Digital Forensic Analysis of Industrial Control Systems Using Sandboxing: A Case of WAMPAC Applications in the Power Systems

Article *in* Energies · July 2019

DOI: 10.3390/en12132598

3 authors, including:

Asif Iqbal
KTH Royal Institute of Technology
17 PUBLICATIONS **68** CITATIONS

SEE PROFILE

Mathias Ekstedt
KTH Royal Institute of Technology
147 PUBLICATIONS **2,021** CITATIONS

SEE PROFILE

energies

MDPI

Article

Digital Forensic Analysis of Industrial Control Systems Using Sandboxing: A Case of WAMPAC Applications in the Power Systems †

Asif Iqbal *, Farhan Mahmood and Mathias Ekstedt

School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm SE-100 44, Sweden

* Correspondence: asif.iqbal@ee.kth.se

† This paper is an extension of the paper Iqbal, A., Mahmood, F., & Ekstedt, M. (2018, November), An Experimental Forensic Testbed: Attack-based Digital Forensic Analysis of WAMPAC Applications. Presented at the 11th Mediterranean Conference on Power Generation, Transmission, Distribution, and Energy Conversion (MEDPOWER 2018), Dubrovnik, Croatia, 12–15 November 2018.

Received: 11 May 2019; Accepted: 3 July 2019; Published: 6 July 2019

Abstract: In today's connected world, there is a tendency of connectivity even in the sectors which conventionally have been not so connected in the past, such as power systems substations. Substations have seen considerable digitalization of the grid hence, providing much more available insights than before. This has all been possible due to connectivity, digitalization and automation of the power grids. Interestingly, this also means that anybody can access such critical infrastructures from a remote location and gone are the days of physical barriers. The power of connectivity and control makes it a much more challenging task to protect critical industrial control systems. This capability comes at a price, in this case, increasing the risk of potential cyber threats to substations. With all such potential risks, it is important that they can be traced back and attributed to any potential threats to their roots. It is extremely important for a forensic investigation to get credible evidence of any cyber-attack as required by the Daubert standard. Hence, to be able to identify and capture digital artifacts as a result of different attacks, in this paper, the authors have implemented and improvised a forensic testbed by implementing a sandboxing technique in the context of real time-hardware-in-the-loop setup. Newer experiments have been added by emulating the cyber-attacks on WAMPAC applications, and collecting and analyzing captured artifacts. Further, using sandboxing for the first time in such a setup has proven helpful.

Keywords: forensic investigations; forensic evidence substation; wide area monitoring protection and control; phasor measurement units (PMUs); industrial control systems; sandboxing

1. Introduction & Motivation

An increasingly digitized or smart world has created dangerous times. Incidents related to cyberweapons like BlackEnergy [1] started as a simple distributed denial of service (DDoS) platform to a quite sophisticated plug-in based malware and Stuxnet [2]. This included the destruction of equipment in the operational technology (OT) environment which is a reminder about the vulnerabilities of this digital world. The impacts of such cyber-physical attacks on critical infrastructures resonate far beyond the confines of Iran and Ukraine. These were very well coordinated attacks, well-structured and pre-planned. In today's multi-polar world, it is foreseeable to consider that such types of attacks would continue to prosper with increased complexity.

Hence, in such a volatile world, it is of paramount importance to be well-prepared in terms of threat analysis and collection of digital evidence in order to attribute attacks to state and non-state

actors. Forty-six cyber-attacks incidents were reported in the energy sector in 2015 [3], mostly related to the IT system of power utilities and their dealers. The U.S. Department of Energy indicates that the actual number of cyber-attacks is higher than reported [4].

The conventional electrical power grids are being transformed into smarter grids. Wide area monitoring protection and control (WAMPAC) systems, is one of the many advanced capabilities that are being equipped with the area of electric power systems. WAMPAC helps to improve planning, operation, and maintenance of electric grids [5]. The major components of this system are the phasor measurement units (PMUs) and the phasor data concentrators (PDCs). In a WAMPAC system, time-synchronized phasor data from multiple PMUs are integrated into a PDC, to produce a time-aligned output PDC data stream. A PDC is usually compliant with the IEEE C37.118 standard. PDC, being one of the most important parts of WAMPAC, is vulnerable to cyber-attacks.

Motivation

It is extremely important for a forensic investigation to get credible evidence for any cyber-attack attribution as required by the Daubert standard for it to be admissible in a court of law. Evidence should follow the Daubert standard and the integrity of the evidence must be flawless. If the integrity of evidence can be ensured and the Daubert standard is followed, only then can attributing evidence incriminating the culprits be presented. All of this only possible if there is a controller environment in which the parameters have been set and the type of the variations occurring with respective changes is known. In other words, the exact activity is mapped with exact attributing evidence.

A closed loop, non-interfering environment, such as sandboxing, helps to provide such an exact mapping. Previously, sandboxing has not been used in power systems, neither in digital forensics context, nor in security context. Thus, it perfectly makes sense to use such an important technique for evidence collection and analysis. All this clearly helps in ensuring the integrity of the acquired evidence, in turn, making a formidable case based on sound forensic artifacts.

2. Related Work

The use of digital forensic investigations in the domain of electric power systems is quite limited. The current research focus for digital forensics usually tends towards supervisory control and data acquisition (SCADA). For example, Ahmed et al. [6] discussed some measures for forensic readiness in the SCADA environment. Similarly, Wu et al. [7] discussed a SCADA digital forensic process consisting of seven steps and Eden et al. [8] discussed a SCADA forensic incident response model. A few other perspectives include works like Ahmed et al. [9] discussing programmable logic controller (PLC) forensics. Many works [10–14] explain the different types of cyber-attacks, testbeds and potential vulnerability in a digital substation in smart grids, however, they seldom discuss anything related to digital forensic investigations. For example, Stellios et al. [15] have discussed advanced persistent threats and zero-day exploits in the Industrial Internet of Things specifically detailing attacks on smart grid SCADA networks and field devices. These include the 2007 Aurora attack scenario that targeted electric power generators demonstrated by Idaho US National Labs [16], the 2015 attack on the Ukraine's smart grid distribution network [17], and the 2016 attack on the Ukraine's Kiev transmission station [18].

Among the first forensic investigations on intelligent electronic devices (IEDs) and phasor measurement units (PMUs) is the work done by Iqbal et al. [19]. They studied digital forensic readiness in industrial control systems (ICS), especially revolving around substation automation and devices called IEDs and PMUs as their case studies in smart grids. Through these case studies, they performed different attacks and tried collecting evidence. It was concluded that current ICS devices, i.e. IEDs and PMUs, in substations were not forensic ready. Similarly, Iqbal et al. [20] in their work investigated different logs of industrial control systems (ICS) on a variety of devices using a variety of operational setups. They concluded that in industrial control systems logs are relatively less mature, hence leading to the inability of logs to ascertain incrimination and attribution of an attack. They suggested the

logs be modified in contents to contain more information in aid of forensic investigations when deemed necessary.

