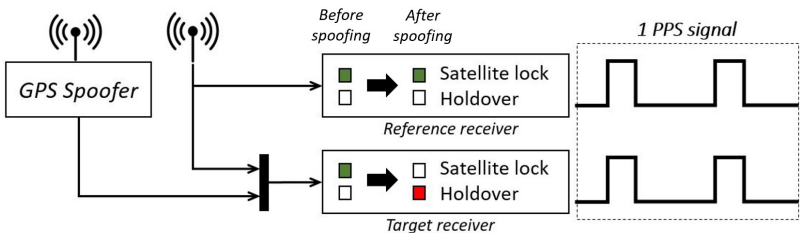


Fig. 3. Experimental setup for testing the feasibility of previous works

4 TIME SPOOFING FOR SUCCESSFUL PHASE MANIPULATION

Building on the findings from Section 3, this section explores the specific requirements for time spoofing aimed at successfully manipulating phase in PMUs without triggering holdover mode. The ability to generate seemingly authentic yet falsified synchrophasor data poses a significant threat to grid operations. For such time spoofing to succeed, two conditions are required: 1) Seamless Takeover of the Control [44] and 2) Gradual Time Manipulation.

4.1 Requirements for Avoiding Holdover during Spoofing

4.1.1 Seamless Takeover of the Control. For successful GPS spoofing, the spoofer must first synchronize with the authentic satellite timing. This synchronization allows the spoofer to seamlessly take over control by broadcasting a stronger signal. Precise time alignment between the authentic and spoofed signals is crucial, which was previously discussed by Tippenhauer et al. [44]. If misaligned, the receiver loses lock on the authentic signal, triggering a holdover notification to the system administrator. To achieve successful synchronization, the spoofer must accurately estimate and compensate for any time offset.

4.1.2 Gradual Time Manipulation. Once the target receiver's time is synchronized with the spoofer using the seamless takeover, the spoofer can introduce an intentional time gap Δt, as shown in Fig. 2b. This gap is then manipulated by adjusting the internal oscillator. However, the rate of time manipulation must not exceed the GPSDO's steering speed. Exceeding this speed leads the receiver to detect a time quality issue and enter holdover mode. To avoid detection, the time manipulation must be gradual, slowly progressing towards the adversary's target time.

4.2 Implementation of GPS Spoofer

4.2.1 GPS Time Spoofing Principle. To manipulate the GPS position and time of a target receiver, the simulated pseudorange must be updated to account for the desired manipulation. For simplicity in our model, we consider a scenario where the spoofer's signal originates from a location (x_u, y_u, z_u) identical to that of the target receiver, and the spoofer's clock is initially synchronized with true GPS time ($b_u = 0$). Under these assumptions, we can modify Eq. (1) as follows:

$$\begin{aligned} R'_k &= R_k + R_s \\ &= \sqrt{(x_u - x_k)^2 + (y_u - y_k)^2 + (z_u - z_k)^2} + t_s \cdot c \end{aligned} \tag{2}$$

To successfully lock a target receiver onto a spoofing signal and manipulate its position and time estimates, the spoofing signal must simulate at least four satellite signals. The composite spoofing signal, denoted as s_p, can be expressed as:

$$s_p(t) = \sum_{k=1}^{n} s_k(t - \frac{R'_k}{c}) \tag{3}$$

where $s_k(t)$ represents the signal generated by satellite k at time t, n is the number of simulated signals, and $\frac{R'_k}{c}$ is the simulated propagation delay. This delay is crucial for the target receiver to measure the intended pseudorange. Due to the continuous orbital motion of satellites, GPS spoofers must periodically update and apply the simulated pseudorange when generating spoofing signals.

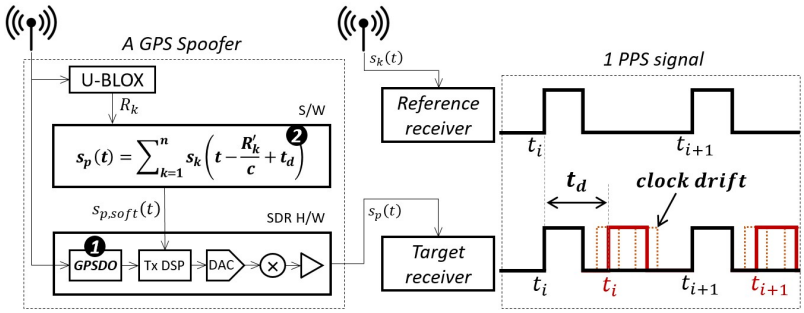


Fig. 4. A GPS spoofer and the setup for the testings

For effective GPS time spoofing experiments on GPS clocks, a spoofer should be capable of configuring both the total amount and rate of time manipulation while maintaining high-precision signal control. However, existing GPS spoofers often lack these advanced functions [14, 29, 39, 46]. To address this limitation, we implemented an enhanced GPS spoofer using *GPS-SDR-SIM* [7], an open-source GPS spoofer based on an SDR. This platform allowed us to easily incorporate new features by modifying its software and structure.

4.2.2 Implementation Details. To successfully take control of a target GPS clock from authentic GPS signals, a spoofing signal must be precisely synchronized with the authentic signals. However, two main challenges can hinder this synchronization:

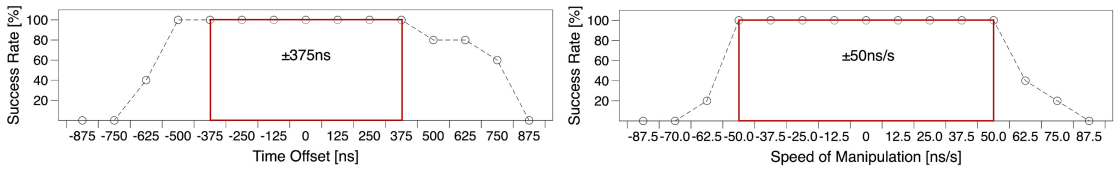
(1) Processing delay: The inherent delay in GPS spoofer processing can cause the spoofing signal to be asynchronous with the authentic signal. This asynchrony can lead the target receiver to lose its lock before time manipulation begins.
(2) Clock drift: Imprecisions in the spoofer's clock can interfere with accurate time manipulation, potentially causing time quality degradation.

To address these challenges, we implemented two key upgrades to our spoofer:

(1) Processing Delay Compensation: We estimated the constant processing delay t_d by measuring the timing difference between two Pulse Per Second (PPS) signals – one from authentic satellites and another from our spoofer. We then modified the software to preemptively adjust for this delay t_d, as illustrated in Fig. 4
(2) GPSDO Integration: We installed a GPSDO module within the SDR device. The GPSDO, synchronized to genuine GPS signals, provides atomic clock-level accuracy. We modified the GPS-SDR-SIM software to use this GPSDO as its clock source, effectively mitigating the clock drift issue.

Finally, we updated the software to incorporate the requirements outlined in Section 4.1. These updates allow the spoofer to configure both the total amount and rate of gradual time manipulation by dynamically updating the simulated pseudoranges R'_k using Eq. (2). Consequently, the signal $s_{p,soft}(t)$ generated by our enhanced software can be expressed as:

$$s_{p,soft}(t) = \sum_{k=1}^{n} s_k(t - \frac{R'_k}{c} + t_d). \tag{4}$$



(a) Maximum time offset for lock takeover

(b) Maximum speed of time manipulation

Fig. 5. Holdover triggering condition

5 REAL WORLD EXPERIMENTS

To validate that time spoofing, as described in Section 4.1, can manipulate phase without triggering holdover, we established a testbed using commercial configurations. Our primary goal was to ensure that *time quality* remains at zero and the *PMU sync error* remains inactive while the GPS spoofer manipulates the time reference.

5.1 Requirements for Spoofing the Target Receiver

We conducted two sets of experiments to investigate the acceptable time offset for seamlessly transitioning the lock from authentic satellites to the spoofer, and the acceptable rate of gradual time manipulation to prevent triggering the holdover mode as described in Section 4.1. Our target device was a commercial GPS receiver currently deployed in real-world power systems. While exact values may vary across different receiver models, our experimental procedure can be used to determine these values for any specific model.

5.1.1 Experimental Setup. We constructed the setup illustrated in Fig. 4. The process involved ensuring the target receiver locked onto genuine GPS signals, generating a spoofing signal using the spoofer configured as described in Section 4.2, and combining the spoofing signal with authentic signals before transmitting to the target receiver.

5.1.2 Acceptable Time Offset for Seamless Takeover. To determine the acceptable range, we tested intentional time offsets between -875 ns and 875 ns at 125 ns intervals. Each test was repeated 5 times, recording the number of successful lock takeovers without activating holdover mode. Results (Fig. 5a) showed that the attack consistently went undetected when the absolute value of the time offset was less than 375 ns.

5.1.3 Acceptable Rate of Gradual Time Manipulation. To identify the acceptable rate of time manipulation, we conducted tests with a total time offset of 10 µs, using rates between -87.5 ns/s and 87.5 ns/s at 12.5 ns/s intervals. Each test was repeated 5 times, recording the number of successful time manipulations without activating holdover mode. Results (Fig. 5b) led us to conservatively determine a maximum rate of 50 ns/s.

5.2 WAMS Test Bed

The configuration of the established real-time simulation testbed is displayed in Fig. 6, using the same operational parameters as an electric utility. Note that we run HILS (Hardware-in-the-loop) simulation, where HYPERSIM simulates an actual electric utility using data obtained from Hydro-Québec, while actual hardware components are used for the rest of the setup.

