Received: 20 November 2020 | Revised: 14 April 2021 | Accepted: 24 May 2021 | IET Cyber-Physical Systems: Theory & Applications

DOI: 10.1049/cps2.12018

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems

Abhijeet Sahu[1] | Patrick Wlazlo[2] | Zeyu Mao[1] | Hao Huang[1] | Ana Goulart[2] | Katherine Davis[1] | Saman Zonouz[3]

[1]Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA

[2]Electronic Systems Engineering Technology, Texas A&M University, College Station, TX, USA

[3]Electrical and Computer Engineering, Rutgers University, New Brunswick, NJ, USA

Correspondence

Abhijeet Sahu, Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA.
Email: abhijeet_ntpc@tamu.edu

Funding information

U.S. Department of Energy, Grant/Award Number: DE-OE0000895

Abstract

A power system is a complex cyber-physical system whose security is critical to its function. A major challenge is to model, analyse and visualise the communication backbone of the power systems concerning cyber threats. To achieve this, the design and evaluation of a cyber-physical power system (CPPS) testbed called Resilient Energy Systems Lab (RESLab) are presented to capture realistic cyber, physical, and protection system features. RESLab is architected to be a fundamental platform for studying and improving the resilience of complex CPPS to cyber threats. The cyber network is emulated using Common Open Research Emulator (CORE), which acts as a gateway for the physical and protection devices to communicate. The physical grid is simulated in the dynamic time frame using Power World Dynamic Studio (PWDS). The protection components are modelled with both PWDS and physical devices including the SEL Real-Time Automation Controller (RTAC). Distributed Network Protocol 3 (DNP3) is used to monitor and control the grid. Then, the design is exemplified and the tools are validated. This work presents four case studies on cyberattack and defence using RESLab, where we demonstrate false data and command injection using Man-in-the-Middle and Denial of Service attacks and validate them on a large-scale synthetic electric grid.

1 | INTRODUCTION

The electric grid is transitioning to a smarter grid that employs advanced communication technologies. With advanced computing and communications, cyber-security has proven to be a critical issue in power transmission, generation, and distribution systems. Cyber adversaries can modify or create data that can impact the grid's normal operation and potentially destabilise its operating point causing cascading failures. Earlier this year, an unidentified threat successfully compromised the administrative systems of the European Network of Transmission System Operators for Electricity (ENTSO-E), with the potential to compromise 42 transmission system operators (TSOs) across 35 member states in Europe [1]. Other attacks are also widely known such as the Ukraine attacks [2], where an attacker targeted three distribution units to cause a power outage after intruding into the Supervisory Control and Data Acquisition (SCADA) system. Attacks like Pivnichna [3] caused a power outage, while Stuxnet [4] allowed control of programmable logic controllers (PLCs), by overspeeding the centrifuges in a nuclear plant.

It is necessary to propose defence mechanisms for such zero-day attacks. The use of firewalls, intrusion detection systems, and intrusion prevention systems is important, but these tools may not work efficiently on stealthy coordinated attacks. Hence, we need to employ the latest tools and techniques to make solutions that are more intelligent and capable of detecting complex attacks. Machine learning, including deep learning or even artificial intelligence, offers advantages that can aid cyber and physical attack detection and localisation. These techniques are data-intensive, as more data provides a better solution. One way to generate those real-time datasets is to mimic those attacks and detect them using data-centric Intrusion Detection Systems (IDS) solutions using a testbed.

This work presents our Resilient Energy Systems Laboratory (RESLab) testbed that forms an environment for researchers and stakeholders to understand the impact of cyberattacks and validate their defences. RESLab provides a platform to evaluate how the power and communication networks perform together based on real-world systems and events, including communication protocols, operations, and latency requirements. It allows other researchers to develop and test intrusion detection tools for defending and mitigating real cyber attacks. The purpose is to enable studies to make cyber-physical power systems more resilient to cyberattacks.

The contributions of this work are to (1) introduce RESLab, a cyber-physical power system testbed that is a mix of emulators, simulators, and real devices designed to study resilience problems and solutions in large-scale power systems; (2) provide a platform for data collection, visualisation, evaluation, and defence against multi-stage cyber threats to the power system; (3) model realistic data flows in RESLab using a large-scale exemplar power system to implement and validate scenarios impacting grid resilience; (4) demonstrate the implementation of Denial of Service (DoS) and variants, based on stealthiness, false data and command injection attacks causing impact to different areas of a large-scale grid; (5) analyse attack practicality of the use cases and validate them with queueing theory; (6) develop a next-generation Energy Management System (EMS) software with the focus on visualising and performing data fusion based on real-time alerts in RESLab.

This work is organised as follows: In Section 2, we briefly review other testbeds and motivate the need for RESLab. Section 3 presents the architecture and components of RESLab. The threat model for this work is presented in Section 4. Section 5 demonstrates its implementation in RESLab with four use cases. Then, we present the analysis of the attacks and their impacts on the physical system. The results are analysed in Section 6.

2 | CYBER-PHYSICAL POWER SYSTEM TESTBEDS

Significant work occurs in developing cyber-physical testbeds. This section provides context about where RESLab fits in with respect to other power system cyber-physical testbeds described in the literature. It is important to recognise that testbeds change continually with use, and this may not be publicly documented. Hence, our perspective below highlights the motivations and needs that drove us in the design and creation of RESLab.

We review testbeds that focus on investigating the vulnerability of power critical infrastructure, including their challenges and limitations. Previous works range from applications in wide-area protection and monitoring in transmission and generation to distributed energy resources (DERs), microgrids and distribution systems, and to operation domains such as Energy Management Systems (EMS) and Distribution Management Systems (DMS).

2.1 | Testbeds and platforms

A cyber-physical testbed architecture is implemented by networking together simulators, emulators, and hardware. The quality of a cyber-physical testbed is measured by its success in advancing the research and applications it supports. It includes a platform-enabling communication between components, a system for data collection, aggregation, visualisation, and a way of executing and evaluating cyber security incidents against the system under study. Cyber-physical power system testbeds are presented in Table 1 based on their components (e.g. power and cyber simulators, software, devices), supported protocols, power system level(s), and intrusion experiments.

Testbed efforts in [5–10] focus on evaluating the impact for physical use cases (e.g., cyberattacks on power flows, loss of load or synchronism, protection systems, and microgrids) while using networking hardware. Some testbeds [11–15] use network simulators to demonstrate the behaviour of the network, while others use emulators to replicate its behaviour. Minimega [16] and SCEPTRE [17] by Sandia National Laboratories provide a platform for large-scale virtualisation and emulation, respectively, of industrial control systems (ICS). HELICS [18] from the National Renewable Energy Laboratory provides a large-scale co-simulation platform that integrates discrete-event simulators such as NS-3 and time-series simulations such as for power flows. Some testbeds [11, 15, 19] provide features to integrate external devices or virtual machines (VMs) to simulators, but these are challenging to scale to large systems.

Power system simulators such as a real-time digital simulator (RTDS), OpalRT, or Typhoon have been used in several testbeds [6–8, 10, 11, 20–24] to mimic the power system with high-fidelity, but these are resource-intensive for simulating large-scale systems. For example, each chassis of RTDS with five cores can run a maximum of 100 buses [25]. These hardware solutions are essential for experiments where fast dynamics are important, for example, electromagnetic transients, power electronics, DERs, or microgrids.

Testbed efforts in [12, 20, 26–31] implement cyber intrusions such as MiTM. MiTM attacks can be performed in different ways such as address resolution protocol (ARP) cache poisoning, Internet protocol (IP) spoofing, or hypertext transfer protocol (HTTP) session hijacking, but this is not always presented. Testbeds such as [11, 32] use frameworks like Ettercap or Metasploit but have limitations in goal-oriented MiTM cyberattacks (e.g., attacks that require a dedicated protocol parser and database to store historical values for a larger grid, or stealthy attacks that need coordination to modify a set of measurements from different locations).

2.2 | Criteria for design decisions

RESLab is comprised of simulators, emulators, and virtualisation, while providing additional features that improve upon six major metrics: scalability, orchestration capability, data collection and fusion, fidelity, cyber threat realism, hardware-in-the-loop (HIL) support etc. These form the basis for the

TABLE 1 Review of cyber-physical power system testbeds based on the components, ICS protocols, system level(s), and intrusion experiments

Ref	Components	ICS Protocols	System Level	Intrusion Expt.
[20]	RTDS, relays, IEDs, gateway	IEC 61850	Substation	No
[21]	RTDS, NS-3/DeterLab, PMUs, phasor data concentrator (PDC), GPS clock	PMU/C37.118	Transmission	DoS, MiTM
[22]	RTDS, Opal-RT, wide area communication emulator, PMUs, SDN, RTAC, PDC, industry-grade SCADA	C37.118	Transmission	MiTM
[5, 6]	RTDS, real Network/SDN, PMU, PDC, relay, industry software from SEL, GE, snort, Wireshark	MODBUS/TCP, IEEE C37.118		Aurora, DoS
[26]	Typhoon HIL 602, DSP, FPGA, SunSpec system validation platform, inverter and converter	IEC 61850	Distribution, DER	No
[29]	Power world DS, wide area communication emulation, NI CRIO, SEL 421, SEL 651R, SEL 734B	DNP3 and GOOSE	Transmission	No
[11]	RTDS, opnet, LibModbus, OPNET, RTLAB	MODBUS	Transmission	MiTM
[10]	RTDS, SDN based switch, firewall, self-developed SCANVILLE, RADICL	IEC C37.118, IEC 61850, DNP3	No specific use case	RADICL for cyberattacks
[13]	PowerWorld, MATLAB, RT-LAB, OP5600, OPNET	Modbus- RSIm	No specific use case	DoS (compromised HMI), SYN ACK flooding
[46]	PowerWorld, RINSE(network emulator)	MODBUS-TCP	Transmission	DDoS attack
[14]	OPAL-RT, No cyber simulator or emulator, Labview CRIO, OSIsoft's PI-Server	DNP3 and MODBUS, C37.118	No	No
[30]	OPAL RT and Typhoon HIL, Xilinx Virtex 6 FPGAs		Microgrid, generator control	No
RESLab	PowerWorld DS, CORE, RTAC, snort, Packetbeat, OpenDNP3	DNP3	Transmission	MiTM and DoS

Abbreviations: CORE, common open research emulator; DER, distributed energy resources; DoS, denial of Service; ICS, industrial control systems; MiTM, man-in-the-middle; RTAC, real-time automation controller; RTDS, real-time digital simulator; SCADA, supervisory control and data acquisition.

design decisions of RESLab. Table 2 presents testbeds based on these metrics.