Forensics investigations require a test setup to be properly configured in order to acquire useful forensic artifacts in case of a cyber-attack. In a power system domain, many testbeds are proposed in the literature for simulation attacks [10–14], however, most of them are not suitable for collecting useful artifacts to be used later in forensic analysis. Among the first testbeds proposed in [21] was suitable for conducting a forensic investigation and potentially collecting artifacts.

One of the challenges associated with the digital forensic investigation is identification, examination, and extraction of digital artifacts with the probative value [22]. The complexity of the digital environment makes this a tedious task if not done properly. Moreover, the process of finding artifacts should be automated. The challenge is usually overcome by using various suitable tools and techniques for this purpose. Sandboxing is one of the suitable techniques used in digital forensics for this purpose.

A sandbox environment is an isolated environment although originally used by programmers to test new code, has now become one of the useful techniques for security and forensic investigations [22]. Although sandboxing has been in use for many years in other domains, but to authors' best knowledge, it has rarely been used in power system testbeds. In [23], the authors have proposed the concept of sandboxing for this first time in this domain, however, the focus of the paper was not exploring the details. The paper identifies attack-based digital forensic evidences (DFEs) for WAMPAC systems). A correlation is performed based on acquired DFEs resulting from system application logs. In [24], intelligent analysis of digital evidence is performed in large scale logs in power system attributed to the attacks.

Paper Contributions

In [21], a forensic testbed was proposed for simulating cyber-attacks on WAMPAC applications. Although the first of its nature for forensic investigations in the power systems, the challenges encountered in the investigation process led to improvisation of our implementation using the sandboxing approach. Additional experiments were performed on top of the existing work which had previously performed by the authors.

In this paper, the concept of sandboxing on the hardware-in-the loop forensic testbed originally proposed in [21] has been introduced. An authentication attack between the communication of PMU and PDC was considered. The PDC system is particularly sandboxed, which provides a controlled environment, thus, facilitates in extracting the artifacts with forensic value. Hence, such artifacts help in the investigation process to trace back to the root cause of the cyber-attacks.

The remainder of the paper is organized as follows:

In Section 3, a substation architecture is presented identifying the vulnerabilities and potential artifacts, which gives a broader overview of forensic investigation in the field of the power system and smart grids. Section 4 provides the theoretical details of the sandboxing approach. Section 5 describes the details of the power system model used to emulate the behavior of the power system used for the testbeds. Section 6 contains the mapping of different attacks in WAMPAC applications. In Section 7, the two approaches of real-time hardware-in-the-loop forensic testbed are presented Finally, Section 8 presents the key conclusions of the paper.

3. Background on Substation Architecture

A substation consists of various entities including hardware and software components. These components may be subjected to various types of attacks. Figure 1 shows a broad overview of the architecture of a substation. The figure identifies most of the probable vulnerabilities of the cyber-attacks. In addition, key potential places are detected where useful forensics artifacts could be acquired. The study focuses on some of the major substation devices, in the context of IEC 61850 substation automation architecture, i.e. PMUs, IEDs and remote terminal units (RTUs), etc.

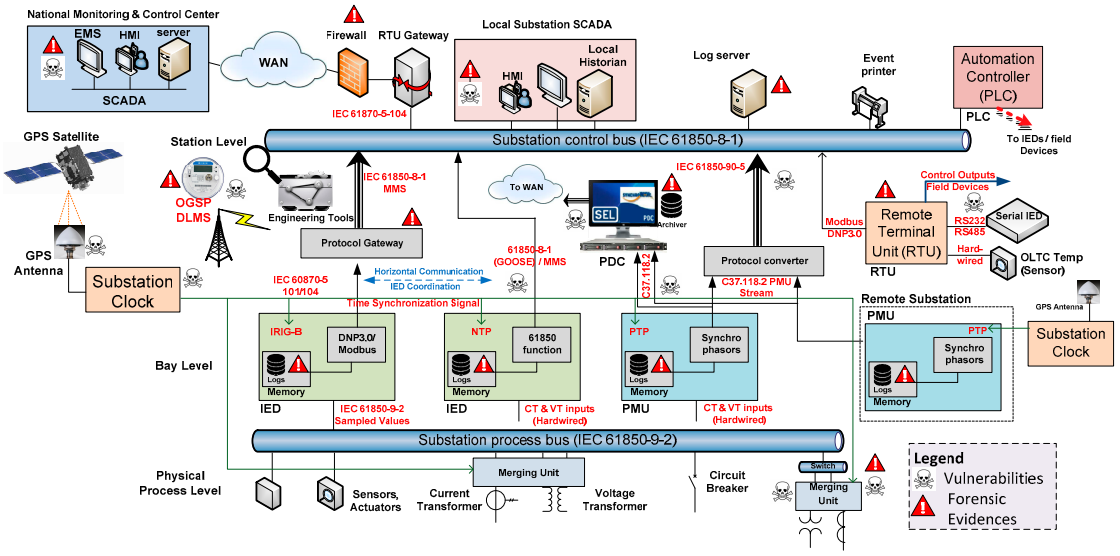

Figure 1. Substation architecture identifying vulnerabilities and forensic evidence.

As shown in Figure 1, data from physical processes are fed to the substation devices (i.e., IEDs and PMUs) at the bay level through the process bus. Based on this data, the IEDs perform various protection/control functions and stream out the status of substation digitally by using different power systems communication protocols, such as IEC 61850-8-1 (GOOSE/MMS) and IEC 60870-5 (101/104).

Protocol converters (protocol gateways) are deployed to map information between various communication protocols. This digital data set enables a station bus to facilitate various monitoring, logging and coordination functions within a substation.

An IED can either directly communicate with a station bus using 61850-8-1 GOOSE/MMS or requires a protocol gateway to publish data from the IED to the substation control bus (in case IED uses DNP3/Modbus or any other protocol which is not 61850 compliant). The data from IEDs and RTUs are sent to the national control center via the RTU gateway using IEC 61870-5-104, where SCADA/EMS system performs various monitoring and control functions.

The synchrophasors data complaint with C37.118.2 protocol streams out by the PMUs. [25]. The phasor data concentrator (PDC) receives data from various PMUs and streams out the time-aligned data via the wide area network (WAN) to a national control center, where the data is used by various monitoring, control, and protection applications. Moreover, a protocol converter parses PMU data (C37.118.2) protocol, maps it to the data model of IEC 61850 and sends the data through either the routed-sampled value or the routed-GOOSE services as per IEC 61850-90-5 protocol [26].

The major components of the substation architecture (shown in Figure 1) are explained briefly as follows:

(1) IED: An IED is a device having various monitoring, protection and control functionalities. It can be used for upper-level communication individualistically. The input to this device could be the data from the sensor and actuators from the field equipment. IED can issue various control orders, such as tripping circuit breakers to protect the network section and expensive equipment.