Power System Simulator: Hypersim, a real-time power system simulator, was used to analyze the impact of time spoofing on the system. It simulated a 36-bus 735 kV HVAC system, which is equivalent to the transmission system of an electric

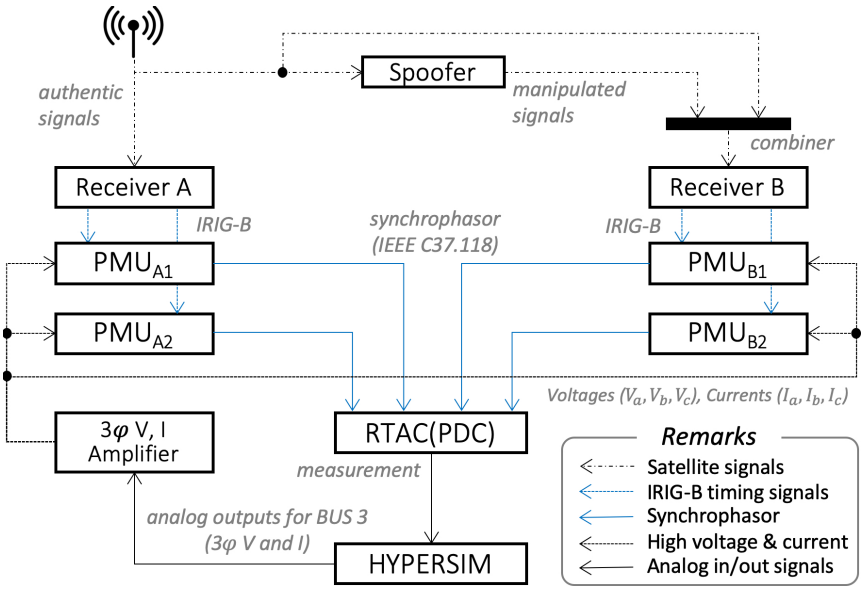


Fig. 6. Device configuration for hardware-in-the-loop simulation and data flow. HYPERSIM simulates the power system, while actual hardware components are used for the rest of the setup.

utility in north America, as shown in Fig. 7a. To ensure that the simulation starts in a steady-state condition, the Hypersim load flow solver was used to set the initial conditions.

GPS Receivers: The GPS receivers used roof-mounted antennas to capture satellite signals, which were then translated into timing signals in the IRIG-B format. These receivers were newer models from the same vendor as those used in Section 5.1. Receiver A received authentic satellite signals directly from the live sky, while Receiver B received a combination of signals from both the live sky and the spoofer.

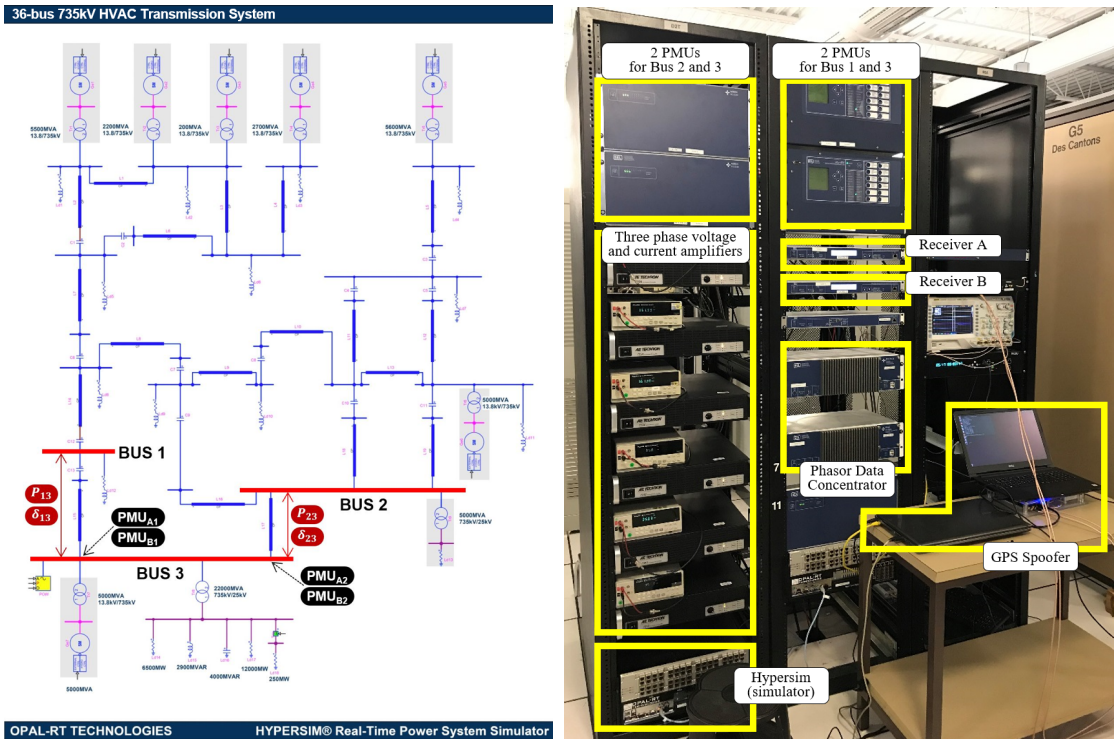
GPS Spoofer: The GPS spoofer we implemented in Section 4.2 generates manipulated signals that meet the two requirements outlined in Section 4.1 and feeds its timing signal into Receiver B.

PMU: Four PMUs were deployed in the test bed to gauge voltages (V) and currents (I) at Bus 3, as illustrated in Fig. 7a. The subscripts "A" and "B" denote the time source (i.e., Receiver A or B), while the numerical subscripts (1 or 2) represent the target bus connected to Bus 3. The PMUs were utilized to determine the phase difference and compute the power flow between the buses.

Amplifiers: The simulated analog values from Hypersim on Bus 3 were transmitted to a three-phase amplifier to raise them to a level that could be physically measured by the PMUs.

Real Time Automation Controller (RTAC): The synchrophasors from the four PMUs were collected by RTAC, acting as a Phasor Data Concentrator (PDC), which then transmitted them to Hypersim for further analysis.

The testbed components were sourced from two major utility companies to ensure real-world relevance. Korea Electric Power Corporation (KEPCO), Korea's largest power company, provided one GPS receiver, two PMUs, and the spoofer. Hydro-Québec, Canada's largest electricity producer, supplied all other hardware and configurations. This collaboration ensured that all hardware, software, datasets, and their configurations accurately reflected commercial, real-world settings in the power industry.



(a) Target buses for simulation (b) Physical setup

Fig. 7. Real-time simulation test bed

5.3 Target Points (Buses)

To analyze the impact of time spoofing, three buses (Buses 1, 2, and 3, as illustrated in Fig. 7a) were selected from the electric network. Synchrophasor data for Buses 1 and 2 were simulated using Hypersim, while the data for Bus 3 were measured with PMUs that received time signals from two receivers. Both simulated and measured synchrophasors were collected to calculate the phase differences between Bus 1 and Bus 3, as well as between Bus 2 and Bus 3. This data was used to determine the power flow on the lines, as detailed in Table 2.

Table 2. Combinations of the Phase Difference and Power Flow Calculations for the Synchrophasors on Bus 3

Simulated (device)	Measured (device)	Calculations
V_1, δ_1 (HYPERSIM)	V_3, δ_3 (PMU_{A1}) V_3, δ_3 (PMU_{B1})	δ_{13}, P_{13} (normal case) δ_{13}, P_{13} (spoofed case)
V_2, δ_2 (HYPERSIM)	V_3, δ_3 (PMU_{A2}) V_3, δ_3 (PMU_{B2})	δ_{23}, P_{23} (normal case) δ_{23}, P_{23} (spoofed case)

5.4 Time Spoofing Scenario

For a seamless takeover of the target receiver, we carefully calibrated the offset of the spoofer with the reference, Receiver A, and manipulated its time at a rate less than 50 ns/s. Our objective for spoofing was to introduce a 500 µs delay in Receiver B. The time spoofing scenario was designed as shown in Fig. 8 with the anticipated phase offset also illustrated using a dotted line. We intentionally incorporated multiple time steps to facilitate the identification of curves in the synchrophasor and power factor calculations. Notably, a 500 µs spoofing operation could potentially result in a phase displacement of 10.8°, as determined by the formula $\Delta\varphi = 2\pi f \Delta t$.

5.5 Results of Time Spoofing Without Activating Holdover

To confirm the success of the time spoofing, subsequent behaviors need to be verified:

- The target GPS receiver should not enter holdover mode but instead follow the spoofing scenario while maintaining good *time quality*.
- The PMUs synchronized to Receiver B should generate synchrophasors without any *PMU sync error*.
- The PDC should receive the synchrophasors and use them to calculate the phase difference and power flow, thereby confirming the success of the spoofing attack.

5.5.1 Target Receiver. The experiment utilized two GPS receivers with identical specifications, each equipped with several front panel indicators, including satellite lock, time quality, and antenna status. The satellite lock indicator lights up green when GPS activation and satellite lock are achieved; otherwise, it turns amber. The time quality indicator remains solid green when time accuracy surpasses 1 µs, flashes green when accuracy is below 1 ms but above 1 µs, and turns red when it falls below 1 ms. The antenna status indicator stays green unless there is no antenna or the cable is shorted. Throughout the experimental period, as shown in Fig. 9 and supported by our video demo [21], both receivers consistently maintained satellite lock and exhibited good time quality, indicating no deviation from expected behavior.

5.5.2 PMUs Synchronized to Receiver B. During the experiment, the PMUs generated valid synchrophasors and avoided a *PMU sync error*, provided that the GPS time was gradually and successfully manipulated by the attack.