Scalability: The primary goal of RESLab is to provide a platform to detect and protect a large-scale cyber-physical electric grid against cyber threats. Hence, we focus on the needs for large-scale grid emulation, where our testbed enables us to analyse the attacks and the impact associated with multi-element outages due to cyber threats. RESLab's integration of large-scale realistic cyber-physical models, including a synthetic test case on the Texas footprint with power [33] and communication [34] systems, balancing authorities, and market participants, strengthens its ability to provide value for power systems' stakeholders.

Automation & Orchestration: Features to support orchestration and automation are essential for smooth and repeatable demonstration of scenarios in testbeds. Orchestration refers to additional software developed to provide user-friendly scenario-specific configurations and model integration. Automation scripts enable interconnections between different components of the testbed, for example, using network sockets or other client-server architectures. For example, Phenix is a monitoring tool orchestrated over SCEPTRE [35]. Other examples include a Labview-based GUI [29], a command-line based attack suite [11], and many others as illustrated in Table 2.

In RESLab, we developed orchestration tools for visualising the cyber network of the synthetic electric grid, implementing cyber-intrusions using a GUI attack suite, aggregating real-time data from simulators as well as integrating monitoring tools like Zabbix. RESLab also uses an OpenDNP3 library that enables flexibility in incorporating a hierarchical DNP3 architecture where a DNP3 master can interact with outstations, usually RTUs in a substation, and those RTUs can further act as master and can control DNP3 outstations which are protective devices such as relays.

Data Collection & Fusion: Currently, few datasets are publicly available that provide cyber-physical features for training IDSs. Most datasets are restricted to either purely physical or cyber features. The widely-known KDD and CIDDS datasets used in developing ML-based IDS are centric to cyber features [36]. Tools such as MATPOWER and pandapower have been used to provide physical-side datasets for bad data detection. Datasets that include measurements for transmission systems are presented in [37–39].

An innovation of RESLab is its *dataset management and availability*. RESLab is a platform that aggregates real-time cyber traffic and power data along with IDS alerts and enables integration of third-party tools including visualisation and data analytics. The dataset [40] for the use cases evaluated, the multi-sensor data fusion engine [41] along with

TABLE 2 Review of Cyber-Physical Power System Testbeds based on **scalability**, **orchestration**, **data fusion**, **fidelity**, **cyber threat realism**, and **HIL support**

Ref	Scalability	Orchestration	Data Fusion	Scenario Details	Practicality Analysis	HIL Support
[21]	IEEE-14 case	RT-VSMAC monitoring	No	Yes, through SoE (seq. Of events)	Yes, MiTM/DoS impacts analysed	Yes
[22]	IEEE-118 case	PMU fault location application	No	Yes, compared simulated and real-time results	Yes, packet delay, packet loss and channel failure	Yes
[7]	WECC-9 bus	No	No	Yes, coordinated attack	No	Yes
[24]	IEEE 9 bus	No	No	Yes, measurement and control attacks impact on AGC	No	Yes
[11]	IEEE 11 bus	Yes, Modbus MiTM attack suite	No	Yes, validated with MiTM attack on inputs to static var compensator	No	Yes
[29]	EMP 60	Yes, Labview based visualisation and commercial EMS integration	No	Yes, fault detection and isolation with protocol parsing latency	No	Yes
[10]	No specific study	Yes RADICL	No	Not validated in the paper	No	Yes
[46]	7 bus case	Yes, network viewer	No	Yes, visualised through impact of line-overflow	No, RINSE architecture presented but experimental analysis	No
[12]	IEEE 13 node feeder	No	No	Yes	No	Yes
[14]	Kundur 2 area 4 machine system	Yes	Yes	Yes	No	Yes
RESLab	Texas 2000 bus	CYPRES EMS, DNP3 master, and MiTM attack GUI	Yes	Yes, validated with FCI and FDI attack impact	Stochastic analysis of MiTM attack challenges	Yes, currently with RTAC

Abbreviations: DoS, denial of Service; EMS, energy management systems; HIL, hardware-in-the-loop; FCI, false command injection; FDI, false data injection; MiTM, man-in-the-middle; RESLab, Resilient Energy Systems Lab.

the different IDS solutions proposed in the work are available online [42].

Cyber Intrusion Practicality Analysis: Some works implicitly assume that an adversary can successfully reach a device and cause MiTM or DoS with high probability. However, cyber incidents with this depth are rare and the targeting adversaries are stealthy. Hence, it is valuable, and essential for defence, to analyse attack strength considering the stealthiness of attacks. RESLab is designed to fulfil this. For example, we enable an in-depth analysis of the practicality of MiTM attacks against DNP3, considering detection tools [43]. RESLab analyses the challenges of incorporating MiTM attacks under different polling rates and numbers of polled DNP3 outstations for a large-scale power system using queuing theory. Extensive research has been proposed on defence against FDI attacks [44, 45]. However, works that address FDI attacks tend to make unrealistic assumptions on the adversary's capabilities in the communication network; RESLab remedies this by enabling its emulation of the communication system and high-fidelity FDI attacks.

Use of Common ICS Software and Hardware: Many testbeds in Tables 1 and 2 contain hardware-in-the-loop (HIL) features, that is, hardware that closes the loop from monitoring to control with the simulation/emulation. RESLab also facilitates HIL studies, currently through integrating the RTAC, CORE, and PWDS. The RTAC reads measurements from PWDS over DNP3 through CORE and implements control logic to generate commands and send them back to PWDS through CORE. In future works, we will integrate simulation measurements into physical protective relays. RESLab integrates commercial monitoring and detection tools. ELK stack is used to monitor ne

twork traffic from CORE as well as Snort IDS logs emulated within CORE. It also integrates the Zabbix monitoring tool using the control network of the CORE emulator.

3 | RESILIENT ENERGY SYSTEMS LAB CYBER-PHYSICAL TESTBED ARCHITECTURE

RESLab is designed to reflect realistic power and cyber components based on the synthetic electric grid model on the Texas footprint [33], and its communication model is introduced in [34]. Figure 1 presents a high-level view of the architecture considered, showing an example of one substation

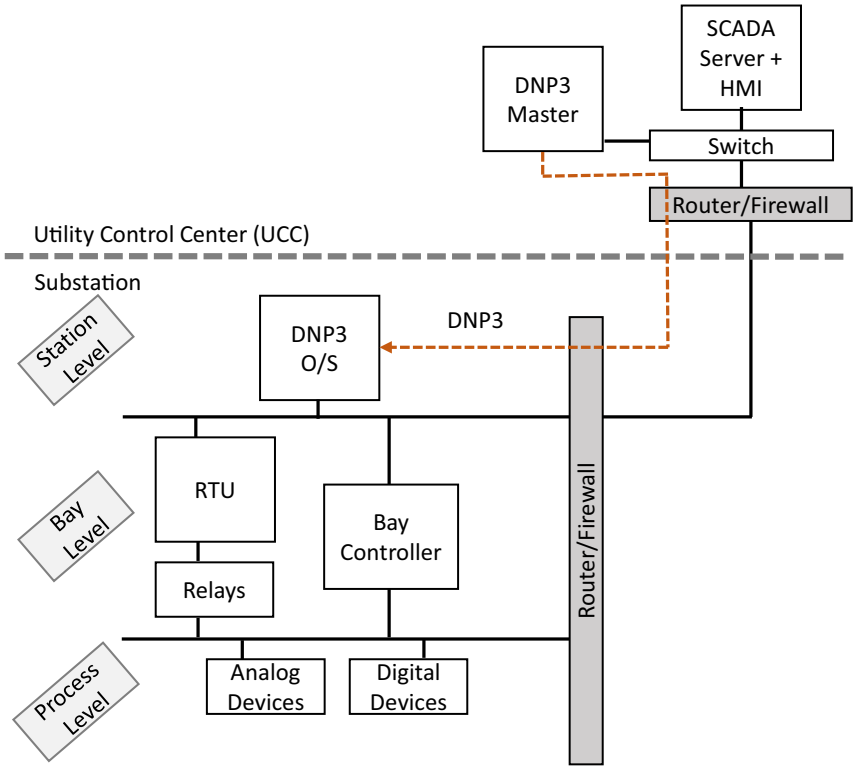

FIGURE 1 Power system cyber-physical architecture with one substation and a utility control centre

and one utility control centre (UCC), with components and data flows. Detailed data flows including balancing authorities and demilitarised zones (DMZs) are presented in our work on firewall policies [47].

In the simplified model in Figure 1, the main data flow depicted is DNP3 traffic, which is initiated at the UCC where there is a DNP3 master and a SCADA server that act as our central control and human machine interface (HMI) applications. At the substation level, there is a DNP3 outstation (DNP3 O/S) which has the data from the field devices that the UCC needs to monitor.

At the *bay level*, devices including RTUs and relays monitor the system status, collect data, and control physical analog and digital devices at the *process level*. Physical devices include circuit breakers, which we call digital devices as they have two states, or generators and load, which we call analog devices. The relays can trip circuit breakers to isolate a faulted circuit. The data from the *process level*, for example, from instrument transformers, is concentrated in RTUs and then transferred to the *substation level*. Within the UCC, the DNP3 master collects the information from each substation for a complete view to understand and control the system. In [48], a typical structure of data concentration and engineer access is presented using the SEL RTAC in SCADA systems, where the RTACs in substations communicate with the RTACs in the UCC and EMS for data collection and control.

The UCC and the substations are in different locations, and in RESLab they are interconnected by an IP network but they can also be connected through a serial link. At each location we have one router: the substation router and the

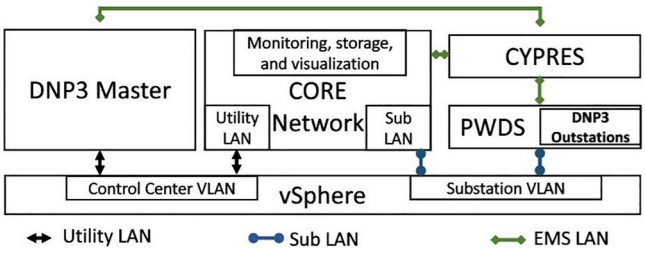

FIGURE 2 The logical connections between the virtual machines (VMs) hosted in Resilient energy systems Lab (RESLab)

UCC router, which also act as firewalls because they are configured to allow only DNP3 packets and block unwanted traffic. Figure 2 illustrates how RESLab follows this data flow pipeline and incorporates real-time power system simulation using PWDS, a physical SEL RTAC, an OpenDNP3 master application, and an emulated communication network using CORE.