(2) PMU: A PMU is a device which estimates the synchrophasors, frequency, and rate of change of frequency (ROCOF) of the input voltage and /or current waveform, based on a common universal time (UTC) time reference. A PMU is usually installed into a power substation and connected to the electric grid via instrument transformers. PMUs have great benefits for situational awareness in WAMPAC and forensic event analysis [27]. For example, a PMU can report the data at a rate as high as up to 120 samples/ seconds. In addition, they have the capability to measure phase angle variations at multiple places which allow grid operators to detect and characterize the grid much faster than the traditional devices. A PMU measurement is time-stamped, and thus coordinated against universal time (UTC) using a time source, such as the GPS. The time synchronization feature of PMU measurements helps to improve the overall coordination of the grid operation.

(3) RTU: It is an integral part of typical SCADA systems used as a communication pivot. The data from sensors and actuators in substations and remote locations are collected by RTUs. It sends the collected data to a master station (national monitoring and control center) via a communication system. RTUs provide historical and sequence of event data for fault investigations and provide historical trend data for power network planning and maintenance.

(4) PDC: It receives time-synchronized phasor data from multiple PMUs to produce a real-time, time-aligned output data stream. A PDC can exchange phasor data with PDCs at other locations. A PDC is usually compliant with the IEEE C37.118 standard, which provides the required capability for the most advanced wide area monitoring applications. Moreover, a PDC also provides a gateway for the interface of PMU applications to the SCADA/EMS system to improve the supervision of the power system.

(5) Merging unit (MU): It is an IED that is used to exchange information between field devices (at process level) and secondary devices at the bay level. The MU collects the inputs from current and voltage transformers synchronously and provides output in the form of digital signals compliant with IEC 61850 protocol.

(6) Local Substation SCADA:

   a. Human machine interface (HMI): HMI is used by system operators and control center engineers to interpret and visualize SCADA system data through a graphical user interface. HMI can also be used for transferring algorithms, configuring set points and adjusting parameters of controllers.
   b. Historian and log servers: It is basically a database management system that acquires and saves data sent to the control center. It is also used to produce audit logs for all events and activities across a SCADA network. Therefore, it is a vital source of evidence for any incident forensic investigations.

(7) Energy management system (EMS) and SCADA: This is an energy management system that optimizes, supervises and controls the transmission grid and generation assets. It hosts all monitoring, control, protection, and planning applications, etc. The SCADA system can have built-in capabilities of EMS or it can be a separate system.

(8) Engineering tools: A set of software tools are the essential part of a modern substation automation architecture. The tools can be used to configure the bay level and process level devices. Moreover, the tools help in the overall system configuration. In addition, some appropriate tools could be used for a real-time cybersecurity monitoring of the substation.

(9) Time synchronization: This is required to ensure that all devices in a substation have accurate clocks for system control and data acquisition, etc. Time synchronization enables electric power utilities to have better coordination of the operation and helps to maintain power supply integrity.

(10) Protocol converters: Protocol converters parses data from one protocol, map it to another desired protocol and finally transmit the data accordingly. Having various protocols in substation architecture, protocol converters become important for the interoperability between different devices.

(11) Substation process bus (IEC 61850-9-2): It is an interface between primary field devices and secondary devices at the bay level. The process bus is compliant with IEC 61850-9-2 standard. Conventional instrument transformers provide analog values which can be exchanged for fiber-optic sensors. The modern non-conventional instrument transformers can communicate with the process bus via digital signals to be fed to metering, protection and control equipment.

(12) Substation station control bus (IEC 61850-8-1): It is an interface between secondary bay level devices and the control center/SCADA. The station bus is usually compliant with IEC 61850-8-1 standard.

4. Sandboxing

A sandbox environment is an isolated environment which is used to safely run suspicious codes without impacting the host. Although originally used by programmers to test the new code, it has now become one of the most useful techniques for security and forensic investigations especially for malware analysis [22]. Sandbox systems allow monitoring suspicious executable files while eliminating the risk of compromising live systems. Another important aspect is that sandboxes eliminate a lot of human effort derived from complex and lengthy tasks, such as disassembling [28]. There are several commercial and open source sandboxes available like Cuckoo Sandbox, Microsoft App-V, VMware ThinApp, Zerowine, etc. all with their pros and cons [29]. The concept of sandboxing has been well known for quite some time in other domains, but it has never been proposed or used with a hardware-in-the-loop (HIL) power system setup for digital forensics to the best knowledge of the authors. This study is using a modified real-time hardware-in-the-loop (HIL) system where some portions of the systems have been sandboxed [21].

There are several ways sandboxes can be implemented, for example, full system emulation, operating systems emulation, etc. In the first approach, a deep inspection is possible because all aspects of the hardware and software are analyzed, resulting in a fine-grained analysis. This is in contrast to the latter approach in which only software and user behavior are monitored. The second approach using Cuckoo Sandbox was chosen, essentially auditing user access, file storage, registry, connections, processes, etc.

A differential forensic analysis (DFA) was performed comparing two or more different digital forensic images and resulted in reporting the changes and modifications between them. By focusing on the changes and modifications, it allows the examiner to reduce the processing time and amount of information under examination. Also, focusing on changes helped segregate activities which potentially were performed by the malicious user [30].

Figure 2 depicts a DFA with an initial system state (SS_0) at an arbitrary t_0, taken as a base state of the system. After initiating an event (E_1), the base state SS_0 changes its state SS_1. All the changes occurring in the time interval (t_1-t_0) are defined as (Δ_1). In order to capture all such changes in the system states (Δ_n), the experiments were repeated several times in order to get a complete set of artifacts [23]. For the duration of our experiments, approximately 2 million logs over several iterations were collected. Since the volume of data, time and power required for processing were not in the scope of work, hence here no comparisons were presented.

