Assessment of Low-Budget Targeted Cyberattacks Against Power Systems

Xiaorui Liu, Anastasis Keliris, Charalambos Konstantinou, Marios Sazos, Michail Maniatakos

Assessment of Low-budget Targeted Cyberattacks Against Power Systems

XiaoRui Liu[1], Anastasis Keliris[2], Charalambos Konstantinou[1], Marios Sazos[3], and Michail Maniatakos[3]

[1] FAMU-FSU College of Engineering, Center for Advanced Power Systems, Florida State University, Tallahassee, FL, USA
[2] New York University Tandon School of Engineering, Brooklyn, NY, USA
[3] Center for Cyber Security, New York University Abu Dhabi, UAE
{xliu9,ckonstantinou}@fsu.edu, {apk5,mks5,mm6446}@nyu.edu

Abstract. The security and well-being of societies and economies are tied to the reliable and resilient operation of power systems. In the next decades, power systems are expected to become more heavily loaded and operate closer to their stability limits and operating constraints. On top of that, in recent years, cyberattacks against computing systems and networks integrated in the power grid infrastructure are a real and growing threat. Such actions, especially in industrial environments such as power systems, are generally deemed feasible only by resource-wealthy nation state actors. This chapter challenges this perception and presents a methodology, named Open Source Exploitation (OSEXP), which utilizes information from public infrastructure to assess an advanced attack vector on power systems. The attack targets Phasor Measurement Units (PMUs) which depend on Global Positioning System (GPS) signals to provide time-stamped circuit quantities of power lines. Specifically, we present a GPS time spoofing attack using low-cost commercial devices and open source software. The necessary information for the instantiation of the OSEXP attack is extracted by developing a test case model of the power system in a digital real-time simulator (DRTS). DRTS is also employed to evaluate the effectiveness and impact of the developed OSEXP attack methodology. The presented targeted attack demonstrates that an actor with limited budget has the ability to cause significant disruption to a nation.

1 Introduction

Since the first public electric power system was established in the 1880's for providing street lighting [1], power systems have significantly evolved and grew to become essential in our everyday life. This is evident by the global demand for energy which is increasing at an accelerating rate [2]. The energy demand is driven with the increasing human population, economic growth, as well as technological advances. As the "backbone" of critical infrastructure on which other sectors (including transportation networks, military defense systems, water treatment and desalination, telecommunications) rely on, electric power systems

need to have sufficient capacity to meet peak demand, flexibility to deal with uncertainty and variability in regards to the desired load demand and generation sources, and be able to maintain voltage and frequency stability criteria [3].

The normal operation of all infrastructures dependent on power systems is maintained only if supply of electrical energy is steady. Power outages (also known as *blackouts*), however, cause large-scale disruptions of electric power supply and can lead to loss of power in parts of a power system's network due to the activation of protection equipment. Typical causes of blackouts include extreme weather and natural phenomena, misoperation, human errors, equipment failures, and animals [4]. Examples of power outages due to extreme weather events include *i)* the nor'easter during March 2018 that caused major impacts across the Northeast US where over 2.2 million customers were without power [5], and *ii)* hurricane Michael which made landfall near Mexico Beach, Florida, on October 10, 2018, leaving approximately 2.5 million electricity customers in the southeast without power [6]. The 2011 Southwest blackout, the largest in California history, was initiated due to a mistake by a technician that caused a $500kV$ line to shut down between two Arizona substations [7]. In 2017, 1205 utility outages lasted eight hours or longer. The financial impact for the 274 of the events was more than $27 million [8].

In power systems, the stable operation could be disrupted not only by natural hazards, operators errors, or failures at production units, but also by software vulnerabilities and errors, malware or intentional criminal cyberattacks [9–11]. The financial loss in 2016 to the US economy caused by malicious cyberattacks is estimated between $57 and $109 billion [12]. One of the first indications that power systems can be vulnerable to cyberattacks was demonstrated in 2007 by the Idaho National Laboratory with the "Aurora Generator Test", showcasing how cyberattacks can transcend the virtual world and cause physical damage on power systems equipment [13]. The test showed how an attacker able to access the control network of a diesel generator could install a malicious program that rapidly opened and closed the relay controllers of a generator. The out-of-sync closing of the relays caused the generator to slip out of synchronism and as a result create a frequency difference between the machine and the grid, maximizing the stress, provoking immoderate torque, and finally causing the generator to spin out of control. Besides proof-of-concept cases, real-world incidents demonstrate that cyberattacks could be disastrous and affect the lives of millions of people [14]. For instance, in December 2015, attackers were able to cause a blackout in Ukraine. The attackers compromised supervisory control and data acquisition (SCADA) systems and infected software with malicious code that tripped breakers, causing a power outage and preventing the utility from detecting the attack [15, 16]. Particularly, the attack initiated with scheduled disconnects for uninterruptible power supply (UPS) systems and telephonic floods against customer supported lines. The primary attack vector hijacked SCADA with malicious commands to open breakers. The amplifying stage of the attack wiped using KillDisk[4] workstations, servers, and human machine in-

[4] KillDisk is a malware variant designed to wipe data from hard drives.

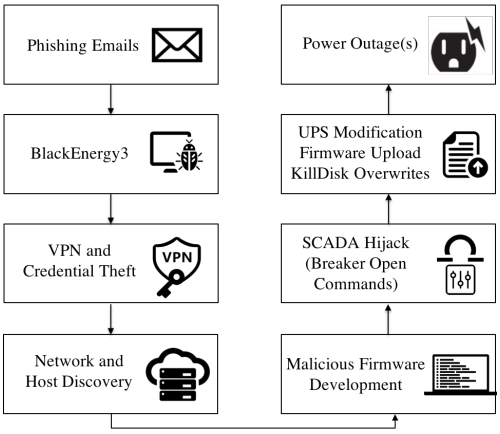

Fig. 1. Cyber kill chain of 2015 cyberattack on the Ukrainian power grid.

terface (HMI) cards while overwriting the legitimate firmware on critical devices at distribution substations, leaving them unresponsive to any remote commands from operators [17]. Fig. 1 graphically depicts the main steps of the kill chain of the 2015 cyberattack on the Ukrainian power grid. One year later (December, 2016), Ukraine suffered another sophisticated attack against the Pivnichna substation near the capital, Kiev [18]. The attack against this transmission facility resulted in power outages across the Kiev wider area for an hour. The adversaries employed the CrashOverride malware, which enables direct control of circuit breakers and switches [19].

Taking into account inadvertent and deliberate incidents, power utilities are taking steps to establish better protective functions against attacks on the grid infrastructure. These systems often incorporate advanced sensing and measurement technologies that include, among others, smart meters, advanced protective relaying systems, asset condition monitors, and Wide Area Monitoring Systems (WAMS). Specifically, WAMS highly rely on Global Positioning System (GPS) and similar time references for substation clock synchronization. WAMS can be utilized to analyze dynamic system events able to augment monitoring, control, and protection functions as shown in Fig. 2 (e.g., state estimation, dynamic monitoring, relay protection schemes, islanding strategies, etc.). Phasor measurements form the cornerstone of WAMS infrastructure. The phasor network consists of Phasor Measurement Units (PMUs) able to provide synchronized voltage and current phasors, as well as frequency measurements. PMUs synchronize phasor measurements across a wide geographical area by leveraging absolute timestamps provided by GPS signals [20, 21]. In particular, PMUs receive and decode the GPS data in order to estimate their clock position offset with respect to the GPS time measured by the on-board satellite clocks. They then leverage GPS data to achieve clock synchronization and derive a Coordinated Universal

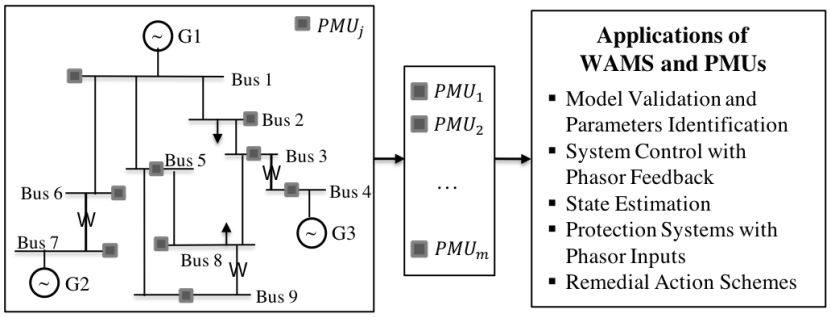

Fig. 2. Applications of Phasor Measurement Units (PMUs) and Wide Area Monitoring Systems (WAMS).