Prior to the initiation of spoofing, the display in Fig. 10a showed timing signals from the reference clock, the spoofer, and Receivers A and B, which were perfectly aligned. The display in Fig. 10b depicted the synchrophasors measured

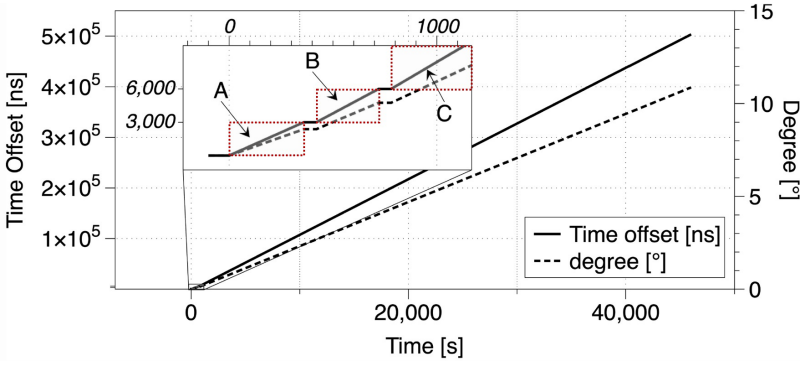


Fig. 8. Time spoofing scenario and the expected phase variation, *Area A*: 100 ns / 12 s during 360 s, *Area B*: 100 ns / 10 s during 300, *Area C*: 120 ns / 10 s until the end of the test, holding time between each area: 60 s

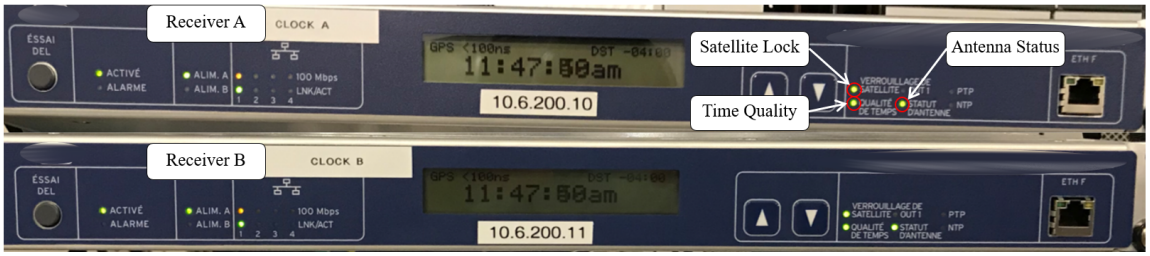
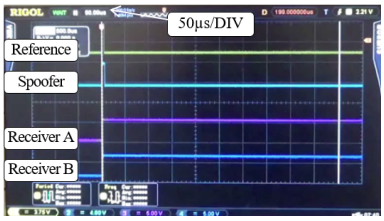


Fig. 9. Maintaining satellite lock and time quality during the spoofing attack

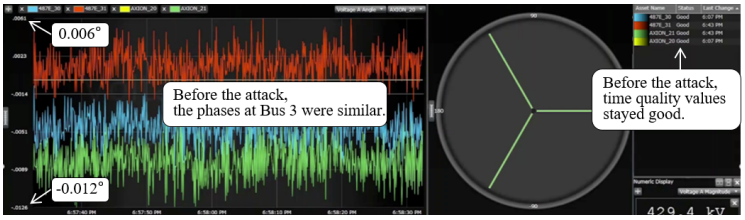
from four PMUs on Bus 3 (PMU_{A1}, PMU_{A2}, PMU_{B1}, PMU_{B2} depicted in blue, yellow, red, green, respectively) showing phases with a minor offset under 0.02 degree. The *Status* section in the upper right side of the figure categorized the synchrophasors' validity into one of four states: *Good*, *PMU Error*, *Time Sync Error*, or *No Data* [37]. These indicators confirmed that the receivers were time-aligned and all PMUs produced consistent phase measurements with good time quality prior to the attack.

Post-attack, the display in Fig. 10c showed a time shift induced by the spoofing, where the spoofer manipulated the time by 500 µs, similarly affecting Receiver B. This manipulation induced phase deviations in the PMUs (PMU_{B1}, PMU_{B2}) synchronized to Receiver B, reaching up to 10.8 degrees in comparison to those synchronized to Receiver A. These deviations are clearly illustrated in Fig. 10d. Despite this, the *Status* indicator remained at *Good*, indicating that Receiver B, unaware of the spoofing, continued to transmit data of good time quality to PMU_{B1} and PMU_{B2}. The entire process and effects of the spoofing attack can be seen in our video demo [20].

5.5.3 PDC. Synchrophasors were extracted from Hypersim to analyze the effects of the attack. We calculated the phase difference and power flow between target points as described in Section 5.3, and the results are illustrated in Fig. 11

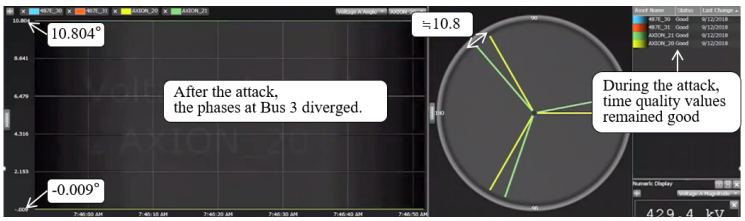


(a) Oscillator before the attack



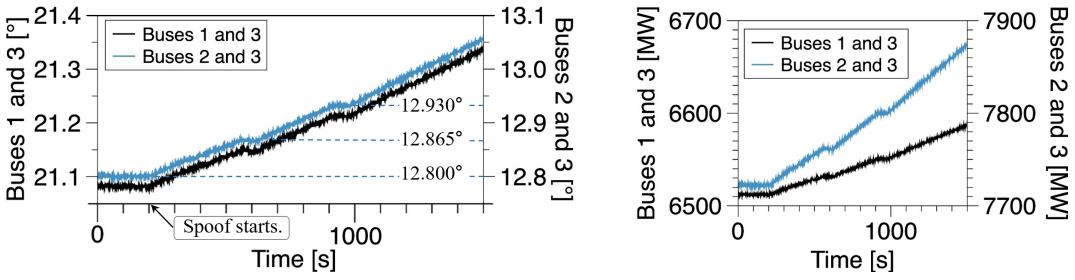
(b) PDC before the attack

(c) Oscillator after the attack



(d) PDC after the attack

Fig. 10. Screen captured before and after the time spoofing attack



(a) Phase difference (b) Power flow

Fig. 11. Impacts due to GPS time spoofing (First 1,500 s)

and Fig. 12. These figures demonstrate the impact of the attack during the initial 1,500 seconds and throughout the entire experimental period, respectively.

The simulation was initiated under steady-state conditions, with no control or protection mechanisms activated during the attack. Under these conditions, the phase difference and power flows between any two buses should remain unchanged. However, at the onset of the attack, the manipulated yet unrecognized synchrophasors caused the phase difference and power flow to begin deviating from their constant values. The three distinct steps that can be observed in Fig. 11a are directly attributed to the time spoofing scenario depicted in the inset box of Fig. 8. This scenario was designed to facilitate the identification of the spoofing pattern. In this spoofing scenario, a time offset (Δt) of 3 µs between steps is observable, which translates to a phase difference ($\Delta\theta$) of approximately 0.065 degrees, as shown in shown in Fig. 11a.

The power flow calculation between the target buses, as computed using Eq. (5), is illustrated in Fig. 11b. Throughout the test, both the voltage (V) and impedance (X) between all buses remained constant, thus making the power flow dependent solely on the sine function of the phase difference. The three distinct steps resulting from the spoofing scenario are observable in the graph and can be clearly identified, demonstrating a strong correlation between power flow and phase difference.

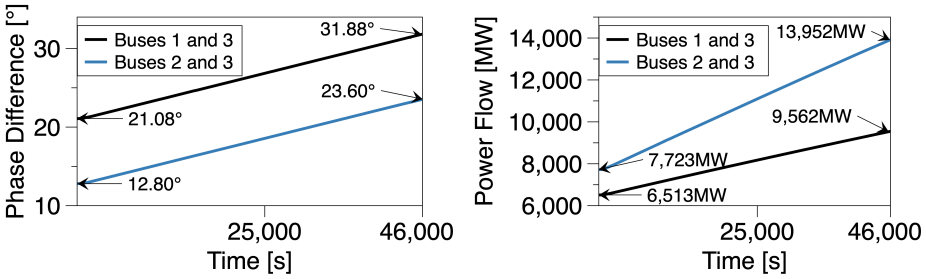
$$P_{XY} = \frac{V_X V_Y}{X_{XY}} sin(\theta_X - \theta_Y) \tag{5}$$

Fig. 12 presents the phase difference and power flow throughout the duration of the experiment. Consistent with expectations outlined in Section 5.4, a 500 µs time spoofing precisely resulted in a 10.8° phase difference over 12 hours. If the attack continues, the phase difference could reach 60°, which would take over 70 hours and could trigger false control actions, as discussed in Section 6.2.

As confirmed by the results, the time spoofing scenario successfully manipulated the time reference while maintaining good time quality. This indicates that the attack effectively evaded the activation of holdover mode during its execution.

5.6 Implications of Our Experiments

In our experiments, we have made several observations regarding the security vulnerabilities in power systems related to GPS spoofing:



(a) Phase difference

(b) Power flow

Fig. 12. Impacts due to GPS time spoofing (Entire experimental period)

- An adversary, equipped with a target receiver, can identify conditions that evade the activation of holdover, as detailed in Section 5.1.
- Given sufficient time, the adversary can gradually manipulate the timing until they decide to end the attack.
- Such time manipulations may result in incorrect phase measurements in power systems.

6 FALSE PROTECTION BY GPS TIME MISALIGNMENT

In addition to monitoring power systems, PMUs are also utilized for protection purposes, which involves automated control to prevent severe damage to electrical devices in the event of actual faults. The international standard IEC/IEEE 60255-118-1 classifies PMUs into two performance categories: the "M" class dedicated to ensuring precise measurement accuracy and the "P" class specifically tailored for protection devices that prioritize minimal latency to ensure rapid responses during fault occurrences or abnormal conditions within the power grid [5, 15]. This classification reflects the dual role of PMUs in power systems: monitoring and protection.

However, inaccurate GPS timing within PMUs can be interpreted as false faults, leading to unnecessary protection triggers even when no actual faults exist. A notable case illustrating this issue occurred in March 2014, when a 500kV transmission line experienced an unintended disconnection due to a false protection event triggered by inaccurate GPS timing at a substation, affecting a line current differential relay at Bonneville Power Administration [26].

In the following section, we will discuss the operating principles and characteristics of a line current differential relay, and explore the causes of false protection triggers due to incorrect GPS timing.

6.1 Line Current Differential Protection

6.1.1 Principles. Line current differential protection is a primary safeguarding mechanism in power systems, designed to detect and isolate faults within a protected zone of a transmission line. This protection strategy is grounded in Kirchhoff's current law, which posits that the sum of currents entering and leaving a protected zone must be zero under fault-free conditions. The methodology for implementing this protection involves assigning a positive sign to currents flowing into the protected zone and a negative sign to those exiting it. A simplified representation of this protection scheme, as shown in Fig. 13, includes current transformers placed at each end of the substation to measure the current and exchange the measurement data, along with a time stamp, with a remote location using a proprietary communication protocol.

