Anomaly Detection and Mitigation in Cyber-Physical Power Systems Based on Hybrid Deep Learning and Attack Graphs

Presekal, Alfan; Ștefanov, Alexandru; Rajkumar, Vetrivel Subramaniam; Palensky, Peter

DOI
10.1002/9781394191529.ch19

Publication date
2025

Document Version
Accepted author manuscript

Published in
Smart Cyber-Physical Power Systems

Citation (APA)
Presekal, A., Ștefanov, A., Rajkumar, V. S., & Palensky, P. (2025). Anomaly Detection and Mitigation in Cyber-Physical Power Systems Based on Hybrid Deep Learning and Attack Graphs. In *Smart Cyber-Physical Power Systems: Fundamental Concepts, Challenges, and Solutions* (Vol. 1, pp. 505-537). Wiley. https://doi.org/10.1002/9781394191529.ch19

Anomaly Detection and Mitigation in Cyber-Physical Power Systems based on Hybrid Deep Learning and Attack Graphs

Alfan Presekal, Alexandru Ştefanov, Vetrivel Subramaniam Rajkumar, Peter Palensky

Intelligent Electrical Power Grids, Department of Electrical Sustainable Energy, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, The Netherlands

1. Power Grid Cyber Resilience

Digitalization is paving the way toward enhanced power grid operational capabilities and intelligence. The adoption of digital technologies is essential for the advancement of the forthcoming power grid. The integration of the Internet of Things (IoT), Artificial Intelligence (AI), and big data analytics are encompassed within this scope. They enhance power system sustainability, affordability, and resilience. The increased digitalization, however, also implies a greater risk from cyber vulnerabilities and threats. Various power systems facets such as transmission and distribution systems, digital substations, control centers, and wide-area communication networks are vulnerable to cyber attacks. It is widely acknowledged that the integration of Information Technology (IT) and Operational Technology (OT) systems introduces new threats and cyber security challenges. When it comes to ensuring the reliability of the future energy system and security of electricity supply, there is a pressing need to give close attention to the new vulnerabilities and dangers posed by grid digitalization. Therefore, cyber resilience is essential for further digitalization of the power grid.

Cyber attacks on power systems are infrequent yet high-impact disruptions that can result in an extensive range of undesirable outcomes, e.g., load shedding, equipment damage, system instability, and power outages. The ramifications of a cyber attack on electrical power grids transcend the immediate disruptions, including cascading effects on interconnected power systems and other critical infrastructures, e.g., water supply, gas distribution, telecommunication, and transportation systems. The most notable cyber attacks on power grids are the twin attacks on the Ukrainian power grid in 2015 and 2016. These incidents clearly highlighted that cyber attacks on power grids are imminent threats that need to be addressed. Cyber attacks were conducted on the power grid in Ukraine on December 23, 2015, leading to power outages that affected approximately 225,000 customers [1]. On December 17, 2016, more advanced cyber attacks were carried out against the Ukrainian power grid. This attack led to a power outage in the distribution network, where 200 MW of load was unsupplied [2]. The capabilities of the adversaries behind these types of advanced cyber attacks pose an existential threat to the security of modern society. The emergence of cyber attacks on power systems has the potential to trigger cascading failures that can culminate in a catastrophic blackout, ultimately leading to a doomsday scenario. Furthermore, the absence of electricity has a significant impact on all social aspects, which can result in financial losses, damages, chaos, or even a loss of lives.

Extensive research on cyber attacks on power grids was conducted in recent years. We identified three main research directions to address these challenges. The first research direction enhances the security of communication protocols utilized in power grid OT systems, which is essential [3]. The second research direction is toward cyber-physical system modeling and co-simulation using testbeds [4]-[7]. A simulated environment is necessary for power grid cyber security due to its nature as critical infrastructure with high availability requirements. Therefore, the implementation of a testbed enables researchers to safely conduct a variety of power system tests and cyber attack simulations. Finally, the third research direction is anomaly detection in power grids due to cyber attacks. It is noteworthy that the predominant focus of anomaly detection in the state-of-the-art pertains to the detection of online attacks on power grids in the context of False Data Injection (FDI) attack scenarios. This line of research concentrates on analyzing power system measurements to find anomalies in power grids [8]-[13]. Nevertheless, the cases of cyber attacks on power grids that have been reported in [1], [2], [14] were not associated with the execution of FDI attacks. In the early stages of the cyber kill chain, attackers target IT-OT systems rather than manipulating measurement data. Hence, there is a need for anomaly detection in OT communication traffic.

This chapter provides essential knowledge of cyber attack mitigation for cyber-physical power systems, i.e., (i) secure communication protocols for operational technologies, (ii) cyber-physical co-simulation and penetration testing using cyber ranges, and (iii) network security controls and intrusion detection and prevention systems. Amongst the wide-scope mitigation, AI is highlighted as an emerging solution. This chapter presents how hybrid deep learning based on Graph Convolutional Long Short-Term Memory is used for anomaly detection in power system OT networks. Unlike traditional signature and supervised learning-based intrusion detection, hybrid deep

learning anomaly detection utilizes the OT traffic throughput. It takes advantage of the OT traffic's deterministic and homogenous characteristics to provide robust and flexible anomaly detection for a wide scope of cyber attacks. The traffic anomalies are incorporated into an attack graph that aids power system operators to identify and localize anomalies of active attacks on power systems in near real-time. Cyber attack case studies and cyber-physical co-simulation results are provided to demonstrate the efficiency of hybrid deep learning for anomaly detection.

The chapter is structured as follows. Section I introduced the overview of power grid cyber resilience. Section II describes operational technologies vulnerabilities and secure communication protocols. In section III we present cyber-physical co-simulation and penetration testing using cyber ranges. Section IV provides state-of-the-art security controls and section V presents hybrid deep learning for anomaly detection in power system OT networks. Case studies are presented in section VI. The conclusions are discussed in section VII.

2. Operational Technologies and Secure Communication Protocols

2.1. Cyber Security of Operational Technology

The term OT pertains to computerized systems that oversee industrial operations, including but not limited to Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Distributed Control Systems (DCS) [15]. SCADA is an OT system architecture designed specifically for managing large and complex processes. It collects data from the field and transmits it to the control center. It includes a control center, local control systems, and local and wide-area communication systems. Meanwhile, the DCS is a comprehensive process control system that comprises a range of components, such as controllers, sensors, actuators, and terminals. DCS systems are typically utilized for on-site control, whereas SCADA systems are commonly employed for remote control purposes. SCADA and DCS are both included under the umbrella term known as ICS.

Typically, OTs have high uptime and availability requirements for mission-critical operations. IT systems, on the other hand, prioritize Confidentiality, Integrity, and Availability (CIA). For OT systems, however, availability and safety have the highest priority [3]. Therefore, cyber security controls ensuring confidentiality and integrity may interfere with the high OT availability requirements. As a result, this conflict leads to a tradeoff between availability and implementation of security controls in OT systems.

In [16], the author demonstrated that OT systems encounter challenges in incorporating cryptography due to the significant computational time required for cryptographic processes. For example, in the IEC 16850 standard for OT systems, fault isolation and protection of Type 1A/P1 requires a maximum delay of 3 milliseconds. Despite the strength of cryptographic algorithms such as 2048-bit RSA and 1024-bit DSA, the processing time of cryptographic operations respectively entailed a total of 61.04 milliseconds and 14.90 milliseconds. Due to time constraints, this circumstance resulted in the adoption of less secure cryptographic methods that require less computational time, or in most applications, the complete absence of cryptographic measures. Consequently, this situation led to cyber security implementation challenges in OT systems compared to IT systems.

According to [17], it has been proposed that the optimal approach for ensuring cyber security best practices is to maintain an air gap between the OT and IT systems. However, in recent years, there has been a growing trend toward the IT – OT convergence [16]. Several contemporary IT-based solutions, such as virtualization technology, Software Defined Networking (SDN), cloud services, and edge computing are gradually being incorporated into OT systems. These technologies are double edge swords that offer benefits and introduce potential vulnerabilities at the same time. Therefore, it is crucial to address the potential threats and vulnerabilities that arise in the convergence of IT and OT.

2.2. Secure Communication Protocols

In order to successfully mitigate the threat of cyber attacks on power grids, it is important to first understand the relationship between computer networking and cyber security. Figure 1 presents the mapping between communication network layers and associated cyber threats and countermeasures, based on the well-known Open Systems Interconnection (OSI) seven-layer and Transmission Control Protocol/Internet Protocol (TCP/IP) four-layer models. The seven-layer OSI abstraction explains the flow of data in computer networks as bits in the physical layer, frames in the data link layer, packets in the network layer, Transport Protocol Data Units (TPDUs) in the transport layer, Session Protocol Data Units (SPDUs) in the session layer, Presentation Protocol Data Units (PPDUs) in the presentation layer, and finally as Application Protocol Data Units (APDUs) in the application layer. SCADA communications typically uses APDUs to deliver the payloads, i.e., measurements and controls. Information exchange and delivery is done either through network layer or data link layer. Layer 2 communication is limited to the confines of a substation where the data is exchanged as a frame. Meanwhile, layer 3

communication is used for communication between the substations and control center. Layer 3 communication uses the TCP/IP stack and network routing mechanisms to deliver information.

Figure 1 also shows the attack types for each layer of the OSI model and its associated countermeasures. The physical layer is prone to attacks such as sniffing and signal jamming. A suitable solution to protect layer 1 is by using physical security such as physical protection of cable connections.

Information exchange at layer 2 uses physical addresses to identify hosts. This is typically implemented at substations, employing a broadcast mechanism for information delivery. Due to this situation, layer 2 communication is prone to spoofing attacks. Attackers can observe all communication traffic in the network and mimic legitimate traffic to launch a spoofing attack. On the other hand, layer 3 communication works based on IP addresses. Unlike layer 2, the network layer is a closed-loop communication from source to destination using IP addresses and routing mechanisms. This form of communication is typically used between substations and the control center through a wide area network. However, layer 3 is vulnerable to man-in-the-middle attacks. Attackers can perform IP spoofing to mimic legitimate IP addresses for a successful man-in-the-middle attack. Layer 4 is the transport layer that defines communication protocols. Attacks on this layer mainly exploit protocol operations. For example, TCP sync mechanism can be exploited to launch a Denial of Service (DoS) sync flood attack. In order to protect layers 2, 3, and 4, security mechanisms such as network firewalls and intrusion detection and prevention systems can be applied.

For power system communication, typically only layer 7 from the upper layers is used wherein the APDU stores traffic payload. Layers 5 and 6 are typically not used. This is due to the limitation of advanced security implementations in the application layers of power system communications. It is difficult to implement cryptographical techniques to secure power system communications due to the increased latencies. SCADA communication in a power system requires low latency and high rates of data exchange. Hence, communications in the power system are unencrypted and less secure in order to provide a better communication performance. Due to these limitations, cyber security of power system communication has become a vital issue. This chapter discusses secure protocols and security controls for power grids.

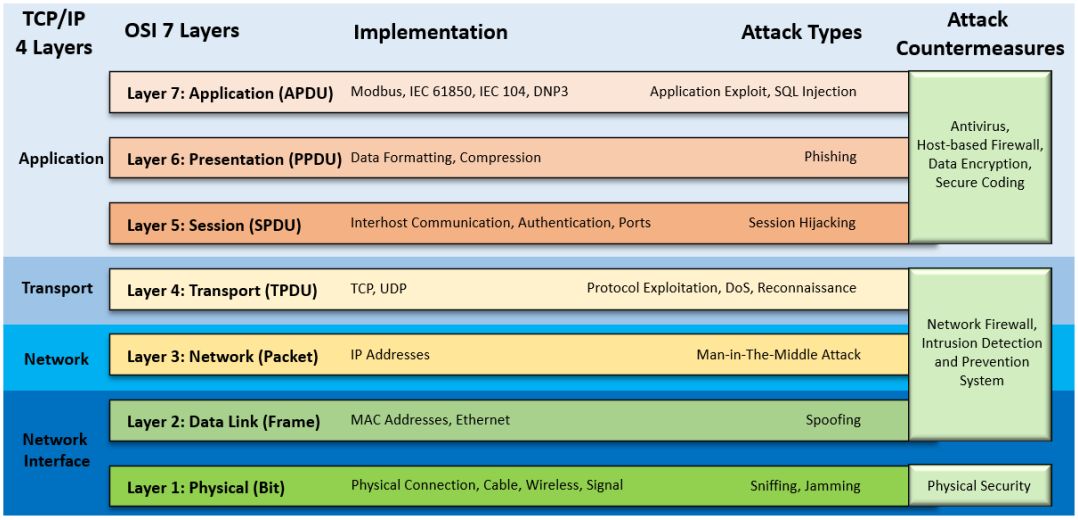


Fig. 1. Mapping of OSI layers, cyber attacks and mitigation techniques.

There are many standard protocols that have been deployed for power grid operations. However, the implementation of secure communication protocols poses a challenge in OT systems, owing to the high-availability requirement. Consequently, security protocols have been identified to be critical areas requiring significant improvement [3]. We identified five approaches to improve the security of OT communication protocols. The first mechanism is achieved through altering the pre-existing protocols. The second approach involves the integration of established legacy power grid protocols with existing protocols that offer enhanced security measures. The third mechanism is achieved by developing a brand-new protocol. The fourth mechanism pertains to the enhancement of key exchange, while the fifth mechanism involves the integration of the protocol with blockchain technology. Figure 2 summarizes the secure OT protocol research directions.