In the testbed, PWDS acts as a collection of DNP3 outstations connected to the substation's control network (shown as Sub LAN in Figure 2). The emulated DNP3 master and SEL RTAC are housed in a control centre network to represent software- and hardware-based control platforms. Each of the emulated components is hosted in a virtual machine management environment, named vSphere. The vSphere environment allows for the creation and management of a large number of VMs. The time synchronisation between VMs is maintained through the Network Time Protocol server within the vSphere client. To ensure that ICS traffic passes through the CORE emulator, batch scripts are run in the VMs to update routing

tables. Further, within vSphere, multiple VLANs are created in a virtual switch to segregate ICS traffic from other background and management traffic. In RESLab, connections between emulated and physical components are made to scale the network depending on the use case. Next, the purpose and functionality of each testbed component are presented.

3.1 | Cyber network emulation: Common open research emulator

RESLab uses the network emulator Common Open Research Emulator (CORE) that provides a platform to run different applications, such as iptables for firewall, Snort for intrusion detection, and services such as Secure Shell (SSH) for remote access. CORE is an open-source network emulator published by the U.S. Naval Research Laboratory. CORE is used for emulating smart grid networks in [49], where the authors compared existing works of co-simulation and discovered CORE to be suitable for large-scale simulations.

The software allows the creation of several BSD jails, similar to Linux containers, that can be connected to emulate realistic communication networks. These containers are used to emulate routers, firewalls, personal computers, and Linux servers in the communication network. CORE can also tap into the hosts' Ethernet connections to connect with external networking devices and VMs housed within vSphere.

In our testbed, CORE is hosted as one of the VMs with each of its virtual network interfaces connected to different VLANs, such the Sub LAN and Utility LAN shown in Figure 2, to emulate a wide-area-network (WAN) between the substations and the UCC. CORE also has a bridge connecting the cyber-physical EMS application (Section 3.5) that monitors real-time traffic from PWDS as well as network traffic in CORE. The WAN setup has direct connections between the gateway routers of the UCC and the substation subnets. The routes within this architecture are created by running Quagga [50] services in the routers running the open shortest path first (OSPF) protocol.

From left to right in Figure 2, the connections are as follows: (1) VM hosting DNP3 master, (2) VM running CORE, (3) VM running a centralised cyber-physical EMS application, and (4) the PWDS VM. To show the emulated network, Figure 3 details the network topology: the DNP3 master and SEL-RTAC are connected to the CORE through a virtual interface [1]; the interface [2] forwards Snort IDS alerts from the control centre router to the EMS application; the VM running the large-scale synthetic electric case in PWDS is connected through the interface [3].

3.2 | Power system simulation: Power world simulator and dynamic studio

RESLab uses PowerWorld Simulator and Dynamic Studio (PWDS) that provides large-scale power system modelling in the steady-state and transient stability timeframes [51–53]. It can emulate large-scale grids (up to 82,000 buses) and a distributed computing feature to perform parallel steady-state contingency, transient stability, and available travel capacity analysis. Since the goal of our testbed is to study the impact of cyber threats on a large-scale grid via a coordinated attack at various locations, PWDS is used in RESLab.

In RESLab, PWDS models the dynamic behaviour of an electric power system in the transient stability timeframe. It does interactive control [33], and serves as a general interface for DNP3 outstations [51, 52]. An outstation, as defined from a power system operational point of view, typically includes one substation and its devices, including branch breakers, generators, load breakers, and shunts. The DNP3 tags generate

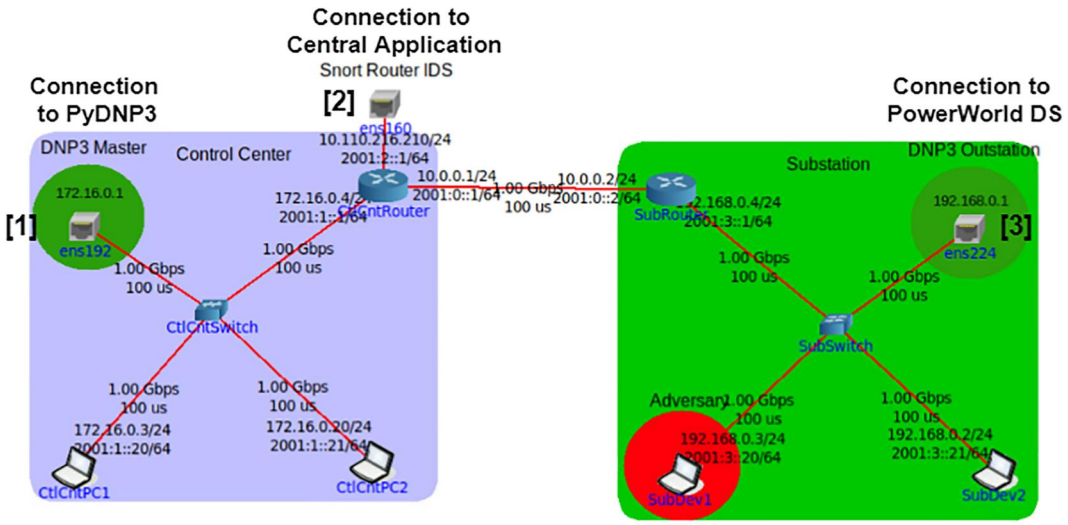

FIGURE 3 Common open research emulator (CORE) network topology showing emulated PC nodes and connections to the following: [1] DNP3 master, [2] cyber-physical resilient energy systems (CYPRES) app, and [3] power world simulator and dynamic studio (PWDS) DNP3 outstations

binary data, such as the status of all devices, and allow the devices to be controlled by other DNP3 masters/clients. The DNP3 tags can also be set to send analog data, such as measurements of generator real and reactive output, allowing DNP3 masters to change the generator setpoints. A DNP3 master is hosted in a VM running OpenDNP3. Another VM runs the SEL acSELerator software to configure the RTAC as a DNP3 master.

PWDS also serves as a simulation engine with a generic interface for integration into other applications [53]. In our experiments, PWDS simulates the power system in a real-time environment in which cyber threats and defence mechanisms are implemented. The large-scale test case on the Texas footprint [33, 34] is implemented as our exemplar power system and maintained at Texas A&M. CORE's WAN is used to forward the breaker status and control commands between VMs.

3.3 | DNP3 and master application

DNP3 is extensively used by electric utility companies for communication between equipment [54]. The protocol utilises the master/outstation architecture. A network can be configured to have one DNP3 master communicate with more than one DNP3 outstation as a multi-drop network. Alternatively, there can be one DNP3 master that communicates with one DNP3 outstation.

DNP3 messages contain a 10-octet DNP3 header and a maximum 292-octet DNP3 payload carried over TCP/IP packets. The DNP3 header contains link control, length, sync, source, and destination address fields with a cyclic redundancy check (CRC) to ensure data integrity. The purpose of the CRC is to ensure that bits have not been changed accidentally during their transmission from source to end node. Some intruders may modify the traffic yet fail to modify the CRC, which can be easily detected by the receiver or by implementing DNP3 specific decoders in IDS. Inside the DNP3 payload, function codes identify the operation the outstation performs. These are the function codes used in our simulations: Confirm (0x00), Read (0x01), Read (0x2), Select (0x03), Operate (0x04) Direct Operate with Acknowledge (0x05), Solicited Response (0x81), and Unsolicited Response (0x82).

The DNP3 master application in RESLab uses the PyDNP3 library and a Python wrapper for the C++ based OpenDNP3 module to run the master as a console and a graphical user interface (GUI) application (Figure 5a). The purpose of the master application is to continuously monitor the status of the circuit breakers, generators, and loads in the DNP3 outstations that are running in PWDS. The application also forwards the response of the DNP3 outstations as well as the connection status to the central application via CORE's WAN. This application is configurable to change the polling rates and visualise real-time traffic. It runs in an isolated VM but exists in the UCC LAN with its default gateway set to 172.16.0.4, which is the UCC router (see Figure 3). The application is located in one of the nodes within the UCC LAN and allows the user to choose outstations to monitor and control the substations that are under the UCC.

3.4 | Real-time automation controller integration

RESLab integrates SEL-3530 RTAC to explore different variants of the DNP3 master. The RTAC provides flexible system control with integrated management of security, configuration, and logic. It supports multiple communication protocols, such as DNP3, Modbus, and IEC 61,850, and comes with an embedded IEC 61,131 logic engine. RTAC has been utilised in several hardware-in-the-loop testbeds for data collection and signal conversion [22, 29], but it has not been used for communication studies or to emulate cyber adversaries associated with specific hardware.

Within RESLab, for each substation, there is a DNP3 master in the RTAC to collect analog input data, such as power flow and binary input data, and the status of the transmission lines from PWDS. Furthermore, each client in the RTAC controls the corresponding devices through analog and binary outputs to change the generator setpoint and device status (on/off). Thus, the integration of an industrial standard control device in RESLab allows researchers to gain a deeper understanding of how cyber adversaries can impact the devices and the system as well as develop more practical detection and defence logic in the field.

3.5 | Cyber-physical energy management system

A centralised cyber-physical energy management application named Cyber-Physical Resilient Energy Systems (CYPRES) that our team developed is designed to house algorithms for monitoring and analysis, run SCADA applications, and visualise the system. CYPRES is developed and deployed in RESLab as an exemplar use case for the testbed. CYPRES aggregates information from the cyber-side CORE emulation environment, the power side from PWDS, as well as from the DNP3 masters regarding DNP3's communication status as illustrated in Figure 4b. CYPRES is used to visualise the control network of the synthetic utilities and their substations in the synthetic power grid (Figure 4b). To detect intrusions, it also probes real-time traffic where CYPRES then performs data fusion from multiple sensors in the synthetic network. The CYPRES application is currently envisioned to be housed at a central location (i.e., at a balancing authority or utility) and used to analyse the system with respect to cyber intrusions. Furthermore, CYPRES provides cyber-physical situational awareness in RESLab using attack tree visualisations to access risks related to cyber and physical assets and impact, and to recommend mitigation actions for the identified risks.