Time (UTC) time-stamp reference for their measurements (typically reported at 30-120 samples/second [22]).

Despite the transition towards grid modernization and the inclusion of monitoring systems across the power infrastructure, WAMS, control, and protection schemes can be exposed to malicious interference. For example, GPS signals are vulnerable to jamming, spoofing, and accidental receiver malfunctions [23]. The vulnerability of time synchronization protocols of PMU devices to such attacks is a potential risk factor that may lead to falsified data measurements, and at a larger scale, may lead to inaccurate monitoring and trigger unnecessary, and possibly destabilizing, remedial control actions which can become hazardous for system safety [24]. Oftentimes, such attack scenarios are considered to only be within the reach of well-funded organizations or nation states, and require substantial technical education [25]. However, given the plethora of publicly available information regarding power systems and the dependency of these systems on public infrastructure, we argue that it is feasible for actors with lower budgets to also develop and instantiate disrupting attacks. To that end, we introduce a low-budget methodology capable of causing wide area blackouts, solely relying on public information and public infrastructure.

Similar to Open Source Reconnaissance[1], where meaningful information is extracted from public sources [26], we introduce Open Source Exploitation (OSEXP) in which the information required to deploy an attack is extracted from public resources and infrastructure [27]. Low budget attack vectors are constructed against judiciously GPS time spoofing, that exploits the reliance of power systems and specifically PMU devices on GPS for time synchronization.

Furthermore, in order to verify the feasibility of the proposed method, we run real-time test simulations based on the OPAL-RT platform. Digital real-time simulation (DRTS) is a technique for the simulation of very complex and large models in real-time with time steps as low as tens of microseconds. In regards

[1] The term open source is not related to open source software throughout this work, unless explicitly stated.

to power systems, DRTS reproduces the voltage and current waveforms with the desired accuracy, that are representative of the behavior of the real power system being modeled [28]. In this work, we utilize DRTS in order to model power system test case, as well as identify the angle difference between two sets of phasors measured at two different places that could serve as an indicator of grid stress. The attack vector – forged signals in the GPS receiver of PMUs – is demonstrated in DRTS in order to verify how an increasing phase angle difference can cause erroneous protection decisions by triggering circuit breakers to trip.

Our main contribution in this work is the characterization and experimental verification of GPS time spoofing attacks against carefully selected power grid devices using *low-cost Commercial-Off-The-Shelf (COTS) equipment and open source software*. Prior literature has demonstrated the potential of GPS spoofing attacks to affect power system measurements but required specialized, expensive equipment and extended technical knowledge [24,29]. Our approach significantly reduces the cost and complexity of GPS time spoofing, "open sourcing" the exploitation phase of campaigns targeting power systems. Furthermore, it enables a one-time design of an exploitation vector and reuse of the same vector worldwide, as GPS is employed for time synchronization purposes in systems across the globe. The effectiveness of the developed low-budget attack vector is validated using DRTS on the IEEE 9-bus system. In particular, the real-time model streams phasor data using the standard IEEE C37.118 protocol mimicking the behavior of an actual transmission network employed with PMUs, i.e., the test case of the grid is monitored by modelled PMUs (available in OPAL-RT) across the network resembling their placement in a real network.

This chapter challenges the perception that extensive damage and/or disruption of a nation's computers and networks are feasible only by resource-wealthy nation state actors. To that end, we introduce a methodology dubbed OSEXP, which leverages public infrastructure to execute an advanced cyberattack on critical infrastructure. The first section of this chapter provides preliminaries on power systems along with the background information about PMU and GPS systems. The next section discusses our proposed end-to-end open source approach for constructing attack vectors against power systems, introduces OSEXP, and elaborates on a specific OSEXP attack, GPS time spoofing. Next, we experimentally verify the feasibility of this attack using low-cost equipment and open source software. In addition, we provide simulation results and verify the feasibility of the attack vector in DRTS. The last section concludes the chapter.

2 Background

2.1 Power systems

Electrical power systems consist of a variety of generation plants, substations, transmission lines, distribution lines, and loads. In general, power systems are comprised of four stages, namely generation, transmission, distribution, and con-

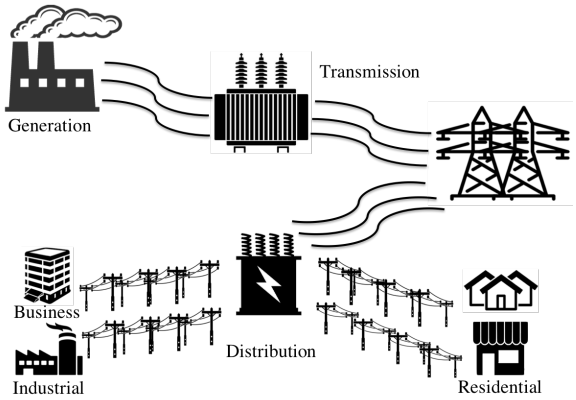

Fig. 3. Power grid architecture.

sumption. As seen in Figure 3, all the components are interconnected in a large scale network, also known as power grid.

The *generation* part is the first stage of a power system. It is the procedure of generating electric power from sources of primary energy. The three major categories of energy for electricity generation are fossil fuels (coal, natural gas, and petroleum), nuclear energy, and renewable energy sources. Most electricity is generated with steam turbines using fossil fuels, nuclear, biomass, geothermal, and solar thermal energy. Other electricity generation technologies include gas turbines, hydro turbines, wind turbines, and solar photovoltaics.

The power is then transferred through high-voltage lines and substations via the *transmission* network. Specifically, high-voltage transmission lines span across large geographical regions and carry electricity over long distances to where consumers need it. In the U.S. 97% of transmission lines are overhead [30]. Electric power can also be transmitted by underground power cables instead of overhead power lines. However, underground transmission systems have higher initial construction costs due to the requirement of insulated cables and excavation. For example, the estimated cost for constructing underground transmission lines ranges from 4 to 14 times more expensive than overhead lines of the same voltage and same distance [31].

The energy is then distributed via the *distribution* stage to end consumers. Distribution lines span in smaller distances and operate at lower voltages compared to transmission lines. Step down transformers are used to reduce the voltage levels to ranges that match the operational voltages of end consumers. Finally, electricity is utilized in the *consumption* stage. Electric utilities typically distinguish between consumers based on the type of activity they perform: residential, commercial, and industrial.

2.2 Protection and control equipment

Protection and control devices deployed in power systems are used to ensure the automatic isolation of faults (e.g., short circuits), abnormal conditions, or equipment failures through the disconnection of the faulted parts from the rest of the network. This separation into protective zones ensures the stable and secure power system operation and can limit or prevent damages to equipment and personnel. For example, a protection relay senses the abnormal conditions in a part of the power system and controls the trip operation of a circuit breaker when a fault is detected. Other protective equipment includes fuses, sectionalizers, as well as automatic operation devices such as auto-reclosers.