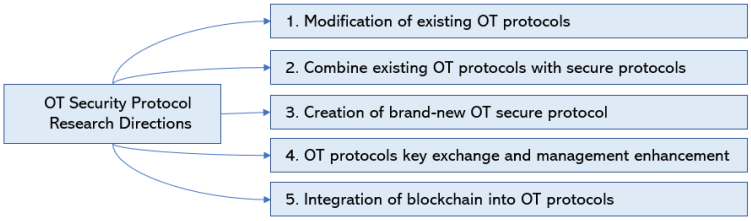


Fig. 2. Summary of secure protocol research and classification.

The first mechanism proposed an alteration of the existing protocols. The authors in [18] carried out a study utilizing formal methods to examine potential authentication vulnerabilities present in Distributed Network Protocol 3 (DNP3). Upon the identification of vulnerabilities, the authors subsequently suggested the implementation of security enhancements for the DNP3 secure authentication broadcast [19]. The conventional implementation of DNP3 employs a broadcast mechanism for the purpose of verifying the authenticity of communication that is transmitted between the master and remote station. The default broadcast mechanism sends information arbitrarily without a well-defined mechanism. This mechanism may lead to potential vulnerabilities like a man-in-the-middle attack, modification, replay, and injection attacks. The research in [19] proposes a modification of the DNP3 secure authentication broadcast message and checks the validity of the established connection. The proposed solution improves the efficiency and enhances the resiliency of DNP3 broadcast messages against man-in-the-middle attacks. In [20], the authors describe the Secure DNP3 protocol with additional authentication mechanism for enhancing communication integrity. An authentication challenge is issued by the slave when the master station requests a "write" message. The master station sends an authentication response. The slave confirms with acknowledgment and response messages. At this stage, it is inferred that the master station is recognized as a trustworthy and legitimate entity. The authors in [20] also present the security enhancement of Inter-Control Center Communications Protocol (ICCP) through the utilization of digital certificates to improve communication integrity.

In the second direction, there is already research being done with the intention of using a combination of existing protocols to put the approach into practice. Authors in [21] proposed the utilization of Modbus communication via Transport Layer Security (TLS) Protocol to create a secure communication channel. The Modbus protocol is a conventional communication standard utilized in power grid systems that lacks security mechanisms. Meanwhile, TLS is considered a broadly adopted mechanism for facilitating secure communication through the use of encrypted data. The proposed mechanism involves the encapsulation and encryption of Modbus information within a TLS packet. The aforementioned mechanism necessitates the process of encapsulating and subsequently de-encapsulating data. Therefore, this approach shows that it is possible to implement power grid communications utilizing pre-existing security protocols.

Instead of modifying existing protocols, the third direction is to create new protocols and standards. An example of a new standard is Open Platform Communication-Unified Architecture (OPC-UA), which replaces the previous versions of OPC through the integration of cryptographic and authentication mechanisms [20]. Another example is IEC 62351 which aims to mitigate cyber security concerns in current protocols via the implementation of cryptographic techniques [22]. Nevertheless, the deployment of cryptographic techniques presents several obstacles. One of the foremost challenges is related to the distribution of keys. Therefore, it comes to the fourth approach using key exchange and management enhancement. Key exchange and management have been identified as a challenge in the SCADA system [23]. Numerous key exchange and management schemes have been suggested to enhance the security of SCADA communication. However, a comprehensive solution to this issue cannot be achieved through a silver bullet solution. The proposed solutions inevitably entail a trade-off between real-time availability and security. The authors in [24] propose a scheme for the pre-distribution of SCADA network keys. The secret key is transmitted over the untrusted network using a pre-distributed matrix-based key. Each device generates unique keys using an algorithm for key generation based on a preliminary matrix reference. This mechanism prevents a man-in-the-middle attack against the key. Unfortunately, if attackers successfully compromise a device, they may still be able to circumvent the secure communication process.

The fifth proposed solution for enhancing security in power grid communications involves the implementation of blockchain technology. Data in the blockchain is stored in the form of a chain of information to preserve integrity [25]. The authors in [26] present diverse potential applications of blockchain technology in the context of power systems. The primary purpose of blockchain technology is to enhance credibility and safeguard the confidentiality of transactions within the energy sector. The proposal of utilizing blockchain technology to enhance the security of message exchange protocols in ICS was proposed in [27]. It is anticipated that blockchain technology will enhance the mechanisms for protocol identification, methods for authentication, and chain of encrypted information. This type of scenario could be appropriate for limited message transmissions. Nevertheless, the

communication traffic of power grids primarily comprises telemetry and measurement data that exhibit a high volume of traffic. Therefore, the implementation of blockchain remains challenging and there is currently no practical implementation of blockchain to improve the security of power grid communication protocols.

To summarize, the implementation of the first and second mechanisms represents a straightforward approach to promptly enhance the security of power grid communication protocols. These solutions exhibit a high degree of elegance in addressing deficiencies pertaining to data encryption and authentication in legacy power grid protocols. Nevertheless, these mechanisms may lack reliability due to the absence of inherent security within the protocols. The fourth and fifth mechanisms have the potential to serve as alternative solutions for augmenting the key exchange and authentication aspects of the protocol. Nevertheless, similar to the aforementioned alternatives, these approaches are not inherently incorporated within the existent protocols. Therefore, the third mechanism has the potential to emerge as a viable alternative for enhancing protocol security over a longer time frame. New security standards, e.g., IEC 62351, provide guidelines and requirements for implementing security measures to protect the operation and data exchange within OT systems, including protection against cyber threats and unauthorized access. Unfortunately, the implementation of new protocols is a time-intensive process. Moreover, the implementation of new protocols does not always guarantee high reliability and security. For instance, in [28], it was demonstrated that IEC 62351 is still susceptible to resource exhaustion attacks.

3. Cyber-Physical System Co-Simulation and Cyber Ranges

A power grid is an example of critical infrastructure that requires a high level of availability. Conducting experiments on actual power grids is a challenging task owing to their stringent operational requirements. Therefore, Cyber-Physical System (CPS) modeling and simulation are essential components of the research. In this section, we classify the CPS modeling and simulation into two parts. The first part provides an overview of power grid co-simulation testbeds. Meanwhile, the second part elaborates on the integration of cyber ranges in the CPS testbed.

3.1 Cyber-Physical Power System Co-Simulation

The utilization of CPS modeling and simulation provides significant importance in the domain of power system resilience research. Many survey papers concerning the current state of the art in smart grid modeling can be found in [29]-[33]. This section focuses on CPS models with cyber security capabilities. The CPS modeling framework comprises two primary components, i.e., the power systems and IT-OT systems. Table I provides a summary of the CPS model simulators utilized in power systems. There are many power system simulators currently available, including but not limited to Real-Time Digital Simulator (RTDS), OPAL-RT, Typhoon HIL, DIgSILENT PowerFactory, GridLab-D, OpenDSS, Siemens PSS/E, Homer, Cymdist, PSAT, and MATPOWER. Numerous communication network simulators are also available, including NS-2, NS-3, OPNET, OMNeT++, NetSim, NeSSi, DeterLab, and Mininet. Therefore, there are numerous potential combinations of power systems and communication network simulators for the purpose of modeling the cyber-physical power system.

Table I. Cyber-physical system models for power systems research.

Cyber-Physical System	**Power System Simulator**	**IT-OT Simulator**	**Protocols**
TASSCS [34]	Software Based	OPNET	DNP3, IEC 61850, OPC UA
SCADASim [35]	Software Based	OMNeT++	DNP3, Modbus
Washington State University [36]	RTDS	Mininet, Core	IEC 61850, Modbus, DNP3
DeterLab [37][38]	Software Based	Virtual Machine	-
ISAAC [39]	RTDS	Real Hardware	IEC 61850, IEEE C37.118, DNP3
SCEPTRE [40]	PyPower, OpenDSS, PowerWorld	Virtual Machine	-

According to the state-of-the-art literature review [29]-[33], RTDS has emerged as the preeminent simulator for power systems. RTDS is a computational tool that enables the simulation of power systems in real-time, allowing for the accurate representation of the dynamic behavior of these systems in synchronization with the actual system time. This capability is important in the context of testing and validating control systems, protection schemes, and other applications that require timely execution. In the meantime, for IT-OT communication networks, the majority of organizations are moving toward adopting a virtual environment that is based on Virtual Machines. Over the past ten years, there has been a rise in alternative communication network simulators for the CPS model of power grids, including OPNET [41]-[43], OMNET++ [44], [45], and NS2/NS3 [46]. Nevertheless, the fidelity of these simulators is inferior when contrasted with the virtual environment.

In summary, the communication network simulators utilized for CPS modeling of power grids can be classified into four different categories. They are 1) code/script-based, 2) software-based, 3) virtualization-based, and 4) real hardware implementation. Figure 3 displays the clustering and categorization for each respective category. In Figure 3, each category is evaluated according to its scalability and level of fidelity. It would be preferable for the CPS model to have higher scalability as well as fidelity. The most realistic and least scalable form of simulation is real hardware. The most scalable simulators, meanwhile, are code-based simulators. Code-based simulators enable the simulation of a network at a large scale. However, the code-based needs to specify what constitutes communication and it requires to manually specify each type of communication functionality in the code. Furthermore, unlike in a real system, the communication process is not natural. The subsequent category pertains to simulators that are based on software. The low scalability and low fidelity of these particular simulators leave it a less desirable alternative. Considering the aforementioned factors, it is very likely that the optimal choice for simulation would be based on virtualization.

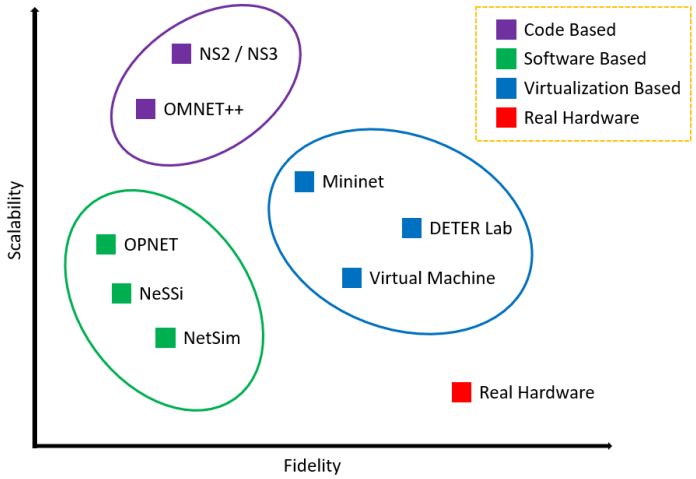


Fig. 3. Comparison of communication network simulators for CPS modelling.

A Virtual Machine (VM)-based simulator is likely to provide an environment that is nearly identical to that of real hardware. It also can be more scalable than real hardware through hardware virtualization techniques using hypervisor. For instance, DETERLab is classified as a VM because it consists of a cluster of VMs. The other option is Mininet, an operating-system level virtualization, which works based on the Linux namespace over containerization. In contrast to VMs, containers employ virtualization to encapsulate the Operating System (OS) and application dependencies, thereby allowing for the sharing of the host OS kernel across multiple containers. In summary, it can be concluded that the most suitable alternatives for communication network simulation are those based on VM and container technologies, as they offer an optimal equilibrium between scalability and high fidelity.

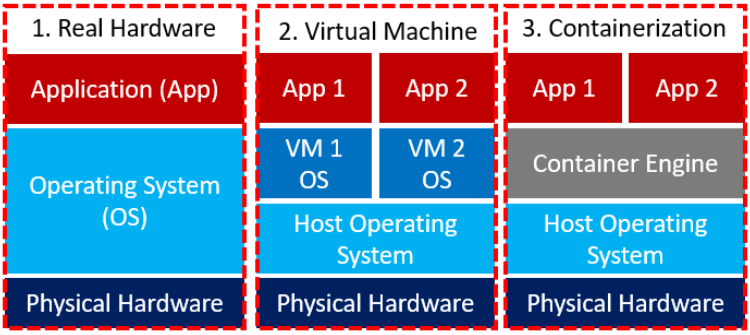


Fig 4. Comparison of real hardware, virtual machines, and container-based system.

The differences between an application running on actual physical hardware, virtual machine, and containerization are illustrated in Figure 4. When compared to actual hardware, VM allows us to run applications in a more isolated manner within the operating system. This feature enables users to simulate a greater number of virtual environments within the IT-OT network. However, as illustrated in Figure 4, the VM was required to install the guest operating system on top of the host operating system. The scenario involving the stacking of operating

systems is known to significantly consume a substantial amount of resources. To address this challenge, operating system level virtualization through containerization applications such as Docker and Linux-based namespace have experienced an increase in popularity in the past few years [47]. One of the reasons for this is that they are able to deploy applications directly on top of the host operating system by utilizing an isolation mechanism, which optimizes the utilization of available resources. In addition, the utilization of containers enables users to emulate a greater number of hosts and larger networks in comparison to VMs. Due to the aforementioned factors, operating system virtualization solutions may become the most suitable network communication simulation tool for modeling power grid CPS. However, the current implementation of power grid CPS models developed through containerization is limited. It is likely that the number of implementations will increase in the near future, which will align with the development of virtualization technology.