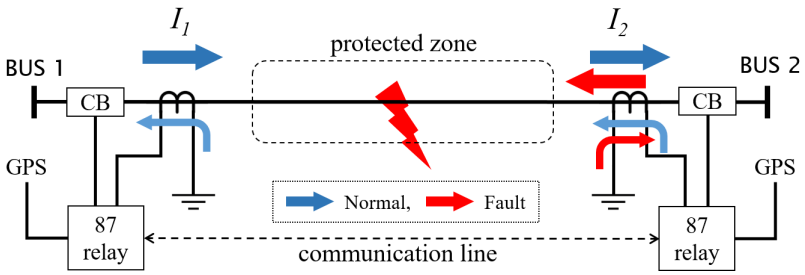


Fig. 13. Simplified diagram of line differential protection scheme

During normal operation, the current entering the protected zone from one bus (a local bus, referred to as I_1) is matched by an equal current leaving towards another bus (a remote bus, referred to as I_2), adhering to Kirchhoff's law. This balance leads to induced currents at both ends of the area with opposite polarities, effectively canceling each other out mathematically and resulting in a net current of zero. Conversely, in the event of a fault within the protected area, the situation changes significantly. Both I_1 and I_2 currents flow into the protected zone, indicating a disturbance. This deviation causes induced currents at both ends to align in the same direction, deviating from the expected zero-sum condition under normal circumstances. Once a fault is identified, the protection mechanism triggers the circuit breaker (CB) to isolate the fault and prevent further damage to the power system infrastructure. Therefore, this differential protection system is crucial for upholding the stability and reliability of power transmission lines.

6.1.2 Operating vs. Restraint Current. Fig. 14 shows a comparison between operating and restraint currents, as a graphical representation employed most frequently in the field of protection mechanism engineering [50]. The visual representation offers a detailed breakdown of how differential protection functions by graphing the operating current $I_{Op} = |I_1 + I_2|$ on the vertical axis and the restraint current $I_{Res} = |I_1| + |I_2|$ on the horizontal axis.

This representation effectively discriminates between normal operation, external faults, and internal faults within the protected zone. Area α symbolizes normal or external fault conditions, ideally positioned along the horizontal axis to indicate the predominance of restraint current, albeit practical scenarios might show minor operating currents due to transformer inaccuracies and charging current. Conversely, Area β represents internal fault conditions, characterized

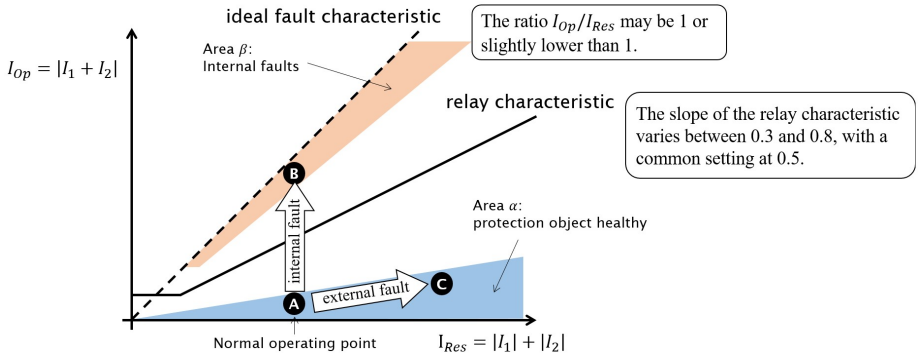


Fig. 14. I_{Op} / I_{Res} diagram (scalar diagram)

by in-phase currents leading to equal operating and restraint currents, depicted by a 45° line. This ideal fault response is slightly adjusted in reality to account for internal faults, lying just below the 45° line.

The relay characteristic slope, adjustable between 0.3 to 0.8, serves as a critical parameter to distinguish between normal and fault conditions, with a common setting at 0.5. This graphical analysis aids in visualizing how differential protection responds to varying conditions. Under normal operation, the system operates at Point A. During internal faults, it transitions to Point B, crossing the relay characteristic line and activating protection. During external faults, it moves to Point C, staying within Area α. This approach ensures precise fault detection and system integrity.

6.2 Triggering False Protection

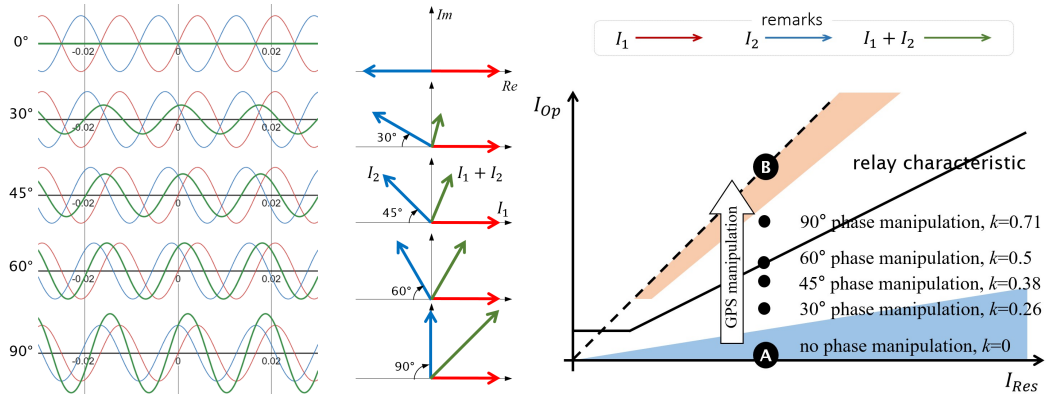
There exist two methods for exchanging current phasors between two substations in order to compare the local (I_1) and remote (I_2) phasors [19].

- In the case of a symmetrical communications line, clock offset can be adjusted through compensation of the channel delay, thereby eliminating the requirement for an external time source.
- Conversely, in the case of near-symmetrical or asymmetrical communication lines, the utilization of an external time source becomes crucial for the objectives of channel monitoring or the alignment of current phasors. In such cases, the guarantee of time precision is of utmost significance, leading to the need for the implementation of fallback mechanisms for situations when the time source quality declines.

In the latter case, if the protection system detects degradation in the quality of the source time, the fallback mechanism is activated. If degradation is not detected, the system continues to use the time reference from the external source, thereby exposing it to potential risks from the sophisticated time spoofing. Such manipulation of time can gradually alter the phase of I_2, which might lead to false faults by subtly aligning the phase of I_2 with that of I_1. This alignment could result in an increase in the operating current.

This process is depicted in Fig. 15a, illustrating the phase manipulation across both time and complex domains and describing a scenario where the phase angle of a remote current, denoted as I_2, is deliberately altered or manipulated across a spectrum of angles (0°, 30°, 45°, 60°, and 90°) in relation to a fixed local current, I_1. This manipulation is visualized in both time and complex (phasor) domains, with the intention to progressively align I_2's phase closer to I_1's phase. As I_2's phase shifts to more closely match I_1's, the vector sum of these two currents—termed the operating current—increases in magnitude.

A configurable relay characteristic is determined by the ratio between the operating current (I_{Op}) and the restraint current (I_{Res}), which is depicted as the slope in Fig. 15b. When the relay characteristic is preconfigured as 0.5, it enables the precise calculation of the necessary phase manipulation to activate an erroneous protective signal. The currents I_1 and I_2 are expressed in the complex plane as $I_{mag}(1, 0)$ and $I_{mag}(-\cos\theta, \sin\theta)$ respectively, with I_{mag} denoting the current's magnitude and θ indicating the phase manipulation of I_2. The magnitudes of the local and remote currents are nearly equivalent during normal operations or faults. In this context, k is defined as the ratio of I_{Op} to I_{Res} and can be expressed mathematically as shown in Eq. (6).



(a) Phase manipulation in I_2 (b) Operating current variation

Fig. 15. Operating current variation by phase manipulation

$$
\begin{aligned}
k &= \frac{I_{Op}}{I_{Res}} = \frac{|I_1 + I_2|}{|I_1| + |I_2|} \\
&= \frac{I_{mag}\sqrt{(1 - cos\theta)^2 + sin^2\theta}}{2I_{mag}} \\
&= \frac{\sqrt{2(1 - cos\theta)}}{2} = \frac{\sqrt{2 \cdot 2sin^2\frac{\theta}{2}}}{2} \\
&= sin\frac{\theta}{2}
\end{aligned}
\tag{6}
$$

Hence, if the relay is configured with a characteristic (k) value of 0.5, a 60° phase adjustment could result in an incorrect protection signal being issued to the circuit breaker.

7 MITIGATION

As shown in Section 6, false faults induced by GPS spoofing in line current differential protection systems for high-voltage transmission lines pose a significant risk to grid operations. These false faults trigger inappropriate protection controls that may disconnect the transmission line even in the absence of actual faults. If false faults can be distinguished from actual faults caused by lightning strikes or ground shorts, we can suspend these inappropriate protection controls.

We propose a mitigation strategy that utilizes the distinct characteristics of phase variation between false and actual faults. This approach is crucial for maintaining the integrity and reliability of grid operations, especially considering the growing threats posed by GPS spoofing.

7.1 Characteristics of Phase Variation

7.1.1 Actual Faults in Power Systems. An actual fault in power systems is described as a situation that leads to a deviation of electrical current from its intended course, thereby causing an abnormal state that compromises the insulation between conductors. This deterioration in insulation integrity can result in significant damage to the system, potentially

causing fires and the physical deformation of system components. In order to mitigate the effects of overcurrent and prevent such damage, it is crucial for a relay to swiftly identify a fault. However, the process for a digital or numeric protection relay to detect a fault involves sampling the signal, converting it to digital form, comparing the settings with the obtained measurements, and ultimately pinpointing the fault, a procedure that can take up to about three electrical cycles [24]. The characterization of an actual fault can be summarized as follows:

- An actual fault is identified within three cycles by a protection relay when it occurs [24].
- At the precise moment of an actual fault, the phases of two currents, denoted as I_1, I_2, shift from being inverted to in-phase instantaneously, indicating a phase shift of approximately 180°, as explained in Section 6.1.1.