As reported from North American Electric Reliability Council (NERC), 70% of the major disturbances in the U.S. are associated with faulty operation of relay controllers [32]. Optimal attack strategies may require changing the breaker status signal at only one transmission line [33]. Furthermore, traditionally, power systems are designed to sustain a single component outage ($N-1$ criterion). Due to the growing complexity of modern power systems (e.g., significant generation uncertainty, malicious cyber-threats, distributed generations, etc.) regulatory agencies also require operators to ensure system stability in the event of multiple (two or more) contingencies k: either k (near-)simultaneous losses [$N-k$ ($k \geq 2$) contingency] or consecutive losses [$N-1-1$ contingency] [34]. The above highlight the necessity of constant and reliable operation of circuit breakers and relay controllers for avoiding catastrophic to the power grid consequences (e.g., cascading failures leading to blackouts).

2.3 Grid modernization

An important step towards grid modernization is the integration of Operational Technology (OT) and Information Technology (IT). Components in power grid are being upgraded with "smart" counterparts that enable fine-grain control, faster incident response times, and decision-making strategies. In addition, the incorporation of such units in control systems within the grid contributes in having increased efficiency, reliability and lower production and maintenance costs. The enabler of grid modernization four decades ago was the inclusion of microprocessor-based devices in control processes. Nowadays, the enablers of grid modernization are the advanced computation and networking abilities of these "smart" comprising components. To achieve these goals while keeping development costs low, vendors of power equipment typically leverage COTS technology, use common general-purpose microprocessor architectures (e.g., ARM, Intel x86) and real-time versions of commercial operating systems (e.g., Windows and Linux) [35].

The driving factors of grid modernization contribute to the development of grid systems equipped with embedded devices and communication protocols. The main grid components (generation, transmission, distribution, and consumption) are equipped with various embedded systems including communication networks,

control automation systems, and Intelligent Electronic Devices (IEDs). In general, IEDs deployed in power systems gather data from sensors across the grid, observe the variables and state of the system, store necessary data, make decisions, and take protection and control actions towards preserving performance and stability. For example, WAMS highly rely on IEDs to gather system information from multiple sources. WAMS are mainly enabled by PMUs that take synchronized snapshots of electrical quantities across the system, and use the comparative measurements to estimate the health and power quality of the grid.

Phase Measurement Units (PMUs) : PMUs are deployed primarily in the transmission stage and provide synchronized phasor (synchrophasor) measurements of voltage and current levels as well as frequency data at several locations in order to provide time-aligned information of the system's state. Due to their ability to monitor and analyze power system behavior, NERC's CEO Rick Sergel has said in 2008 that synchrophasors are "like the MRI of the bulk power system" [36].

Given the dispersed topology of the power grid, accurate time synchronization between such devices is essential for their operation. To that end the 50/60 Hz analog AC waveforms of the collected measurements are digitized via analog to digital converters and the majority of PMUs rely on timing provided by GPS modules for capturing synchronized snapshots of the system across geographically dispersed locations. In contrast with traditional SCADA systems that collect data every 2-4 seconds, the collection of PMUs' synchronized measurements at rates of 30 to 120 samples/second enable real-time situational awareness [37]. Current uses of synchrophasor technology for power grid situational awareness include wide-area visualization, oscillation detection, voltage stability and phase angle monitoring, state estimation, fault location, etc. In addition, PMU data can be utilized for offline analysis such as identification of equipment problems and misoperations, model validation (e.g., equipment, generation), forensic event analysis, NERC standard compliance, field equipment commissioning, etc [38].

A major limitation to large-scale deployment of PMUs is their high capital cost. The average overall cost per PMU (cost for procurement, installation, and commissioning) often ranges from $40,000 to $180,000 [39]. Due to the significant costs related with PMU installation, utilities often follow two major site selection methods. The first method follows a *i) function-dominant approach* in which the location meet utilities' needs relative to the desired synchrophasor data applications (e.g., placement of PMUs for power system observability [40–42]), including location choices driven by regional or NERC criteria. The power utility then upgrades its communication infrastructure to support the PMU-based applications being deployed. The second selection strategy follows a *ii) site-dominant approach* in which locations are identified based on the existing communication infrastructure and the utility stations that are sufficient to support the applications being deployed. The locations are then selected based on the utility's needs as driven by regional and/or NERC disturbance recorder placement criteria.

2.4 Global Positioning System

Global Navigation Satellite Systems (GNSS), an example of which is GPS, is an earth-orbiting satellite system where receivers on or near the Earth could collect the geolocation and time information from GNSS transmitters. The time measurements are based on atomic clocks on the satellites which are synchronized to the UTC. The geolocation information of the transmitters is assumed known at all times, as the satellites follow predetermined trajectories. As of December 2018, there were a total of 31 operational satellites in the GPS constellation, not including the decommissioned, on-orbit spares [43]. The constellation requires a minimum of 24 operational satellites. The U.S. is committed to maintaining the availability of at least 24 operational GPS satellites, 95% of the time. The U.S. Air Force normally flies more than 24 GPS satellites to maintain coverage whenever the baseline satellites are serviced or decommissioned.

Each satellite is broadcasting a navigation signal with time stamp data and the deviation from its predetermined trajectory. The GPS space segment consists of a constellation of satellites transmitting radio signals to users. It ensures that users have, at least, four simultaneous satellites in view from any point at the Earth surface at any time. Receivers obtain such signals from satellites within their field of view, and use the signal propagation delays to calculate their three-dimensional location data and time [44]. Each GPS satellite simultaneously transmits on two L-band frequencies denoted by L1 and L2, which are 1575.42 and 1227.60 MHz and are utilized in civilian and military applications (encrypted restricted signals), respectively. Additional GPS signals are used or being proposed as summarized below [45]:

- L1 - 1575.42 MHz: this GPS signal is used to provide the course-acquisition (C/A) and encrypted precision P(Y) codes. It is also used for the L1 civilian (L1C) and military (M) codes on the Block III satellites.
- L2 - 1227.60 MHz: this signal is used to carry the P(Y) code, as well as the L2C and military codes on the Block IIR-M and later satellites.
- L3 - 1381.05 MHz: this frequency is used to carry information regarding any nuclear detonation and high-energy infrared events.
- L4 - 1379.913 MHz: this signal is being studied for use with additional ionospheric correction.
- L5 - 1176.45 MHz: this GPS signal is being proposed for use as a civilian safety-of-life signal.

In this work, we focus on L1 signals, as PMUs utilize these signals for time synchronization.

3 Open sourcing power system cyberattacks

Adversaries can utilize a plethora of tools and approaches for disrupting national power grids. In this section, we focus on how malicious campaigns could adopt end-to-end open source approaches (i.e., cyberattacks based solely on public

information and infrastructure). Retracing the steps of a malicious actor whose objective is causing a wide area blackout, we identify three main requirements for achieving this goal. These are:

1. Formulate and construct an as accurate as possible model of the target system. This model is necessary for understanding the system, its dependencies, and also identifying weak spots.
2. Analyze the model to identify and evaluate critical targets. By carrying out analytical, data-driven studies of the system model, adversaries can identify critical locations, which could lead to cascading failures.
3. Instantiate attack vectors that target the critical locations identified in the previous step, materializing the attack towards achieving its objectives.

3.1 Threat model

The increased complexity and the modernization of power systems expose them to several vulnerabilities that one can use to gain access to the control network of the power systems. For example, COTS-based designs, including IEDs like PMUs, integrated in various parts of the grid are plagued by the same vulnerabilities present in processors and microcontrollers. In our scenario, the threat actors are considered to have the technical expertise to operate power systems. Moreover, they should have the knowledge of leveraging public resources and infrastructure to achieve their goals. The ultimate goal is to interrupt the normal operation of the power system and cause a large scale power blackout.

The threat model adopted in this analysis considers adversaries whose aim to cause power system disruption that would result in large scale power outages. We assume that the adversaries are proficient in power system operations, have sufficient technical expertise, and can, if required, be in physical proximity to power grid assets. However, we do not consider them to possess confidential information, or have network access to the equipment and control center of the target power system (e.g., phishing power system administrator credentials is outside the scope of this chapter).