Figure 5 depicts an example of CPS co-simulation architecture implemented in Control Room of the Future (CRoF) technology centre at Delft University of Technology (TU Delft). It is composed of a simulation of the power system as well as an IT-OT simulation. DIgSILENT PowerFactory and RTDS are used for the simulation of the power system, i.e., IEEE 39-bus. The power system model provides circuit breaker status and measurement data of active and reactive powers, voltages, and currents from busbars, lines, and generators. The implementation of OPC-UA facilitates the interfacing of data exchange between power grids and IT-OT simulation. The implementation of the IT-OT architecture is carried out through the application of Mininet. Each host in the IT-OT network, e.g., merging units, intelligent electronic devices, network switches, routers, databases, etc., are implemented in Mininet using containers. Every container incorporates a tailored application for IT-OT host operations, such as the acquisition and transmission of measurement data, control setpoints, database access, and so forth. The current implementation of CPS comprises of 27 substations and 210 hosts. A unique application has been tailored for each host to replicate the CPS of power grid components. At present, the simulation of all 27 substations runs on 50,000 lines of code on 26 VMs.

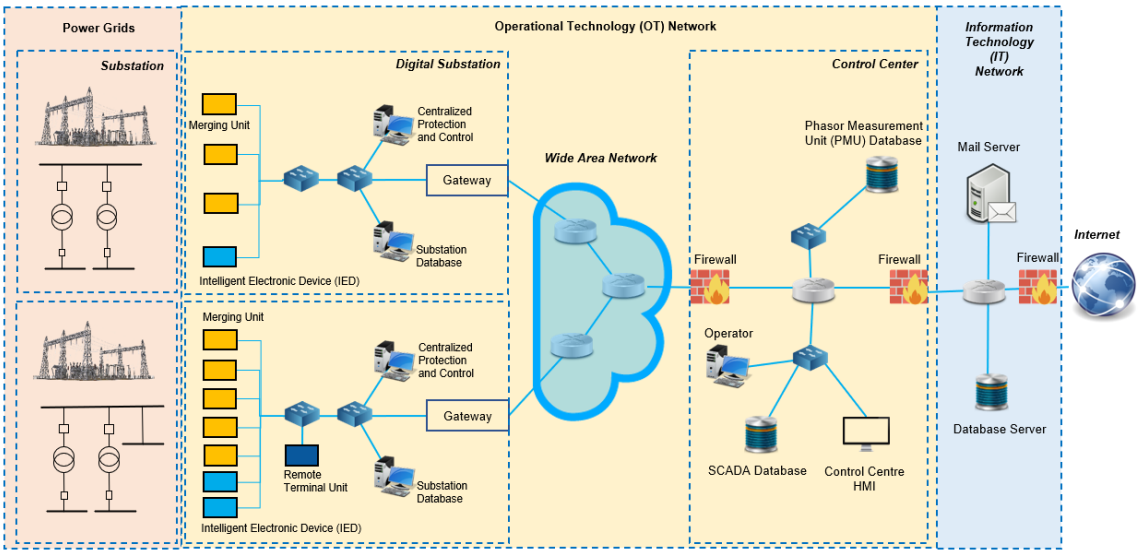


Fig. 5. CPS architecture in CRoF at TU Delft.

3.2 Cyber Range for Cyber-Physical Power Systems

Cyber ranges have emerged as a prevalent approach for evaluating defense mechanisms and simulating potential attack strategies in the domain of cyber attack and defense simulations [48]. Typically, cyber ranges have been predominantly utilized in the environment of IT systems. In order to align with forthcoming power grid operations, it is essential that CPS models possess cyber range capabilities to enable investigation and assessment of future power grid cyber security.

In accordance with the CPS model depicted in Figure 5, a cyber range was incorporated into CRoF. Figure 6 depicts the CPS and cyber range architecture, enabling blue and red teams experiments. The blue team is typically responsible for safeguarding an organization's IT-OT assets and infrastructure, serving as the internal security team or defenders [49]. Their responsibility entails upholding the security posture of both the IT-OT systems and networks. The blue team has several key objectives, e.g., system monitoring, defending, incident response, and cyber security assessment. Meanwhile, the red team plays the offensive or adversarial role in the cyber range exercise [49]. The red team conducts realistic cyber attacks and attempts to get past the organization's security

controls. The main goals of the red team are penetration testing, vulnerability analysis, reporting and providing security recommendations.

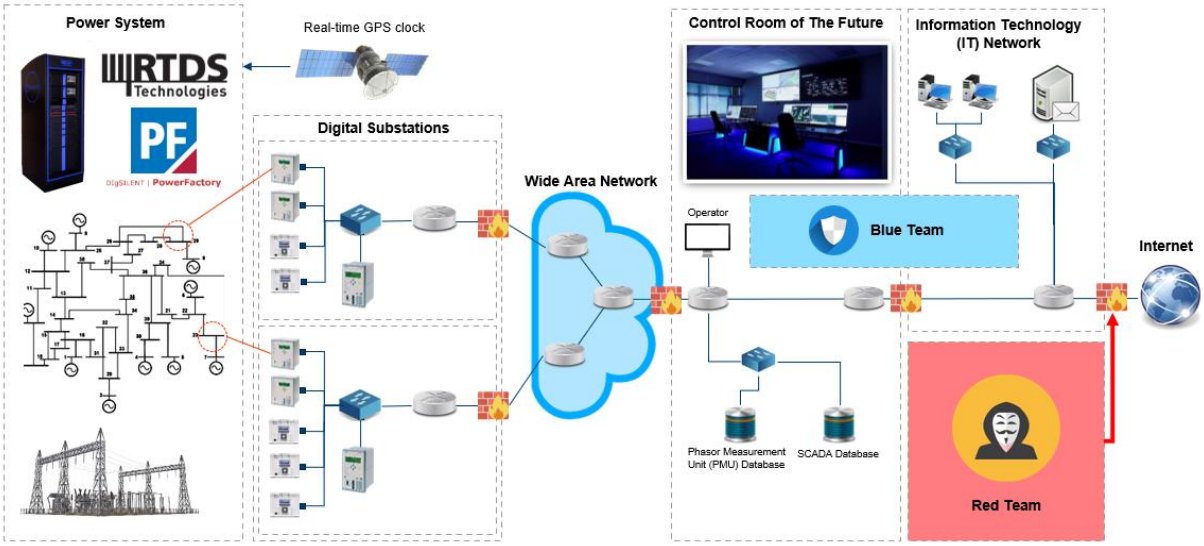


Fig. 6. CPS and cyber range architecture of CRoF at TU Delft.

Figure 7 presents the deployment of blue and red team's instruments for the power grid IT-OT systems in CRoF. The blue team employs multiple applications to ensure the secure operation of the power system. These applications include Security Information and Event Management (SIEM), intrusion detection and prevention systems, SDN, impact analysis and defense against cascading failures, and power system restoration. Contrariwise, the red team employs cyber attack tools to execute Open Source Intelligence (OSINT), payload delivery, IT-OT reconnaissance, lateral movement, response function inhibition, and malicious control. The red and blue teams are engaged in a cyber range competition to evaluate the capabilities of power system operators and Computer Security Incident Response Team (CSIRT) to mitigate the impact of cyber attacks on power grid operation.

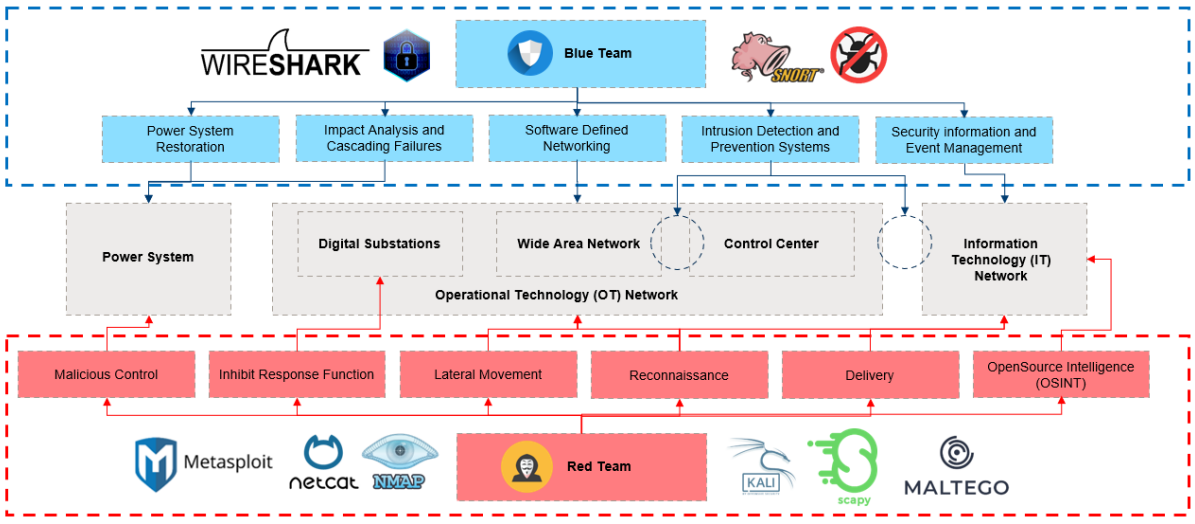


Fig. 7. Blue and red team tools for power grid IT-OT systems in CRoF at TU Delft.

4. Network Security Controls

Security controls are a set of measures and mechanisms that are put in place to ensure the protection of information systems from potential threats, vulnerabilities, and unauthorized access. Security controls have been devised with the purpose of reducing potential hazards and guaranteeing the confidentiality, integrity, and accessibility of both data and resources. This section discusses the state-of-the-art research conducted on network security controls for power grids, which are divided into two categories, i.e., firewalls and Intrusion Detection System and Prevention Systems (IDPS). The summary of network security controls is provided in Table II.

TABLE II. Summary of network security control applications.

Security Control	Methods	Protocols	References
Firewall	Packet filtering	DNP3	[50]
		Modbus	[51]
	Next Generation Firewall / Deep Packet Inspection	Not specified	[52]
		IEC 104	[53]-[55]
IDPS	Signature-based	Not specified	[56],[57]
		IEC 104	[58],[59]
		Modbus	[60]-[63]
		DNP3	[60],[64]
		Siemens S7	[65]
		IEC 61850	[66]-[69]
		IEEE C37.118	[70]
	Anomaly-based and AI-based	Not specified	[71]-[88]
		IEC 104	[90]
		DNP3	[91]-[93]

4.1 Firewalls

The firewall was initially designed to operate predominantly through conventional IT systems. However, the implementation of a firewall is also a viable measure for enforcing security controls for power grids. In [50], a proposal was made for a Linux-based firewall modification intended for use in power grid applications. The Linux operating system features a firewall application that is configured through the implementation of iptables rules. Iptables enables the user to designate IP address origin and destination, port, and packet type for inclusion in either a blacklist or whitelist reference. Furthermore, the study suggests the utilization of an extra 32 bits of header data derived from the DNP3 protocol. The decision to filter is made using 32 bits of information extracted from DNP3 packets. In [51], another variant with a comparable filtering mechanism was proposed for the Modbus protocol. In general, implementing security measures based on firewalls represents a straightforward approach to safeguarding communication networks for power grids. The firewall operates on predetermined rules that are hardcoded, and subsequently applies these rules to filter packets accordingly. Unfortunately, a firewall is considered inadequate for dealing with advanced cyber attacks. By utilizing advanced methods of attack, adversaries may circumvent the static firewall rules.

Another type of firewall known as Next-Generation Firewall (NGF) is equipped with the capacity to perform Deep Packet Inspection (DPI). DPI enables NGF to not only inspect the header information of a packet, but also to inspect the contents and contextual information of the packet payload. Several studies have suggested the utilization of DPI applications for enhancing security measures in power grids. For instance, the DPI application for IEC 104 protocol is researched in [53]-[55] and other OT protocols in [52]. NGF exhibits superior performance when compared to traditional packet filtering firewalls. Prior knowledge of the traffic is a prerequisite for NGF to effectively execute traffic classification and filtering. Consequently, NGF exhibits limitations in its ability to identify anomalies from new types of cyber attacks.

4.2 Intrusion Detection and Prevention Systems

IDPS is a security mechanism that was specifically developed to identify and counteract any malicious actions or unauthorized entry attempts that may occur within an IT-OT system. The operational mechanism involves the monitoring of network traffic, system events, and user activities with the aim of detecting potential security breaches or policy violations. In general, there exist two primary classifications of IDPS, namely signature-based and anomaly-based.

A signature-based IDPS operates by utilizing a predetermined set of information, i.e., signatures for known cyber attacks, for classifying the network traffic. Numerous studies have been carried out related to the utilization of

signature-based IDPS in various power systems-related communication protocols. These include IEC 104 [58], [59], Modbus [60]-[63], DNP3 [60],[64], Siemens S7 [65], IEC 61850 [66]-[69], and IEEE C37.118 [70]. Additionally, certain implementations have been developed for carrying out general OT protocols as described in [56]-[57].

An alternative type of IDPS runs through the application of anomaly detection techniques. Rather than depending on pre-defined attack signatures, this approach establishes a standard baseline for typical behavior for the network, systems, and users' activities. The system continuously observes network traffic and system events, seeking out any deviations or anomalies from the normal pattern. An alert is generated if an activity or behavior deviates significantly from what is considered normal. An anomaly-based IDPS is an effective method for detecting previously unseen or zero-day attacks and advances attack techniques.

Statistical analysis, expert systems, and AI are three techniques that can be employed to identify an anomaly. In recent years, the AI-based technique gained more attention. In general, AI-based methods can be subdivided into machine learning and deep learning. Prior studies have proposed the application of machine learning techniques for IDPS in power grids. The vast majority of the research focuses on IDPS in general and does not address any specific OT protocols [71]–[88]. Some of them also implement anomaly-based IDPS for specific protocols, e.g., IEC 104 [89], IEC 61850 [90].

