Model-Based Evaluation of GPS Spoofing Attacks on Power Grid Sensors

Ilge Akkaya, Edward A. Lee, Patricia Derler
University of California at Berkeley
{ilgea, eal, pderler}@eecs.berkeley.edu

***Abstract*—Emerging cyber-physical system (CPS) applications require reliable time synchronization to enable distributed control and sensing applications. However, time reference signals are vulnerable to attacks that could remain undetected for a long time. Sensor-rich distributed CPS such as the "smart grid" highly rely on GPS and similar time references for sub-station clock synchronization. The vulnerability of time synchronization protocols to spoofing attacks is a potential risk factor that may lead to falsified sensor readings and, at a larger scale, may become hazardous for system safety. This paper describes a simulation-based assessment of the effect of time accuracy on time-centric power system applications. In particular, the vulnerability of power grid sensors to erroneous time references and the potential risks of time-base spoofing on power grid health are studied, using the Ptolemy modeling and simulation tool. Both the false alarm and the missed generation scenarios are considered, where the GPS spoofer may lead the substation to declare an erroneous out-of-phase situation, or the substation may be disabled to detect anomalies that are present in the incoming phase data.**

I. Introduction

Cyber-physical systems are becoming increasingly complex due to the growing number of components in the next generation distributed CPS and the climb in the sensor data rates for precise control and monitoring applications.

In many CPS applications, due to increased sampling rates at sensors and the need to aggregate data from multiple nodes that are possibly operating at distant locations, the accuracy of component clocks has become a point of concern. Time synchronization protocols such as PTP [1] are being widely deployed for precise synchronization of substation clocks to a master time reference. However, the vulnerability of systems against time synchronization attacks is still a concern in many systems including Unmanned Air Vehicles (UAV) [2] Audio-Video Bridging [3], automotive and power grid applications.

The power grid is a large scale CPS, which relies on GPS time synchronization for time-alignment of spatially distributed sensor data. It is predicted that over 100 million sensors and meters will be present in the future power grid [4]. Installation of high-throughput precise-time phasor measurement units (PMUs), also known as *synchrophasors*, into the grid infrastructure has enabled the acquisition of time-synchronized measurements of state variables at electrical nodes in the transmission network. Requirements on time-synchronization and clock precision at local substations has subsequently become a point of attention, since the benefit of the time-stamped data for real-time control and detection purposes is directly determined by the integrity of the measurements.

The wide accessibility and high precision of GPS signals have promoted GPS time synchronization as a trusted wireless clock synchronization technique for synchronized sensor devices. However, civilian GPS signals are susceptible to spoofing, putting numerous safety-critical sensors at risk of producing unreliable data, while remaining undetected by the target platform over long periods of time [5].

In the case of large distributed CPS, pre-deployment modeling and simulation is a desirable method for assessing protocols and infrastructures. Time synchronization is a well-fit simulation problem, since testing against time-base spoofing attacks in practice require deployment of complex equipment and more importantly, it is an extremely time-consuming process [6]. Spoofing attacks usually require time commitments in the order of millions of seconds, causing pre-deployment spoofing tests to become extremely difficult, if not impossible.

In this paper, we present a simulation-based assessment of the effect of time precision on PMU data streams and evaluate potential risks of erroneous time references on power grid health. As a case study, we quantify the vulnerability of PMU readings under two GPS spoofing scenarios, which may either trigger false generator trips or conceal existing phase angle deviations in the power grid to cause potential grid instability.

II. Related Work

Recent research has shown that GPS receivers in many sensor devices, including synchrophasors are vulnerable to GPS time-base spoofing attacks [2]. Experiments have indicated that following a 10-15 minute take over period required for the PMU receiver to be completely captured by the spoofer, it is possible to drift the time reference of the PMU local clock in the order of tens of microseconds in several minutes, causing the phasor measurements to become entirely unreliable.

Some countermeasures against GPS spoofing have been proposed and experimented [7], [8]. However, systematic clock manipulations that are in comparable rates to the local clock jitter are drastically difficult to detect. Simulation-based assessment of such scenarios is therefore essential for pre-deployment evaluation of potential security risks.