In addition, we assume that the malicious actors can leverage publicly available information and infrastructure at scale to achieve their objectives. An immediate and noteworthy implication of this assumption is that adversaries are not limited to resource-wealthy nation states. Their motivation falls outside the scope of this paper, but it can for example be political, financial or to divert national resources in restoring the power while they pursue another primary objective.

3.2 Open Source Intelligence for modeling power systems

Comparing the several incidents that have led to power outages to date, most of them are the result of faults occurring on the transmission stage. Thus, adversaries are most likely to focus on this stage to cause power outages. To that end, a target model could be constructed that includes the network topology of all the

transmission substations, transmission lines, loads and their interconnections to enable further studies of the target system.

To the aid of adversaries, there exists a plethora of public information regarding power systems available, concerning system parameters, energy generation, power consumption, network topology, etc. From such sources it is possible for adversaries to reconstruct a model. Evidently, this form of "open source reconnaissance" or Open Source Intelligence (OSINT) is employed in an ongoing campaign against U.S. systems [46].

Some examples of sources include: a) public reports, such as blackout reports, regional expansion planning reports, load forecast reports, b) power system databases, such as Enipedia [47] and Open Energy Information [48], and c) press releases and success stories from power utilities and power grid equipment vendors. By combining and fusing information from such sources, a model of a target power system can be constructed for carrying out subsequent analyses. For example, detailed information regarding the construction of a power system model using public information can be found in [49, 50].

3.3 Identifying critical locations with contingency analysis

Identification of the critical locations for a given model is crucial for an attacker because it provides information both on the particular locations and also on the complexity of the final attack vector. To achieve this, power studies on the constructed model can enable judicious selection of optimal target locations for materializing an attack.

Contingency analysis is one of the most important studies for a security assessment of a power system, and one of particular usefulness to malicious actors. Contingency studies aim to analyze unscheduled events (e.g., generator, transformer, and/or transmission line failures) in a power system, and provide details on the stability of the system in case of any component failure within the power grid. In general, power systems are designed to sustain a single component failure, which is $N-1$ criterion. For example, North America Electric Reliability Corporation (NERC) power security standards require system operators to maintain continuous and reliable operation power systems under the $N-1$ constraint. Due to the computational overhead of contingency analysis, most research currently focuses on $N-2$ contingency analyses. Further information can be found in [51].

Nevertheless, for all systems there exists a number of contingencies that can lead to non-sustainable scenarios and cause cascading failures and ultimately a power outage. By applying contingency analysis techniques on the model constructed in the previous step, adversaries can identify the critical transmission lines and interconnections of a system, and focus their attacks against these particular locations to maximize disruption.

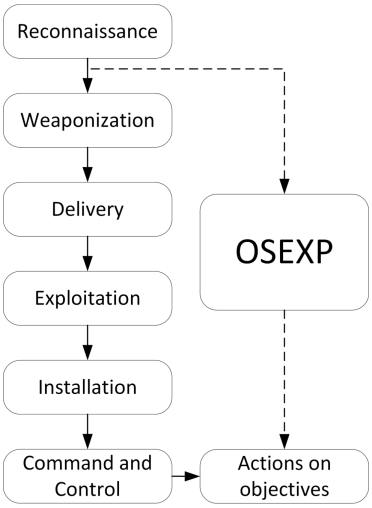

Fig. 4. Conventional Cyber Kill Chain with our proposed OSEXP step.

3.4 Open Source Exploitation - OSEXP

With knowledge of the critical points of a power system, adversaries need to construct attack vectors against the system. More specifically, they need to devise ways to disconnect critical transmission lines capable of a nonsustained contingency scenario. In this work, we focus on the exploitation of *public infrastructure*, and propose an open source methodology, which we call Open Source Exploitation (OSEXP). OSEXP techniques can be used both standalone, or in conjunction with conventional cyberattack techniques (e.g., phishing, credential harvesting, lateral movement, etc.), depending on the campaign objectives and resources available to the malicious actors. For a campaign whose target is to cause large scale power outages rather than just get information and leverage on a target system, we argue that OSEXP techniques can be advantageous.

In general, the Cyber Kill Chain (CKC) model can be used to describe the structure of a cyberattack [52]. The seven steps of the conventional CKC model are: 1) reconnaissance, where information is gathered, 2) weaponization, where a payload is designed, 3) delivery of the payload, 4) exploitation, where a vulnerability of the target system is exploited, 5) installation, where the payload is installed and executed on the target system, 6) command and control, where adversaries remotely tweak and instruct the payload and finally 7) actions on objectives, where adversaries fulfill the objectives of their campaign. By exploiting public infrastructure using OSEXP, steps 2 to 6 are replaced with an OSEXP step leading to an alternative path in the CKC, depicted in Fig. 4. The resulting CKC using OSEXP attacks has fewer steps, is reusable and leaves less evidence behind, making forensic studies and attribution harder.

3.5 Instantiation of an OSEXP attack: GPS time spoofing against PMUs

As outlined in Section 2, PMUs can take protective control actions in addition to their monitoring role. Taking advantage of this, judicious manipulation of PMU measurements can destabilize a system, making PMUs attractive targets for malicious actors. The OSEXP attack against PMUs we describe in this section exploits the reliance of PMUs on GPS (which is a public resource) for time synchronization. Our OSEXP attack introduces erroneous PMU measurements by manipulating the timing source of PMUs, effectively disconnecting selected PMU-controlled transmission links.

Corroborating the feasibility of OSEXP GPS attacks, information, implementation details, and software regarding GPS are part of the public domain. Open source implementations of GPS receivers and transmitters for Software Defined Radios (SDRs), software GPS simulators and available literature lower the technical requirements for successful GPS spoofing attacks [53]. Furthermore, the global nature of GPS ensures that a GPS spoofing attack can be reused in diverse systems employing different hardware across the globe. In contrast, techniques that require identifying and exploiting deployed devices, software, and network channels are system-specific and require undertaking laborious research for each system. These observations render GPS time spoofing an effective attack vector that can be developed once and reused several times against disparate systems.

GPS receivers inherently trust the signals they receive, assuming the signals have not been tampered with. In most countries in the world, any transmission in the frequency band of GPS is illegal, addressing the risk with policy safeguards. However, from a technical standpoint L1 GPS signals do not have any built-in integrity protection mechanisms. With OSEXP GPS spoofing attacks, we challenge the inherent trust in the integrity of these signals, arguing that adversaries with far-reaching agendas, such as causing blackouts, will not be bound by ethical and legal concerns.

Given the reliance of PMUs on GPS for capturing the state of a power system in a synchronized manner, we describe the process of introducing errors in PMU measurements by manipulating GPS signals in their vicinity. This can cause desynchronized snapshots of the system state from PMUs in different geographical locations, leading to system destabilization and even cascading failures. In particular, GPS time spoofing attacks can introduce errors in the absolute time perceived by the affected PMUs. For an f-Hz signal the relationship between the clock offset error $\widetilde{t_\delta} - t_\delta$ and the phase angle measurement error ϵ are described by the following equation [54]:

$$\epsilon = [f \times (\widetilde{t_\delta} - t_\delta) \times 360^\circ] \pmod{360^\circ} \tag{1}$$

PMUs with control capabilities have a preconfigured threshold for allowed phase angle difference, that is dependent on the specifics of the system they are deployed in. Phase differences larger than this threshold cause connected CBs to open for avoiding fault propagation and protecting the equipment. However, introducing timing errors with GPS spoofing to instantly change the perceived

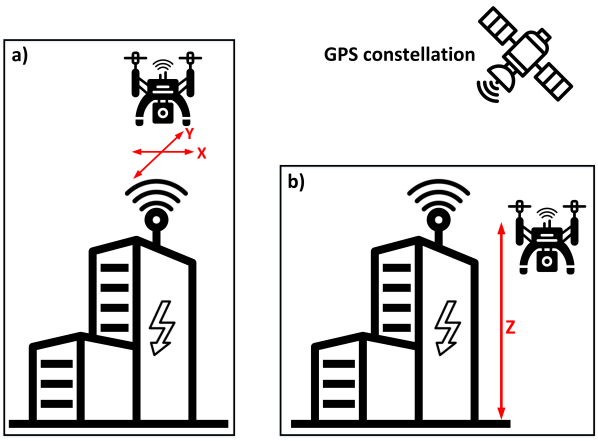

Fig. 5. Estimation of 3D location of a static GPS receiver using a drone. a) x,y coordinates. b) z coordinate.

state of the system for a PMU to exceed this threshold is not possible, because of the standards that govern PMUs. In particular, the IEEE standard for Synchrophasor Measurements for Power Systems (C37.118) dictates that clock synchronization errors between any two measurements from different PMUs should not exceed 31(26) μs for 50(60) Hz systems [55]. For a successful attack, it is thus necessary to slowly drift angle measurements, without exceeding these limits.

