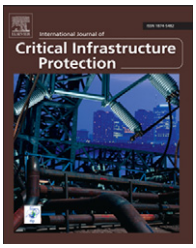
Available online at www.sciencedirect.com
SciVerse ScienceDirect
www.elsevier.com/locate/ijcip



Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks

Daniel P. Shepard[a,*], *Todd E. Humphreys*[a], *Aaron A. Fansler*[b]

[a]*Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin, 210 E. 24th Street, Austin, Texas 78712, USA*
[b]*Northrop Grumman Information Systems, 7745 Chevy Chase Drive, Austin, Texas 78752, USA*

ARTICLE INFO

Article history:
Received 21 March 2012
Accepted 22 September 2012
Available online 2 October 2012

Keywords:
Electrical power grid
Phasor measurement units
GPS spoofing
Vulnerabilities

ABSTRACT

Results of Global Positioning System (GPS) spoofing tests against phasor measurement units (PMUs) are presented, which demonstrate that PMUs are vulnerable to spoofing attacks. A GPS spoofer can manipulate PMU time stamps by injecting a counterfeit ensemble of GPS signals into the antenna of the PMU's time reference receiver. A spoofer-induced timing error of only a few tens of microseconds causes a PMU to violate the maximum phase error allowed by the applicable standard. These and other larger errors can give automated or human power grid controllers a false perception of the state of the grid, leading to unnecessary, and possibly destabilizing, remedial control actions. To emphasize this threat, this paper shows that a particular PMU-based automatic control scheme currently implemented in Mexico whose control architecture and setpoints have been published in the open literature could be induced by a GPS spoofing attack to trip a primary generator.

1. Introduction

The infrastructure that supports the generation and distribution of electric power, collectively known as the power grid, is regarded in the United States and other industrialized nations as critical national infrastructure. Past power disruptions and numerous government demonstrations have revealed that the power grid is vulnerable not only to natural disasters but also to malicious cyber activities, which are on the rise in the United States. The consequences of previous power disruption incidents were annoyance and economic losses; however, future disruptions caused by malicious entities could lead to crippling large-scale failures.

The power grid originally operated without an external time reference, but increased demand for reliability and capacity has spurred the introduction of grid sensors that can trace their timing accurately to Universal Coordinated Time (UTC). In the next-generation "smart grid" infrastructure, accurate timing signals will be broadly required – from generation plants to distribution substations to individual smart grid components [9].

The value of time synchronization is best understood by recognizing that the power grid is a complex, interconnected and interdependent network. Thus, events in one part of the grid affect operations elsewhere, and extend beyond the grid to other systems that are reliant on stable power, much like what was observed in the 2003 Northeast Blackout [18]. Time-synchronized measurements, such as the so-called "synchrophasors" produced by phasor measurement units (PMUs), allow more accurate real-time estimation of the state of the power grid than do legacy sensors. The resulting reduced state uncertainty leads to (i) refined grid dynamical models

*Corresponding author.
E-mail address: dshepard.ut@gmail.com (D.P. Shepard).

1874-5482/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2012.09.003

for operations planning, which improve long-term grid reliability; and (ii) increased grid capacity because utilities can operate with less conservative stability margins [1,9]. Ultimately, PMU-based energy management systems will be designed to anticipate failures, making it possible to take remedial actions before failures spread across the power grid [12].

PMUs rely on the Global Positioning System (GPS) for synchronization. This reliance creates a vulnerability to a particular type of malicious attack called GPS spoofing [4]. In 2001, the U.S. Department of Transportation evaluated the vulnerabilities of the transportation infrastructure and raised concerns about the threat of GPS spoofing [19]. More recently, the North American Electric Reliability Corporation has recognized the vulnerability of the GPS-dependent U.S. power grid to GPS spoofing [10].