III. Modeling Time in Cyber-Physical Systems

Time is an ambiguous notion for a cyber-physical system. CPS consist of distributed physical and computational com-

ponents that have hardware and software clocks that could either be synchronized to a master clock or be running in standalone mode. This variation of components combined with the physical clock imperfections such as clock drift induced by temperature and vibration gives rise to the need of more detailed clock implementations in CPS simulation.

Ptolemy is a modeling and simulation tool that is widely used for heterogeneous system design [9]. Ptolemy provides support for modeling different notions of time at different components of a composite model. Every level of hierarchy in a Ptolemy model has a `director` that governs the execution semantics of the sub-model according to a model of computation. Each director has a *local clock* that keeps track of the model time within the sub-model. Local time is related to the time of the enclosing model (environment time) via a parameter called `clockRate`. The global time resolution of the model is also a user-defined parameter, which should be adjusted according to the order of magnitudes of the clock parameters.

A clock rate of `1.0` at the sub-model indicates that model time advances in exactly the same rate within the sub-model as in the enclosing director. In many CPS applications, this will not be the case. Platform clocks in general have offsets from the global time reference (UTC, GPS) and have crystal imperfections that cause the local clock to drift. This effect can be encapsulated within the multiform time enabled by the Ptolemy model.

In a CPS model, the top level time is referred to as *oracle time*. This can be considered a global time reference for the model and is not an actual physical quantity.

A. Clock Imperfections

Although the `clockRate` parameter in Ptolemy models provides a means to model different clock rates, clock imperfections still need to be modeled to account for random jitter in the oscillator.

In Ptolemy, Discrete-Event(DE) model of computation is the most natural model to represent the "cyber" behavior in a CPS, due to the discrete nature of computation and communications. A sub-system with DE semantics has a local clock that runs at a relative speed to its environment. Using a discrete clock within this sub-model will directly enable simulating ticks produced by an imperfect oscillator.

To introduce random oscillator deviations from the clock rate, we use an additional synchronization block. One example of such component is given in Figure 4, called `Noise/Drift Generator`. The `Noise/Drift Generator` component has the following parameters

1) `syncPeriod`: The synchronization period to the master clock
2) `freeRunDrift`: The part-per-million (PPM) clock drift, denoting the drift rate of the oscillator in free run mode
3) `oneSigmaNoise`: The one sigma positive or negative time excursion from the mean clock rate
4) `impairmentPeriod`: Period of the sawtooth clock deviation.

B. Modeling Time Synchronization

Components of a distributed system usually share a common reference of time through synchronization protocols. In the most general case of physical systems, the reference time can be UTC time. PTP [1] and NTP [10] are common time synchronization protocols used for synchronization of distributed sub-station clocks. It is also common practice to use the direct GPS signal to discipline a local oscillator.

GPS clock synchronization is a common method of time synchronization for synchrophasors. Most commercially available PMUs contain a GPS disciplined oscillator (GPSDO) for maintaining the local clock at the PMU substation. A 1 pulse-per-second (PPS) broadcast GPS clock signal is used to discipline the local oscillator.

In Figure 4, the `Noise/Drift Generator` component performs clock synchronization by comparing the local time to the received master clock time and adjusting the local clock rate accordingly. This base mechanism may be configured to implement any given well-defined clock synchronization protocol. In the following sections, this component will be used to synchronize sub-station times to the GPS clock reference.

IV. Time Synchronization in the Power Grid

The "smart grid" is incorporating sensor devices capable of providing precise-time high quality measurements of the grid variables. These sensors depend on precise time measurements to be able to produce reliable data.

One prominent example of a sensor that requires extremely precise time alignment is a phasor measurement unit (PMU). PMUs are sensors that perform synchronized real-time measurements of the grid state (voltage, current, phase). The local clock of the PMU must be synchronized to a global time reference with relatively low deviation rates. Considering that a $1\mu s$ deviation in the local clock causes a 0.021° phase detection error, it is important to maintain local clock rate synchronized to the global time reference, on average. Since all generators in a grid segment must operate "in phase" within a fraction of 1°, it becomes essential to ensure that the local clock of the PMU satisfies the precision requirements of power grid applications.