Another requirement for a successful GPS spoofing attack is knowledge of the legitimate GPS signal as it is perceived by the target receiver, including location information. This requirement can be fulfilled by co-locating the spoofing equipment in the physical vicinity of the target. The location information of a receiver is static, as the antenna is mounted on a building. Towards measuring the receiver location, attackers can measure their relative distance from the receiving antennas and calculate the offset, for example by employing drones equipped with cameras and GPS receivers. By flying directly over the target antenna, adversaries can capture the x,y location using the drone mounted GPS receiver. Subsequently, the z coordinate can be measured independently. Fig. 5 illustrates this scenario.

In addition to identifying receiver location, generation of appropriate synthetic GPS signals requires that the spoofed and legitimate GPS signals are time-synchronized [56]. This enables attackers to concurrently transmit a spoofed signal that is synchronized with the legitimate signal, gradually increase the transmitting power overtaking the GPS receivers in the affected vicinity, and then introduce time delays that will cause erroneous PMU measurements. The naive approach of recording legitimate GPS signals and replaying them after introducing the necessary time delays is not possible due to non-deterministic delays introduced by the retransmitting equipment's hardware components and the strict timing requirements of the IEEE C37.118 synchrophasor standard. To

overcome this challenge, attackers can generate a *leading* GPS signal, and then gradually introduce appropriate delays to achieve synchronization between their spoofed and the legitimate GPS signals. The equipment required for this are two GPS receivers (one for the legitimate and one for the spoofed signal) and means to measure the time difference between the two signals.

An observation regarding the GPS OSEXP attack is that it requires simultaneous physical proximity to all target locations is required, meaning that adversaries need to coordinate an attack at k locations in the case of attacking a system to trigger an $N-k$ contingency. For most power systems, opening CBs at two judiciously selected locations is sufficient to destabilize the system. We argue here that requiring two to three field agents for launching an attack of this scale and impact is realistic and by no means prohibitive.

4 Experimental Evaluation

In this section we evaluate the feasibility of the proposed GPS time spoofing OSEXP attack. To that end, we present two experimental setups. The first one utilizes DRTS and specifically the OPAL-RT platform in order to perform a real-time simulation of a test case power system. From an attacker's standpoint, this step will verify the developed power grid model using OSINT as well as extract required information to be utilized for the instantiation of the OSEXP attack vector. In the second experimental setup, we verify that open source software and SDR platforms are capable of launching GPS time spoofing attacks with the necessary granularity as this is defined by IEEE C37.118.

4.1 Power System Modeling

The model of a power system is developed in RT-LAB. RT-LAB is the software platform of OPAL-RT's simulation systems. It can communicate with hardware equipment through FPGA I/O interfaces and is used for the execution of the MATLAB/Simulink blocks, including those in the SimPowerSystems (SPS) blockset, in real-time on a PC-based cluster. Time domain simulation method is used in this work to assess the stability of the power system. The time step, Δt, for the simulations is set at 0.02 seconds. The model is developed in the RT-LAB/Simulink environment offline, and then, compiled and downloaded to the OPAL-RT simulator that performs a real-time simulation with a cluster of processors.

The power system used in this study is the IEEE 9-bus case which represents a simple approximation of the Western System Coordinating Council (WSCC) to an equivalent system with three generators and nine buses [57]. The single line diagram of the WSCC 9-bus system is presented in Fig. 6. The system was slightly modified for simulation purposes: circuit breakers are included at each line and after each generator before connected to the grid. Also, the power system is monitored by modelled PMUs (available in OPAL-RT) across the network resembling their placement in a real power grid network. PMUs are added to

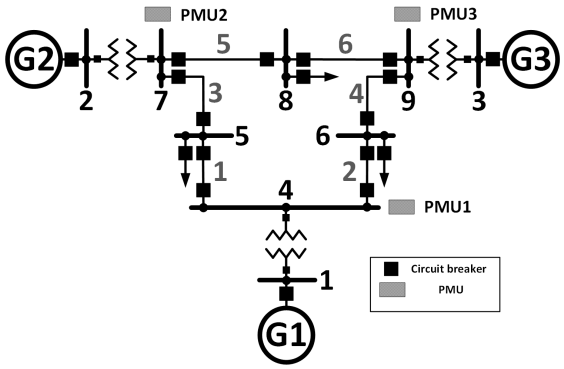

Fig. 6. Modified WSCC 9-bus system.

three of the system buses to monitor the real-time phasors of both voltages and currents. The simulation model consists of 3 subsystems: a master subsystem (SM), a slave subsystem (SS), and a console subsystem (SC). The SM is the main subsystem of the model which includes all computational and measurements elements. The SS includes the PMU models distributed across multiple nodes of the grid. The SC is the interface module available during execution in order to interact with the system while it is running. Our objective is to collect phase angle measurements from the PMUs before and after a set of events (e.g., faults, breaker tripping, etc.). The angle difference between two sets of phasors measured at two different locations can serve as an indicator of the grid stress [24]. Thus, an attacker able to manipulate GPS signals in the receiver of PMUs could trigger protection and control schemes.

As mentioned in Section 2, a major drawback to large-scale deployment of PMUs is the cost related with their installation. In our work, the minimum number as well as the optimal locations of the PMUs in the system follows a *function-dominant approach* from literature which aims to make the system topologically observable [40, 41]. An integer linear programming (ILP) method that generates all possible candidate PMU placement solutions to guarantee topological observability is as follows [40]:

$$\begin{aligned} N_{PMU} &= min \sum_{i=1}^{n} y_i \\ s.t.\ T_{PMU} Y &\geq b \end{aligned} \tag{2}$$

where T_{PMU} is a binary connectivity matrix [40], $b = [1, 1, ..., 1]^T_{n\times 1}$, $Y = [y_1, y_2, ..., y_n]^T$, where $y_i \in \{0, 1\}$ is the PMU placement variable on the i_{th} bus, with 1 indication a placement and 0 indicating no placement. This method gives only one possible solution for the minimum number of PMUs N_{PMU}. Adding an auxiliary parameter $D = [d_1, d_2, ..., d_n]$, $d_i = rand(0, 1)$, $i = 1, 2, ..., n$ to the

cost function of the above equation and when the number of realizations of D is sufficiently large, all the possible of candidate optimal PMU placement solutions can be generated [41]:

$$\begin{aligned} & min\ DY \\ N_{PMU} = & min \sum_{i=1}^{n} y_i \\ & s.t.\ T_{PMU} Y \geq b \end{aligned} \tag{3}$$

The outcome of the placement modified algorithm using (3) allows for more than one optimal solution to exist. For the implemented 9-bus test case, four sets of three buses are determined to place PMUs. The four solutions are $\{2, 4, 9\}$, $\{3, 7, 4\}$, $\{1, 7, 9\}$ and $\{4, 7, 9\}$. The optimal solution considered for this work, places PMUs in the following set of 9-system buses $\{4, 7, 9\}$, as shown in Fig. 6. Based on our threat model, the locations of those installed PMUs can be identified using OSINT methods such as using satellite images to identify the GPS antennas at the grid substations [50].