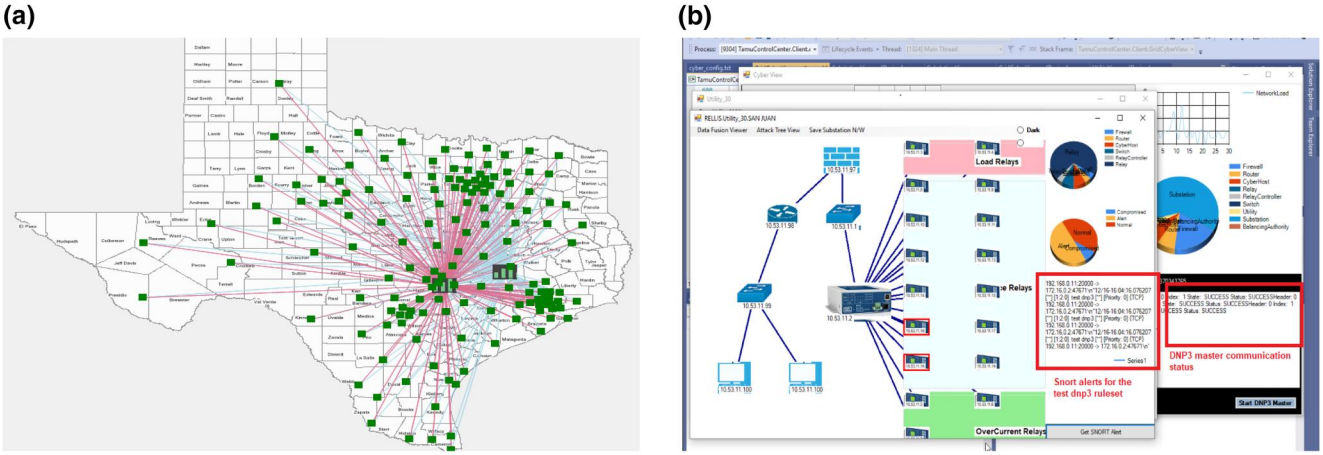

FIGURE 4 (a) Cyber focussed energy management systems (EMS) tool in resilient energy systems lab (RESLab) for visualising threats in the synthetic communication network to access different control centre and substation networks. The green icons indicate the utility control centres with two balancing authorities (b) Panel to visualise real-time Snort alerts from the common open research emulator (CORE) emulator in the substation window (front), along with the control centre window (back) to get update from DNP3 Master

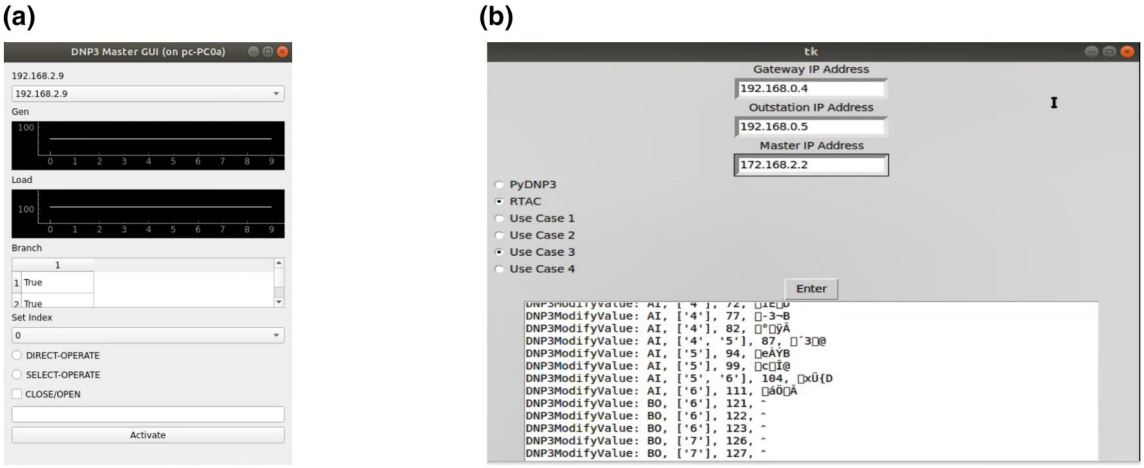

FIGURE 5 (a) A DNP3 master graphical user interface (GUI) that enables control of different outstations using analog and binary commands (b) An MiTM attack suite to configure the address resolution protocol (ARP) poisoning targets and select a use case to sniff and modify DNP3 points

3.6 | Man-in-the-middle intrusion attack suite

MiTM intrusions have been incorporated in many testbeds targeting control commands and measurements in small-scale systems. Creating significant impact in a larger system requires coordinated manipulation of measurements and commands since the larger system is N-x resilient for smaller x, where x is the number of contingencies. Existing tools such as Ettercap can only assist in the prior steps of MiTM such as ARP cache poisoning. Hence, we developed an attack orchestration suite that can assist in configuring targets, selecting scenarios, and visualising intercepted traffic for designing stealthy intrusions as shown in Figure 5b. This enables modularity by segregating the details of MiTM dynamics from a power system researcher who is concerned with the traffic that is modified rather than how they are modified. The algorithms incorporated for different use cases in Figure 5b are presented in [43].

3.7 | Intrusion detection system

The role of an IDS is to detect cyber intrusions. Rule-based and anomaly-based IDS's are predominantly used in the industry, but they lack the capability of detecting zero-day attacks. As an initial approach, RESLab integrates the Snort IDS which is used to detect and generate alerts for cyber intrusions based on the defined rule sets, preprocessors, and decoders. In RESLab, Snort protects the control centre and substation LANs by running in the routers. The alerts are forwarded to the CYPRES application in real-time. We improve the IDS accuracy by training various machine learning-based IDS using data fusion, presented in our work [42].

3.8 | Storage and visualisation

RESLab implements a platform that the team has created to probe the traffic at all the network interfaces inside CORE, to collect the traffic, to use Elasticsearch Logstash Kibana (ELK) stack to store the traffic in an Elasticsearch index, and to visualise them using Kibana dashboard with the Packetbeat plugin [55]. One can configure the Packetbeat plugin to modify the number of interfaces and the type of traffic to probe. Kibana provides a platform to write Lucene queries to filter out a search in the Elasticsearch index. RESLab uses Logstash to collect Snort alerts to visualise in Kibana. In addition to the ELK stack, RESLab also integrates Zabbix [56] for network monitoring, as it provides a platform to configure custom alert rules and triggers. We have configured a Zabbix server in the base operating system hosting CORE, and the Zabbix agents in all the routers in CORE. The agents within CORE use the CORE control network to interact with the server using the ZBX protocol [56].

4 | THREAT MODEL

The threat model we present and implement in this work is based on emulating a multi-stage attack in the large-scale synthetic test system's communication model. In the first stage, the adversary gains Secure Shell (SSH) access to a machine in the substation LAN. In the second stage, the adversary performs steps that are tailored to the system under study and to power system protocols, allowing the adversary to achieve MiTM and DoS attacks that cause physical impact. The RESLab framework can not only support MiTM and DOS but also integrate other attack vectors.

4.1 | Man-in-the-middle attack

Man-in-the-middle (MiTM) is one of the oldest forms of cyber intrusion where a perpetrator positions himself or herself in a conversation between two end points to either passively eavesdrop or to impersonate one of the endpoints, making it appear to be a normal exchange of information. MiTM encompasses different techniques and potential outcomes depending on the threat model. During the second stage of our presented threat model, we compromise the target outstation and its router by performing an ARP spoof attack by poisoning the ARP cache of both the substation's gateway and the DNP3 outstation [57]. Then, in the third stage, we modify the control and monitoring traffic to have different implications on the electric grid.

Such tampering of commands and measurements would normally go undetected by the outstation using CRC error checking, since the data chunk in the DNP3 payload's has its CRC recalculated by the adversary before the modified packet is forwarded to the outstation. The intruder causes false command injection (FCI) and false data injection (FDI) attacks by first storing the DNP3 polling response for the targeted outstations, then manipulating measurements in some cases and commands in other cases, as well as manipulating a mix of both to carry out one of the most critical contingencies presented in our N-x contingency discovery article [58]. Such an attack is hard to be detected by an IDS such as Snort if the intruder not only tampers the command but also takes care of the CRCs.

In RESLab, the MiTM attack is developed and implemented to change binary and analog commands sent by the DNP3 master to the outstation as well as the polled response from the DNP3 outstations. The intruder not only modifies the commands but also eavesdrops and then modifies the current state of the system by tampering with its real-time measurements. In Table 3, the procedure for performing a MiTM attack in RESLab is listed. The details on the various combination of attacks that are performed in the third stage of the threat model are presented through four use cases detailed in Section 5.

4.2 | Denial of Service attack

As another attack vector, we implement a DoS attack to exhaust victim nodes' processing capability and link bandwidth. There are many different methods of denial of service (DoS) attacks that can be used, which include but are not limited to user datagram protocol (UDP) flood, Internet control message protocol (ICMP) flood, and Ping of Death (PoD) [59]. While each of these DoS attack types uses different Open Systems Interconnection (OSI) layers such as application, presentation, session, transport, network, data link or even physical layer protocols to carry out the attack, all DoS methods attempt to disrupt the communication channels of the targeted node. In our threat model, the intruder within the substation LAN targets routers at the substation and at the control centre by flooding the routers with ICMP traffic.

TABLE 3 The steps taken in RESLab to implement FCI injection

Sequence	Description
1	a. Start the CORE, PWDS, and OpenDNP3 master. b. Allow time for DNP3 communication between master and outstation to be established.
2	a. Start CYPRES app to monitor cyber data. b. Start running snort in substation router. Run the ELK services and Packetbeat.
3	a. ARP cache poisoning of substation's gateway and outstation.
4	a. Sniff traffic to and from the outstation. b. Forward non-DNP3 traffic to/from outstation.
5	a. Send command from master to outstation. b. Modify command and forward to outstation.
6	a. Modify acknowledgements from outstation.

Abbreviations: ARP, address resolution protocol; CORE, common open research emulator; CYPRES, cyber-physical resilient energy systems; ELK, elasticsearch logstash kibana; FCI, false command injection; PWDS, power world dynamic studio; RESLab, resilient energy systems lab.