A. Time Synchronization for Signal Processing Accuracy

The PMU includes a signal processing block for the synchrophasor estimation of the phase of the power signal. The input signal (voltage or current) is sampled simultaneously with two local quadrature oscillators that have a 90° phase shift, constituting the local phasor reference. Complex multiplication of the input phasor with the local reference followed by low pass filtering yields the phase angle of the input signal Consider a reference input voltage signal at a reference node in the power grid, given by

$$v(t) = cos(2\pi f_n t + \theta(t)) \quad (1)$$

where f_n is the nominal grid frequency that is 60 Hz for the US grid, and $\theta(t)$ is the phase at time t. The magnitude is assumed to be unity for simplicity. Time in the physical system, denoted by t, advances at a rate denoted by a reference time, i.e. GPS. Consider the sampling of $v(t)$ by a PMU substation. A sample of the signal at GPS time t_0 will have the value $v(t_0) = cos(2\pi f_n t_0 + \theta(t_0))$. The following derivations consider the amplitude detection is performed with negligible error during sampling.

If the local oscillator of the PMU is not perfectly synchronized to the reference physical clock, which is the common case, there will be an offset at the platform time of the PMU at the time of sampling. We denote the platform time as τ. Assume that at the time of sampling, platform time is related to the GPS time by the equation $\tau = t_0 + \epsilon(t_0)$, where $\epsilon(t_0) < 0$ for a platform time that lags behind GPS time. Note that the offset in the platform time will cause the local phasor reference to be produced at a different GPS time and in turn, the GPS time representation of the signal will have the form

$$v_{PMU}(t) = cos(2\pi f_n \tau) + jsin(2\pi f_n \tau) \quad (2)$$

The process of phase angle detection as outlined above, requires complex phasor multiplication of the local phasor reference V_{PMU} with the signal $v(t)$, represented as

$$V_0 = e^{i\theta(t_0)}$$

in phasor notation at the time of sampling, with a reference angular frequency $\omega = 2\pi f_n$ and GPS time reference t. The PMU phasor using the same reference will then be

$$V_{PMU} = e^{i2\pi f_n \epsilon(t_0)}$$

where the error in platform time reference appears as a phase term in the PMU phasor. Complex multiplication followed by low-pass filtering of the high-frequency terms will yield the phase estimate at t_0 to be

$$\tilde{\theta}(t_0) = \theta(t_0) - 2\pi f_n \epsilon(t_0) \quad (3)$$

The absolute phase angle error is given by $|\hat{\theta}(t_0)| = |\tilde{\theta}(t_0) - \theta(t_0)| = 2\pi f_n \epsilon(t_0)$. This error is purely induced by the local clock deviation. If synchronization error is random around the nominal value, there is no systematic deviation in the phasor measurements. However, a systematic deviation of time from the GPS clock, i.e. by a constant factor, will cause the phase readings to significantly deviate from the actual value, relative to GPS clock.

B. Modeling Synchrophasor Measurement Accuracy

The IEEE Standard for Synchrophasor Measurements for Power Systems states that the synchrophasor measurements must be accurate within 1% of the "ideal" phase [11]. The deviation from the reference is measured by a quantity called *total vector error* (TVE) that aggregates errors that could happen in *amplitude* and in *phase* during phasor estimation.

Assuming a perfect amplitude estimate, a phase error of $0.57°$ will cause a 1% TVE, which corresponds to an error

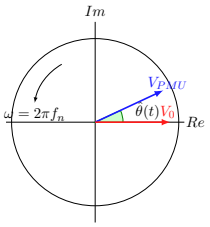


Fig. 1: Phasor representation of phase detection process

of approximately 26.39 μs in the time reference [11]. While this upper bound implies certain requirements on the local accuracy of the PMUs, imperfect clock references can lead to the violation of the standard [12].

Before we assess the effect of GPS time-base spoofing on PMU operation, we initially study the stability of local PMU clock and its effect on phase detection performance. We consider a model-based approach to simulate the average absolute phase error caused by oscillator imperfections. A synchrophasor model given in Figure 4 is used to model the behavior of a time-synchronized Phasor Measurement Unit. By setting `free run clock drift` and `one-sigma noise` on the clock jitter, it is possible to simulate physical oscillator characteristics in a consistent way.

Figure 2 shows the correspondence between one sigma clock noise and phasor measurement accuracy. The tests are carried out using a 1 PPS GPS pulse for time synchronization. The phase angle error is calculated by averaging the phase difference measured by a synchrophasor with an imperfect oscillator and a reference synchrophasor set to have zero clock drift and noise, over 2 seconds, at a sampling rate of 900 Hz.