In the developed model of the power system, three-phase (3-ϕ) faults are created at different locations of the system at any one time. In power systems, faults could occur as a result of eventful conditions such as natural events and accidents in which phase(s) establish a connection with other phase(s), the ground, or both in some circumstances. This results in a rapid and massive flow of current via an improper path which could cause injuries and death, interruption of power, as well as equipment damage. Faults in power systems are classified into open and short circuit faults which can either symmetrical or unsymmetrical [58]. During a fault, the power system goes through pre-fault, fault-on, and post-fault stages [59]. In our model, we simulate 3-ϕ faults at the lines of the system; when a fault occurs, a breaker operates and disconnects the corresponding line at the fault clearing time (FCT) which is set at the 4 cycles ($4 \times 16.7\ ms$). The protection system clears the fault instantaneously without intentional time delay. We consider a normal clearing time of 4 cycles: 2 cycles for relay/PMU time and 2 cycles for breaker time [60].

Modeling Results After constructing the IEEE 9-bus simulation model and adding the three required PMUs in the system at buses $\{4, 7, 9\}$, we run simulations for different fault scenarios and we observe the differences on the PMU phase angle measurements. Specifically, for each case we introduce a 3-ϕ to ground fault at the transmission line ij between bus i and bus j, and measure the phase angle difference from the, simulated in OPAL-RT, PMU before and after (2 cycles) the fault has been triggered. The simulation results are shown in Table 1. For example, in case 5 where a $3-\phi$ fault is applied to line between buses 7-8, the phase angle difference $\Delta\theta = \theta_{PMU2} - \theta_{PMU3}$, i.e., between the PMUs installed at buses 7 and 9 respectively, changes from 1.8° in normal operating conditions to $-72.2307°$ 2 cycles after the fault. Fig. 7 presents the

Table 1. Positive-sequence voltage phase angle difference ($\Delta\theta$) between PMU-supported buses of modified WSCC 9-bus system. $\Delta\theta_0$ indicates normal operation and each presented scenario is $\Delta\theta$ 2 cycles after the 3-ϕ fault at the lines between buses $i-j$.

A/A	**Line** $(i-j)$	$\boldsymbol{\Delta\theta^{\circ}_{(PMU_1-PMU_2)}}$ $\boldsymbol{\Delta\theta_0} = -5.841^{\circ}$	$\boldsymbol{\Delta\theta^{\circ}_{(PMU_2-PMU_3)}}$ $\boldsymbol{\Delta\theta_0} = 1.8^{\circ}$	$\boldsymbol{\Delta\theta^{\circ}_{(PMU_1-PMU_3)}}$ $\boldsymbol{\Delta\theta_0} = -4.0414^{\circ}$
1	4-5	-15.9893	5.2364	-10.7530
2	4-6	-15.1038	2.0563	-13.0475
3	5-7	-15.9932	5.2271	-10.7661
4	6-9	-18.4971	80.1049	61.6078
5	7-8	59.0539	-72.2307	-13.1768
6	8-9	-18.4997	85.3294	66.8297

difference in the positive-sequence voltage phase angle between the two PMUs before, during, and after the clearing time of the fault at line 5 (buses 7-8). The data are obtained in real-time using the simulated PMUs of OPAL-RT. As shown in Table 1, phase angle difference can serve as an effective indicator of the performance of a power system. Monitoring and protective schemes often utilize such data to detect reliably, among others, instantaneous changes in the transmission lines' impedance and thus contingency conditions. In our presented results, an angle difference threshold of 70° can detect, for example, the occurrence of the presented case 5 for PMU_2 and PMU_3. System operators can utilize this information to set the PMU-based protective configuration accordingly in order to trip the breaker once this phase angle difference occurs between PMU at bus 7 (PMU_2) and bus 9 (PMU_3). However, such schemes can be leveraged by the presented spoofer attacker who may target one or both PMUs as the target the OSEXP attack. The timing error introduced by spoofing the GPS receiver of the PMU(s) will cause a corresponding phase error in the reported synchrophasor data, and therefore trigger the presented scheme unnecessarily (without any actual fault in the system). A series of such attacks has the potential to cause cascading effects in the system leading to instability conditions and power outages.

4.2 GPS Experimental Setup

In this part, we evaluate the feasibility of a low cost GPS time spoofing attack. For our GPS spoofing experiments we assume that attackers have synchronized their synthetic signals to legitimate GPS signals and have taken over control of the GPS receiver. These are realistic assumptions if an attacker can introduce *arbitrary delays* to a GPS signal, as arbitrary delays can be leveraged to achieve synchronization of leading signals with the legitimate ones. After the two signals are synchronized, attackers can gradually increase the spoofed signal power, overtaking control of receivers within their vicinity [29].

The hardware in our experimental setup consists of a GPS receiver, an Arduino board, a SDR, a logic analyzer and a host computer. The GPS receiver

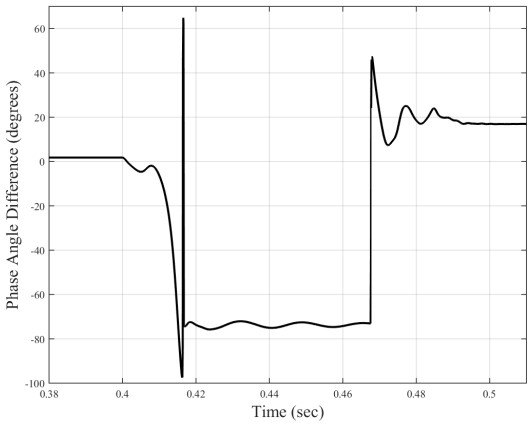

Fig. 7. Positive-sequence voltage phase angle difference between PMU_2 and PMU_3 at buses 7 and 9 respectively before, during, and after the clearing time of a three-phase (3-ϕ) fault at line 5 (buses 7-8) applied at $0.4s$ for $0.1s$.

employs the Venus638FLPx chip, which is a commercial, high performance receiver with 29 seconds cold start time-to-first-fix, up to 20 Hz update rate, and built-in jamming detection and mitigation. The GPS receiver is powered by an Arduino UNO board, which is also connected to the host computer for receiving and outputting the decoded NMEA messages. We utilize a Saleae Logic Pro 8 logic analyzer for sampling the Pulse-Per-Second (PPS) output pin of the receiver at a sampling rate of 10 MHz, which is satisfactory given the GPS receiver's PPS measured accuracy of 2 μs. For transmitting GPS signals we use an Ettus USRP N210 SDR, equipped with a GPSDO kit and a 40 MHz SBX 400-4400 MHz Rx/Tx. Respecting the legal framework concerning GPS signal transmission over-the-air, we conduct all of our experiments using cable connections and never transmit signals over-the-air, without loss of generality. To further ensure no side-effects we attenuate the USRP output to -140dBm, which is close to the minimum required signal by our GPS receiver for a fix (-148 dBm). Finally, we enclose the experimental setup in RF shielding fabric to avoid leakage. Our experimental setup is depicted in Fig. 8.