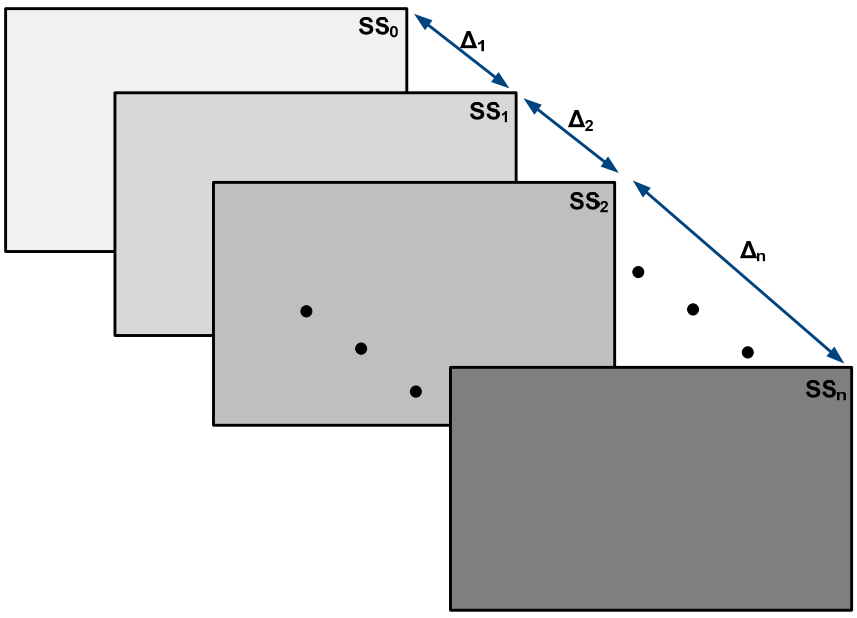

Figure 2. The concept of sandboxing and differential forensics analysis [23].

5. Power System Modeling

To emulate the behavior of the power systems, an IEEE 3-machine 9-bus [31] power system model is used as shown in Figure 3. The power system contains 3 generators available at three end buses (bus 1–3) of the network. The transformers are used to step up/down the voltage of the power network. Moreover, 3 loads (which consume power) are connected at bus 5, 6 and 8. The transmission lines are used to transfer power from generation points to the load centers. Each line, loads and generators are equipped with circuit breakers (CB), which gives the flexibility to only disconnect faults part of the power network. This increases the reliability of the network and gives improved availability of electric power.

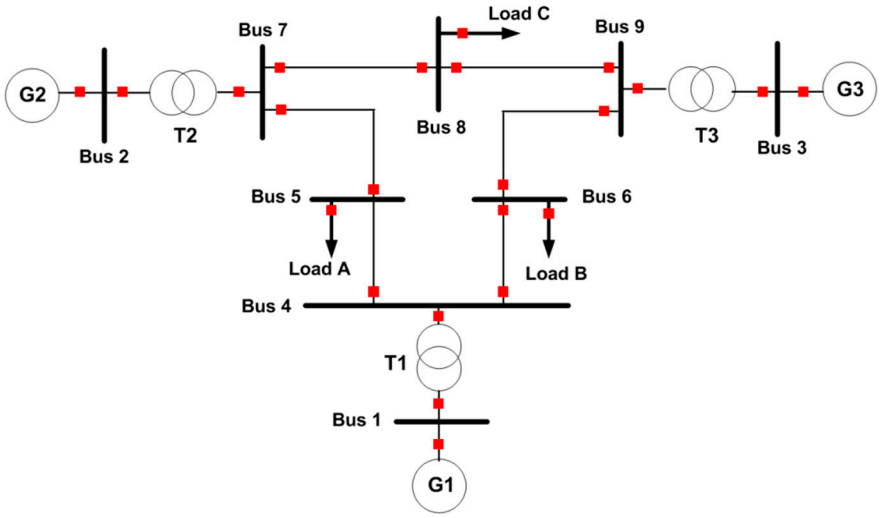

Figure 3. IEEE 3-machine 9 bus power system model.

The model was first designed for offline simulations in MATLAB/SIMULINK. The model was further prepared for real-time simulation using RT-LAB from Opal-RT real-time simulator (RTS). Figure 4a shows different steps of the offline model in Simulink prepared for its execution in the RTS. The Simulink model is first divided into sub-systems. The model is loaded into the RTS using the RT-LAB software interface. Finally, the model is executed in the RTS.

A detailed execution architecture for the real-time simulation of the model is shown in Figure 4b. The Simulink model can be broadly classified into computations part and the graphical user interface (GUI) part. The computation part is mostly executed in a real-time target, whereas the GUI part is executed in the local host computer.

In the real-time simulation, the build process contains the following steps. First, the Simulink model is divided into various subsystems for efficient computation purposes. It is then followed by C code generation, transfer of the generated code and finally building the generated code. After the build process, it is then followed by load process, in which the model is loaded into the real-time target as shown in Figure 4b. Once the model is loaded, it is finally executed. It should be noted that all the computation part is executed in real-time on the target, whereas all the graphics, including plots and display, is executed into the host computer.

In this paper, IEEE 9 bus model shown in Figure 3 is used to design, test and validate the attack simulation experiments. The model is an essential component of the forensic testbeds (shown in Section 7) to be used for simulation and analysis of cyber-attacks on substation devices.

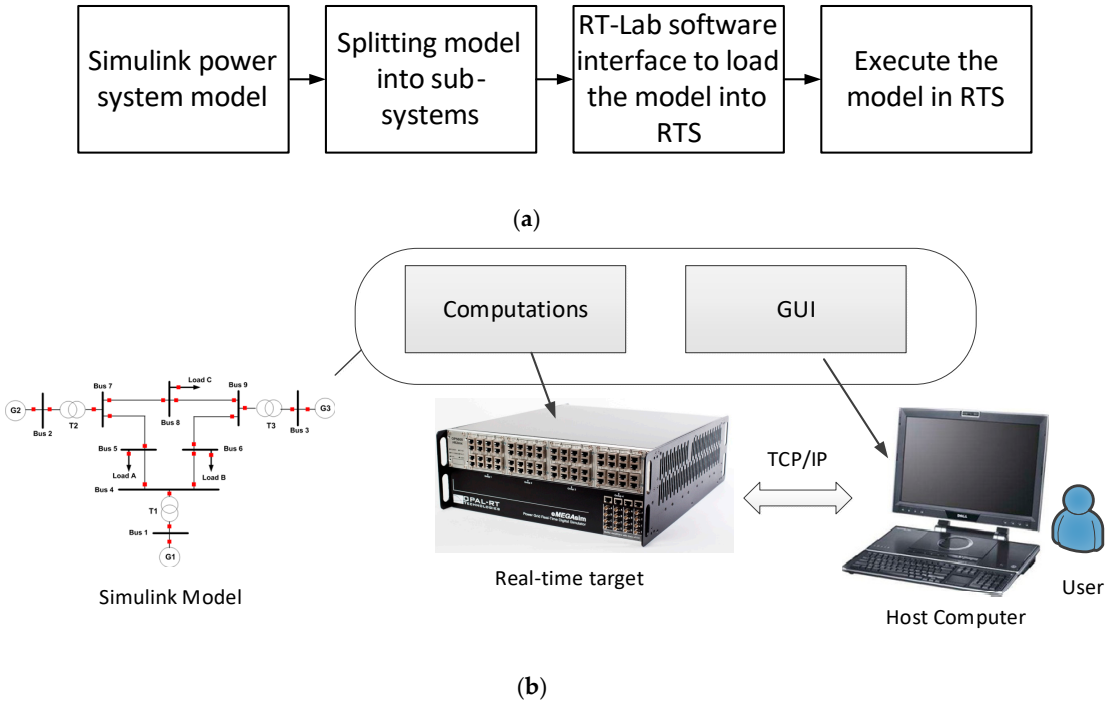

Figure 4. (**a**) Model preparation steps for real-time simulation; (**b**) Detailed execution architecture for real-time simulation.