Analysis of Figure 2 reveals that the maximum allowable phase error of $0.57°$ is only achievable with clock jitter within tens of microseconds, under normal operating conditions. The two test cases with one-sigma noise of 0.1 ms and 1 ms were shown to have an average phase error of more than $1°$, which violates the IEEE Standard. Commercially available PMUs are currently adopting more precise GPS clock receivers to overcome this challenge [13].

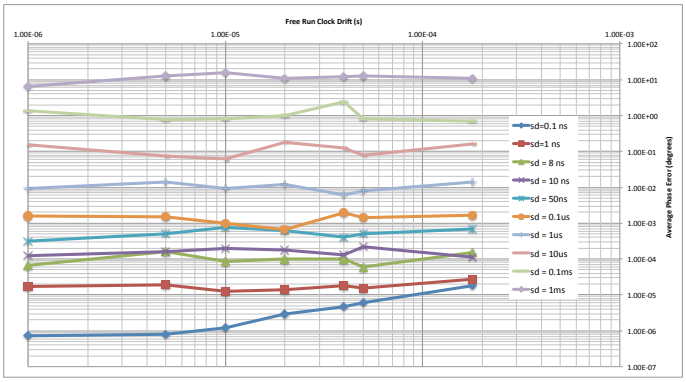


Fig. 2: Effect of Clock Precision on the Phase Estimation Accuracy

V. Assessment of the Effect of GPS Spoofing on Synchrophasor Measurements

GPS spoofing is a security threat that has been successful in causing erroneous data references in several commercial GPS based systems [14], [15]. Increasing dependence on GPS synchronization has caused the power grid to become a vulnerable candidate for such spoofing attacks. PMUs with individual GPS receivers that receive direct civilian GPS signals to discipline their local clock are a natural point of exposure to time-base spoofing attacks.

In a simple scenario, at a reference bus in the power grid, we consider two co-located Phasor Measurement Units (PMUs) measuring the power signals at the same electrical node on the power system. [12] has shown that a GPS spoofer located at some proximity of the GPS receiver of the PMU can successfully take over the GPS receiver and carry off the time reference at the substation by an arbitrary amount in time to cause false power flow and phase angle readings at the node.

We will additionally explore a more sophisticated scenario, where the spoofer is also assumed to be able to access the phase measurements from the unaffected PMU at the same node. This scenario is particularly realistic for PMUs that send data wirelessly to a data concentrator for further data aggregation and analysis. In this case, it is also possible to induce a non-constant time deviation to drive the phase measurement in an arbitrary manner from the actual value, with a purpose to cause missed detections of grid disturbances. This scenario is potentially much more hazardous for the power grid health, since it is likely to delay or completely disable the detection of certain anomalies.

A model-based approach for studying possible GPS spoofing attacks and their effect on system stability has numerous advantages. In a simulation environment, it is convenient to specify desired clock characteristics for systems and experiment seamlessly with interchangeable models of sub-stations.

A. Inducing False Alarms in the Power Grid

We use the top level Discrete Event model presented in Figure 3 for investigating a spoofing attack to induce false alarms due to erroneous time reference at the local substation. The top level model has a local clock that advances at a rate of 1.0, in the global time reference for the entire model, called *oracle time*. The model includes a `GPS Transmitter`, that is assumed to have a clock that advances synchronously with oracle time. There are two `Synchrophasor` components with identical local clock characteristics (clock jitter and clock drift). The `GPS Synchrophasor` is assumed to have a local clock synchronized to the 1 PPS GPS signal. The `Spoofed Synchrophasor`, however, models a synchrophasor captured by the spoofer unit `GPS Spoofer`, which first manipulates the actual GPS time reference and delivers an erroneous master clock reference to the synchrophasor.