In terms of software, we rely solely on open source software. For generating synthetic GPS data we use the Software-Defined GPS Signal Simulator (`gps-sdr-sim`) [61]. We download the required ephemerides data that indicate the current state of the satellite constellation from the Crustal Dynamics Data Information System [62]. Using `gps-sdr-sim` and the current ephemerides we create a raw synthetic static L1 GPS signal with a 2.5 MHz sampling rate, that is leading the current wall time by a few seconds. We input this signal to GNU Radio to perform the necessary type conversions, and add a delay block of user-

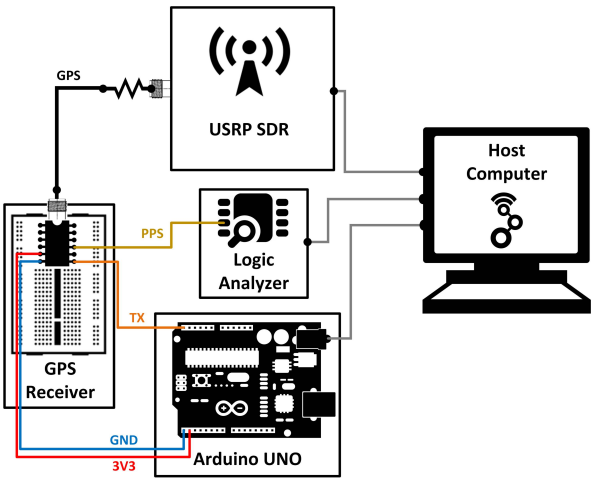

Fig. 8. Experimental setup for GPS spoofing attack.

specified duration between the file source and the USRP sink. This entire process is automated.

GPS Spoofing Results : Since the maximum clock offset error required by the IEEE C37.118 protocol is $31\mu s$ for a 50Hz system, we aim to introduce approximately 30 μs delay to the targeted PMU in order for the attack to remain undetected. To that end, we select 30 μs as the user-specified delay duration in our GNU Radio flowchart and launch the automated script. We present the experimental results regarding time as it is perceived by the receiver in Fig. 9. In particular, the figure presents the absolute duration of PPS signals as it is perceived by the GPS receiver and measured by the logic analyzer. We observe that up to $t = 16s$ (which is when the attack is launched), each PPS signal is received exactly every one second, as expected. After the attack is launched, the particular pulse duration at $t = 16s$ becomes 1.0000289 s, indicating a shift in the perceived time by the GPS receiver as a result of our GPS signal manipulation. The introduced delay of 28.9 μs is below the 31 μs threshold, verifying the feasibility of using COTS equipment and open source software to launch fine-grain GPS time spoofing attacks.

The introduced time delay of the GPS spoofing attack introduces errors in the absolute time perceived by the targeted PMUs which can be calculated using (1). This allows to examine the impact of the spoofing scenario on the power system. In particular, the 28.9 μs time delay results in a shift of 0.54° in the measured angle by the corresponding PMU. *Delays of arbitrary duration* can be introduced by repeatedly applying the same time-shifting technique. Accumulation of such delays can gradually increase the phase difference between actual and measured angles, reaching the pre-programmed threshold at which the respective circuit breakers are tripped, leading to sectionalization and cascading failures. Note that

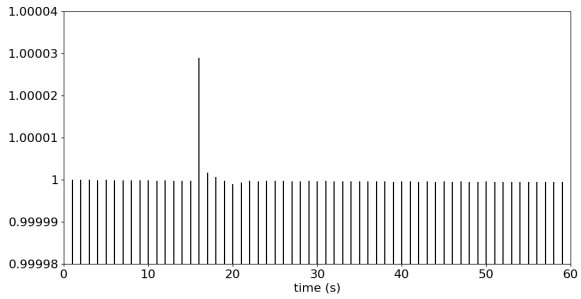

Fig. 9. Experimental results showing GPS receiver output PPS duration. The GPS spoofing attack is launched at $t = 16$ seconds.

in addition to introducing erroneous measurements to PMUs, the same time-shifting technique can be employed to synchronize leading synthetic signals and legitimate GPS signals. In the presented case 5 of Section 4.1, the protection scheme automatically triggers the corresponding circuit breakers to disconnect the line after a fault occurs. In order for an attacker to shift the obtained PMU phase angle measurements by $\geq 70^\circ$ and thus activate the control algorithm resulting in falsified protection actions, she is required to repeat the above step 130 times ($130 \times 0.54 = 70.2^\circ$).

4.3 Budget

Our first experimental setup utilizes a DRTS to model the power grid. The reason is twofold: verify the developed power system model and identify the synchronized phase angle difference measurements by PMUs which are utilized to detect topology changes. The cost of acquiring and utilizing the described DRTS and its functions is in the order of a few tens of thousands of dollars. However, this can be additionally reduced by using newer versions of DRTS equipment which can a substantial lower cost.

The cost of the equipment we utilize for GPS time spoofing mainly consists of the Ettus USRP SDR (and its respective add-on modules) and the Saleae Pro 8 logic analyzer. Their costs are $3529 USD and $699 USD respectively, for a total of $4228 USD. Launching a concurrent attack against k locations to materialize an $N - k$ contingency would require $k\times$ $4228 USD (typically $k = 2$ or $k = 3$ locations are sufficient), which is low given the attack's far-reaching impact.

Our equipment costs in the GPS spoofing attack are dominated by the Ettus USRP SDR and they can be further reduced by replacing it with cheaper hardware, such as the bladeRF ($420 USD), or HackRF ($295 USD). An inherent limitation of these lower-cost devices is the reduced accuracy of their built-in oscillator, which is not adequate for transmitting GPS signals. However, this problem can be alleviated with OSEXP by leveraging another public infrastructure; *GSM base stations* [63]. As cell towers must be accurate within 0.5 parts-per-million (which is sufficient for GPS transmission), we can initially con-

figure SDRs as GSM receivers. Using GSM signals, we can calculate the internal clock drift of our SDR with reference to the GSM base station clock, and then reconfigure the SDR as a GPS spoofer to carry out the spoofing technique as described above.

5 Conclusions

In this work, we introduce OSEXP, a technique that utilizes public infrastructure towards constructing an attack vector against power systems. We experimentally verify a specific OSEXP vector, GPS time spoofing, that can cause inaccuracies and errors in the measurements of PMUs deployed in WAMS applications. As a result, the GPS spoofing attack can desynchronize phase angle measurements of judiciously selected PMUs and can further cause deterioration to the system or even cause wide-area blackouts. The demonstrated OSEXP vector employs COTS hardware and open source software, enabling reusable low-budget high-impact attacks against power systems. For simulating the power system as well as determining the angle which an attacker needs to shift in order to trigger protective schemes, we use real-time data from simulated PMUs in a DRTS. With this study we aim to challenge the perception these attacks are feasible only by resource-wealthy nation state actors, and assist stakeholders and regulators take informed decisions to secure power grids around the world.

References

1. R. Lobenstein and C. Sulzberger, "Eyewitness to dc history," *IEEE Power and Energy Magazine*, vol. 6, no. 3, 2008.
2. Enerdata, "Electricity domestic consumption," [Online]. Available: https://yearbook.enerdata.net/electricity/electricity-domestic-consumption-data.html.
3. U.S. Department of Energy, "Maintaining reliability in the modern power system," [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Maintaining%20Reliability%20in%20the%20Modern%20Power%20System.pdf.
4. Eaton, "Blackout tracker: United States annual report 2017," 2017.
5. P. Strange, "Monster nor'easter pummels east coast," vol. 126, no. 9, pp. 863–868, 1979.
6. Wikipedia, "Hurricane michael," [Online]. Available: https://en.wikipedia.org/wiki/Hurricane_Michael, 2018.
7. J. Ditler, "The great coronado blackout of 2011," 2011.
8. Department of Defense, "Annual Energy Management and Resilience Report (AEMRR)," [Online]. Available: https://www.acq.osd.mil/eie/Downloads/IE/FY%202017%20AEMR.pdf, 2018.
9. Kaspersky, "Cyperthreats to ics systems," [Online]. Available: http://media.kaspersky.com/en/business-security/critical-infrastructure-protection/Cyber_A4_Leaflet_eng_web.pdf, 2014.
10. S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.