Changes in the phase relationship between local and remote currents provide essential clues for detecting faults in power systems. These changes offer critical insights that enable protection relays to detect and address issues both promptly and accurately. Therefore, understanding these characteristics of actual faults is essential for developing effective mitigation strategies that prevent incorrect protection controls.

7.1.2 False Faults by GPS Spoofing. Phase manipulation through GPS spoofing can be successful if the time adjustment does not exceed the acceptable rate of gradual time manipulation outlined in Section 5.1.3. Our experiment has confirmed that the highest level of time manipulation attainable on the specified GPS receiver in our experimental configuration is 50 nanoseconds per second. This level of manipulation has the capacity to generate a gradual phase discrepancy of $1.08{\cdot}10^{-3}$ ° per second, as calculated by the formula $\Delta\varphi = 2\pi f \Delta t$. Therefore, an attempt to conduct a spoofing attack that replicates the same level of phase variation observed in an actual fault may require a significantly longer period, as indicated in Table 3. There exists a clear differentiation between actual faults and false ones in terms of the time required to achieve a specific degree of phase manipulation, which could be a crucial aspect in devising mitigation strategies.

Table 3. Time Required to Achieve a Specific Variation of Phase Difference Between I_1 and I_2

Variation of phase difference	Actual faults in power systems	False faults by GPS spoofing
180 °	less than three cycles (≈ 50 ms)	166,667 s (≈ 1.93 day)

7.2 Mitigation Method

The primary objective of the proposed strategy for mitigation is to prevent the occurrence of erroneous protections that could result from GPS spoofing. A strategic suggestion entails a technique that suspends the activation of protection control once a relay meets the protection criteria and identifies GPS spoofing. The graphical representation in Fig. 16 demonstrates the contrasting behaviors witnessed in two distinct scenarios. In instances of an actual fault, depicted in Fig. 16a, there is an immediate variation in phase difference between currents I_1 and I_2, graphed on the y-axis. This sudden change facilitates a transition from Area α to β, subsequently triggering the protection mechanism. Conversely, in the event of GPS spoofing, as illustrated in Fig. 16b, a deliberate manipulation on the remote substation can induce a gradual phase shift in current I_2. This prolonged manipulation gradually accumulates the phase differences until it reaches the relay's threshold, consequently activating the protection control in a similar manner.

These observations lead to the identification of a distinct pattern in the phase difference between currents I_1 and I_2 in the several cycles leading up to the relay's activation. In cases of an actual fault, the phase variation $\Delta\theta_f$ is substantial,

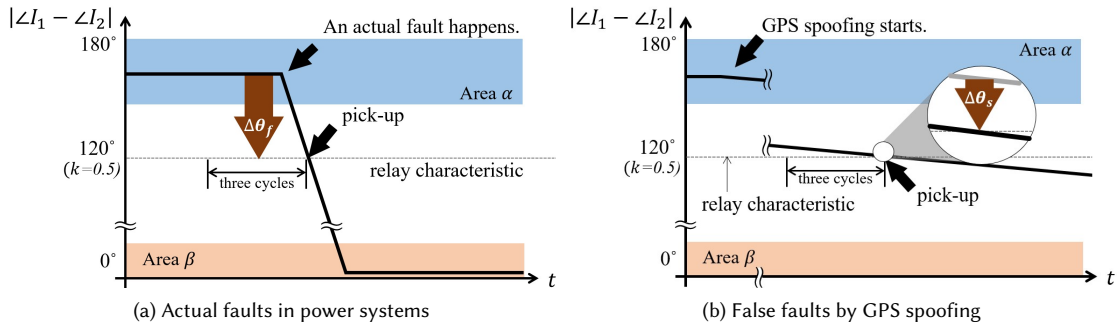


Fig. 16. Diagram illustrating the differentiation of actual and false faults

detectable by the relay, and can reach up to 60° . Conversely, during a GPS spoofing attack, the phase variation $\Delta\theta_s$ is minimal, often below 1 millidegree, which falls below the margin of measurement error. Considering that actual faults are typically detected within fewer than three electrical cycles[36, 38, 40], the categorization of scenarios is based on the observed pattern of phase variation over this defined time frame.

Fig. 17 displays an abridged flowchart depicting the proposed strategy for mitigating false protection activated by GPS spoofing. The approach consists of a pair of conditional components and three distinct states, all highlighted in dotted red for emphasis. Once the conditions of a protection are satisfied, the spoofing detection module makes a determination regarding the occurrence of a GPS attack by analyzing the phase variation over the preceding three electrical cycles. In the case of a typical line differential relay, renowned for its high sampling rate of several thousand times per second for current estimation, intricate computations are carried out to decide on the issuance of protection control eight times

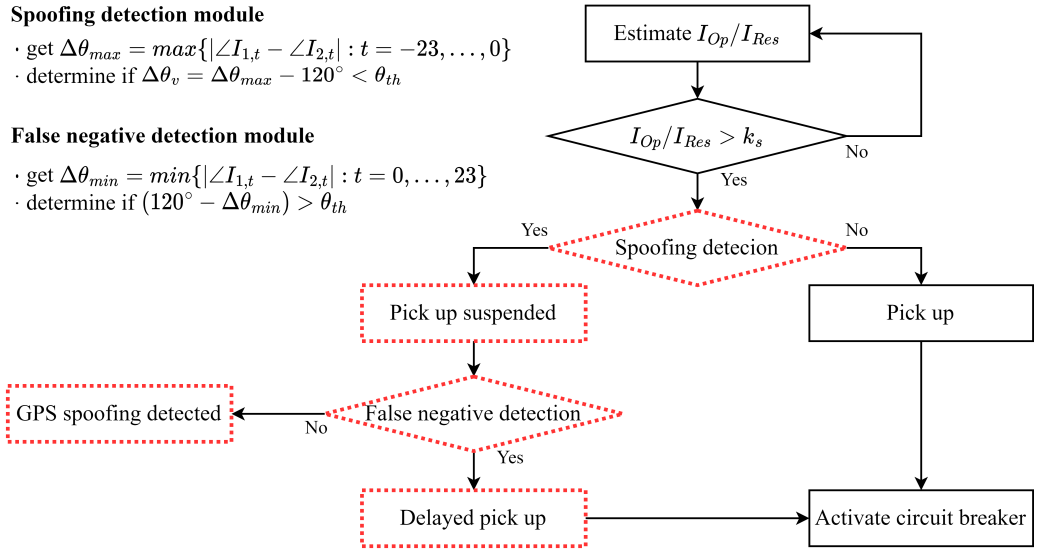


Fig. 17. Simplified flowchart of proposed mitigation strategy

within each electrical cycle. Consequently, the spoofing detection module necessitates access to 24 prior phase values for its functionality. It computes the phase variation $\Delta\theta_v$ through the deduction of the relay characteristic from the maximum phase difference between I_1 and I_2 over a specified time frame, subsequently contrasting it with a preset threshold (θ_{th}). The decision-making threshold has been set at 20 degrees to ensure clear distinction[3]. This particular value is chosen based on the observation that actual faults generally manifest a phase variation of up to 60°, depending on the specific policy configurations, while false faults typically result in variations of less than 1°. In instances where the phase variation $\Delta\theta_v$ surpasses the established threshold, the relay enters the pick up mode, identifying an actual fault and initiating the transmission of a protection instruction to the circuit breaker. Conversely, the pick up operation of the relay is suspended when the threshold criterion is not exceeded. The proposed approach effectively combats false protections caused by GPS spoofing.

To ensure the reliable operation of the mitigation method, it is important to address false negative cases. These cases are examined through a conditional process, referred to as 'False Negative Detection' in Fig. 17. In instances of missed detection, the system is programmed to reactivate the pick up within several electrical cycles, as detailed in Section 8.1. Otherwise, the proposed mitigation confirms the presence of GPS spoofing. Upon the identification of GPS spoofing, a notification should be promptly dispatched to the operator for further inquiry and analysis. Furthermore, adjustments should be made to the phase of I_2 to ensure it is situated in Area α, thereby mitigating the potential for actual faults to occur.

8 EVALUATION

It is essential to ensure that the protection relay, enhanced with the proposed mitigation method, functions as originally designed to protect the electrical equipment and counteracts malicious external time spoofing attacks. Essentially, the proposed mitigation method suspends the triggering of protection mechanisms upon the detection of suspicious behavior. Therefore, this approach does not generate a false positive.

8.1 False Negative Cases

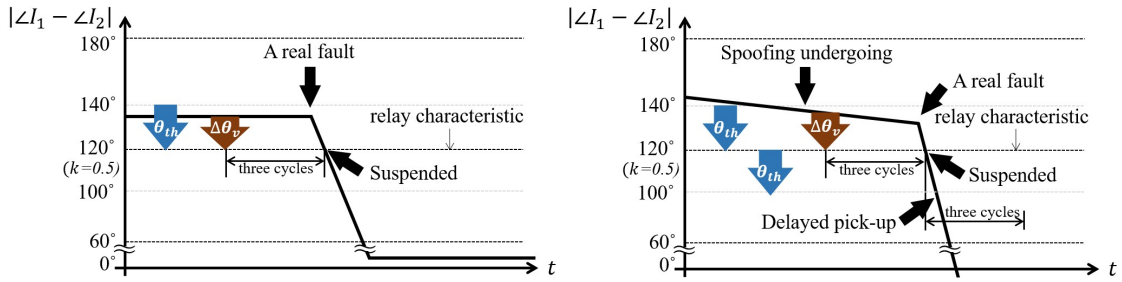
We introduced modifications to the original protection scheme, which could potentially result in false negatives. This means that an actual fault could be unintentionally suspended by the proposed mitigation. Such a scenario could occur when the phase variation ($\Delta\theta_v$) is below the threshold at the moment of the pick up, as illustrated in Fig. 18. We summarize the two typical cases as follows.