The details of the `Synchrophasor` implementation are given in Figure 4. The functional flow of this component consists of time synchronization to the master clock reference

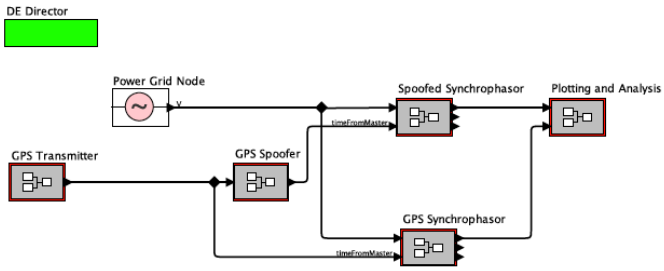
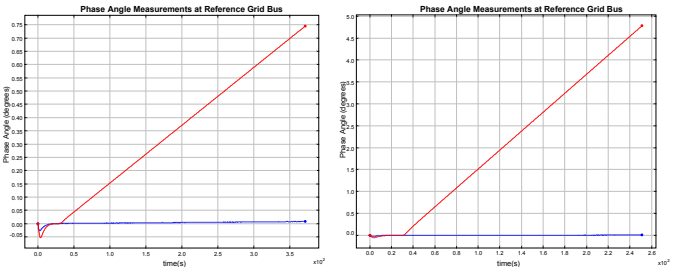


Fig. 3: Top Level Ptolemy Model for the GPS spoofing setup



(a) $\epsilon(t) = 0.1\mu s$ (b) $\epsilon(t) = 1\mu s$

Fig. 5: Phase Angle Measurements from two PMUs located at the same node of the power grid. [red: PMU synchronized to spoofer clock, blue: PMU with perfect time reference

followed by the signal processing unit to estimate phase angle, which is outlined in Section IV-A.

The spoofer is assumed to have captured the GPS receiver of the compromised PMU at the beginning of simulation. After time synchronization to the master clock (from `GPS Spoofer`) has been established, the spoofer deviates its reference clock rate from the GPS reference at a rate of $\epsilon(t)$ per second. For $\epsilon(t) = 0.1\mu s$, this corresponds to a deviation of 0.1 PPM.

Figure 5 demonstrates the phase measurements from the `Spoofed Synchrophasor` plotted in oracle time, for two clock deviation rates. For a deviation rate of $0.1\mu s/s$, the C37.118.1-2011 standard is violated at t = 290.7 s, that is, approximately 260 s since the beginning of the spoofing attack. For a more aggressive attack with $\epsilon(t) = 1\mu s/s$, the standard violation occurs shortly before the 60 s mark, approximately 30 s after the beginning of attack.

B. Time-Stamp Manipulation to Mitigate Existing Phase Faults in the Grid

With the existing model for the synchrophasor-GPS communications, we next investigate a more complicated spoofer model that has access to the readings from the non-spoofed `GPS Synchrophasor` readings with some feedback delay. The model for this test is given in FIgure 6. The modification in this model variant is that, the spoofer clock has access to the phasor readings from the non-spoofed synchrophasor at the same node, which is used to modify the time reference with the aid of a PID controller, to force the phase reading of the spoofed synchrophasor towards zero.