6. Mapping of Different Attacks in WAMPAC Networks

In Figure 5, a comprehensive mapping was performed for different attacks in WAMPAC network. The focus was to map the attacks corresponding to potential forensic evidence that could be generated in a WAMPAC network. The mapping could help to get a quick understanding of the types of cyber-attacks, usually targeted resources, applications under attack and their potential impact on the power system.

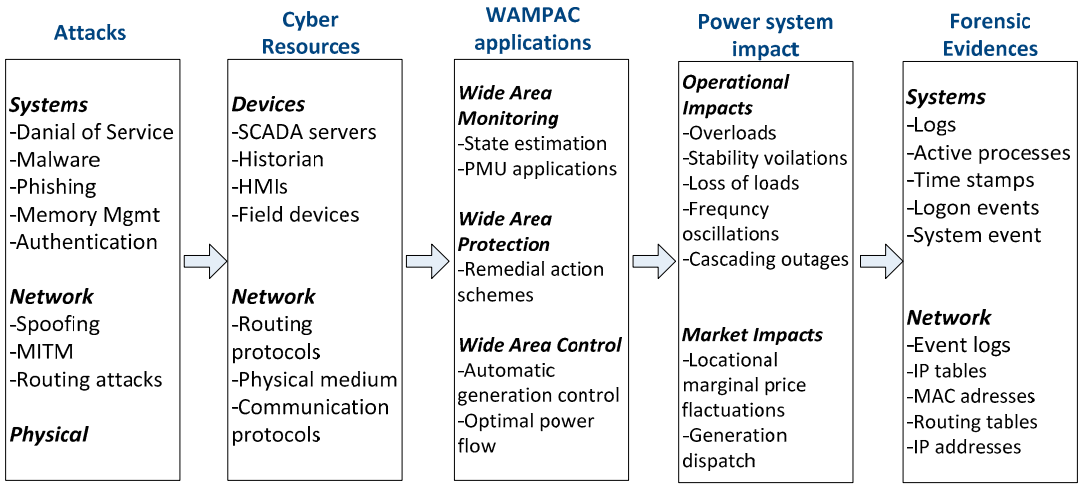

Figure 5. Mapping of different attacks in WAMPAC network with respect to potential forensic evidence [32].

The mapping is first of its kind in the field of WAMPAC applications with a specific focus on digital forensic evidence. The forensic evidence is broadly classified into system evidence and network evidence. This mapping provides a useful starting point for the digital forensics researchers to explore the applications of digital forensics into the field of power systems.

7. Real-time Hardware-in-the-Loop Forensic Experimental Testbed-Approaches

7.1. Without Sandboxing

A real-time HIL testbed was proposed in [21] as shown in Figure 6. The testbed is suitable for performing digital forensic experiments in the domain of the power system. A power system model was simulated as shown in Section 5. PMUs are fed by simulated voltage and current from the RTS. The synchrophasors are estimated by the PMUs in c37.118 data format. The data from multiple PMUs are collected and time-aligned by PDC, transmitting the data stream via WAN to the monitoring and control center. The monitoring, control and protection applications use PMU data and perform various functionalities accordingly. In this case, a time synchronization signal to the PMU is subjected to a cyber-attack.

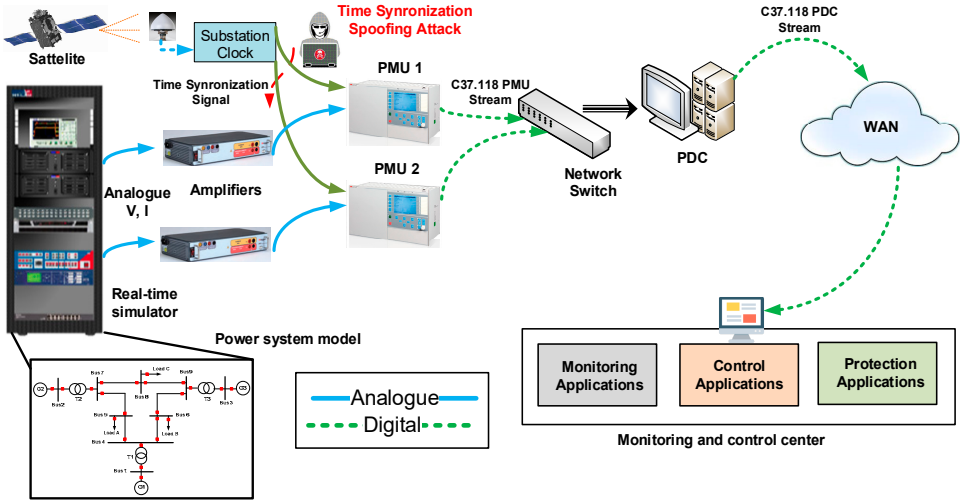

Figure 6. Forensic experimental testbed (Without Sandboxing).

Basically, the authors tried to retrace the steps of the time synchronization attacks, to find out potential forensic artifacts using the proposed testbed shown in Figure 6. However, due to the lack of a suitable mechanism, the evidence collection was manual in nature and was a tedious time-consuming task.

In Figure 7, a detailed sequence of time synchronization attack is shown. As the figure shows that a power system model is created, compiled, loaded and consequently simulated for both normal operation and operation under attack. In normal operation, healthy time synchronization signal is fed to PMUs, and PDC stream is being published to the target application to perform the relevant functions. However, in case of an attack, the attacker injects a spoofed time signal to a PMU and PDC publishes an infected stream to the target application which could negatively impact the performance of the target application.

The time synchronization input to a PMU is considered to be one of the most susceptible signals for a cyber-attack. An attack on time synchronization input signal infects PMU data, which could badly impact the end-user applications. For instance, a PMU based monitoring application shown in Figure 8, i.e., steady state model synthesis (SSMS) [33], produces reduced equivalent network models using PMU data. The attack on time-stamp could corrupt the calculations of the parameters of the equivalent network model. The system operator utilizing the output of the SSMS application could potentially take wrong decisions based on the corrupted results. This could result in unwanted interruptions in the power network and eventually could result in a blackout of the power network.