Deep learning is a subset of machine learning that involves more complex neural network layers and higher computing demands. Some of the popular deep learning models include Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long-Short Term Memory (LSTM), and Graph Neural Network (GNN). In [92], the authors proposed IDPS based on deep learning to classify DNP3 traffic. The traffic is classified into four categories, i.e., normal, DoS attack, unsolicited attack, and cold restart attack. Another example, CNN-based attack detection for DNP3 protocol was proposed in [91]. More deep learning-based IDPS examples are provided in Table II. Although deep learning requires more computational resources, it outperformed traditional machine learning in terms of performance. As a result, the majority of IDPS research in recent years has focused on applications of deep learning.

5. Hybrid Deep Learning for Anomaly Detection in Power System OT Networks

This section provides an anomaly-based IDPS solution using hybrid deep learning for power grid OT systems. The vast majority of deep learning-based IDPS is mainly focused on IT system applications [93]-[96]. Despite the integration of a utility's IT and OT systems, the traffic patterns exhibit distinctive characteristics. The network traffic in OT systems is generated from automated processes that exhibit deterministic and homogenous behavior, whereas the network traffic in IT systems is composed of user-generated data that exhibits a stochastic behavior [97]. Consequently, the deployment of traffic-based anomaly detection in OT systems differs from IT. In order to solve this challenge, hybrid deep learning techniques are used to develop an IDPS for OT systems.

Deep learning-based IDPSs are encountering challenges due to their reliance on training datasets for their objectives of anomaly detection and classification. Consequently, it cannot detect new or unknown types of cyber attacks. In order to fill this gap, rather than relying on data that has been specifically labeled for each type of attack, quantitative anomaly is used. The OT communication traffic throughput is utilized in quantitative anomaly detection. The quantification of throughput is represented as a time series, resulting in a distinctive waveform pattern, as demonstrated in [98]-[100]. Therefore, rather than classifying specific attack types or sequences, the time series traffic flow throughput is classified into two categories, i.e., normal and anomalous. The following subsections provide more detailed explanations on hybrid deep learning for anomaly detection in power system OT networks. They are classified into three parts including wide area monitoring for OT networks, hybrid deep learning model for anomaly detection, and attack graph methods for power system wide situational awareness in near real-time.

5.1. Wide-Area Monitoring of OT Networks

The implementation of wide area monitoring is needed for the purpose of observing traffic behavior within control center and substation OT networks. Wide area OT traffic monitoring for power grids can be enabled by using SDN. The SDN networking paradigm is founded on the principles of network virtualization and the separation of data and control planes [93]. Figure 8 represents the SDN architecture for power grids consisting of three different abstraction layers. These layers are referred to as the data plane, control plane, and management plane. The conventional OT communication networks are represented by the data plane, whereas the control plane provides control capabilities over the data plane. The deployment of various network applications, such as routing algorithms, load balancers, IDPS, attack graph models, and so on, is made possible by the SDN management plane. While SDN is a relatively new concept in computer networking, prior studies have explored its application in cyber-physical power systems, as evidenced by other research [94]-[98].

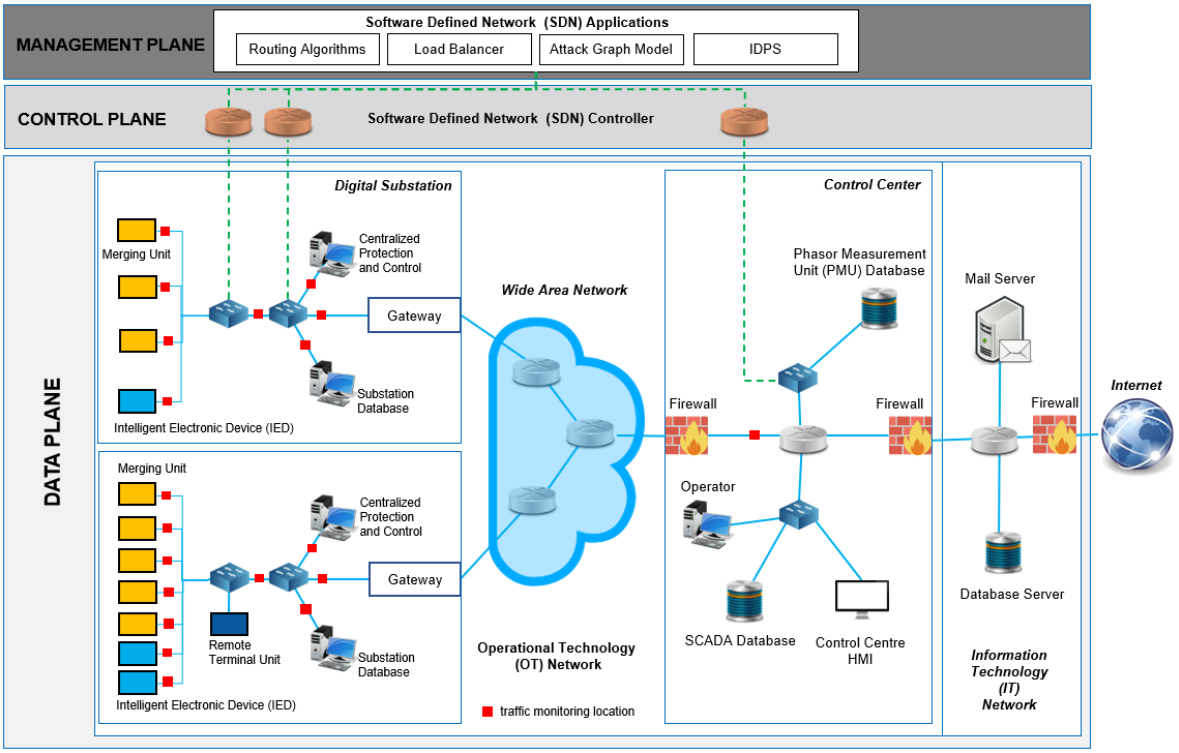


Fig. 8. SDN architecture for power grid OT networks.

Previous studies have utilized SDN to detect anomalies by relying on traffic flow data [99], [100]. However, these works do not aim to identify anomalies caused by cyber attacks in OT networks. Furthermore, an analysis that is critical in nature of the state-of-the-art techniques for detecting anomalies in communication traffic indicates the following. (1) Current SDN applications designed for cyber-physical systems lack emphasis on securing OT networks against cyber threats [99], [95]-[100]. (2) The rules governing them are exclusively developed on packet flow [100]. (3) The cyber kill chain is disregarded and stealthy cyber attacks are not taken into account [99],[100].

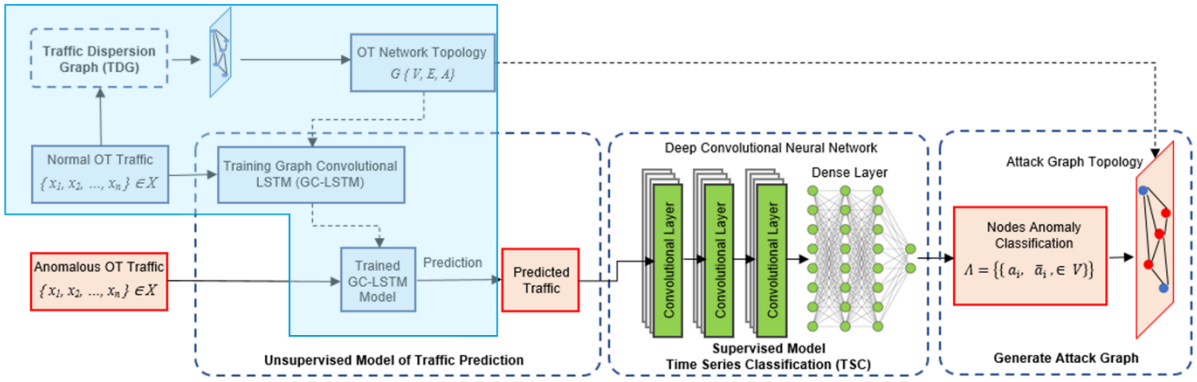
SDN can be used to perform real-time monitoring of network traffic that originates from the data plane of the power system OT networks. In addition, the primary emphasis of this research is placed on the detection of anomalies during the early stages of the cyber kill chain in order to minimize the severity of the impact during the later stages. Network virtualization enables the SDN controller to monitor and control network traffic as well as implement custom network applications. SDN enhances monitoring and control of OT networks by gathering communication traffic reports in the control center. The traffic observation points are depicted as small red squares that are dispersed throughout the substations and control center. Using these observation points, the real-time OT network traffic is monitored from the control center in order to detect traffic anomalies at each substation and generate an attack graph in near real-time. Spatial-temporal data is obtained by collecting OT network traffic throughputs for each observation point. This data is subsequently utilized for hybrid deep learning techniques.

5.2. Hybrid Deep Learning Model for Anomaly Detection

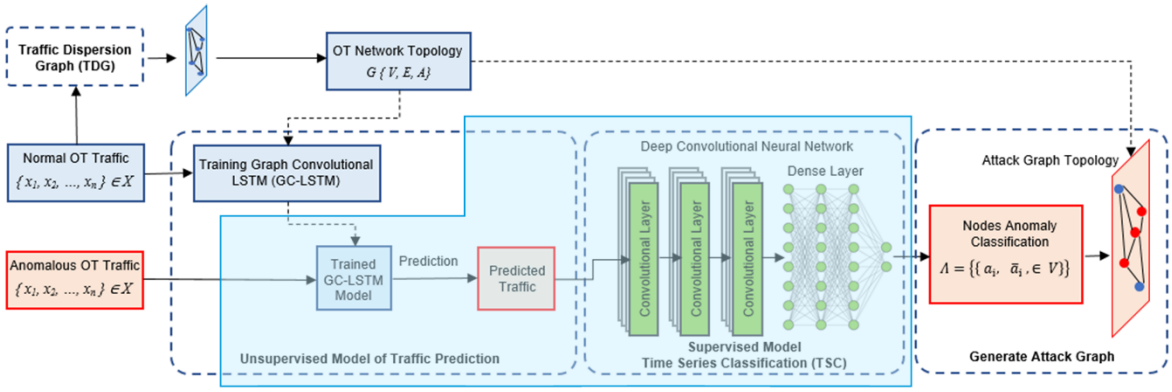
Previous research has investigated the detection and classification of anomalies using time series data [101]-[104]. The state-of-the-art Time Series Classification (TSC) techniques have been built on deep learning models [103],[104]. Nevertheless, their efficacy in identifying stealthy attacks is limited due to their inability to detect small changes in network traffic throughput. Furthermore, these techniques exhibit poor performance owing to the presence of imbalanced data, as evidenced by their F1 and Geometric mean scores. Therefore, a hybrid deep learning approach can be used to tackle these challenges in detecting anomalies in the traffic of power grid OT networks. The hybrid model employs CNN, Graph Convolutional Network (GCN), and LSTM. The methodology utilizes unsupervised learning techniques to acquire knowledge on the intricate patterns of OT network traffic throughput, and supervised learning techniques to accurately classify the OT traffic.

The proposed method uses Graph Convolutional Long Short-Term Memory (GC-LSTM) to learn the traffic behavior of the OT network. Two machine learning models are applied in GC-LSTM, i.e., GCN and LSTM. The GCN utilizes graph-based representations of the OT network topology and incorporates localized features from neighboring communication nodes in the spatial domain. Subsequently, the LSTM will carry out temporal learning based on the time-series data of the observed OT network traffic. The integration of GCN and LSTM confers the

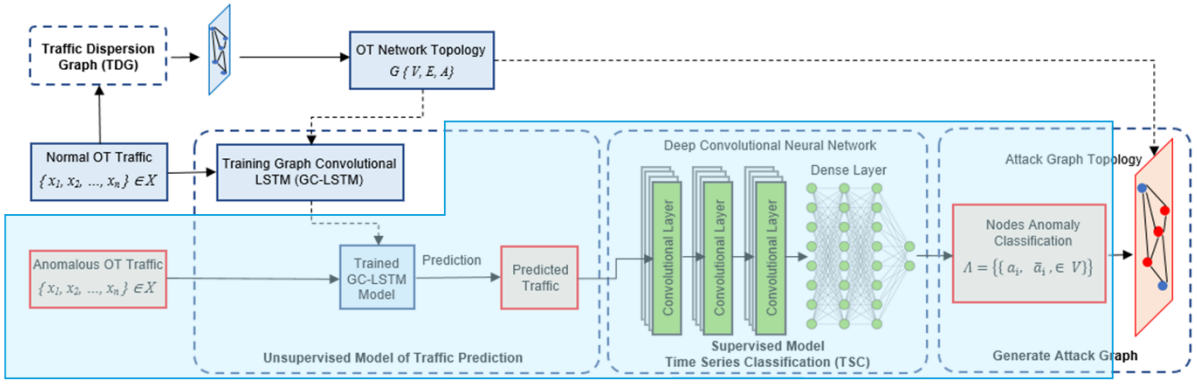
benefit of acquiring knowledge from both the spatial and temporal domains. Several applications utilizing spatial and temporal models based on graphs have been proposed in [105]–[108].