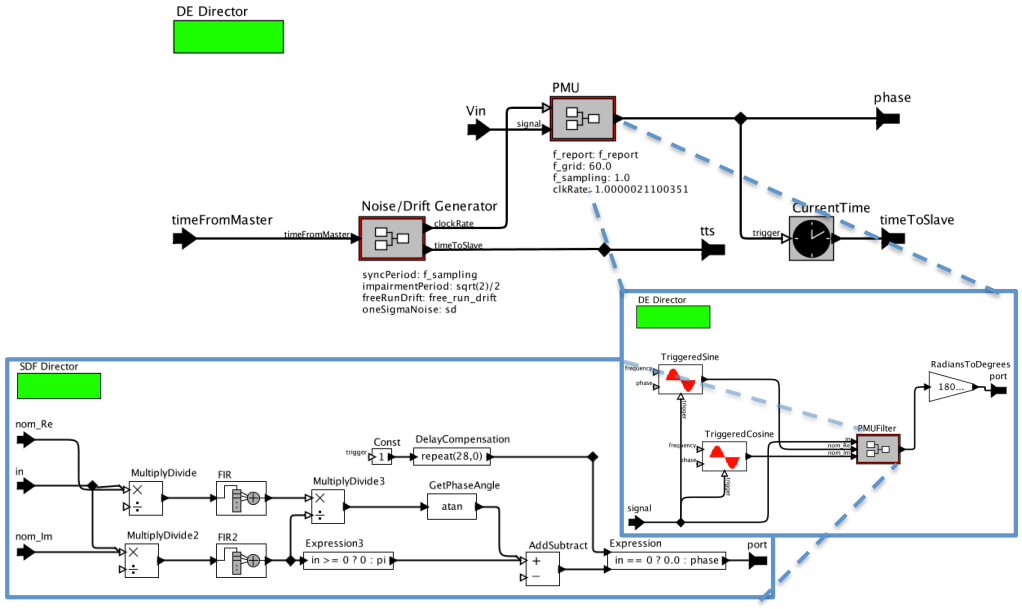


Fig. 4: The Synchrophasor Model

A worst-case feedback delay of 10 samples is modeled on the phase-feedback connection to the spoofer. At a sampling rate of 900 Hz, this roughly corresponds to a network delay of 11.1 ms.

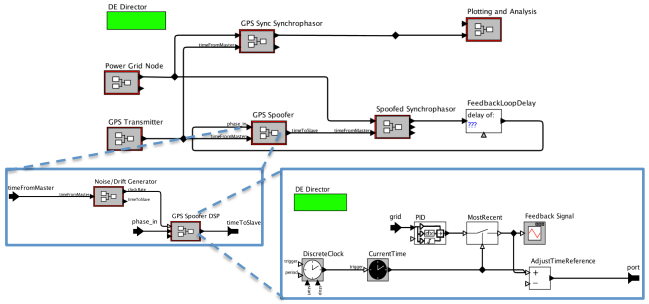


Fig. 6: Detailed Model for Phase-Feedback GPS Spoofing

A commonly observed grid disturbance is a growing sinusoidal phase harmonic that may eventually cause the responsible generator to be tripped, to maintain grid stability. This kind of disturbance is usually detected within several seconds and remedial action is taken [16]. The spoofing model with feedback capability is used to simulate one such disturbance in the grid. Figure 7 shows the simulated waveforms of the measured phase angle under such condition. The blue waveform denotes the phasor estimates performed by the healthy synchrophasor and the red waveform corresponds to the phase estimate of the spoofed platform. It can be seen that detection of the harmonic disturbance can be significantly delayed due to the time-base spoofing attack. In this scenario, it is not possible to completely cloak the presence of the disturbance, since we assume a 1PPS synchronization signal, as well as some feedback delay due to a realistic network

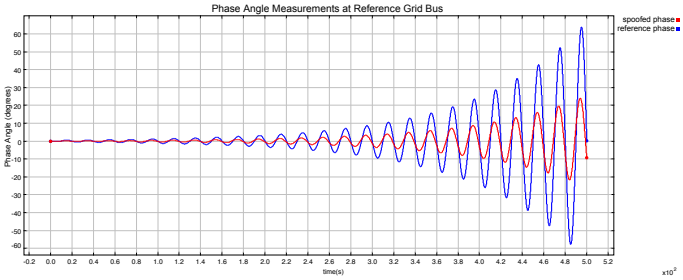


Fig. 7: Time-base spoofing attack for delaying out-of-phase tripping action for an unstable harmonic phase disturbance

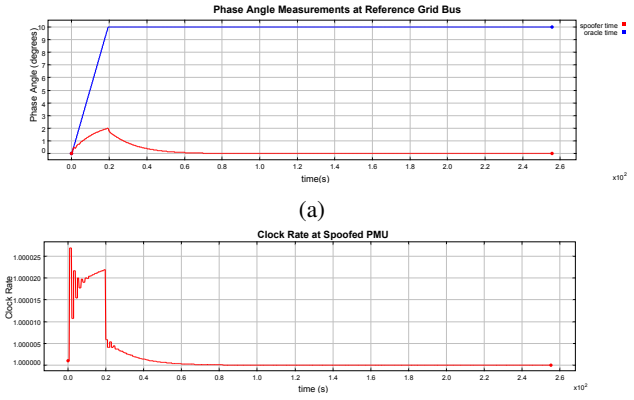
infrastructure.

Table I presents a quantitative evaluation of the delay in detection caused by the spoofer at the protective relay. For 1° allowable phase margin relative to nominal grid phase angle (0°), the detection of the harmonic disturbance is delayed by approximately 90 seconds. During the delay, the phase angle at the node has exceeded the maximally allowed deviation by 2.3°.