11. C. Konstantinou and M. Maniatakos, "Security analysis of smart grid," *Communication, Control and Security Challenges for the Smart Grid*, vol. 2, p. 451, 2017.
12. The Council of Economic Advisers, "The cost of malicious cyber activity to the u.s. economy," [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, 2018.
13. CNN, "Mouse click could plunge city into darkness, experts say," [Online]. Available: http://www.cnn.com/2007/US/09/27/power.at.risk/index.html, 2007.
14. K. Yamashita, S.-K. Joo, J. Li, P. Zhang, and C.-C. Liu, "Analysis, control, and economic impact assessment of major blackout events," *European Transactions on Electrical Power*, vol. 18, no. 8, pp. 854–871, 2008.
15. D. Trivellato and D. Murphy, "Lights out! who's next? how to anticipate the next "cyber-blackout"," 2016.
16. D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.
17. K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," [Online]. Available: http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
18. D. Goodin, "Hackers trigger yet another power outage in ukraine," [Online]. Available: https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/, 2017.
19. Dragos, Inc., "Crashoverride: Analysis of the threat to electric grid operations," [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, 2017.
20. C. P. Steinmetz, "Complex quantities and their use in electrical engineering," in *Proceedings of the International Electrical Congress*, 1893, pp. 33–74.
21. A. G. Phadke, "Synchronized phasor measurements-a historical overview," in *Transmission and Distribution Conference and Exhibition 2002: Asia Pacific. IEEE/PES*, vol. 1. IEEE, 2002, pp. 476–479.
22. North American Synchrophasor Initiative (NASPI), "Time synchronization in the electric power system," [Online]. Available: https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf, 2017.
23. T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Radionavigation Laboratory Conference Proceedings*, 2008.
24. C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos, "Gps spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 180–187, 2017.
25. C. Konstantinou and M. Maniatakos, "Hardware-layer intelligence collection for smart grid embedded systems," *Journal of Hardware and Systems Security*, pp. 1–15, 2019.
26. R. D. Steele, "Open source intelligence," *Handbook of intelligence studies*, pp. 129–147, 2007.
27. A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos, "Low-budget energy sector cyberattacks via open source exploitation," in *2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2018, pp. 101–106.
28. M. O. Faruque, T. Strasser, G. Lauss, V. Jalili-Marandi, P. Forsyth, C. Dufour, V. Dinavahi, A. Monti, P. Kotsampopoulos, J. A. Martinez *et al.*, "Real-time sim-

ulation technologies for power systems design, testing, and analysis," *IEEE Power and Energy Technology Systems Journal*, vol. 2, no. 2, pp. 63–73, 2015.
29. D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.
30. F. Alonso and C. Greenwell, "Underground vs. overhead: Power line installation-cost comparison and mitigation," *Electric Light & Power*, 2013.
31. Public Service Commission of Wisconsin, "Underground electric transmission lines," [Online]. Available: https://psc.wi.gov/Documents/Brochures/Under%20Ground%20Transmission.pdf, 2011.
32. North American Electric Reliability Council, New Jersey, "NERC Disturbance Reports 1992-2009."
33. D. Deka, R. Baldick, and S. Vishwanath, "One breaker is enough: hidden topology attacks on power grids," in *Power & Energy Society General Meeting, 2015 IEEE*. IEEE, 2015, pp. 1–5.
34. NERC, "Standard TPL-001-1," [Online]. Available: https://www.nerc.com/files/TPL-003-0.pdf.
35. K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems security," *NIST special publication SP 800-82*, 2011.
36. E. O. Schweitzer, D. Whitehead, G. Zweigle, K. G. Ravikumar, and G. Rzepka, "Synchrophasor-based power system protection and control applications," in *Modern Electric Power Systems (MEPS), 2010 Proceedings of the International Symposium*. IEEE, 2010, pp. 1–10.
37. Y.-J. Kim, J. Lee, G. Atkinson, and M. Thottan, "Griddatabus: Information-centric platform for scalable secure resilient phasor-data sharing," in *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*. IEEE, 2012, pp. 115–120.
38. A. Silverstein, "Synchrophasors & the grid," [Online]. Available: https://www.naspi.org/sites/default/files/reference_documents/naspi_naruc_silverstein_20170714.pdf.
39. U.S. Department of Energy, "Factors affecting pmu installation costs," [Online]. Available: https://www.smartgrid.gov/files/PMU-cost-study-final-10162014_1.pdf.
40. B. Gou, "Optimal placement of pmus by integer linear programming," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 1525–1526, 2008.
41. X. Tai, D. Marelli, E. Rohr, and M. Fu, "Optimal pmu placement for power system state estimation with random component outages," *International Journal of Electrical Power & Energy Systems*, vol. 51, pp. 35–42, 2013.
42. S. Chakrabarti and E. Kyriakides, "Optimal placement of phasor measurement units for power system observability," *IEEE Transactions on power systems*, vol. 23, no. 3, pp. 1433–1440, 2008.
43. U.S. Government, "GPS.gov," [Online]. Available: https://www.gps.gov/support/faq/#gap1.
44. E. Kaplan and C. Hegarty, *Understanding GPS: Principles and applications*. Artech house, 2005.
45. A. El-Rabbany, *Introduction to GPS: the global positioning system*. Artech house, 2002.
46. U.S. DHS and FBI, "Russian government cyber activity targeting energy and other critical infrastructure sectors," [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-074A.

47. C. Davis, A. Chmieliauskas, and I. Nikolic, "Enipedia," *Energy & Industry group, TU Delft*, 2015.
48. "Open energy information," [Online]. Available: http://openei.org.
49. C. Konstantinou, M. Sazos, and M. Maniatakos, "Attacking the smart grid using public information," in *IEEE Latin-American Test Symposium*, 2016, pp. 105–110.
50. A. Keliris, C. Konstantinou, M. Sazos, and M. Maniatakos, "Open source intelligence for energy sector cyberattacks," in *Critical Infrastructure Security and Resilience*. Springer, 2019, pp. 261–281.
51. S. Pajic, "Power system state estimation and contingency constrained optimal power flow: A numerically robust implementation," 2007.
52. Lockheed Martin, "Cyber Kill Chain," [Online]. Available: https://www.lockheedmartin.com, 2014.
53. E. Blossom, "GNU radio: tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, p. 4, 2004.
54. X. Jiang, "Spoofing GPS receiver clock offset of phasor measurement units," Master's thesis, UIUC, 2012.
55. P. S. R. Committee, "IEEE Standards for synchrophasor measurements for power systems C37.118," *New York, USA*, 2011.
56. N. O. Tippenhauer, C. Pöpper, K. B. 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.
57. Illinois Center for a Smarter Electric Grid (ICSEG), *WSCC 9-Bus System*. Information Trust Institute (ITI), 2017.
58. P. M. Anderson and A. A. Fouad, *Power system control and stability*. John Wiley & Sons, 2008.
59. N. Amjady and S. F. Majedi, "Transient stability prediction by a hybrid intelligent system," *IEEE Transactions on Power Systems*, vol. 22, no. 3, pp. 1275–1283, 2007.
60. North American Electric Reliability Corporation, "Protection system reliability redundancy of protection system elements," [Online]. Available: https://www.nerc.com/docs/pc/spctf/Redundancy_Tech_Ref_1-14-09.pdf.
61. T. Ebinuma, "Software-Defined GPS signal simulator," [Online]. Available: https://github.com/osqzss/gps-sdr-sim.
62. C. E. Noll, "The Crustal Dynamics data information system: A resource to support scientific analysis using space geodesy," *Advances in Space Research*, vol. 45, no. 12, pp. 1421–1440, 2010.
63. G. N. Varma, U. Sahu, and G. P. Charan, "Robust frequency burst detection algorithm for gsm/gprs," in *Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th*, vol. 6. IEEE, 2004, pp. 3843–3846.