- An actual fault having less than 20° phase variation, but crossing the relay characteristic
- An actual fault while a GPS attack is underway

Thorough evaluation is imperative to ensure that these cases do not occur in real-world scenarios, or alternatively, to address the issue through different strategies.

8.1.1 Actual Fault Exhibiting Minor Phase Variation. In the context of an extended transmission line exceeding 80 km in length and operating at a voltage of 765 kV or higher, the presence of charging current at remote sites becomes a crucial consideration, significantly affecting the initial phase difference denoted as I_1 and I_2, as depicted in Fig. 18a. In this case, phase variation $\Delta\theta_v$ could not reach to the spoofing detection threshold (θ_{th}) even though an actual fault occurs. The research conducted by Bell et al. [3] specifically addresses this scenario and proposes various measures,

[3]This threshold can be adjusted based on variations in inaccuracies of the current transformer and charging current on a transmission line



(a) Actual fault exhibiting minor phase variation

(b) Actual fault following prolonged GPS spoofing

Fig. 18. Potential false negative cases

including the adjustment of a high pick up value, leading to lower relay characteristic, as a preemptive action. In such circumstances, proper calibration of the spoofing threshold θ_{th} is imperative.

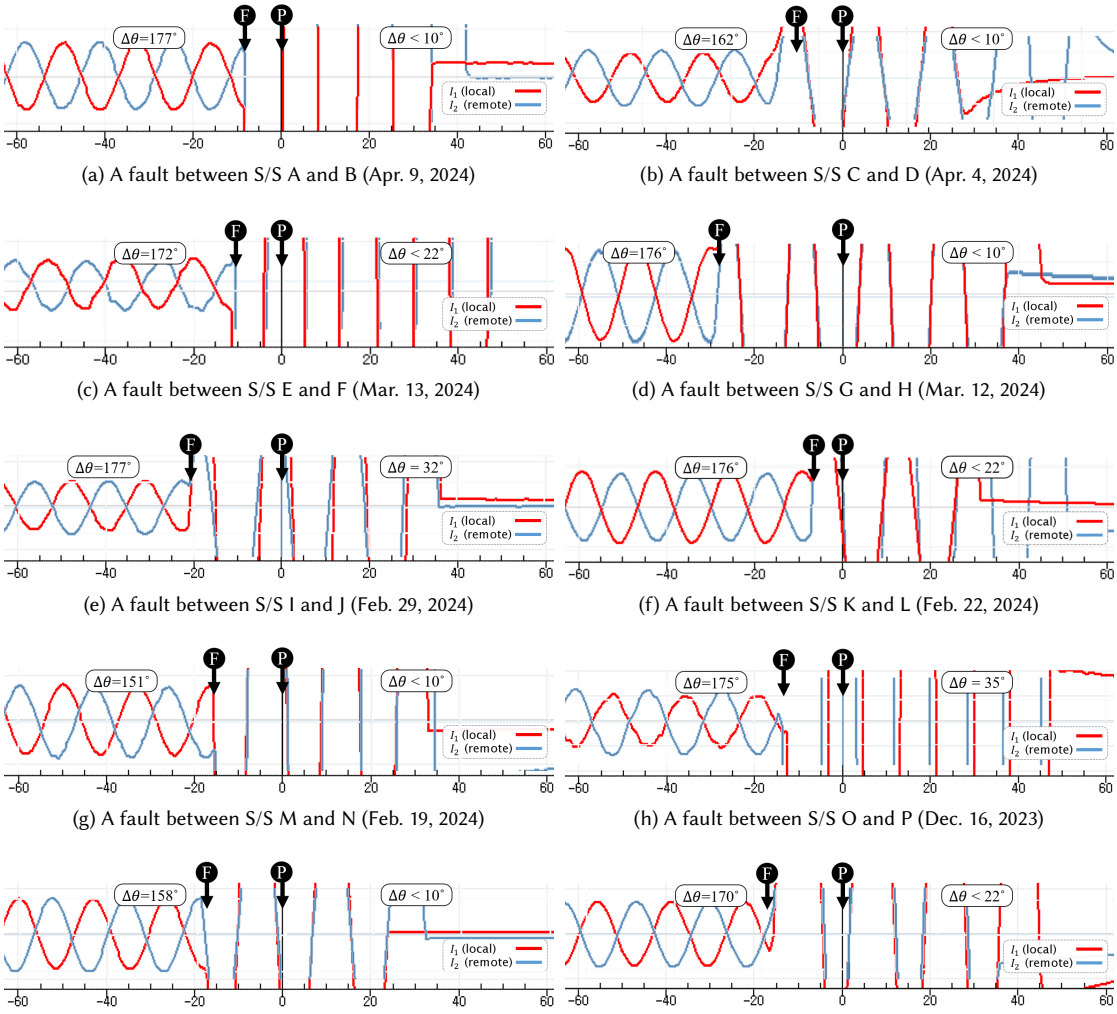
In contrast, under normal operational circumstances, the phase variation $\Delta\theta_v$ tends to be quite significant, exceeding 20° when an actual fault is detected. The plots in Fig. 19 present the occurrences of real faults over a six-month period on a 345 kV high-voltage transmission line operated by KEPCO. These examples demonstrate the features detailed in Section 7.1.1, which involve approximately 180° of phase variation within three electrical cycles. It is evident that all phase shifts $\Delta\theta_v$, when subtracting 120° from the initial phase difference, exceed 30 degrees, thereby making false negatives unlikely to occur in practical scenarios.

8.1.2 Actual Fault Following Prolonged GPS Spoofing. An additional challenge that leads to false negatives arises when a fault occurs concurrently with an ongoing GPS spoofing attack, as depicted in Fig. 18b. During a persistent and prolonged GPS attack, the phase difference between I_1 and I_2 may gradually decrease and approach 140°, the predefined threshold for spoofing detection. If the phase difference falls below this threshold, it becomes impossible to distinguish between an actual fault and a false fault by GPS attack. This issue cannot be effectively addressed by merely adjusting the threshold (θ_{th}).

The proposed compensatory method entails delaying the pick up decision subsequent to a suspension determination, leveraging the distinct phase behavior observable post-suspension. Specifically, during an actual fault, the phase difference between I_1 and I_2 significantly decreases to approximately 0° as shown in Fig. 19. Conversely, in the event of a GPS spoofing attack, this phase difference stays around 120°. Consequently, the false negative detection module is designed to ensure that actual faults are not overlooked. Following a suspension, the mitigation strategy involves continuous monitoring of the phase difference to ascertain whether it surpasses a recalibrated threshold, defined as the relay characteristic diminished by θ_{th}. With the characteristic threshold set at 0.5 and θ_{th} established at 20°, the recalibrated threshold equates to 100°. If the phase difference goes down below 100° within three electrical cycles, it is classified as a false negative, thereby initiating the delayed pick up mechanism, as illustrated in Fig. 17.

8.2 Performance Overhead

In addition to addressing the false negative to ensure that actual faults are not missed, it is essential to consider the computational load, as it has a direct impact on the responsiveness, dependability, and overall effectiveness of protection relays. These relays must promptly and accurately react to faults, even when equipped with the mitigation features. In



(a) A fault between S/S A and B (Apr. 9, 2024)
(b) A fault between S/S C and D (Apr. 4, 2024)
(c) A fault between S/S E and F (Mar. 13, 2024)
(d) A fault between S/S G and H (Mar. 12, 2024)
(e) A fault between S/S I and J (Feb. 29, 2024)
(f) A fault between S/S K and L (Feb. 22, 2024)
(g) A fault between S/S M and N (Feb. 19, 2024)
(h) A fault between S/S O and P (Dec. 16, 2023)
(i) A fault between S/S Q and R (Dec. 6, 2023)
(j) A fault between S/S S and T (Dec. 1, 2023)

Fig. 19. Phase difference between I_1 and I_2 before and after actual faults on 345-kV transmission lines in KEPCO over a six-month period (In the figures, 'F' and 'P' represent the times of the fault and pick up, respectively, while 'S/S' denotes a substation. The names of substations are randomly assigned for security reasons.)

this section, we determine whether the added computational requirements of the mitigation could potentially hinder the relay's response time or affect its real-time operational capabilities.

8.2.1 Base Computational Load. The relay's computational load is primarily influenced by its high sampling rate of 8,000 samples per second, resulting in demanding requirements on its processing capabilities. With a standard grid frequency of 60 Hz, this translates to around 133 samples per electrical cycle. These samples go through complex filtering techniques, which are essential for signal processing within the relay.

The filtering process involves both full-cycle cosine and half-cycle Fourier filters. These filters are applied following initial low-pass filtering, both analog and digital, to refine the signal for accurate phasor calculations. The full-cycle cosine filters, which compute the cosine of each data point, require substantial computation, typically consuming multiple processor cycles per computation due to the mathematical complexity involved. Similarly, the half-cycle Fourier filters, which decompose the signal into its frequency components using Fast Fourier Transform (FFT) algorithms, involve $O(n \log n)$ operations, where n is the number of samples. These FFT computations are significant as they involve logarithmic iterations over all samples, making them computationally intensive.

8.2.2 Computational Overhead Introduced by the Mitigation. Our mitigation method, introduced to enhance security against GPS spoofing attacks, imposes additional but relatively light computational tasks on the relay. This method involves retrieving and comparing the maximum or minimum values of 24 pre-calculated current phases against a predefined threshold to detect anomalies that are indicative of spoofing. Since these phase values are already computed and stored, the overhead primarily stems from the retrieval and comparison operations. Numerically, for each of the eight computational instances within a cycle, the relay needs to perform 24 comparison operations. Thus, the additional overhead for each computational instance introduced by the mitigation method totals to 24 constant time operations, culminating in 192 operations per cycle (24 comparisons x 8 instances).

This overhead analysis reveals that while there is an increase in the number of operations, the nature of these additional operations is significantly less complex compared to the base computational tasks such as cosine calculations and FFT. Given the relay's existing high-frequency processing capability, this added complexity is expected to have a minimal impact on the overall computational burden. Therefore, each cycle now entails an additional fixed number of simple operations, which are efficiently manageable within the high-speed operational framework of the relay, ensuring that the introduction of the mitigation technique does not compromise the system's real-time processing efficiency and reliability.