Phase Error Tolerance(°)	Nominal Tripping Time (s)	Delayed Tripping Time (s)
0.20	11.29	12.80
0.50	14.11	104.07
1.00	84.05	173.60
2.00	153.95	244.00

TABLE I: Phasor Measurement Spoofing to Cause Delayed Detection of Out-Of-Phase Tripping for an Unstable Harmonic Phase Disturbance

Another disturbance pattern that may be observed in power grid nodes is a ramp deviation from the nominal grid phase an-



(a)

(b)

Fig. 8: Time-base spoofing attack for delaying out-of-phase tripping action for a ramp phase disturbance

gle that settles at a steady-state angle. Figure 8a demonstrates a ramp-phase deviation with a 10° steady-state value, and the corresponding spoofer action to suppress and then mask the disturbance pattern completely. The experiments reveal that in less than 220 s, the disturbance is entirely hidden by the spoofed time reference, making the disturbance virtually undetectable by the synchrophasor, with an overshoot of 2°. Once the time offset at the synchrophasor local clock has been established by the GPS spoofer, the steady-state clock rate deviation needed to conceal the phase disturbance becomes zero, as demonstrated in Figure 8b.

VI. Conclusion

We presented a simulation based evaluation of potential implications of imperfect time references in cyber-physical systems. We studied GPS spoofing attacks and their possible effect on PMU data quality. It was shown that, under certain circumstances, GPS spoofing may lead to missed detections of phase disturbances in the grid and long-term coordinated attacks may even lead to severe consequences, such as cascading blackouts and damage to equipment.

Future work includes investigating alternative time synchronization techniques and modeling security counter-measures for grid components. Additionally, the model-based assessment technique will also be beneficial in modeling architectures that rely on time-synchronization between sensor platforms for systems in which not all sensor devices may have access to the global time reference. This scenario is particularly interesting to demonstrate error propagation and respective cascading faults in the grid.

Acknowledgement

This work is supported in part by the TerraSwarm Research Center, one of six centers supported by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.

References

[1] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588-2002*, pp. i –144, 2002.

[2] D. Shepard, J. Bhatti, T. Humphreys, and A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," 2012.

[3] D. Pannell, "Audio video bridging gen 2 assumptions," March 2012. [Online]. Available: http://www.ieee802.org/1/files/public/docs2012/avb-pannell-gen2-assumptions-1203-v9.pdf

[4] P. A. Craig and T. P. McKenna, "Technology security assessment for capabilities and applicability in energy sector industrial control systems," PNNL - 21313, Tech. Rep., 2012. [Online]. Available: http://www.mcafee.com/us/resources/reports/rp-energy-sector-industrial-control.pdf

[5] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," 2012.

[6] E. Lee, "Cyber physical systems: Design challenges," in *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on*. IEEE, 2008, pp. 363–369.

[7] B. O'Hanlon, M. Psiaki, T. Humphreys, and J. Bhatti, "Real-time spoofing detection in a narrow-band civil gps receiver," in *Proceedings of the 23rd International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2010)*, 2001, pp. 2211–2220.

[8] J. Warner and R. Johnston, "Gps spoofing countermeasures," *Homeland Security Journal*, 2003.

[9] J. Eker, J. W. Janneck, E. A. Lee, J. Liu, X. Liu, J. Ludvig, S. Neuendorffer, S. Sachs, and Y. Xiong, "Taming heterogeneity - the ptolemy approach," in *Proceedings of the IEEE*, 2003, pp. 127–144.

[10] Network time protocol. [Online]. Available: http://www.ntp.org

[11] "IEEE standard for synchrophasor measurements for power systems," *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1 –61, 28 2011.

[12] D. Shepard, T. Humphreys, and A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, 2012.

[13] Model 1133A Power Sentinel Phasor Measurement Unit. [Online]. Available: http://www.arbiter.com/catalog/product/model-1133a-power-sentinel.php#tabs-2

[14] J. Warner and R. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *Journal of Security Administration*, vol. 25, no. 2, pp. 19–27, 2002.

[15] N. Tippenhauer, C. Pöpper, K. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[16] E. Schweitzer, D. Whitehead, A. Guzman, Y. Gong, and M. Donolo, "Advanced real-time synchrophasor applications," in *35th Annual Western Protective Relay Conference, Spokane, Washington, USA*, 2008.