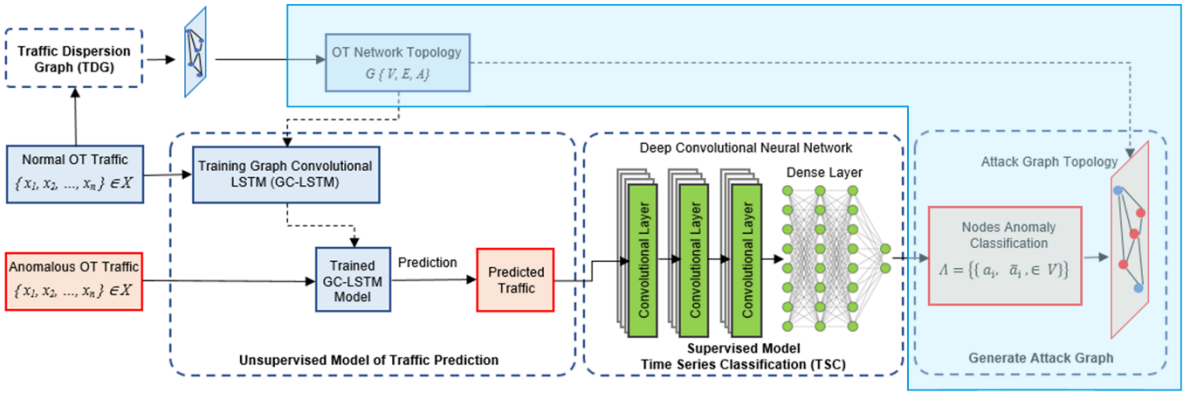
(a) GC-LSTM training for traffic prediction and Traffic Dispersion Graph (TDG)



(b) CNN training for Time Series Classification (TSC)



(c) Near real-time anomaly detection and nodes classification based on pre-trained models



(d) Attack graph generation and visualization based on nodes classification and known graph topology

Fig. 9. CyResGrid attack graph generation processes

This chapter presents CyResGrid [109], an innovative approach for predicting nodal features by leveraging the communication network topology and characteristics of neighboring graph nodes based on the OT traffic observation locations. CyResGrid processes depicted in Fig. 9 consist of four stages, i.e., a) GC-LSTM training and Traffic Dispersion Graph (TDG), b) CNN training for Time Series Classification (TSC), c) near real-time anomaly detection and nodes classification, d) attack graph generation and visualization. Initially TDG and GC-LSTM for analyzing the power system's OT network traffic as shown in Figure 9(a). The TDG extract network topology based on observed traffic in OT network. The GC-LSTM learns the complex behavior of OT traffic data and topology. The prediction output from GC-LSTM subsequently generates traffic for the supervised predictions of CNN as shown in Figure 9(b). Based on GC-LSTM and CNN training results, a hybrid combination of unsupervised and supervised models is used for OT traffic anomaly detection and nodes classification as shown in Figure 9(c). Finally, the nodes classification result and network topology information are integrated into an attack graph depicted in Figure 9d.

The primary input for the GC-LSTM approach is the graph structure of the OT network topology. TDG is used to derive this particular graph structure. The Graph (G) elements are vertices/nodes (V), edges/links (E), and adjacency matrix (A). The adjacency matrix is a representation of elements denoted by $A_{i,j}$, where i and j are node index numbers. $A_{i,j}$ equals 1 when two nodes are connected and 0 when they are not. In Eq. (1), the GCN model is predicated on the Hadamard product multiplication ($\odot$) of the weight matrix (W_{gcn}), adjacency matrix (A), and node features derived from the historical traffic data (X_t). The adjacency matrix is a mathematical representation that encapsulates pertinent details concerning the topology of the OT network. The modified adjacency matrix ($\hat{A}$) is obtained by adding the identity matrix (I) to the original adjacency matrix (A). The time series data set (X_t) is modelled by an equation that accounts for a specific time point (t) and the overall number of time observations (T). The node feature matrix (X) contains information about each node (x_i), where n represents the total number of nodes. The equation takes into account the exponent k, which represents the number of hops from a communication node to its neighbouring nodes, as described in [107] and [110]. Following the acquisition of spatial features through the GCN, the LSTM model is subsequently employed to examine the temporal or time-series characteristics. The functions and processes that occur within an LSTM cell are described in Eq. (2–7). The LSTM process comprises six primary sub-equations, namely the forget gate (f_t), input gate (i_t), output gate (o_t), internal cell state (c'_t), transferable cell state (c_t), and hidden state (h_t).

$$GCN_t^k \leftarrow (W_{gcn} \odot A^k) X_t \tag{1}$$

$$f_t = \sigma((W_f GCN_t^k) + (U_f h_{t-1}) + b_f) \tag{2}$$

$$i_t = \sigma((W_i GCN_t^k) + (U_i h_{t-1}) + b_i) \tag{3}$$

$$o_t = \sigma((W_o GCN_t^k) + (U_o h_{t-1}) + b_o) \tag{4}$$

$$c_t^{'} = \tanh((W_c GCN_t^k) + (U_c h_{t-1}) + b_{c'}) \tag{5}$$

$$c_t = (f_t \odot c_{t-1}) + (i_t \odot c_t^{'}) \tag{6}$$

$$h_t = o_t \odot \tanh(c_t) \tag{7}$$

TSC is implemented using a CNN algorithm with a multi-layer convolutional and ReLU activation function, as depicted in Eq. (8). The variables under consideration in (8) are the number of layers (l), filter size (m), weight (w), and bias (b). This model is trained to optimize classification performance based on previous GC-LSTM output. We perform hyperparameter tuning based on the number of layers, filters, and kernel size to develop our hybrid deep learning model. The deep learning model is optimized by using the technique of Bayesian optimization [111]. The optimization function seeks to maximize the efficacy of deep learning, as described in Eq. (9). The surrogate model and acquisition function are the foundation upon which Bayesian optimization is built. The Gaussian process serves as a surrogate model, enabling the quantification of uncertainty pertaining to regions that are not directly observable. In order to attain the optimal value of the objective function, the Expected Improvement (EI) is employed as the acquisition function. Iterations are carried out in Bayesian optimization in order to obtain a function that has the best possible performance. Through the iterative process, the CNN with the best performance is obtained that consists of three layers, sixty-four filters, and three kernel sizes. After the optimization, CNN is used to perform binary classification for each node into normal and anomalous. The classification is performed based on TSC from time series throughput data for each node (X). The result from the classification is then used to construct a forensic graph in the following stage.

$$y_i^l = \mathrm{Re}\,LU(\sum^{m-1} w y_{(i)}^{l-1} + b) \quad (8)$$

$$x^* = \arg\max_x f(x) \quad (9)$$

5.3. Attack Graph for Situational Awareness

Attack graphs can be used to model CPS vulnerabilities and exploits. An attack graph is an essential instrument for vulnerability analysis and development of mitigation strategies. In the context of a communication network, numerous hosts are susceptible to potential vulnerabilities. Consequently, cyber security of the entire CPS cannot be reliant solely upon the security of an individual host. Hence, it is crucial to detect and classify all susceptible nodes/hosts within a communication network as a group of possible threats in the CPS. Therefore, in this research the observation and analysis of anomalous OT traffic behavior is used to detect potentially compromised nodes in the control center and substations. The data pertaining to anomalous nodes is subsequently utilized to generate an online attack graph in near real-time covering all OT networks of the power grid.

The process of generating an attack graph is described in Algorithm 1. The algorithm takes the OT network traffic (X) as its input. The GC-LSTM algorithm is used to predict the OT traffic based on the network traffic data obtained from each substation (X_n). The GC-LSTM architecture generates a series of traffic forecasts (h_t) as its outputs. The corresponding output obtained from the prediction process is subsequently utilized as an input for the CNN-based TSC. Time series-based anomaly detection is conducted for every node (a) within V. The classifier categorizes individual nodes as either anomalous or normal, utilizing the input OT traffic prediction. Subsequently, the aforementioned data is utilized to formulate the attack graph.

Algorithm 1: CyResGrid Attack Graph Generation

Inputs: $S\{s_1,s_2.,..s_n\}$; X ∈ s_n: Substations traffic data

$\{x_1, x_2, \dots, x_n\} \in X$: Nodes traffic data

Outputs: $\Lambda = \{\{a_i,\ \bar{a}_i,\ \in V\}\}$: Nodes classification as attack graph

Iteration for each substation
for s_i in S **do**
  for t = 1 to T do
    Traffic prediction
    $GCN_t^k \leftarrow (W_{gcn} \odot \hat{A}^k)\, X\{x_1, x_2, \dots, x_n\}_t$
    $h_t, c_t = LSTM\,(X\{x_1, x_2, ..., x_n\}_t, GCN_t^k, h_{t-1}, C_{t-1})$
    Iteration for each node a in V
    for a in V
      Node classification
      $\bar{a}_i = \sum^{m-1} w\, h_{t,(i)}^{l-1} + b$
    end for
  end for
end for
return: $\Lambda = \{\{a_i,\ \bar{a}_i\ , \in V\}\}$

$$\Lambda = \{\{a_i, \bar{a}_i, \in V\}\} \quad (10)$$

$$\Lambda = \{\{a_i, \bar{a}_i, \in V\}, \{u_i \notin V\}\} \quad (11)$$

There are two different types of attack graphs, which can be comprehended by Eq. (10) and (11). Attack graph type I, as described in Equation (10), is generated by applying prior knowledge of the OT network topology and the output of node classification. In the meantime, the attack graph type II presented in Eq. (11) takes into consideration unknown nodes based on the TDG. There are two elements of attack graph (Λ) type I as indicated

in Eq. (10), i.e., normal nodes (a_i), and anomalous nodes ($\bar{a}_i$). Both aforementioned nodes are constituent elements of the set of known nodes (V). On the other hand, the attack graph of type II, which is shown in the Equation (11), consists of one additional element of the unidentified node. Nodes that cannot be identified are regarded as anomalous due to their lack of association with the known nodes (V).

Figure 10 depicts an example comparison of attack graph representations of the OT network under normal OT network traffic conditions in Figure 10(a), and under anomalous traffic conditions in Figure 10(b) and 10(c). The anomalous network traffic conditions are determined based on observed abnormal node behavior shown in red. Subsequently, these nodes are integrated to construct an attack graph (Λ). There are three elements in the attack graph, i.e., normal nodes (a_i), anomalous nodes ($\bar{a}_i$), and unidentified nodes (u_i). The first attack graph type depicted in Figure 10(b) categorizes nodes as anomalous based on the traffic patterns observed from all identified nodes. In contrast, the attack graph of type II depicted in Figure 10(c) considers all unknown nodes to categorize abnormal behavior. The recognition of unidentified nodes (u_i) is dependent upon acquiring addresses from unknown sources or destinations through the TDG. It is presumed that the presence of the unknown nodes (u_i) indicates an active cyber attack that is being launched from an unlisted host within the known OT network (V).

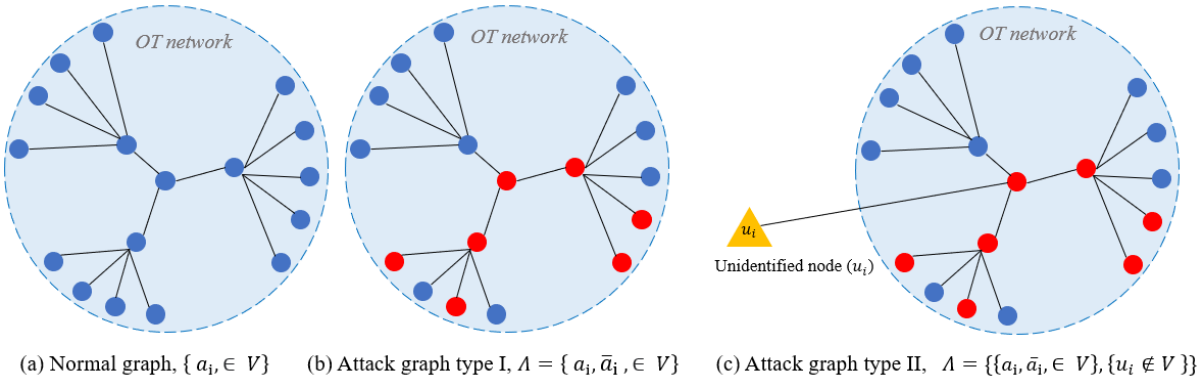


Fig. 10. Attack graph representation for normal and anomalous traffic: a) Normal graph, b) Attack graph type I which contains normal and anomalous nodes, and c) Attack graph type II which contains normal, anomalous and unidentified nodes.

6. Cyber Attack Case Studies

This section presents an analysis of two case studies, which involve instances of cyber attacks on a digital substation and wide area networks. In the first scenario, the digital substation is the target of the cyber attack, whereas in the second scenario, multiple substations are targeted.

6.1 Substation Attack Exploiting GOOSE Protocol Vulnerabilities

The primary objective of a cyber attack targeting a digital substation is to alter, disrupt, or incapacitate the functionality of one or more protection, automation, or control devices. Figure 11 illustrates a Hardware-in-the-Loop (HIL) setup employed to execute cyber attacks on a digital substation and implement the anomaly detection using hybrid deep learning and attack graph method. RTDS is used to model the power system in real-time. The implementation of data exchange between the RTDS and substation OT communication network is facilitated through the utilization of GTNET cards. The OT network within the substation comprises of Intelligent Electronic Devices (IEDs). The IEDs are in compliance with the IEC 61850 standard, including Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SV) messaging. A host was compromised inside the substation from where the cyber attack is conducted.