9 RELATED WORK

9.1 GPS Spoofing on Power Systems

Recent studies have advanced the understanding of GPS spoofing and its impact on power systems as shown in Table 1. Specifically, Musleh et al. [29] showed that an SDR-based GPS spoofer can inject a specific time offset (approximately 7 ms) into the target receiver slightly after jamming it, subsequently claiming that this manipulation could trigger false protections in the system. However, as jamming triggers holdover, this method would likely fail to induce false protection in commercial setups. Similarly, Shepard et al. [39] developed a GPS spoofer that gradually induces a time offset (up to 3.3 μs), claiming that such actions could trigger false protections. However, they neither discussed the need for seamless takeover nor evaluated the validity of synchrophasors, including issues related to holdover and time quality during the attack.

A few other works have analyzed the impact of time offset injection assuming that GPS spoofing can inject arbitrary time offsets. Almas et al. [1] employed a simulation of a GPS receiver using an IRIG-B generator with 10 μs steps to inject time offsets into a target PMU, analyzing the consequent impacts on grid applications. However, such a large time offset would likely trigger holdover, degrading the time quality value. It is unclear if the authors' experiments considered degraded time quality values. Bi et al. [4], Fan et al. [8], Jiang et al. [17], Roberson and O'Brien [34], Sreenath et al. [42], Zhang et al. [49] have collectively highlighted the significant effects of phase and frequency manipulation in synchrophasors, based on the assumption that arbitrary time manipulation is feasible in GPS receivers and PMUs.

Although these studies suggest that spoofing can lead to erroneous situational awareness and potentially compromised grid control mechanisms, such impacts are unlikely to directly affect commercial grid applications due to the holdover mechanisms that would break these assumptions.

9.2 Detection and Mitigation Against GPS Time Spoofing

The increasing sophistication of GPS spoofing attacks on power systems has prompted a diverse range of countermeasures at both the GPS antenna/receiver level and the PMU data (synchrophasor) level, as explored in various studies:

9.2.1 At the GPS Antenna and Receiver Level. Psiaki and Humphreys [33] developed an attack and defense matrix that evaluates the effectiveness of various defense techniques against specific GPS spoofing methods, focusing especially on antennas and receivers. Similarly, Heng et al. [12] propose a robust, multi-layered, multi-receiver architecture to strengthen GPS-based timing systems against jamming, spoofing, and receiver errors. Most of these countermeasures require additional receivers or antennas. However, our mitigation strategy remains effective even when existing defenses in a receiver fail to detect or protect against spoofing attacks. Yu et al. [47] discuss the use of multiple receivers and data communication for collaboration in detecting spoofing attacks and locating a false GPS signal source. However, our mitigation approach neither requires multiple receivers nor requires independent infrastructure for data sharing; instead, it detects GPS spoofing through simple calculations within the protection relay, inherent in power systems.

9.2.2 At the PMU Data (synchrophasor) Level. Fan et al. [8] present signal processing techniques to detect and correct GPS time spoofing by collecting data from a large number of PMUs and using a state estimation method. Although this approach requires complex hardware, communication infrastructure, and extensive data computation, our mitigation method supports the same functionality within protection systems without the need for additional hardware. Almutairy et al. [2] present an application of deep learning for detecting and mitigating the effects of GPS spoofing. However, the transferability of the model can be challenging. When power grid configurations change, the system dynamics can shift significantly, potentially affecting the accuracy and reliability of the trained model. In contrast, our study does not require retraining for configuration changes. Pradhan et al. [31] develop a detection strategy based on hypothesis testing to identify sudden and arbitrary time changes in measurement matrices caused by spoofing attacks. Their simulations suggest that large time jumps (e.g., 8.33 ms) can be easily detected, but smaller time offsets (e.g., 0.83 ms) are more challenging to detect. Sabouri et al. [35] introduce neural network-based GPS spoofing detection under various conditions, such as load changes. However, in their simulation, the phase angle variation due to time spoofing occurs instantly and ranges from 10° to 30°, corresponding to approximately 0.46 ms to 1.4 ms in the time domain. In contrast, we injected 50 ns offset in a commercial setup as shown in Section 5.1, making the proposed method less effective at identifying time spoofing. Fan et al. [9] introduce a dual-layer detection method that combines receiver-level detection, using the carrier-to-noise ratio, with data-level detection using synchrophasor bad data analysis. This approach requires two or more receivers equipped with patch and monopole antennas at the physical layer, along with a data communication infrastructure between PMUs at the data layer. However, our mitigation strategy does not require additional hardware at either the physical or data layers.

10 CONCLUSION

The precise synchronization of GPS time is fundamental for the operation of PMUs due to their reliance on accurate phasor measurements. In commercial operational setups, our findings indicate that for a spoofing attack to manipulate

time without triggering holdover—which would stop the tracking of external signals—two critical conditions must be met: the spoofing signal must be precisely aligned with the authentic GPS timing and adjusted at a nano-scale rate per second. This study demonstrates how such manipulations can lead to incorrect phase measurements and induce false faults. To address these issues, we have developed a mitigation strategy that effectively distinguishes between actual faults and those induced by GPS spoofing, following the analysis of historical data from actual faults.

For field deployment of this solution, additional research would be required. In particular, iterative experiments in power systems equipped with the necessary field devices and communication infrastructure are needed for finding finely tuned thresholds. Furthermore, since our experimental validation was limited to a single WAMS system, broader conclusions involving other GNSS and grid configurations will require further research to build on our findings. Once these experimental limitations are addressed and the generality of our findings is confirmed, the proposed methodology could potentially be integrated into standardization frameworks such as the NIST Cybersecurity Framework (CSF) 2.0, particularly supporting the DETECT and RESPOND functions.

REFERENCES

[1] Muhammad Shoaib Almas, Luigi Vanfretti, Ravi Shankar Singh, and Gudrun M. Jonsdottir. 2018. Vulnerability of Synchrophasor-Based WAMPAC Applications' to Time Synchronization Spoofing. *IEEE Transactions on Smart Grid* 9, 5 (2018), 4601–4612. https://doi.org/10.1109/TSG.2017.2665461

[2] Fayha Almutairy, Lazar Scekic, Mustafa Matar, Ramadan Elmoudi, and Safwan Wshah. 2023. Detection and mitigation of GPS Spoofing Attacks on Phasor Measurement Units using deep learning. *International Journal of Electrical Power & Energy Systems* 151, 109160 (2023), 12. https://doi.org/10.1016/j.ijepes.2023.109160

[3] Jordan Bell, Ariana Hargrave, Greg Smelich, and Brian Smyth. 2019. Considerations when using charging current compensation in line current differential applications. In *72nd Annual Conference for Protective Relay Engineers*. IEEE, College Station, Texas, USA, 1–11.

[4] Tianshu Bi, Jinrui Guo, Kai Xu, Li Zhang, and Qixun Yang. 2017. The Impact of Time Synchronization Deviation on the Performance of Synchrophasor Measurements and Wide Area Damping Control. *IEEE Transactions on Smart Grid* 8, 4 (2017), 1545–1552. https://doi.org/10.1109/TSG.2015.2489384

[5] Jörg Blumschein, Torsten Kerger, and Robert Matussek. 2021. Interoperability of Line Differential Protection. In *2021 74th Conference for Protective Relay Engineers (CPRE)*. IEEE, College Station, Texas, USA, 1–6. https://doi.org/10.1109/CPRE48231.2021.9429837

[6] Jaime De La Ree, Virgilio Centeno, James S. Thorp, and Arun G. Phadke. 2010. Synchronized Phasor Measurement Applications in Power Systems. *IEEE Transactions on Smart Grid* 1, 1 (2010), 20–27. https://doi.org/10.1109/TSG.2010.2044815

[7] Ebinuma, Takuji. 2015. GPS-SDR-SIM: Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim.

[8] Xiaoyuan Fan, Liang Du, and Dongliang Duan. 2018. Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach. *IEEE Transactions on Smart Grid* 9, 5 (2018), 4538–4546. https://doi.org/10.1109/TSG.2017.2662688

[9] Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski, Ju Bin Song, and Husheng Li. 2015. A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids. *IEEE Transactions on Smart Grid* 6, 6 (2015), 2659–2668. https://doi.org/10.1109/TSG.2014.2346088

[10] Evangelos Farantatos, Renke Huang, George J. Cokkinides, and A. P. Sakis Meliopoulos. 2011. A predictive out of step protection scheme based on PMU enabled dynamic state estimation. In *2011 IEEE Power and Energy Society General Meeting*. IEEE, Detroit, Michigan, USA, 1–8. https://doi.org/10.1109/PES.2011.6039836

[11] John F. Hauer, William A. Mittelstadt, Kenneth E. Martin, James W. Burns, Harry Lee, John W. Pierre, and Daniel J. Trudnowski. 2009. Use of the WECC WAMS in Wide-Area Probing Tests for Validation of System Performance and Modeling. *IEEE Transactions on Power Systems* 24, 1 (2009), 250–257. https://doi.org/10.1109/TPWRS.2008.2009429

[12] Liang Heng, Jonathan J Makela, Alejandro D Dominguez-Garcia, Rakesh B Bobba, William H Sanders, and Grace Xingxin Gao. 2014. Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture. In *2014 Power and Energy Conference at Illinois (PECI)*. IEEE, Champaign, Illinois, USA, 1–7. https://doi.org/10.1109/PECI.2014.6804565

[13] Mojgan Hojabri, Ulrich Dersch, Antonios Papaemmanouil, and Peter Bosshart. 2019. A Comprehensive Survey on Phasor Measurement Unit Applications in Distribution Systems. *Energies* 12, 23 (2019), 4552. https://doi.org/10.3390/en12234552

[14] Lin Huang and Qing Yang. 2015. GPS Spoofing: low-cost GPS emulator. In *DEF CON 23*. DEF CON, Las Vegas, Nevada, USA, 54 pages. https://doi.org/10.5446/36387

[15] IEC/IEEE. 2018. International Standard - Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems - Measurements. *IEC/IEEE 60255-118-1:2018* 1, 1 (2018), 1–78. https://doi.org/10.1109/IEEESTD.2018.8577045

[16] Rigas Themistoklis Ioannides, Thomas Pany, and Glen Gibbons. 2016. Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proc. IEEE* 104, 6 (2016), 1174–1194.