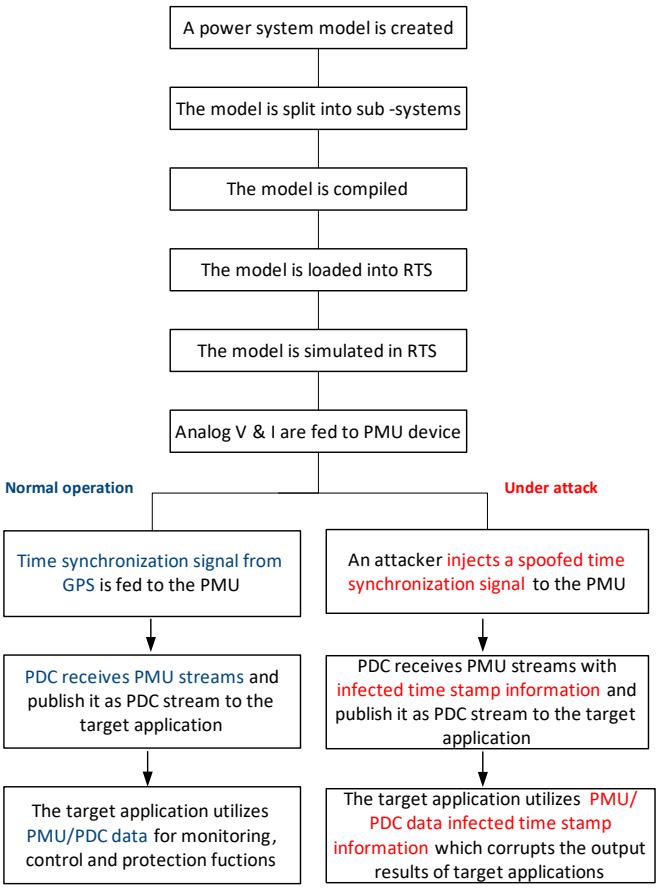

Figure 7. The sequence of operation of time synchronization attack.

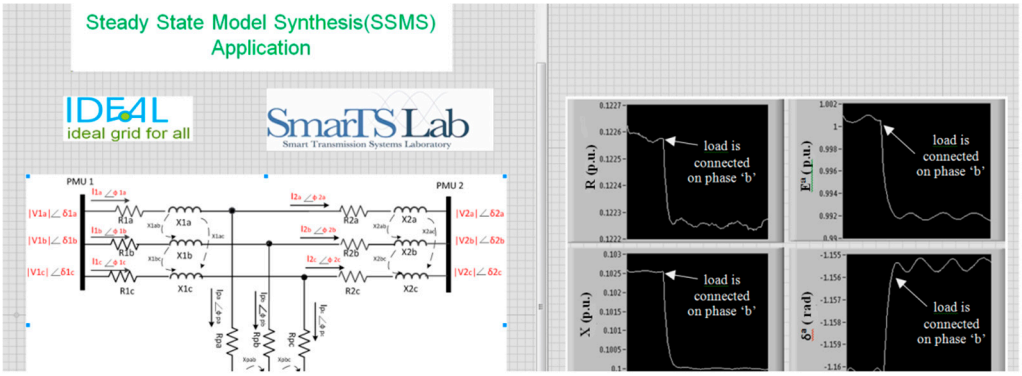

Figure 8. SSMS power system monitoring application.

7.2. With Sandboxing

7.2.1. Design of Sandboxed Forensic Experimental Testbed (Authentication Attack)

In this paper, a forensic experimental testbed is proposed using sandboxing approach as shown in Figure 9. The base design of this testbed is similar to the testbed as described in Section 7.1. The most predominant difference is that the PDC system is sandboxed.

In this testbed, the PDC is subjected to an authentication attack. It is assumed that the attacker has gained unauthorized access to the PDC network and to the PDC's credentials. After gaining access to the credentials of the PDC system, the attacker performs various unwanted malicious activities on the PDC system.

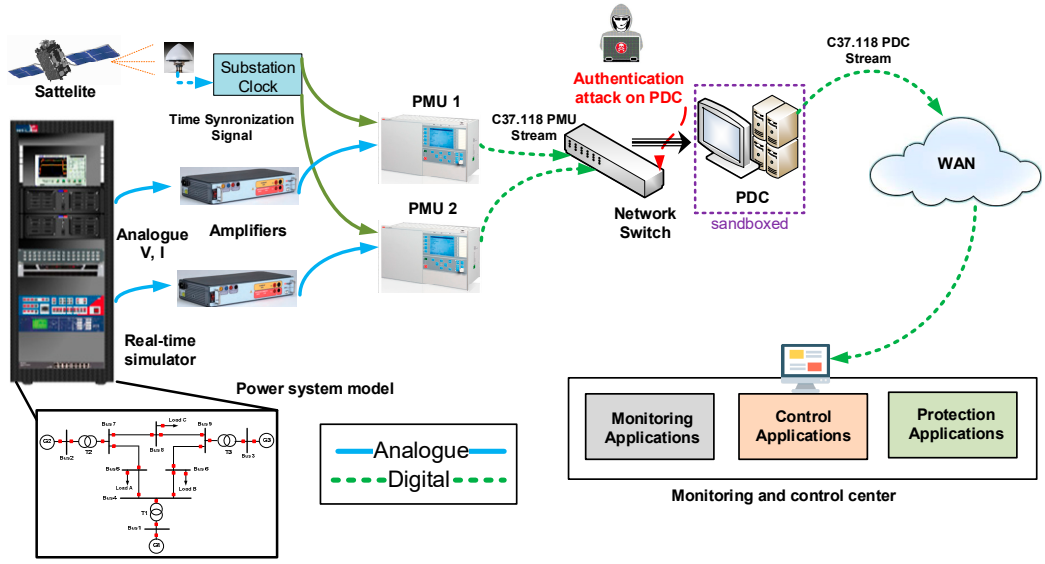

Figure 9. Forensic experimental testbed (With Sandboxing), authentication attack [23].

7.2.2. Authentication Attack Steps

Figure 10 shows the timeline of the list of activities performed by the attacker on the PDC system. The time of occurrence of various activities are plotted on the x-axis and the list of activities are taken on the y-axis. As shown in the figure, the monitoring of PDC started at 16:45. Soon after, 2 minutes, PDC services and PDC graphical assistance software started. The attacker performed a couple of failed attempts to login into the PDC system at 16:50 and 16:52 consecutively. The attacker was able to successfully login into the PDC system at 16:54. At 16:56, the PDC stream was disabled by the attacker, causing a denial of service to the PDC stream. The attacker enabled the PDC stream back in operation after 2 minutes of the attack. The attacker logged out of the PDC assistance software and closed the PDC services at 17:00 and 17:01 consecutively.