The impact of these DoS attacks is then observed and analysed based on round trip times (RTT) and throughput of the communication channel by varying attack strengths such as the length and delay between the ICMP packets infused to disrupt the DNP3 session.

5 | TESTBED EVALUATION OF CYBERATTACK IMPACTS ON POWER SYSTEM OPERATION

This section presents evaluation in RESLab of four use cases targeting operational impacts that affect power system resilience through large-scale grid emulation in RESLab. The synthetic Texas 2000-bus case [33, 34] that we use is a publicly available power system case. This system is N-1 secure, and it is also difficult to cause disruption by exploring N-2 contingencies. Hence, the use cases in RESLab leverage results from our prior work [58] on identifying the most critical multiple-element contingencies based on graph theory and line outage distribution factors (LODFs), which are located in the regions targeted in our use cases (Figure 6).

In the model, branch (x,y) means Bus x to Bus y. To illustrate the contingencies, if branches (5262,5260), (5263,5260), (5317,5260), and (5358,5179) are open, there will be four overflow branches in the system, which are branches (5071,5359), (5138,5071), (8086,8083), and (8084,8083). Branch (5262,5260) and (5263,5260) are located in substation *GLEN ROSE 1* (560), branch (5317, 5260) is at substation *GRANBURY 1* (601), and branch (5358, 5260) is at substation *RIESEL 1* (631). The overflow branches are at substations *WACO 3* (399), *JEWETT 1* (1195) and *FRANKLIN* (1200).

Besides, in those substations, there are several generators. If compromised, there will also be a contingency in the system. These generators are Gen 5262, 5263, 5319, 5321, 5360, 7098, and 7099. Gen 5262 and 5263 are at substation *GLEN ROSE 1* (399), Gen 5319 and 5321 are at substation *GRANBURY 1* (601), Gen 6360 is at substation *RIESEL 1* (631), and Gen 7098 and 7099 are at substation *WADSWORTH* (968). When these generators reduce their output and the branch (5260,5045) in substation *STEPHENVILLE* (390) is open, there will be another overflow in branch (5286, 5046) at substation *STEPHENVILLE* (390).

Thus, we assume that the adversary has the intent and the resources to target the most critical branches and generators, where disrupting their control causes a severe impact. Specifically, we present four use cases to show how cyber threats can compromise a resilient power system. These use cases involve binary and analog command modification, measurement, and status modification. Before exploring the scenarios, we present RESLab's experimental setup, which allows us to collect data at various locations and analyse them from a cyber-physical perspective.

5.1 | Experimental setup

The DoS and the MiTM attacks for the scenarios are performed while running RTAC and OpenDNP3 applications as the DNP3 masters. The resources used to perform all the experiments are illustrated in Table 4. Virtual LANs (VLANs)

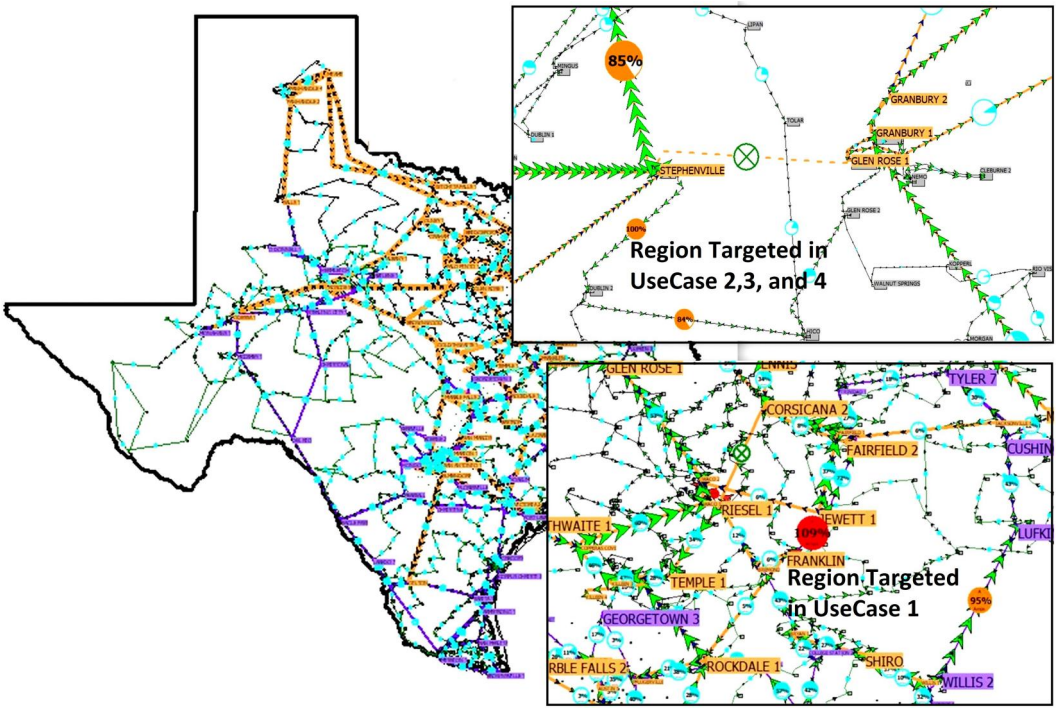

FIGURE 6 The large-scale synthetic electric grid model that is the basis of our exemplar cyber-physical power system

TABLE 4 VM configuration for the RESLab architecture in Figure 2

Virtual machine Allocations in vSphere				
VM name	**Mem.**	**CPU cores**	**VLANs**	**OS**
CORE	12G	4	1,2,3,4	Ubuntu
DNP3_Master	12G	4	1,2,3	Ubuntu
PWDS	10G	2	1,2,4	Windows 10
Central_App	16G	8	1,2	Windows 10
RTAC	4G	2	1,2,3	Windows 10

Abbreviations: CORE, common open research emulator; PWDS, power world dynamic studio; RESLab, resilient energy systems lab; RTAC, real-time automation controller; VM, virtual machines; VLAN, virtual LANs.

are used to ensure that traffic is forwarded by the emulated routers in CORE and to segregate the substation network from the control centre network.

In these simulations, we use a multi-master architecture where each master monitors and controls a substation separately. While the master monitors and controls the outstations, the adversary sniffs all the measurement traffic (requests and responses) from the substations. We capture network traffic at four locations in the network (outstation, master, adversary, and substation router) to evaluate the impact of MiTM attacks on these four use cases. Since the adversary acts as the middle man between the substation router and outstation, we validate the MiTM by checking if the DNP3 packets received at the substation router and at the master are identical and if the DNP3 packets at the outstation and adversary are identical.

To test the detection of DoS and MiTM attacks, we operate Snort at the substation and control centre routers in a Network Intrusion Detection System (NIDS) mode by enabling preprocessors and decoders and including custom rules for ARP, DNP3, and ICMP traffic. Then, we present the alerts along with the physical traffic to correlate the alerts with the measurements and command tampering.

5.2 | Class 1: False command injection

A MiTM attack that modifies binary control commands using relay control blocks can cause line overloading [60]. To achieve this, the adversary first parses the measurements by sniffing the DNP3 responses from the outstation. Then, it sniffs the DNP3 binary *OPERATE* command and forges them. The adversary modifies the commands with function codes of 3 and 4 (*SELECT* and *OPERATE* command) from the RTAC, and it modifies the commands with function code 5 (*DIRECT OPERATE* command) from the OpenDNP3 master application. The adversary modifies all the *CLOSE* commands to *TRIP*, forcing to open the critical branches identified and causing line overloads in four other branches, shown in the data from the scenario in Figure 7. This scenario is referred to as *use case 1 (UC1).*

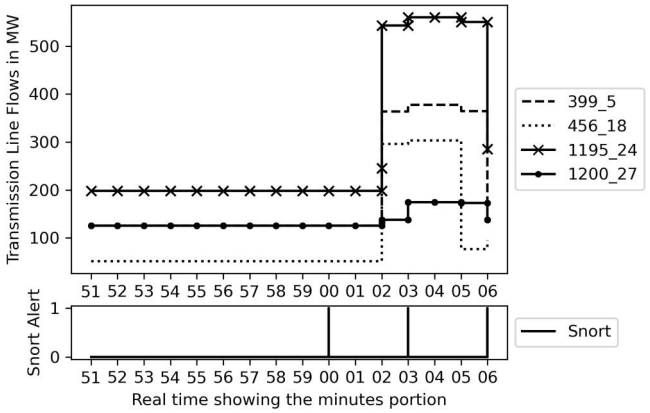

FIGURE 7 *UC1:* Overloaded transmission lines observed at the master application (*WACO 3* [399], *WACO 1* [456], *JEWETT 1* [1195], and *FRANKLIN* [1200]). The legend shows the *outstation_index*. For example, the first legend indicates outstation number 399 and DNP3 index 5. The plot beneath shows the Snort alerts during the intrusion

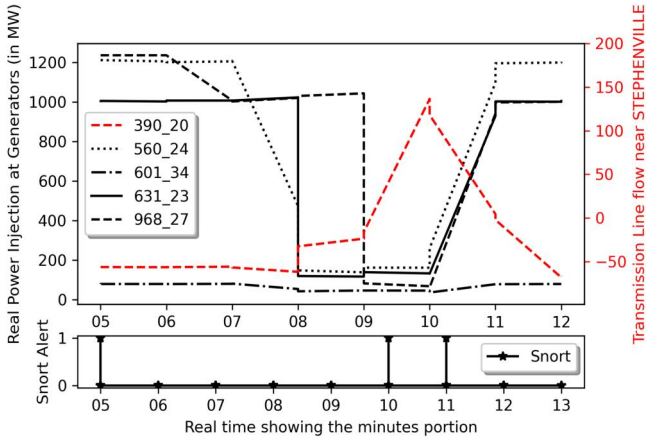

FIGURE 8 *UC2:* The real power injection in generators from substations *WADSWORTH* (968), *RIESEL 1* (631), *GRANBURY 1* (601), *GLEN ROSE 1* (560) (left *y*-axis) and the overloaded line near substation *STEPHENVILLE* (390) (right *y*-axis). The legend shows the *outstation_index*. The plot beneath shows the Snort alerts

The intruder can also modify analog control commands to change the setpoints in generators along with a binary command to control a branch to cause line overloads. The intruder first inspects the DNP3 packets, changes a collection of generator setpoints from the real value to 0, and alters the binary control command as in *UC1*. This scenario compromises seven generators and one branch, referred to as *use case 2 (UC2).*

Figure 8 shows the actual generation output in each substation *WADSWORTH*, *RIESEL*, *GRANBURY*, and *GLEN ROSE* along with the Snort alerts during the 5th, 10th, and 11th mins of the scenario. The intrusion in these substations takes place during the 8th and 9th mins. The intruder's goal is to overload the transmission line near substation *STEPHENVILLE*, accomplished by tampering of the analog setpoints, as observed in the interval 9-11th minute in Figure 8.