[17] Xichen Jiang, Jiangmeng Zhang, Brian J. Harding, Jonathan J. Makela, and Alejandro D. Domı´nguez-Garcı´a. 2013. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *IEEE Transactions on Power Systems* 28, 3 (2013), 3253–3262. https://doi.org/10.1109/TPWRS.2013.2240706

[18] Seethalekshmi K., Sri Niwas Singh, and Suresh Chandra Srivastava. 2011. A Synchrophasor Assisted Frequency and Voltage Stability Based Load Shedding Scheme for Self-Healing of Power System. *IEEE Transactions on Smart Grid* 2, 2 (2011), 221–230. https://doi.org/10.1109/TSG.2011.2113361

[19] Bogdan Kasztenny, Normann Fischer, Ken Fodero, and Adrian Zvarych. 2011. Communications and data synchronization for line current differential schemes. In *Proceedings of the 38th Annual Western Protective Relay Conference*. Washington State Universiry Professional Education, Spokane, Washington, USA, 1–4.

[20] Chunghyo Kim. 2023. A Video Clip Demonstrating the Test Results. Retrieved April 1, 2024 from https://youtu.be/qAiclhGmajY

[21] Chunghyo Kim. 2024. A Video Clip Illustrating Receivers' Responses under a Sophisticated GPS Spoofing Attack. Retrieved April 1, 2024 from https://youtu.be/fLtjvGQ_P7o

[22] Hyojong Lee, Tushar, B. Cui, A. Mallikeswaran, P. Banerjee, and Anurag Srivastava. 2016. A review of synchrophasor applications in smart electric grid: Synchrophasor applications in smart electric grid. *Wiley Interdisciplinary Reviews: Energy and Environment* 6 (07 2016), 1–37. https://doi.org/10.1002/wene.223

[23] Xue Li, Tao Jiang, Haoyu Yuan, Hantao Cui, Fangxing Li, Guoqing Li, and Hongjie Jia. 2020. An eigensystem realization algorithm based data-driven approach for extracting electromechanical oscillation dynamic patterns from synchrophasor measurements in bulk power grids. *International Journal of Electrical Power & Energy Systems* 116 (2020), 105549. https://doi.org/10.1016/j.ijepes.2019.105549

[24] Justin Mahaffey. 2013. Timing is everything. https://www.csemag.com/articles/timing-is-everything/.

[25] Ruikun Mai, Zhengyou He, Ling Fu, Brian Kirby, and Zhiqian Bo. 2010. A Dynamic Synchrophasor Estimation Algorithm for Online Application. *IEEE Transactions on Power Delivery* 25, 2 (2010), 570–578. https://doi.org/10.1109/TPWRD.2009.2034293

[26] Aeron Martin. 2016. Why Industry Need Time. In *IEEE/NIST Timing Challenges in the Smart Grid Workshop*. NIST, Gaithersburg, Maryland, USA, 25–30.

[27] Enrique Martínez, Nicolás Juárez, Armando Guzmán, Greg Zweigle, and Jean León. 2006. Using synchronized phasor angle difference for wide-area protection and control. In *proceedings of the 33rd Annual Western Protective Relay Conference*. Washington State University Professional Education, Spokane, Washington, USA, 1–11.

[28] A Muir and J Lopatto. 2004. *Final report on the August 14, 2003 blackout in the United States and Canada : causes and recommendations.* Technical Report. NERC.

[29] Ahmed Musleh, Charalambos Konstantinou, Marios Sazos, Anastasis Keliris, Ahmed Al-Durra, and Michail Maniatakos. 2017. GPS Spoofing Effect on Phase Angle Monitoring and Control in an RTDS based Hardware-In-The-Loop Environment,. *IET Cyber-Physical Systems: Theory & Applications* 2 (06 2017), 180–187. https://doi.org/10.1049/iet-cps.2017.0033

[30] Arun G. Phadke and Bogdan Kasztenny. 2009. Synchronized Phasor and Frequency Measurement Under Transient Conditions. *IEEE Transactions on Power Delivery* 24, 1 (2009), 89–95. https://doi.org/10.1109/TPWRD.2008.2002665

[31] Parth Pradhan, Kyatsandra Nagananda, Parv Venkitasubramaniam, Shalinee Kishore, and Rick S. Blum. 2016. GPS spoofing attack characterization and detection in smart grids. In *2016 IEEE Conference on Communications and Network Security (CNS)*. IEEE, Philadelphia, Pennsylvania, USA, 391–395. https://doi.org/10.1109/CNS.2016.7860525

[32] William Premerlani, Bogdan Kasztenny, and Mark Adamiak. 2008. Development and Implementation of a Synchrophasor Estimator Capable of Measurements Under Dynamic Conditions. *IEEE Transactions on Power Delivery* 23, 1 (2008), 109–123. https://doi.org/10.1109/TPWRD.2007.910982

[33] Mark L. Psiaki and Todd E. Humphreys. 2016. GNSS Spoofing and Detection. *Proc. IEEE* 104, 6 (2016), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

[34] Dakota Roberson and John F. O'Brien. 2018. Variable Loop Gain Using Excessive Regeneration Detection for a Delayed Wide-Area Control System. *IEEE Transactions on Smart Grid* 9, 6 (2018), 6623–6632. https://doi.org/10.1109/TSG.2017.2717449

[35] Mohammad Sabouri, Sara Siamak, Maryam Dehghani, Mohsen Mohammadi, and Mohammad Hassan Asemani. 2021. Intelligent GPS Spoofing Attack Detection in Power Grid. In *2021 11th Smart Grid Conference (SGC)*. IEEE, Tabriz, Iran, 1–6. https://doi.org/10.1109/SGC54087.2021.9664217

[36] Schneider Electric 2023. *Line Differential Protection and Control Device Easergy MiCOM P532 Technical Manual.* Schneider Electric. https://www.se.com/il/en/download/document/P532_EN_M_R-m8__308_675/.

[37] Schweitzer Engineering Laboratories 2018. *Synchrowave Central Software Instruction Manual.* Schweitzer Engineering Laboratories. https://selinc.com/products/5078-2/.

[38] Schweitzer Engineering Laboratories 2020. *Data Sheet for SEL-787 Transformer Protection Relay.* Schweitzer Engineering Laboratories. https://selinc.com/api/download/2818/.

[39] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. 2012. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection* 5, 3 (2012), 146–153. https://doi.org/10.1016/j.ijcip.2012.09.003

[40] Siemens 2011. *SIPROTEC Line Differential Protection 7SD80 Manual v4.6.* Siemens. https://cache.industry.siemens.com/dl/files/528/109742528/att_900609/v1/7SD80xx_Manual_A1_V040003_us.pdf.

[41] Alison Silverstein. 2017. Synchrophasors and the Grid. https://www.naspi.org/sites/default/files/reference_documents/naspi_naruc_silverstein_20170714.pdf.

[42] J. G. Sreenath, Sindhuja Mangalwedekar, Anju Meghwani, Saikat Chakrabarti, Ketan Rajawat, and Suresh Chandra Srivastava. 2018. Impact of GPS Spoofing on Synchrophasor Assisted Load Shedding. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, Portland, Oregon, USA,

1–5. https://doi.org/10.1109/PESGM.2018.8586533

[43] Jaume Sanz Subirana, José Miguel Juan Zornoza, and Manuel Hernández-Pajares. 2013. *GNSS Data Processing, Volume I: Fundamentals and Algorithms*. ESA Communications, Noordwijk, the Netherlands.

[44] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. 2011. On the Requirements for Successful GPS Spoofing Attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11)*. Association for Computing Machinery, Chicago, Illinois, USA, 12 pages. https://doi.org/10.1145/2046707.2046719

[45] Thomas R. Walsh, Saqer Alhloul, and Meghdad Hajimorad. 2014. Estimating the remaining useful life of power grid transmission lines using synchrophasor data. In *2014 International Conference on Prognostics and Health Management*. IEEE, Spokane, Washington, USA, 1–8. https://doi.org/10.1109/ICPHM.2014.7036392

[46] Kang Wang, Shuhua Chen, and Aimin Pan. 2015. Time and position spoofing with open source projects. In *Black Hat Europe 2015*, Vol. 148. UBM, Amsterdam, The Netherlands, 1–8.

[47] Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun, and David Basin. 2014. Short paper: detection of GPS spoofing attacks in power grids. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks* (Oxford, United Kingdom) *(WiSec '14)*. Association for Computing Machinery, New York, NY, USA, 99–104. https://doi.org/10.1145/2627393.2627398

[48] Yingchen Zhang, Penn Markham, Tao Xia, Lang Chen, Yanzhu Ye, Zhongyu Wu, Zhiyong Yuan, Lei Wang, Jason Bank, Jon Burgett, Richard W. Conners, and Yilu Liu. 2010. Wide-Area Frequency Monitoring Network (FNET) Architecture and Applications. *IEEE Transactions on Smart Grid* 1, 2 (2010), 159–167. https://doi.org/10.1109/TSG.2010.2050345

[49] Zhenghao Zhang, Shuping Gong, Aleksandar D. Dimitrovski, and Husheng Li. 2013. Time Synchronization Attack in Smart Grid: Impact and Analysis. *IEEE Transactions on Smart Grid* 4, 1 (2013), 87–98. https://doi.org/10.1109/TSG.2012.2227342

[50] Gerhard Ziegler. 2012. *Numerical Differential Protection: Principles and Application*. John Wiley & Sons, Hoboken, New Jersey, USA. 30–34 pages.

[51] Yihui Zuo, Guglielmo Frigo, Asja Derviškadić, and Mario Paolone. 2020. Impact of Synchrophasor Estimation Algorithms in ROCOF-Based Under-Frequency Load-Shedding. *IEEE Transactions on Power Systems* 35, 2 (2020), 1305–1316. https://doi.org/10.1109/TPWRS.2019.2936277

Received 30 April 2024; revised TBD; accepted TBD