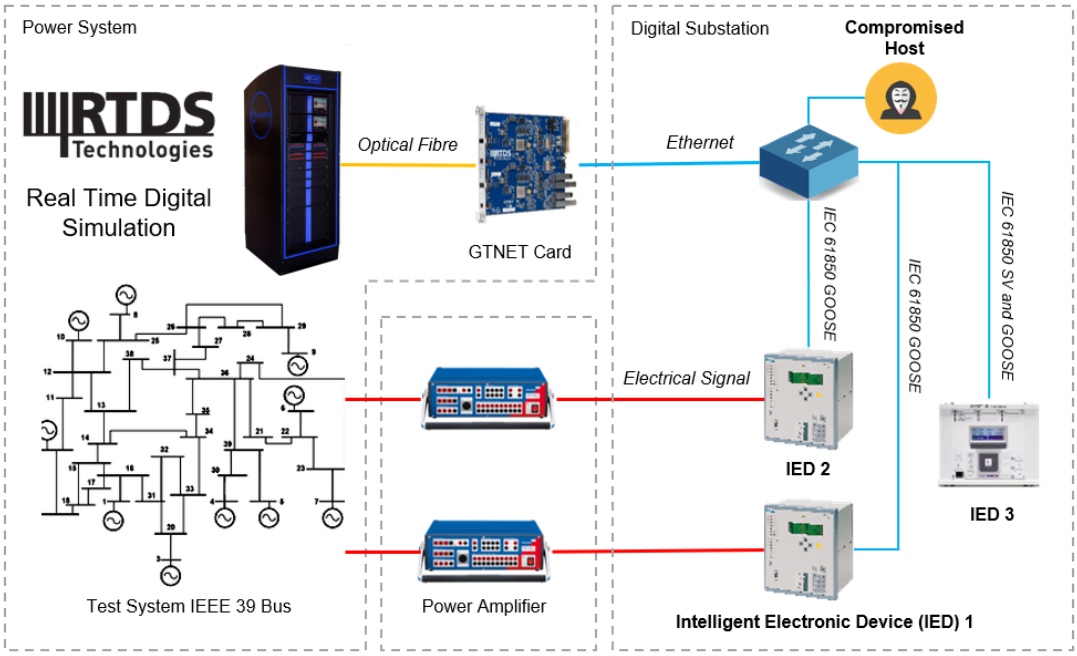


Fig. 11. Cyber-physical experimental architecture to analyze impact of cyber attacks on digital substations.

During simulation, the GTNET cards periodically send IEC 61850 SV packets to IEDs communicating sampled voltage and current measurements. A switch that functions at the Data Link Layer (Layer 2) of the OSI model is connected to the hosts that make up the substation network. As a consequence, in the configuration of the substation network, each packet is sent to all hosts that are connected to the switch. The IEDs can detect a fault simulated in RTDS and issue control commands using IEC 61850 GOOSE to open circuit breakers and clear the fault. The compromised host is connected to the Ethernet switch. The attacker uses various tools to perform network reconnaissance and sniff the OT network traffic through the network switch. Following weaponization, the attacker injects spoofed GOOSE packets into the switch to open circuit breakers [112],[113]. Based on the HIL setup and cyber attack scenarios, OT network traffic data is collected from the switch for analysis using CyResGrid. The OT data collection process is carried out through Wireshark, in accordance with the substation network configuration.

Figure 12 presents the attack graph results for the cyber attack conducted on the digital substation, i.e., network reconnaissance and GOOSE attacks. There are 85 nodes in total present in each graph (a)-(c).Figure 12(a) depicts the attack graph while the OT network is operating normally indicated with blue nodes. Meanwhile, Figure 12(b) and 12(c) shows the attack graphs under GOOSE and network reconnaissance attacks. The anomalous communications are indicated with red nodes. The GOOSE attack is characterized by targeting specific nodes, which are linked to IEDs and compromised host, resulting in anomalous traffic patterns. During a reconnaissance attack, the attackers focus on targeting numerous hosts within the IP address ranges. As a result, a greater number of nodes exhibit anomalous behavior depicted with red, indicating the presence of anomalous OT traffic in the digital substation.

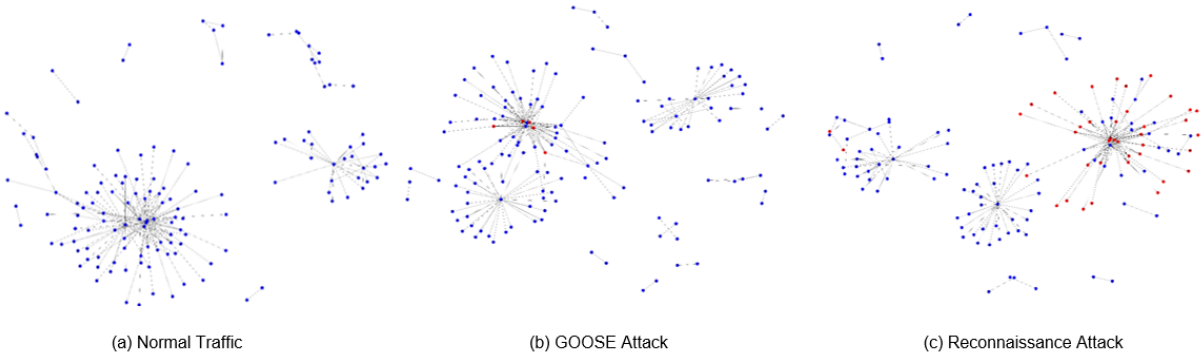


Fig. 12. Attack graph results for cyber attacks on digital substation.

6.2 Wide-Area OT Anomaly Detection with Attack Graphs

The monitoring of OT traffic over a wide area is facilitated by SDN using the architecture depicted in Figure 8. The traffic data is collected as spatial-temporal dataset in real-time. It serves as input for the hybrid deep learning model, which is used to generate attack graphs in near real-time. Figure 12 depicts the comprehensive attack graph map utilized for the purpose of identifying and visualizing online cyber attacks on the power grid, i.e., Distributed Denial of Service (DDoS) and network reconnaissance. The attack graph illustrates the OT network deployed in the CPS model of IEEE 39-bus comprising of 27 substations and one control center. The control center is depicted by a central node, while the remaining nodes situated at the edges represent the IEDs in substations. Table III shows nine different levels of cyber attack intensity with specific time duration. The DDoS attacks were executed with hping3 and network reconnaissance were executed with nmap. The cyber attacks last for a total of 345,000 seconds, and data is collected every second to generate the dataset.

TABLE III CYBER ATTACK SCENARIOS

Attack Type	Intensity	Tool	Time Duration (s)
DDoS	High	*hping3*	30,000
	Medium	*hping3*	30,000
	Low	*hping3*	30,000
Reconnaissance	Paranoid	*nmap*	75,000
	Sneaky	*nmap*	50,000
	Polite	*nmap*	40,000
	Normal	*nmap*	30,000
	Aggressive	*nmap*	30,000
	Insane	*nmap*	30,000

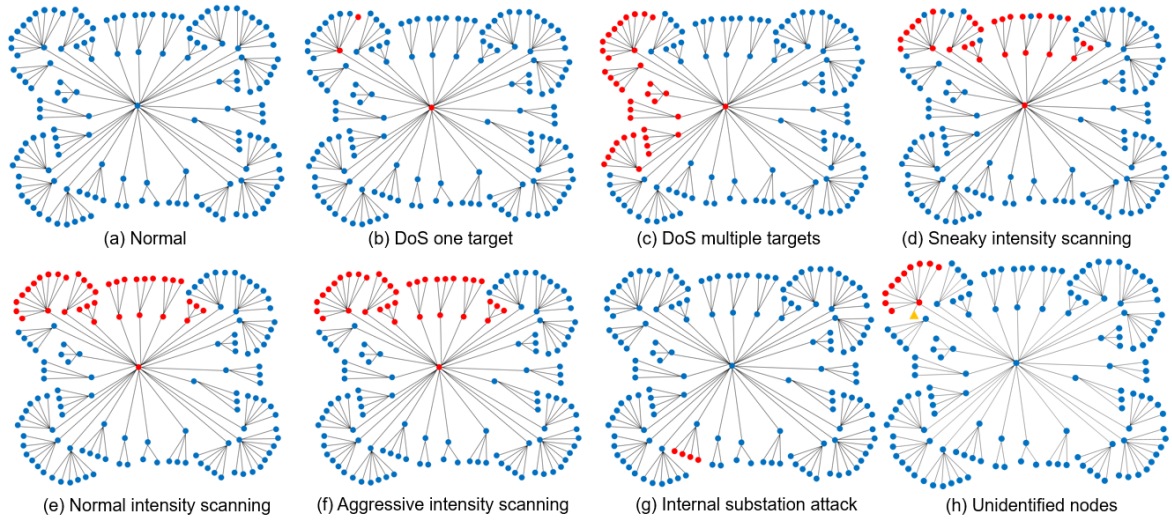


Fig. 13. Cyber attack location identification and visualization using attack graph maps.

Figure 13(a) depicts the attack graph in a normal state, where all nodes are represented with blue. Figure 13(b) and 13(c) illustrate the attack graph when subjected to a DDoS attack, both in a single target and multiple targets scenario. In Figure 13(b), DDoS targets a single node in substation number 7 and Figure 13(c) DDoS targets multiple nodes in substations 2-7. The DoS attacks are initiated from the control center. Consequently, the control center node, substation gateways, and nodes are exhibiting anomalous behavior indicated with red. Based on Figure 13(b) and 13(c), DDoS attacks can be classified with high accuracy using hybrid deep learning. The reason for this is that DDoS attacks generate a more significant traffic increase than normal.

The attack graphs under the reconnaissance attack are depicted in Figure 13(d), (e), and (f). The control center is the source of the attacks, which are specifically aimed at substation numbers 7 through 13. During both normal and aggressive scanning, all nodes located within the targeted substations are shown with red. However, under stealthy scanning intensities, some of the targeted nodes do not turn red. This occurrence can be attributed to a false negative generated by the traffic classifier. Notwithstanding the limitations, the CyResGrid methodology has already exhibited superior performance in comparison to state-of-the-art time series classification. Table IV presents a comparative analysis of the performance of CyResGrid and other TSC techniques, including ResNets

[114], Inception [104], FCN [115], and MLP [116]. As indicated by Table IV, the classifiers' performance declines in the event of stealthy attack scenarios. The reason for this phenomenon is that stealthy attacks produce a relatively minor impact on traffic anomalies. As a result, the classifier algorithm is likely to produce higher rates of False Negatives (FNs) and False Positives (FPs). Additionally, the outcomes generated by the classifier will result in reduced values for various performance metrics, including Area Under the Curve (AUC), True Negative (TN), True Positive (TP), Accuracy, F1, and G mean.

TABLE IV. PERFORMANCE COMPARISON OF ANOMALY DETECTION METHODS

No	Methods	AUC	TN	FP	FN	TP	Accuracy	F1	G mean	Time (s)
					Combined attack scenarios					
1	ResNet	0.849	82.27	11.32	3.49	2.92	85.19	28.29	15.50	633
2	Inception	0.961	93.50	0.20	4.10	2.31	95.71	51.76	14.68	976
3	FCN	0.955	88.16	5.43	3.92	2.49	90.65	34.76	14.81	1016
4	MLP	0.758	72.22	21.37	4.86	1.55	73.77	10.55	10.57	113
5	GC-LSTM + Resnet	0.974	93.29	0.31	3.27	3.14	96.42	63.77	17.12	1056
6	GC-LSTM + Inception	0.976	92.10	1.49	3.35	3.06	95.16	55.87	16.79	1409
7	GC-LSTM + FCN	0.972	92.28	1.30	3.68	2.73	95.01	52.26	15.87	1342
8	GC-LSTM + MLP	0.937	93.40	0.19	6.13	0.28	93.68	8.14	5.12	765
9	**CyResGrid**	**0.984**	**93.47**	**0.13**	**3.42**	**2.99**	**96.45**	**65.03**	**17.16**	**714**
					Stealthy attack scenarios					
10	ResNet	0.8637	86.94	12.02	0.96	0.08	87.02	1.26	2.69	91
11	Inception	0.9887	98.93	0.02	1.04	0.0004	98.93	0.09	0.22	224
12	FCN	0.9833	87.82	11.13	1.01	0.02	87.85	0.47	1.58	240
13	GC-LSTM + Resnet	0.9524	89.93	9.02	0.95	0.09	90.02	1.87	2.92	226
14	GC-LSTM + Inception	0.9489	89.96	8.99	0.95	0.10	90.05	1.87	2.92	303
15	GC-LSTM + FCN	0.9491	89.96	8.99	0.95	0.10	90.05	1.87	2.92	304
16	**CyResGrid**	**0.9243**	**91.15**	**7.81**	**0.94**	**0.111**	**91.25**	**2.32**	**3.08**	**138**

Figure 13(g) depicts a DDoS attack scenario originating from internal substation number 26. The internal substation was identified as the source of the attack, and it is noteworthy that the substation gateway and control center remain unaffected, as denoted by the blue nodes color. This scenario demonstrates that the attack graph has the capability to incorporate a wide-area network monitoring and identify localized anomalies within a substation. The network scanning aimed at substation 7 is depicted in Figure 13(h), wherein an unidentified node is observed to be the source of the activity, as denoted by an orange triangle. The origin of the attack is categorized as unidentified due to its absence from the lists of recognized nodes within the OT network.