5.3 | Class 2: false data injection with false command injection

The MiTM intruder can also perform false data injection (FDI) with the false command injection (FCI) to create more difficult-to-detect attacks. First, the intruder falsifies polled measurements, causing the operator to re-send a control command to the field device. Then, the intruder modifies the control command, as in the previous use cases, by changing the generator setpoint. The actual generation measurements for the same seven generators in *UC2* are falsified to 20 MW, and the flow measurement coming from branch [5260, 5045] is changed to 3000 MW, which is above its capacity. Based on these observations, the operators or a pre-defined control logic within devices such as a SEL RTAC would re-send the control command to increase the generators' output and open the branch. However, when sending those commands, the intruder modifies the setpoints to 20 MW, making the physical system unreliable. This scenario is referred to as *use case 3 (UC3)*.

Figure 9 shows the system after the output of a generator in substation *WADSWORTH* is changed in the polled measurements by the intruder from 1000 to 20 MW as observed in the master and the router from 52nd to 55th min. The Snort alerts are observed from the 53rd to 56th mins. The alerts at 50th and 51st min are due to an attack in other targeted substations such as *GLEN ROSE*, *RIESEL*, and *GRANBURY*, whose generation set points are tampered.

Another example of a three-stage attack is referred to as *use case 4 (UC4)*, where the intruder first changes the measurements polled by the DNP3 master, as in *UC3*. Once the operator re-sends the control command, the intruder changes the setpoints from the real value to a low value, as in *UC2*, but the intruder also falsifies the measurement packets, masking the true measurements and showing the original setpoint values. The result is that the operator believes his/her command has been successfully received and committed. However, in the true physical system, the generators' outputs decrease, and opening a line will then cause an overload.

Figure 10 shows the generation output at substation *WADSWORTH* as observed at four locations. During the intrusion on *WADSWORTH*, within the 34th and 44th mins, the adversary first forces the master to take a wrong action to change the generation output to 1000 MW once the master observes low generation output at the 34th minute due to modification of the measurements of the generation output. Further, when the operator takes this action to address the low generation output, the intruder changes the command from 1000 to 0 MW to cause contingency. To be stealthier, the intruder also modifies the polled response from the outstation with the same setpoint value of 1000 MW from the interval of 39 to 44 min except at 42nd min, as set by the operator to prevent the master from observing the contingency caused by the intruder in the first two stages. The snort alerts generated in this interval are shown in Figure 10. Both Figures 9 and 10 demonstrate the effective implementation of the use cases by observing measurements at different locations at the testbed.

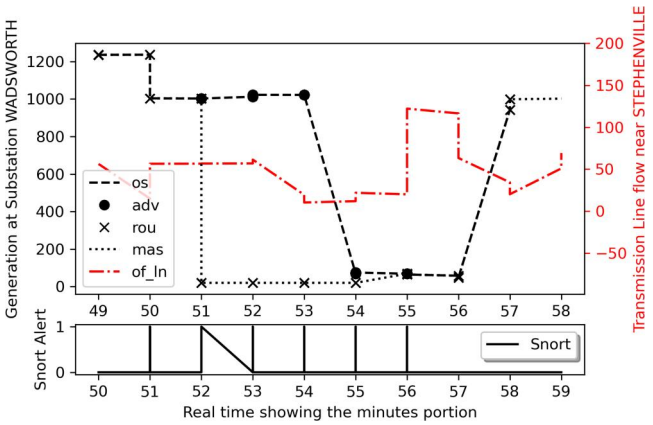

FIGURE 9 *UC3:* The real power injection at one generator in substation *WADSWORTH* as observed by the master (*mas*), substation router (*rou*), adversary (*adv*), and the outstation (*os*), along with the overloaded line (*of_ln*) near substation *STEPHENVILLE*. The plot beneath shows the Snort alerts during the intrusion

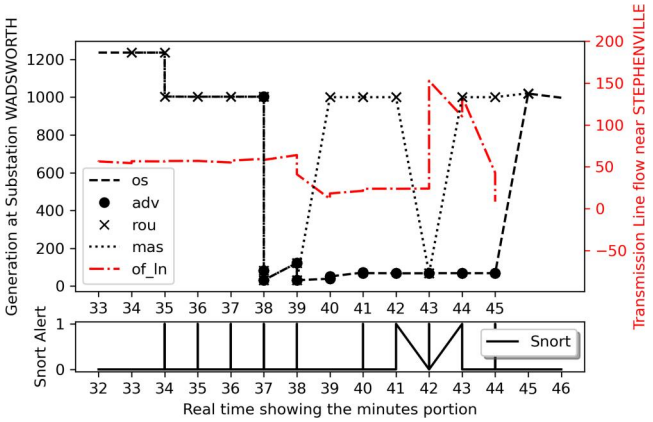

FIGURE 10 *UC4:* The real power injection at one generator in substation *WADSWORTH* as observed by the master(*mas*), router(*rou*), adversary(*adv*), and the outstation(*os*). The overloaded line magnitude (right *y*-axis) near *STEPHENVILLE* (*of_ln*)

6 | RESULTS AND ANALYSIS

In this section, we evaluate the testbed's functionality by studying the impact of MiTM and DoS attacks on the DNP3 sessions between the masters and outstations. The effectiveness of the DoS attack is evaluated by varying the attack strength and studying its impact on the RTT and throughput of DNP3 traffic. The timeframe of power system operations compared with the attack timeframe plays a major role; for example, the timeframe of the inverter and stator transient control is in the order of milliseconds, while the control of voltage stability, power flow, and unit dispatch range from 10 to 1000 s. Hence, it is essential to analyse RTT to ensure that the control commands reach the field devices on time.

The four use cases for MiTM attacks, summarised in Table 5, are tested with the RTAC and OpenDNP3 master. Experiments are conducted by varying the number of DNP3 outstations polled and the polling interval. Each master

communicates with its substation, and we assume that five or 10 masters are connected with their respective outstations. These experiments are performed to study the success rates of the attacker (i.e. the number of attempts) in causing the desired contingency of each use case. The adversary is restricted by the available resources in the Linux containers in CORE, thus the attacks are stochastic in nature. As the number of masters increases, the amount of traffic an intruder processes increases, which results in higher attack miss rates, that is, the probability that the attacker fails to modify a sniffed packet.

We monitor the number of active TCP connections as impacted by retransmission during the progression of the attack, based on different polling rates and varying DNP3 masters. The adversary success probability, the average retransmission rates, the packet processing times, the average RTT for performing each FCI and FDI attack, and the Snort alert statistics are key characteristics for detection. Snort IDS is used to detect the ICMP flood attack as well as the ARP spoof attack (Section 4), which reroutes packets to the adversary and allows modifications to take place.

6.1 | Denial of service attack evaluation

The DoS attack is targeted at the control centre and substation router from a compromised device in the substation LAN, encircled in red, as shown in Figure 3 and we seek to determine which target caused more impact, latency and throughput. The strength of the attacks is evaluated by varying the DoS ICMP payload size for a fixed attack interval and the interval rate with fixed payload size. For all the experiments, the communication link in the network has a fixed bandwidth (BW) of 10 Mbps and a propagation delay of 160 usec.

The latency between the DNP3 master and outstation (PWDS) is the sum of three types of delays: *propagation*, *transmit*, and *queuing* delays [61]. The transmit delay is given by $\frac{payload\ size}{BW}$. Hence, we study the impact of payload size, while the queueing delay is dependent on the service rate (μ) and packet arrival rate (λ) at the router. For example, when modelling a M/M/1 queue for the router, the average queuing delay is given by $\frac{1}{\mu-\lambda}$ [62]. Hence, we study the impact of attack interval on the latency. The RTT is the sum of upstream and downstream latencies, which can increase substantially if the packets are lost causing retransmissions.

Without the DoS attack, the RTT should have been around 0.96 to 1.24 msec, considering a DNP3 request and response payload size varying between 50 and 300 bytes, with no queueing delay. DoS attacks are performed by keeping a fixed interval rate of 1000 ms and increasing the payload size of the ICMP packets from 800 to 1800 bytes in increments of 200 bytes for each trial. It can be observed from Figure 11 that the average RTT increases with the payload size, and that the attack on the control centre router has a higher impact in comparison to the substation router. A sudden rise at 1400 bytes can be observed due to complete congestion of the links leading to packet collisions, which causes retransmissions.

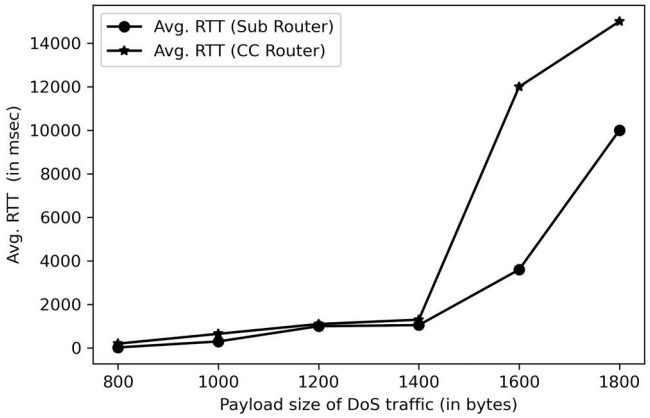

FIGURE 11 Impact of denial of service (DoS) on round trip times (RTT) by varying payload size

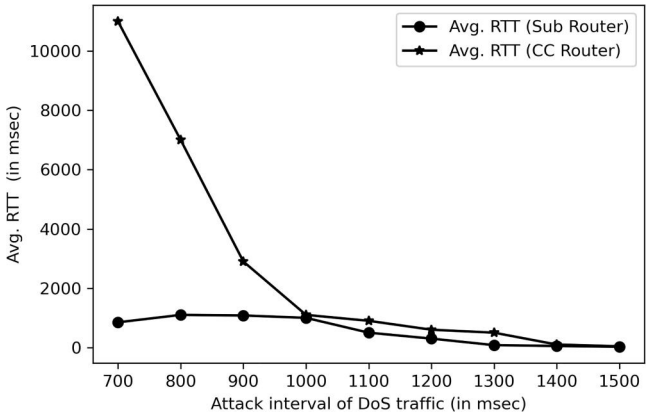

FIGURE 12 Impact of denial of service (DoS) on round trip times (RTT) by varying attack interval

Further, DoS attacks are performed by keeping the payload size of the ICMP packet fixed at 1000 bytes while decreasing the ICMP packet attack interval from 1500 to 500 ms in step decrements of 100 ms for each consecutive trial. Figure 12 shows that the average RTT decreases with the increase in attack interval and that the lower attack interval has a higher impact on the control centre router in comparison to the substation router. As the arrival rate λ increases, the waiting period of the packets at the queue increases and based on different queuing policies, the packets are dropped, resulting in retransmissions.