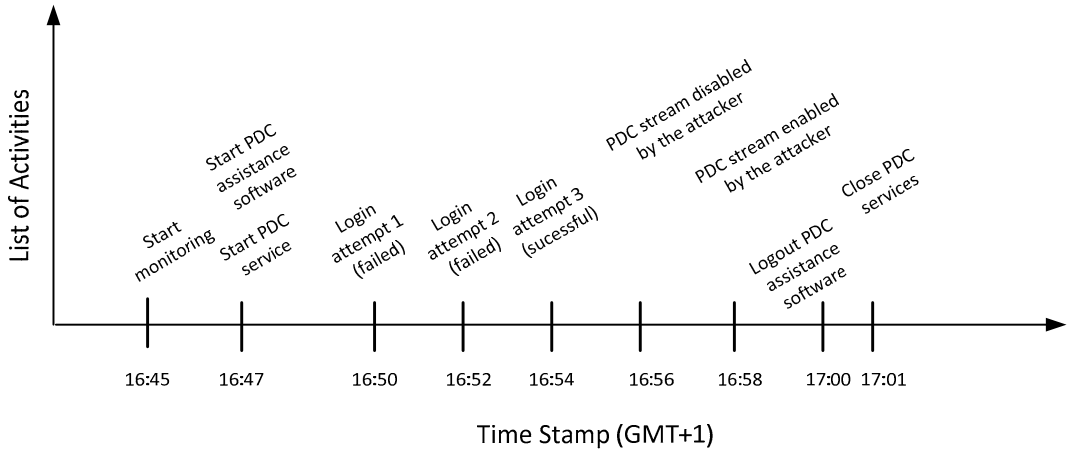

Figure 10. Timeline analysis of the activities performed.

7.2.3. Sandboxing on PDC System

The architecture of the PDC system is shown in Figure 11. As shown in the figure, C37.118 2005 clients communicate with the PDC C37.118 2005 server. The PDC first collects the data from different PMUs, processes the data by time aligning and it finally broadcasts it in the form of the data stream. The database in the PDC system logs all the events. The configurations and settings of PMU/ PDC streams by the users are performed using graphical user interface assistance software on a local computer. Whereas, once the configurations are saved, the updated data is transferred to the PDC server.

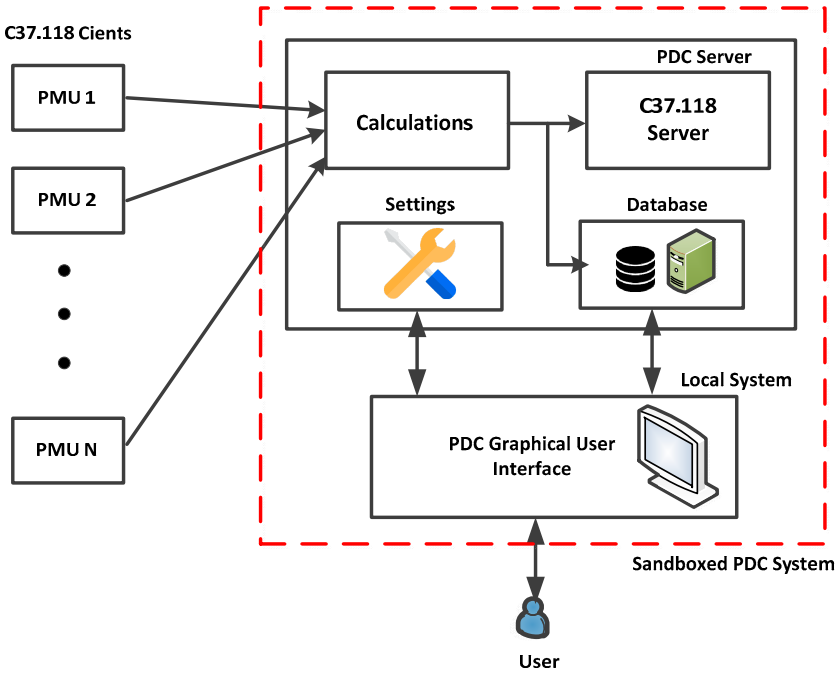

Figure 11. The architecture of a PDC system with sandboxing.

As shown in Figure 11, the PDC system, i.e., server and GUI, are sandboxed. All the attack steps performed by the attackers on the PDC system generated some potential digital artifacts on the PDC system. For example, the evidence generated as a result of most of the malicious activities shown in the timeline in Figure 10 can be associated with their respective steps. The extraction of these useful artifacts could only be made possible due to a controlled sandboxed, which keeps track of each minor change on the PDC system. These recorded changes provide vital input for a successful forensic investigation.

8. Conclusions

The paper proposes the design of a real-time hardware-in-the-loop forensic experimental testbed to conduct investigations on power systems as a whole. This is quite a unique work in its own since nothing comparable existed before [21]. The proposed test setup is used for forensic analysis of substation devices particularly focusing on WAMPAC applications. As a result of cyber attacks, constituent devices leave the traces behind known as forensic artifacts as per Locard's principle. These forensic artifacts were identified, preserved, collected and studied to know how exactly such attacks impacted the system and what traces they left behind.

Secondly, based on the challenges and difficulties faced in conducting such investigations, certain improvements were made specifically adding and implementing the sandboxing technique. Sandboxing has been used frequently by programmers in the past, and now-a-days is considered very important while performing security analysis. It has proven to be very useful as an aid in forensic analysis but is rarely used in the context of industrial control systems.

This study successfully implemented the sandboxing technique in RT-HIL for conducting forensic analysis. Problems such as volume of data involved and tracking different kinds of changes in the file systems which not only took more time, but also was tedious in nature and time-consuming task. Sandboxing helped in reducing these difficulties considerably. While previously, the authors were only able to perform and analyze time synchronization and GPS spoofing attack in this work, we expanded our horizons by adding authentication attack. These attacks resulted in successful identification and collection of more forensic artifacts.

In future work, the authors potentially see the opportunity to perform different attacks. This can include different types of attacks on the same device to find out which attacks leave more artifacts and which attacks leave less artifacts. This may also be useful for mapping all the relevant artifacts to different attack types. Another possible direction is to increase the scope of sandboxing which may be helpful in conducting a wider collection and analysis of artifacts.

Author Contributions: The corresponding author, A.I. and co-author, F.M. have both performed the experiments and wrote the paper whereas co-author, M.E. has helped through reviewing and feedback.

Funding: This work has received funding from the Swedish Civil Contingencies Agency (MSB) through the research center Resilient Information and Control Systems (RICS).