7 Conclusions

Given the increasing risk of cyber attacks targeting power grids, strengthening attack detection capabilities in OT systems has become imperative. This chapter provides essential knowledge of cyber attack mitigation for cyber-physical power systems, i.e., secure communication protocols for operational technologies, penetration testing using cyber ranges and cyber-physical co-simulation, and network security controls including firewalls and intrusion detection and prevention systems. Amongst the wide-scope mitigation, AI is highlighted as an emerging solution. A hybrid deep learning model is presented that combines GC-LSTM and CNN for detecting anomalies in OT communication networks for power grids. The GC-LSTM algorithm predicts OT traffic based on the spatial and temporal characteristics of the input data. By means of its forecasting capabilities, the data's variability and outliers are mitigated. The utilization of GC-LSTM can enhance the efficacy of TSCs in detecting anomalies. Unlike traditional signature and supervised learning-based intrusion detection, the hybrid deep learning anomaly detection utilizes the OT traffic throughput. It takes advantage of the OT traffic deterministic and homogenous characteristics to provide robust and flexible anomaly detection for a wide scope of cyber attacks at early stages of the cyber kill chain. The traffic anomalies are incorporated into an attack graph that aids power system operators identify and localize anomalies of active attacks on power systems in near real-time. Cyber attack case studies and cyber-physical co-simulation results are provided to demonstrate the efficiency of hybrid deep learning for anomaly detection in power grid OT networks.

Acknowledgements

This work was supported by the Designing Systems for Informed Resilience Engineering (DeSIRE) program of the 4TU Center for Resilience Engineering (4TU.RE) and the EU H2020 project, ERIGrid 2.0 with Grant Agreement Number 870620. DeSIRE is funded by the 4TU-program High Tech for a Sustainable Future (HTSF). 4TU is the federation of the four technical universities in the Netherlands.

List of Acronyms

AI	Artificial Intelligence
APDU	Application Protocol Data Unit
AUC	Area Under the Curve
CIA	Confidentiality, Integrity, and Availability
DCS	Distributed Control System
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
DPI	Deep Packet Inspection
FDI	False Data Injection
FN	False Negative
FP	False Positive
GC-LSTM	Graph Convolutional Long Short-Term Memory
GCN	Graph Convolutional Network
GNN	Graph Neural Network
GOOSE	Generic Object Oriented Substation Event
HIL	Hardware-in-the-Loop
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control System
IDPS	Intrusion Detection System and Prevention System
IED	Intelligent Electronic Device
IoT	Internet of Things
IT	Information Technology
LSTM	Long-Short Term Memory
MITM	Man-in-the-Middle
NGF	Next-Generation Firewall
OPC-UA	Open Platform Communication-Unified Architecture
OSI	Open Systems Interconnection
OSINT	Open Source Intelligence
OT	Operational Technology
PPDU	Presentation Protocol Data Unit
RNN	Recurrent Neural Network
RTDS	Real-Time Digital Simulator
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SPDU	Session Protocol Data Unit
SV	Sample Value
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

TN	True Negative
TP	True Positive
TPDU	Transport Protocol Data Unit
TSC	Time Series Classification
VM	Virtual Machine

References:

[1] D. E. Whitehead, K. Owens, D. Gammel and J. Smith, "Ukraine cyber-induced power outage: analysis and practical mitigation strategies," in Proc. Int. Conf. for Prot. Relay Engineers, Texas, USA, Apr. 2017, pp. 1-8.

[2] M. J. Assante, R. M. Lee, and T. Conway, "ICS defense use case no. 6: modular ICS malware," Electricity Information Sharing Center (E-ISAC) Tech. Report, pp. 1-27, vol. 2, no. 1, Aug. 2017.

[3] ENISA, "Communication network dependencies for ICS/SCADA Systems," Feb. 2017. Accessed on: Jun. 27, 2023. [Online]. Available: enisa.europa.eu/publications/ics-scada-dependencies

[4] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," IEEE Comm. Surv. Tutorials, vol. 19, no. 1, pp. 446–464, Nov. 2016.

[5] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," Int. J. Electr. Power Energy Syst., vol. 99, pp. 45–56, Jul. 2018.

[6] B. B. Gupta and T. Akhtar, "A survey on smart power grid: frameworks, tools, security issues, and solutions," Annals of Telecommunications, vol. 72, no. 9, pp. 517-549, Oct. 2017.

[7] J. Montoya et al., "Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: a survey of smart grid international research facility network activities," Energies, vol. 13, no. 12, p. 3267, Jan. 2020.

[8] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, "A review of false data injection attacks against modern power systems," IEEE Trans. on Smart Grid, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[9] R. Deng, G. Xiao, R. Lu, H. Liang and A. V. Vasilakos, "False data injection on state estimation in power systems attacks, impacts, and defense: a survey," IEEE Trans. Ind. Inform., vol. 13, no. 2, pp. 411–423, Apr. 2017.

[10] A. S. Musleh, G. Chen and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," IEEE Trans. Smart Grid, vol. 11, no. 3, pp. 2218–2234, May 2020.

[11] H. T. Reda, A. Anwar and A. Mahmood, "Comprehensive survey and taxonomies of false injection attacks in smart grid: attack models, targets, and impacts," Renew. Sustain. Energy Rev., vol. 163, no. 112423, pp. 1-24, Jul. 2022.

[12] A. Sayghe et al., "Survey of machine learning methods for detecting false data injection attacks in power system," IET Smart Grid, vol. 3, no.5, pp. 581-595, Oct. 2020.

[13] H. Zhang, B. Liu and H. Wu, "Smart grid cyber-physical attack and defense: a review," IEEE Access, vol. 9, pp. 29641–29659, Feb. 2021.

[14] SANS ICS, "White analysis of the cyber attack on the ukrainian power grid," Electricity Information Sharing Center (E-ISAC) Tech. Report, pp. 1-29, vol. 388, no. 1, Mar. 2016.

[15] Securicon, "What's the difference between OT, ICS, SCADA and DCS?," May. 2019. Accessed on: Jun. 23, 2023. [Online]. Available: https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

[16] A. Hahn, "Operational technology and information technology in industrial control systems" in Cyber-Security of SCADA and Other Industrial Control Systems., Berlin, Germany: Springer, pp. 51-68, 2016.

[17] A. Ginter, Secure Operations Technology. Abterra Technologies Incorporated, 2018.

[18] R. Amoah, S. Camtepe, and E. Foo, "Formal modelling and analysis of DNP3 secure authentication," J. Netw. Comput. Appl., vol. 59, pp. 345–360, Jan. 2016.

[19] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 broadcast vommunications in SCADA systems," IEEE Trans. Ind. Inform., vol. 12, no. 4, pp. 1474–1485, Jul. 2016.

[20] E.D. Knapp, and J.T. Langill. Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems, Syngress, 2014.

[21] M. K. Ferst, H. F. M. De Figueiredo, G. Denardin, and J. Lopes, "Implementation of secure communication with modbus and transport layer security protocols," in Proc. IEEE Int. Conf. Ind. Appl., Sao Paulo, Brazil, 2018, pp. 155–162.

[22] S. M. S. Hussain, T. S. Ustun and A. Kalam, "A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges," IEEE Trans. on Indus. Inform., vol. 16, no. 9, pp. 5643-5654, Sept. 2020.
[23] A. Rezai, P. Keshavarzi, and Z. Moravej, “Key management issue in SCADA networks: A review,” Eng. Sci. Technol. an Int. J., vol. 20, no. 1, pp. 354–363, Feb. 2017.
[24] P. T. C., K. G. Boroojeni, M. Hadi Amini, N. R. Sunitha, and S. S. Iyengar, “Key pre-distribution scheme with join leave support for SCADA systems,” Int. J. Crit. Infrastruct. Prot., vol. 24, pp. 111–125, Mar. 2019.
[25] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: a survey," Int. J. of Web and Grid Ser., vol. 14, no. 4, pp. 352-375, Oct. 2018.
[26] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, “Blockchain in smart grids: a review on different use cases,” Sensors, vol. 19, no. 22, pp. 1–25, Jan. 2019.
[27] R. Brandão, “A blockchain-based protocol for message exchange in a ICS network: student research abstract,” in Proc. ACM Symp. Appl. Comput., Brno, Czech, 2020, pp. 357–360.
[28] A. Carcano, A. Di Pinto, Y. Dragoni, and A. Carcano, “The future of securing intelligent electronic devices using the IEC 62351-7 standard for monitoring,” in Proc Black Hat USA, Las Vegas, USA, 2019, pp. 1-21.
[29] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, “A survey on smart grid cyber-physical system testbeds,” IEEE Commun. Surv. Tutorials, vol. 19, no. 1, pp. 446–464, Nov. 2016.
[30] C. C. Sun, A. Hahn, and C. C. Liu, “Cyber security of a power grid: State-of-the-art,” Int. J. Electr. Power Energy Syst., vol. 99, pp. 45–56, Jul. 2018.
[31] B. B. Gupta and T. Akhtar, “A survey on smart power grid: frameworks, tools, security issues, and solutions,” Annals of Telecommunications, vol. 72, no. 9, pp. 517-549, Oct. 2017.
[32] M. Z. Gunduz and R. Das, “A comparison of cyber-security oriented testbeds for IoT-based smart grids,” in Int. Symp. Digit. Forensic Secur., Antalya, Turkey, 2018, pp. 1–6.
[33] J. Montoya et al., “Advanced laboratory testing methods using real-time simulation and hardware-in-the-loop techniques: a survey of smart grid international research facility network activities,” Energies, vol. 13, no. 12, p. 3267, Jan. 2020.
[34] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in Inn. Smart Grid Tech., Anheim, USA, 2011, pp. 1-7.
[35] C. Queiroz, A. Mahmood and Z. Tari, "SCADASim a framework for building SCADA simulations," IEEE Trans. on Smart Grid, vol. 2, no. 4, pp. 589-597, Sep. 2011
[36] V. Sarker, et al., “Cyber-Physical Security and Resiliency Analysis Testbed for critical microgrids with IEEE 2030.5,” in Work. on Mode. and Sim. of Cyber-Physical Energy Systems, Sydney, Australia, 2020, pp. 1-6.
[37] J. Mirkovic and T. Benzel, “Teaching cybersecurity with DeterLab,” IEEE Secur. Priv., vol. 10, no. 1, pp. 73–76, Feb. 2012.
[38] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S. Schwab, “The DETER project: advancing the science of cyber security experimentation and test,” in IEEE Int. Conf. Technol. Homel. Secur., Waltham, USA, 2010, pp. 1–7.
[39] I. A. Oyewumi et al., “ISAAC: the idaho CPS smart grid cybersecurity testbed,” in IEEE Texas Power Energy Conf., College Station, USA, 2019, pp. 1-6.
[40] J. Johnson, I. Onunkwo, P. Codeiro, B. Wright, N. Jacobs, and C. Lai, “Assessing DER network cybersecurity defences in a power-communication co-simulation environment,” IET Cyber-Physical Syst. Theory Appl., pp. 1–11, Oct. 2020.
[41] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, “A testbed for analyzing security of SCADA control systems (TASSCS),” in Proc. IEEE PES Innov. Smart Grid Tech. Conf., Anheim, USA, 2011, pp. 1–7.
[42] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, “Implementing a real-time cyber-physical system test bed in RTDS and OPNET,” in North Am. Power Symp., Pullman, USA, 2014, pp. 1–6.
[43] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed,” in Proc. IEEE Int. Work. Tech. Comm. Commun. Qual. Reliab., Charleston, USA, 2015, pp. 1-6.
[44] C. Queiroz, A. Mahmood and Z. Tari, "SCADASim a framework for building SCADA simulations," IEEE Trans. on Smart Grid, vol. 2, no. 4, pp. 589-597, Sep. 2011.
[45] A. Allaoua, T. M. Layadi, I. Colak and K. Rouabah, "Design and simulation of smart-grids using OMNeT++/matlab-simulink co-simulator," in Int. Conf. on Ren. Energy Research and Appl., Istanbul,