A DoS attack primarily affects the target's downstream bandwidth. Hence, the average throughput will be affected as the bandwidth of the link is affected. The average throughput for the substation router is calculated using the transmission time of DNP3 packets, that is, the ratio of *Total data payload in bytes* and *Total transmission time*.

The average throughput depends on the type of command from the DNP3 master. For example, the response payload size for the polling will be quite high compared to the response of the *OPERATE* commands. The goodput is equal to the throughput if there are no retransmissions.

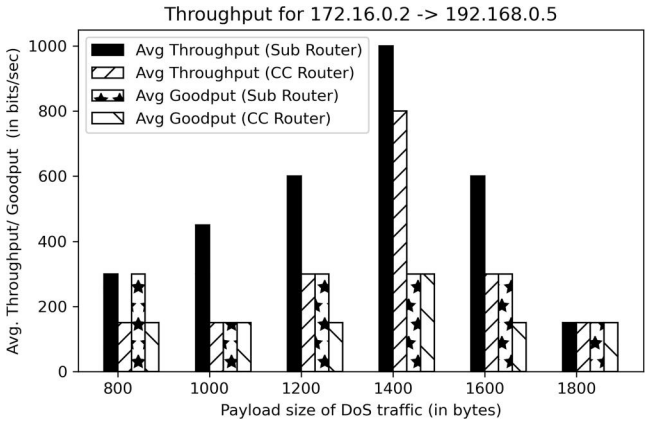

FIGURE 13 Impact of denial of service (DoS) on varying payload size on average throughput and goodput at both substation and control centre routers

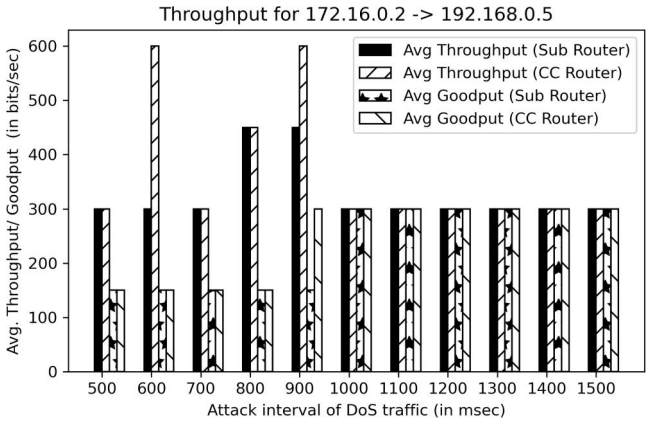

FIGURE 14 Impact of denial of service (DoS) on varying attack interval on average throughput and goodput at both substation and control centre routers

In Figure 13, we observe that the throughput and goodput increase as the payload size increases up to a certain extent, then they decrease due to congestion in the network. It can also be observed that the difference between throughput and goodput increases as the payload size increases due to high retransmission caused by the congestion. Similarly, reduced goodput is also observed when the attack interval is lowered from 1500 to 500 ms as seen in Figure 14.

6.2 | Man-in-the-middle attack evaluation

In the MiTM attacks, both the master and outstation DNP3 packets are captured at the adversary's machine located in substation LAN. Figure 15 shows Wireshark sniffing the DNP3 *DIRECT OPERATE* command from the master in addition to the response from the outstation. As described in Section 5, the *CLOSE* command is replaced by the *TRIP* command as observed from the response as well as the DNP3 log of PWDS as seen in Figure 15.

The RTT for MiTM attacks is small compared to the RTT for a DoS attack. In a DoS attack, the RTT depends on the number of retransmissions but in a MiTM attack, the RTT depends on how much time the attacker takes to parse the packet, modify the payload, recalculate the checksum and CRCs, and forward the packet to the target. There is no substantial retransmission in the case of MiTM attacks if the intrusion is stealthy.

The occurrence of a MiTM attack is validated both by observing a rise in RTT compared to the normal operation in Figure 17 and from its sequence number graph Figure 16. Specifically, in Figure 17, the MiTM attack is performed from 200 s to 1000 s, and the RTT is observed to increase to almost 150 ms during sniffing and FCI attack and to almost 200 ms during FDI attacks on measurement, indicating that the time taken by the adversary's machine for parsing and modification affects the overall RTT. Additionally, as the sequence number remains at 18 from 3.3 to 3.4 s in Figure 16, it indicates that the attacker used the same sequence number to forward the modified packet.

6.3 | Use case specific physical impact evaluation

The physical impact is evaluated based on the four use cases shown in Table 5, described in detail in Section 5. The target of the MiTM intruders in *UC2*, *UC3*, and *UC4* is the same but they adopt different strategies to accomplish it. These use cases detailed in Section 5 demonstrate increasing complexity. The time to cause the same overload in branch [5286, 5046] differs based on the strategy in each use case, as illustrated in Figure 18. For use cases 2, 3, and 4, the overload occurs at 173 s, 216 s, and 541 s, respectively. The differences in time as well as the system dynamics are due to the amount and sequence of intrusions in these three strategies.

6.4 | Evaluation of Man-in-the-middle attack practicality

The successful implementation of the attack use cases requires the intruder to cause the binary operate (BO) and analog operate (AO) FCIs and read response (RR) FDIs in a particular sequence as shown in Figure 19. Due to the resource limitations at the attacker, such as sniffing from a single network buffer, it can only accomplish the modification operations with a success probability of q, p, and r for BO, AO, and RR packets separately, which are 0.8, 0.85, and 0.62, computed empirically using the Table 6.

The intruder continues the attack until it reaches its goal to overload the branch (5285,5046). Hence, we evaluate the average (over all the scenarios in each use case) minimum number of FCI and FDI modifications the intruder has to perform to reach its target. Table 7 shows the minimum number of FCI and FDI attempts on average, experimentally performed to accomplish the final goal of the intruder for each use case with both the RTAC and the OpenDNP3 master. For *UC4*, the number of FDI attempts is higher because the processing time of an FDI is higher than the processing time of an FCI, as it involves parsing the DNP3

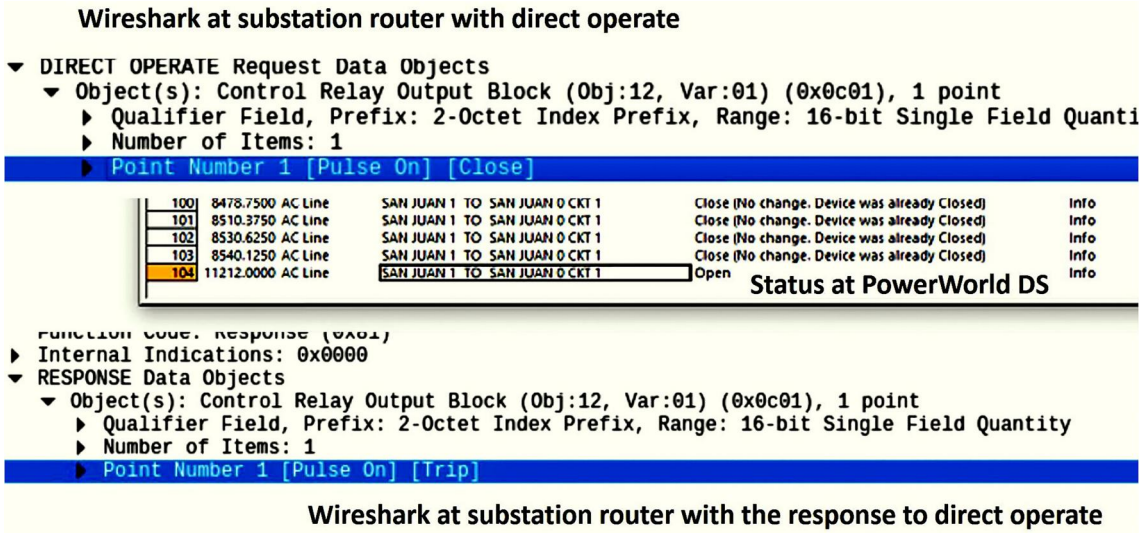

FIGURE 15 DNP3 *DIRECT OPERATE* command altered by intruder

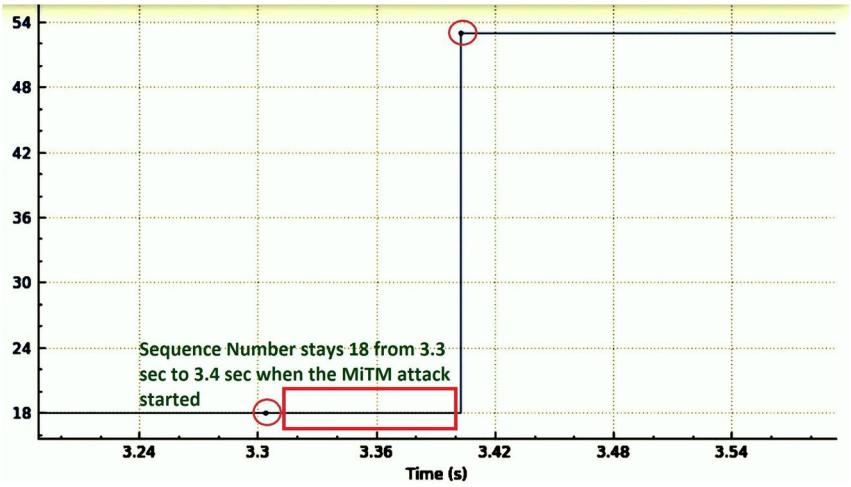

FIGURE 16 Verification that the intruder used the same sequence number to forward the modified packet