Spoofers generate counterfeit GPS signals that current civilian (i.e., non-military) GPS receivers are unable to distinguish from authentic GPS signals. The counterfeit signals can be used to commandeer the tracking loops of a targeted receiver and induce spoofer-controlled time or position offsets. The U.S. Department of Transportation report cited above noted the absence of off-the-shelf defenses against civilian GPS spoofing and recommended a study to characterize the effects and observables of spoofing attacks. In 2008, Humphreys et al. [4] demonstrated that an inexpensive portable software-defined GPS spoofer could be built from off-the-shelf components, again highlighting the threat of spoofing.

In December 2011, Northrop Grumman Information Systems and the University of Texas Radionavigation Laboratory jointly conducted a functional test and evaluation of the effects of spoofed GPS timing signals on synchrophasor measurements produced by PMUs. GPS spoofing attacks were launched via cable and over-the-air inside an RF shielded tent against a GPS time reference receiver that sourced timing to a PMU. The goal of this exercise was to determine the extent of the adverse effects that GPS spoofing can have on synchrophasor measurements and investigate the consequences of these effects on power grid management. This paper presents the results of the effort, which demonstrate that PMUs are, indeed, highly vulnerable to GPS spoofing attacks.

2. Background

This section briefly discusses synchrophasors and GPS spoofing.

2.1. *Synchrophasors*

As electric power grids continue to expand and as transmission lines are pushed to their operating limits, the dynamic operation of the power system has become more of a concern and more difficult to accurately model. Moreover, effective real-time control is now seen as a key to preventing large-scale cascading outages such as the 2003 Northeast Blackout [1,18].

For years, electric power control centers have inferred the state of the power system (i.e., the positive sequence voltage and angle at each network node) from indirect measurements (i.e., power flows). However, to improve the accuracy of power system state estimation, it will be necessary to feed existing estimators with a richer measurement ensemble or to measure the grid state directly [1,9].

Alternating current (AC) quantities have been analyzed for more than a century using the phasor construct developed by Steinmetz in 1893. A relatively new synchronization technique developed in the mid-1980s [11], which allows the referencing of measured current or voltage phasors to absolute time, is currently being implemented throughout the world. The measurements produced by this technique are known as "synchronized phasor measurements" or "synchrophasors." Synchrophasors provide a real-time snapshot of current and voltage amplitudes and phases across a power system. Drawing this data from a geographically dispersed set of nodes can give a complete picture of the state of a power system at any instant in time. This makes synchrophasors useful for measurement, analysis, and control of electrical power infrastructures [9,12].

In a typical deployment, synchrophasors are integrated in protective relays and are sampled from widely dispersed locations in the power network. The synchrophasors are synchronized with respect to a common time source (UTC) via GPS time reference receivers. In short, synchrophasors are basically measurements of AC voltage (or current) and absolute phase angle made at selected points and times in an electric transmission or distribution system.

2.2. *GPS spoofing*

GPS spoofing is the act of producing a counterfeit version of the GPS signal ensemble with the goal of seizing control of the position–velocity–time (PVT) solution of a targeted GPS receiver. This is most effectively accomplished when the spoofer has knowledge of the GPS signal as seen by the target receiver so that the spoofer can produce a matched version of the signal [4,15,19,20]. In the case of military GPS signals, this type of attack is nearly impossible because military signals are encrypted and are, therefore, unpredictable to a would-be spoofer [3]. On the other hand, the civilian GPS signal is publicly known and readily predictable.

In recent years, civilian GPS spoofing has been recognized as a threat to critical infrastructure applications that rely heavily on the publicly known civilian GPS signal [2]. A number of promising methods are being developed to defend against civilian GPS spoofing attacks [2,7,8,13,21,22], but it will take several years for these technologies to mature and see widespread implementation. At this time, no off-the-shelf defenses are available to combat civilian GPS spoofing attacks.

3. GPS spoofer

The civilian GPS spoofer used in the tests reported in this paper is an advanced version of the spoofer described in [4]. This improved spoofer, which is shown in Fig. 1, is the only device reported in open literature that is capable of precisely aligning the spreading codes and navigation data of its counterfeit signals with those of authentic GPS signals.