Acknowledgments: Authors would like to thank Lars Nordström Head of EPE Department, Deputy Head School of EECS, KTH and Gunnar Björkman of ABB for their support.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

WAMPAC	Wide Area Monitoring Protection and Control
IED	Intelligent Electronic Device
PMU	Phasor Measurement Device
RTU	Remote Terminal Units
PDC	Phasor Data Concentrator
RTS	Real-time Simulator

References

1. Khan, R.; Maynard, P.; McLaughlin, K.; Laverty, D.M.; Sezer, S. Threat Analysis of Black Energy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In Proceedings of the ICS-CSR, Belfast, UK, 23–25 August 2016.
2. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv.* **2011**, *9*, 49–51. [CrossRef]
3. NCCIC; ICS-CERT. *NCCIC/ICS-CERT 2015 Year in Review*; NCCIC; ICS-CERT: US Department of Homeland Security: Washington, DC, USA, 2016.
4. The US Department of Energy. *Cyber Threat and Vulnerability Analysis of the US Electric Sector*; US Department of Energy: Washington, DC, USA, 2016.
5. Terzija, V.; Valverde, G.; Cai, D.; Regulski, P.; Madani, V.; Fitch, J.; Skok, S. Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. *Proc. IEEE* **2011**, *99*, 80–93. [CrossRef]
6. Ahmed, I.; Obermeier, S.; Naedele, M.G.G.R. SCADA Systems: Challenges for Forensic Investigators. *Computer* **2012**, *45*, 44–51. [CrossRef]
7. Wu, T.; Pagna Disso, J.F.; Jones, K.; Campos, A. Towards a SCADA forensics architecture. In Proceedings of the 1st International Symposium for ICS SCADA Cyber Security Research, Leicester, UK, 16–17 September 2013.
8. Eden, P.; Blyth, A.; Burnap, P.; Cherdantseva, Y.; Jones, K.; Soulsby, H.; Stoddart, K. A cyber forensic taxonomy for SCADA systems in critical infrastructure. In Proceedings of the International Conference on Critical Information Infrastructures Security, Berlin, Germany, 5–7 October 2015.
9. Ahmed, I.; Obermeier, S.; Sudhakaran, S.; Rousse, V. Programmable Logic Controller Forensics. *IEEE Secur. Priv.* **2017**, *15*, 1518–1524. [CrossRef]
10. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
11. Xu, Y.; Yang, Y.; Li, T.; Ju, J.; Wang, Q. Review on cyber vulnerabilities of communication protocols in industrial control systems. In Proceedings of the 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017.
12. Leger, A.S.; Spruce, J.; Banwell, T.; Collins, M. Smart grid testbed for Wide-Area Monitoring and Control systems. In Proceedings of the 2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), Dallas, TX, USA, 21–23 September 2016.

13. Zhong, X.; Jayawardene, I.; Venayagamoorthy, G.K.; Brooks, R. Denial of Service Attack on Tie-Line Bias Control in a Power System with PV Plant. *IEEE Trans. Emerg Top. Comput. Intell.* **2017**, *1*, 375–390. [CrossRef]
14. Calvo, I.; Etxeberria-Agiriano, I.; Iñigo, M.A.; González-Nalda, P. Key vulnerabilities of industrial automation and control systems and actions to prevent cyber-attacks. *Int. J. Online Eng. (IJOE)* **2016**, *12*, 9–16. [CrossRef]
15. Stellios, I.; Kotzanikolaou, P.; Psarakis, M. Advanced Persistent Threats and Zero-Day Exploits in Industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things. Advanced Sciences and Technologies for Security Applications*; Alcaraz, C., Ed.; Springer: Cham, Switzerland, 2019.
16. Srivastava, A.; Morris, T.; Ernster, T.; Vellaithurai, C.; Pan, S.; Adhikari, U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. *IEEE Trans. Smart Grid* **2013**, *4*, 235–244. [CrossRef]
17. Case, D.U. *Analysis of the Cyber-Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): Washington, DC, USA, 2016.
18. Goodin, D. Hackers Trigger Yet Another Power Outage in Ukraine. Available online: https://arstechnica.com/security/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/ (accessed on 18 May 2019).
19. Iqbal, A.; Ekstedt, M.; Alobaidli, H. Digital Forensic Readiness in Critical Infrastructures: A case of substation automation in the power sector. In Proceedings of the International Conference on Digital Forensics and Cyber Crime, Prague, Czech, 9–11 October 2017.
20. Iqbal, A.; Ekstedt, M.; Alobaidli, H. Exploratory studies into forensic logs for criminal investigation using case studies in industrial control systems in the power sector. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017.
21. Iqbal, A.; Mahmood, F.; Ekstedt, M. An Experimental Forensic Testbed: Attack-based Digital Forensic Analysis of WAMPAC Applications. In Proceedings of the Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MedPower 2018), Dubrovnik, Croatia, 12–15 November 2018.
22. Iqbal, A.; Al Obaidli, H.; Guimaraes, M.; Popov, O. Sandboxing: Aid in digital forensic research. In Proceedings of the 2015 Information Security Curriculum Development Conference (InfoSec '15), New York, NY, USA, 10 October 2015.
23. Iqbal, A.; Mahmood, F.; Shalaginov, A.; Ekstedt, M. Identification of Attack-based Digital Forensic Evidences for WAMPAC Systems. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA; 2018; pp. 3079–3087.
24. Iqbal, A.; Shalaginov, A.; Mahmood, F. Intelligent analysis of digital evidences in large-scale logs in power systems attributed to the attacks. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018.
25. IEEE. *IEEE Standard for Synchrophasor Data Transfer for Power Systems*; IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005); IEEE: Piscataway, NJ, USA, 2011; pp. 1–53.
26. Firouzi, S.R.; Vanfretti, L.; Ruiz-Alvarez, A.; Mahmood, F.; Hooshyar, H.; Cairo, I. An IEC 61850-90-5 gateway for IEEE C37.118.2 synchrophasor data transfer. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 21–27 July 2016.
27. Mahmood, F. Synchrophasor Based Steady State Model Synthesis of Active Distribution Networks. KTH, 2018. Available online: http://kth.diva-portal.org/smash/get/diva2:1223943/FULLTEXT01.pdf (accessed on 18 May 2019).
28. Vasilescu, M.; Gheorghe, L.; Tapus, N. Practical malware analysis based on sandboxing. In Proceedings of the 2014 RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference, Chisinau, Moldova, 11–13 September 2014.
29. Kale, G.; Bostanci, E.; Çelebi, F. Differences between Free Open Source and Commercial Sandboxes. In Proceedings of the International Conference on Cyber Security and Computer Science, Safranbolu, Turkey, 18–20 October 2018.
30. Garfinkel, S.; Nelson, A.J.; Young, J. A general strategy for differential forensic analysis. *Digit. Investig.* **2012**, *9*, S50–S59. [CrossRef]
31. Aggarwal, G.; Mittal, A.; Mathew, L. MATLAB/Simulink Model of Multi-machine (3-Machine, 9-Bus) WSCC System Incorporated with Hybrid Power Flow Controller. In Proceedings of the 2015 Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22 February 2015.

32. Ashok, A.; Govindarasu, M.; Wang, J. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proc. IEEE* **2017**, *105*, 1389–1407. [CrossRef]
33. Mahmood, F.; Hooshyar, H.; Lavenius, J.; Bidadfar, A.; Lund, P.; Vanfretti, L. Real-Time Reduced Steady-State Model Synthesis of Active Distribution Networks Using PMU Measurements. *IEEE Trans. Power Deliv.* **2017**, *32*, 546–555. [CrossRef]