Turkey, 2021, pp. 141-145.
[46] C. B. Vellaithurai, S. S. Biswas, and A. K. Srivastava, “Development and application of a real-time test bed for cyber–physical system,” IEEE Syst. J., vol. 11, no. 4, pp.2192–2203, Nov. 2015.
[47] J. Watada, A. Roy, R. Kadikar, H. Pham, and B. Xu, “Emerging trends, techniques and open issues of containerization: a review,” IEEE Access, vol. 7, pp. 152443–152472, Oct. 2019.
[48] M.M. Yamin, B. Katt, V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” Computers & Security, vol. 88, no. 101636, Jan. 2020.
[49] Y. Diogenes and E. Ozkaya, Cybersecurity, attack and defense strategies infrastructure security with Red Team and Blue Team tactics. Birmingham Packt Publishing, 2018.
[50] J. Nivethan and M. Papa, “A Linux-based firewall for the DNP3 protocol,” in IEEE Symp. Technol. Homel. Secur., Waltham, USA, 2016, pp. 1–5.
[51] J. Nivethan and M. Papa, “On the use of open-source firewalls in ICS/SCADA systems,” Inf. Secur. J., vol. 25, no. 1–3, pp. 83–93, Apr. 2016.
[52] D. Li, H. Guo, J. Zhou, L. Zhou, and J. W. Wong, “SCADAWall: a CPI-enabled firewall model for SCADA security,” Comput. Secur., vol. 80, pp. 134–154, Jan. 2019.
[53] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, “Intrusion detection system for IEC 60870-5-104 based SCADA networks,” in IEEE Power Energy Soc. Gen. Meet., Vancouver, Canada, 2013, pp. 1-5.
[54] J. Chromik, A. Remke, B. R. Haverkort, and G. Geist, “A parser for deep packet inspection of IEC-104: a practical solution for industrial applications,” in Proc. IEEE/IFIP Int. Conf. Dependable Syst. Networks Ind. Track, Portland, USA, 2019, pp. 5–8.
[55] R. Sommer, J. Amann, and S. Hall, “Spicy: a unified deep packet inspection framework for safely dissecting all your data,” in ACM Int. Conf. Proc. Ser., Los Angles, USA, 2016, pp. 558–569.
[56] T. Cruz et al., “A cybersecurity detection framework for supervisory control and data acquisition systems,” IEEE Trans. Ind. Informatics, vol. 12, no. 6, pp. 2236–2246, Aug. 2016.
[57] S. Pan, T. Morris, and U. Adhikari, “A specification-based intrusion detection framework for cyber-physical environment in electric power system,” Int. J. Netw. Secur., vol. 17, no. 2, pp. 174–188, Mar. 2015.
[58] P. Maynard and K. McLaughlin, “Towards understanding man-on-the-side Attacks (MotS) in SCADA networks,” arXiv: 2004.14334, pp. 1-9, Apr. 2020.
[59] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, and H. F. Wang, “Rule-based intrusion detection system for SCADA networks,” in IET Conf. Publ., Beijing, China, 2013, pp. 8–11.
[60] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParland, and A. Scaglione, “A hybrid network IDS for protective digital relays in the power transmission grid,” in IEEE Int. Conf. Smart Grid Commun. SmartGridComm, Venice, Italy, 2014, pp. 908–913.
[61] N. Goldenberg and A. Wool, “Accurate modeling of modbus/TCP for intrusion detection in SCADA systems,” Int. J. Crit. Infrastruct. Prot., vol. 6, no. 2, pp. 63–75, Jun. 2013.
[62] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. Alghamdi, and A. Y. Zomaya, “An efficient data-driven clustering technique to detect attacks in SCADA systems,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 5, pp. 893–906, Dec. 2015.
[63] N. Erez and A. Wool, “Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems,” Int. J. Crit. Infrastruct. Prot., vol. 10, pp. 59–70, Sep. 2015.
[64] H. Lin, A. Slagell, Z. Kalbarczyk, and R. K. Iyer, “Semantic security analysis of scada networks to detect malicious control commands in power grids (poster),” in ACM Int. Conf. Proceeding Ser., Glasglow, UK, 2014, pp. 492–495.
[65] A. Kleinmann and A. Wool, “Automatic construction of statechart-based anomaly detection models for multi-threaded industrial control systems,” ACM Trans. Intell. Syst. Technol., vol. 8, no. 4, pp. 1–21, Feb. 2017.
[66] O. Koucham, S. Mocanu, G. Hiet, J. M. Thiriet, and F. Majorczyk, “Efficient mining of temporal safety properties for intrusion detection in industrial control systems,” IFAC-PapersOnLine, vol. 51, no. 24, pp. 1043–1050, Jan. 2018.
[67] H. Lahza, K. Radke, and E. Foo, “Applying domain-specific knowledge to construct features for detecting distributed denial-of-service attacks on the GOOSE and MMS protocols,” Int. J. Crit. Infrastruct. Prot., vol. 20, pp. 48–67, Mar. 2018.
[68] I. E. C. S. Networks, “Multidimensional intrusion detection system for IEC 61850-based SCADA networks,” IEEE Trans. Power Deliv., vol. 32, no. 2, pp. 1068–1078, Aug. 2016.

[69] H. Yoo and T. Shon, “Novel approach for detecting network anomalies for dubstation sutomation based on IEC 61850,” Multimed. Tools Appl., vol. 74, no. 1, pp. 303–318, Jan. 2014.
[70] S. Pan, T. Morris, and U. Adhikari, “Developing a hybrid intrusion detection system using data mining for power dystems,” IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 3104–3113, Mar. 2015.
[71] L. Reuter, O. Jung, and J. Magin, “Neural network based anomaly detection for SCADA systems,” in Conf. Innov. Clouds, Internet Networks Work., Paris, France, 2020, pp. 194–201.
[72] S. P. and V. S. S. S. P. S. Chaithanya, S. Priyanga, “SSO-IF: an outlier detection approach for intrusion detection in SCADA systems,” in Inventive Communication and Computational Technologies, Singapore: Springer, 2020, pp. 921-929.
[73] L. Maglaras, T. Cruz, M. A. Ferrag, and H. Janicke, “Teaching the process of building an intrusion detection system using data from a small-scale SCADA testbed,” Internet Technol. Lett., vol. 3, no. 1, p. e132, Jan. 2020.
[74] M. Kalech, “Cyber-attack detection in SCADA systems using temporal pattern recognition techniques,” Comput. Secur., vol. 84, pp. 225–238, Jul. 2019.
[75] S. Selvarajan, M. Shaik, S. Ameerjohn, and S. Kannan, “Mining of intrusion attack in SCADA network using clustering and genetically seeded flora-based optimal classification algorithm,” IET Inf. Secur., vol. 14, no. 1, pp. 1–11, Dec. 2020.
[76] A. Derhab et al., “Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security,” Sensors (Switzerland), vol. 19, no. 14, pp. 1–24, Jan. 2019.
[77] S. Tamy, H. Belhadaoui, M. A. Rabbah, N. Rabbah, and M. Rifi, “An evaluation of machine learning algorithms to detect attacks in SCADA network,” in Mediterr. Congr. Telecommun., Fez, Morocco, 2019, pp. 1-5.
[78] J. Suaboot et al., “A taxonomy of supervised learning for IDSs in SCADA environments,” ACM Comput. Surv., vol. 53, no. 2, Apr. 2020.
[79] M. Al-Asiri and E. S. M. El-Alfy, “On using physical based intrusion detection in SCADA systems,” Procedia Comput. Sci., vol. 170, pp. 34–42, Jan. 2020.
[80] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, “Hml-ids: a hybrid-multilevel anomaly prediction approach for intrusion detection in scada systems,” IEEE Access, vol. 7, pp. 89507–89521, Jul. 2019.
[81] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren, “Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks,” Appl. Soft Comput. J., vol. 71, pp. 66–77, Oct. 2018.
[82] R. S. N. Neha, S. Priyanga, Suresh Seshan and and V. S. S. Sriram, “SCO-RNN: a behavioral-based intrusion detection approach for cyber physical attacks in SCADA systems,” in Lecture Notes in Networks and Systems, Singapore: Springer, 2020, pp. 911–919.
[83] G. Zizzo, C. Hankin, S. Maffeis, and K. Jones, “Intrusion detection for industrial control systems: evaluation analysis and adversarial attacks,” arXiv: 1911.04278, pp. 1-12, Nov. 2019.
[84] J. Gao et al., “LSTM for SCADA intrusion detection,” in IEEE Pacific Rim Conf. Comm. Comp. Sig. Proc., Victoria, Canada, 2019, pp. 1–4.
[85] J. Gao et al., “Omni SCADA intrusion detection using deep learning algorithms,” IEEE Internet Things J., vol. 8, no.2, pp. 951-961, Jul. 2020.
[86] M. Ahsan and K. Nygard, “Convolutional neural networks with LSTM for intrusion detection,” in CATA, San Fransisco, USA, 2020, pp. 69–57.
[87] T.-Y. Kim and S.-B. Cho, “CNN-LSTM neural networks for anomalous database intrusion detection in RBAC-administered model,” in Int. Conf. on Neural Information Processing, Sydney, Australia, 2019, pp. 131–139.
[88] K. Praanna, S. V. P. Sruthi, K. V Kalyani, and A. S. Tejaswi, “A CNN-LSTM model for intrusion detection system from high dimensional data,” J. of Inf. and Comp. Science, vol. 10, no. 3, pp. 1362–1370, Mar. 2020.
[89] C. Lin and S. Nadjm-tehrani, “Timing patterns and correlations in spontaneous SCADA traffic for anomaly detection,” in Int. Sym. on Research in Attacks, Intrusions and Defenses (RAID), Beijing, China, 2019, pp. 73–88.
[90] J. L. Rrushi and R. H. Campbell, “Detecting attacks in power plant interfacing substations through probabilistic validation of attack - effect bindings,” in Proc. SCADA Secur. Sci. Symp., 2008, pp. 1–24.
[91] H. Yang, L. Cheng, and M. C. Chuah, “Deep-learning-based network intrusion detection for SCADA systems,” in IEEE Conf. Commun. Netw. Secur., Washington, USA, 2019, pp. 1-7.
[92] M. Altaha, J.-M. Lee, M. Aslam, and S. Hong, “Network intrusion detection based on deep neural networks

for the SCADA system," J. Phys. Conf. Ser., vol. 1585, p. 012038, Jul. 2020.
[93] A. Khraisat, I. Gondal, P. Vamplew and J. Kamaruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, pp. 1-22, Dec. 2019.
[94] H. Liu and B. Lang, "Machine learning and deep learning methods for intrusion detection systems: a survey," Appl. Sci., vol. 9, no. 20, pp.1-28, Oct. 2019.
[95] A. Aldweesh, A. Derham and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues," Knowledge-Based Syst., vol. 189, no. 105124, pp. 1-19, Feb. 2020.
[96] P. Mishra, V. Varadharajan, U. Tupakula and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," IEEE Comm. Surv. & Tutor,, vol. 21, no. 1, pp. 686-728, Jun. 2018.
[97] R. Barbosa, R. Sadre and A. Pras, "Difficulties in modeling SCADA traffic: a comparative analysis," in Proc. Passive and Active Measure., Berlin, Germany, Mar. 2012, pp. 126-135.
[98] X. Guan, T. Qin, W. Li and P. Wang, "Dynamic feature analysis and measurement for large-scale network traffic monitoring," IEEE Trans. Inf. For. Sec., vol. 5, no. 4, pp. 905–919, Dec. 2010.
[99] A. Kind, M. P. Stoecklin and X. Dimitropoulos, "Histogram-based traffic anomaly detection," IEEE Trans. Netw. Serv. Manag., vol. 6, no. 2, pp. 110–121, Jun. 2009.
[100] K. Xu, Z. L. Zhang and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," IEEE ACM Trans. Net., vol. 16, no. 6, pp. 1241–1252, Dec. 2008.
[101] H. Wu, "A survey of research on anomaly detection for time series," in Proc. 13th Int. Compt. Conf. on Wav. Act. Med. Tech. and Inf. Proc. (ICCWAMTIP), Chengdu, China, Dec. 2016, pp. 426-431
[102] K. Shaukat et al., "A review of time-series anomaly detection techniques: a step to future perspectives," in Proc. Future of Information and Communication Conf., Vancouver, Canada, Apr. 2021, pp. 865-877.
[103] I. Fawaz, G. Forestier, J. Weber, L. Idoumghar and P. Muller, "Deep learning for time series classification: a review," Data Mining and Knowledge Discovery, vol. 33, no. 4, pp. 917-963, Jul. 2019.
[104] I. Fawaz et al., "Inceptiontime: finding alexnet for time series classification," Data Mining and Knowledge Discovery, vol. 34, no. 6., pp. 1936-1962, Sep. 2020.
[105] W. Lin, D. Wu and B. Boulet, "Spatial-temporal residential short-term load forecasting via graph neural networks," IEEE. Trans. on Smart Grid, vol. 12, no. 6, pp. 5373-5384, Nov. 2021.
[106] O. Boyaci, M. R. Narimani, K. R. Davis, M. Ismail, T. J. Overbye and E. Serpedin, "Joint Detection and Localization of Stealth False Data Injection Attacks in Smart Grids Using Graph Neural Networks," IEEE Trans. on Smart Grid, vol. 13, no. 1, pp. 807-819, Jan. 2022
[107] Z. Cui, K. Henrickson, R. Ke and Y. Wang, "Traffic graph convolutional recurrent neural network: a deep learning framework for network-scale traffic learning and forecasting," IEEE Trans. on Intel. Transp. Sys., vol. 21, no. 11, pp. 4883-4894, Nov. 2020.
[108] L. Deng, D. Lian, Z. Huang and E. Chen, "Graph convolutional adversarial networks for spatiotemporal anomaly detection," IEEE Trans. on Neur. Net. and Learn. Sys., vol. 33, no. 6, pp. 2416-2428, Jun. 2022.
[109] A. Presekal, A. Ştefanov, V. S. Rajkumar and P. Palensky, "Attack Graph Model for Cyber-Physical Power Systems using Hybrid Deep Learning," IEEE Transactions on Smart Grid, early access.
[110] J. Chen, X. Wang, and X. Xu, "GC-LSTM: graph convolution embedded LSTM for dynamic link prediction," Applied Intelligence, pp. 1-16, Sep. 2021.
[111] J. Snoek, H. Larochelle, and R. Adams, "Practical bayesian optimization of machine learning algorithms," Adv. in Neu. Infor. Proc. Sys., vol. 25, pp. 1-9, Dec. 2012.
[112] V. S. Rajkumar, M. Tealane, A. Ştefanov and P. Palensky, "Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis," in Proc. 8th Work. on Mod. and Simu. of Cy.-Phy. En. Sys., Sydney, NSW, Australia, 2020.
[113] V. S. Rajkumar, M. Tealane, A. Ştefanov, A. Presekal and P. Palensky, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in Proc. ISGT-Europe, The Hague, Netherlands, 2020, pp. 247-254.
[114] K. He, X. Zhang, S. Ren and J. Sun, "Deep residual learning for image recognition," in Proc. of the IEEE Conf. on Comp. Vis. and Pat. Recog., Las Vegas, USA, Jun. 2016, pp. 770-778.
[115] J. Long, E. Shelhamer and T. Darrell, "Fully convolutional networks for semantic segmentation," in Proc. of the IEEE Conf. on Comp. Vis. and Pat. Recog., Boston USA, Jun. 2015, pp. 3431-3440
[116] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436-444, May 2015.