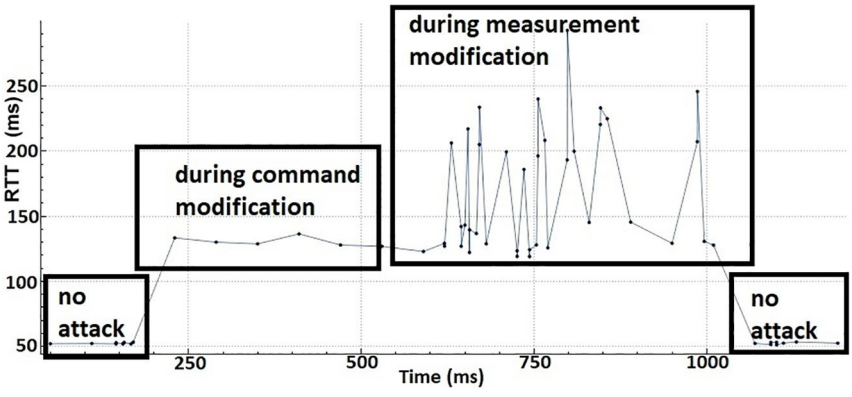

FIGURE 17 Round trip times (RTT) of DNP3 traffic through the substation router during the false command injection (FCI) and false data injection (FDI) attack in use case 4 at substation *WADSWORTH*

TABLE 5 Use cases based on the type and sequence of modifications performed to study physical impacts

FCI		FCI with FDI	
UC1	**UC2**	**UC3**	**UC4**
Binary commands	Analog and binary commands	Measurements followed by commands	Measurements, commands and measurements

Abbreviations: FCI, false command injection; FDI, false data injection.

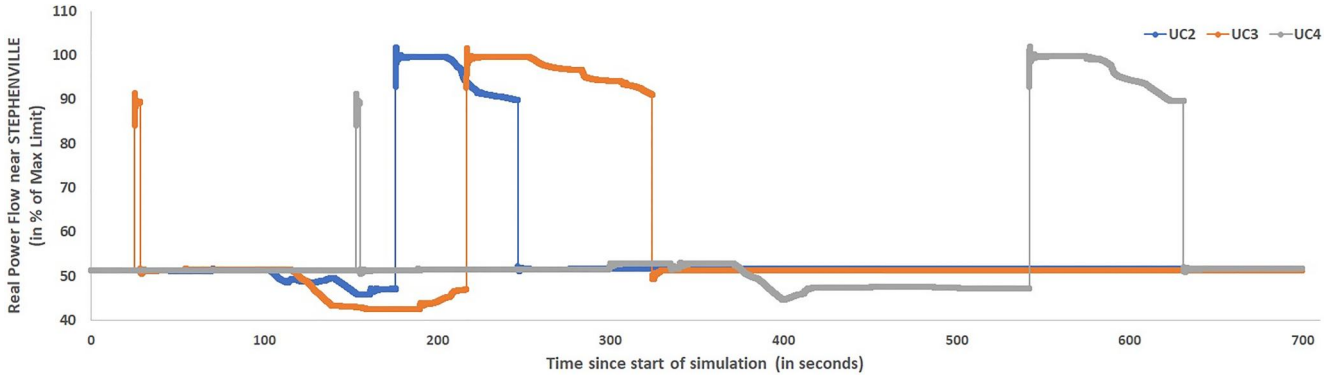

FIGURE 18 Impact of line overload caused through different use cases

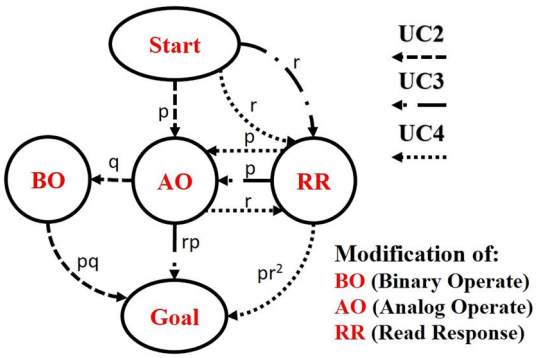

FIGURE 19 Action sequence of intrusions for *UC2*, *UC3*, and *UC4*

TABLE 6 Successful attempts for different MiTM scenarios with the Open DNP3 Master used to empirically compute the success probability q, p, and r

Scenarios		UC2		UC3		UC4	
OS/Poll	Type	Succ	Total	Succ	Total	Succ	Total
5/30s	BO	1	1	-	-	-	-
	AO	7	10	7	8	9	11
	RR	-	-	23	23	33	48
5/60s	BO	1	1	-	-	-	-
	AO	7	8	7	7	7	8
	RR	-	-	13	14	22	34
10/30s	BO	1	2	-	-	-	-
	AO	7	11	7	7	8	8
	RR	-	-	46	48	37	103
10/60s	BO	1	1	-	-	-	-
	AO	7	9	7	8	11	12
	RR	-	-	16	19	17	49

Abbreviations: AO, analog operate; BO, binary operate; MiTM; Man-in-the-middl; RO, read response.

response from outstations that usually have large payloads. This higher processing time reduces the success probability of the FDI attack. For *UC3*, in the RTAC case, an exception

TABLE 7 Minimum number of FCI and FDI attempts required on average by the intruder for accomplishing its goal in *UC2*, *UC3*, and *UC4*

	OpenDNP3 Master			RTAC Master		
Type	UC2	UC3	UC4	UC2	UC3	UC4
FDI	N/A	25.5	27.25	N/A	17.7	30.3
FCI	16.75	15.5	18.6	27.3	54.7	17.4

Abbreviations: FCI, false command injection; FDI, false data injection; RTAC, real-time automation controller.

TABLE 8 Minimum number of FCI and FDI attempts required for *UC2*, *UC3*, and *UC4*, based on the success probabilities p, q, r computed empirically

	Formulae			Evaluation OpenDNP3		
Type	UC2	UC3	UC4	UC2	UC3	UC4
FDI	N/A	o/r	2°/r	N/A	11.29	16.47
FCI	m/q + n/p	n/p	n/p	9.48	8.235	8.235

Abbreviations: FCI, false command injection; FDI, false data injection.

of higher FCIs is observed due to the automated generation protection control logic incorporated in the RTAC that caused more control traffic. Based on the success probabilities computed empirically using Table 6, the expected number of steps for FCI and FDI attacks for the use cases are computed using the formulae in Table 8, where the numerators indicate the BO, AO, and RR manipulations m, n, and o, respectively, and the denominators indicate the success probabilities. The m, n, and o will vary when we select a different contingency as a target. The formulae are based on the fact that the expected number of trials until success is inverse of the success probability and each of the manipulations is independent. For experiments with the OpenDNP3 master, the minimum number of FDI attempts is more than the FCI attempts, validated both from experiments (Table 7) and from the theory (Table 8) with $m = 1$, $n = 7$, and $o =$, for the $N - 8$ contingency (one branch and 7 generators) in *UC 2, 3,*and *4*. The experimental results can only match exactly with the theoretical ones if the success probabilities are computed from more samples, as per the law of large numbers.

Analysing the results from the queueing theory perspective, the traffic intensity ρ is computed based on the packet arrival rate λ and the service rate μ as $\rho = \frac{\lambda}{\mu}$ [62]. From the intruder reference, the arrival rate λ is determined by the polling rates from the master as well as the number of DNP3 masters. The service rate μ is fixed since it is the single intrusion node that processes the incoming traffic. The higher the ρ, the lower the success probability for the intruder to modify the traffic. In our simulation, since we observe polled traffic as well as commands, the arrival rate follows a random distribution. Every payload that the intruder fails to forward results in the drop of the packet and triggers retransmissions from the sender. The impact of polling rates, number of polled DNP3 outstations on the number of retransmissions, as well as the analysis of processing time and its impact on RTT for different attacks is presented in our work [43].

6.5 | Elasticsearch logstash kibana stack visualisation

RESLab visualises the results using Elasticsearch Logstash Kibana (ELK) stack, where Figure 20 shows a real-time count of the number of active TCP flows while the experiments are being performed for the four use cases with 5 and 10 DNP3 masters. Since the number of active TCP flows is an indicator of the number of connected clients, it helps us detect the

FIGURE 20 Count of TCP flows from Packetbeat using Kibana when the use cases with 10 and 5 masters are incorporated

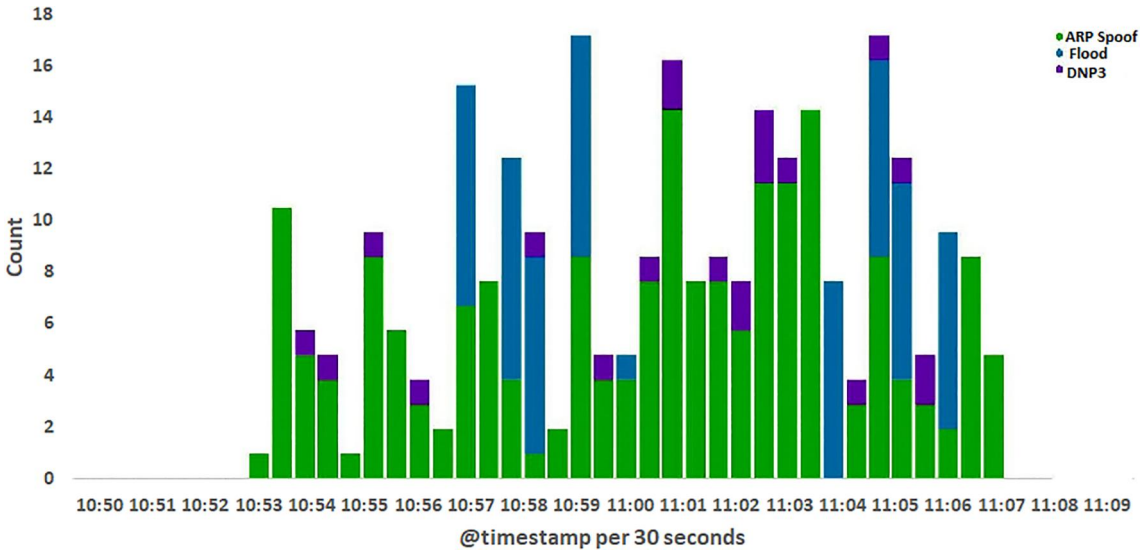

FIGURE 21 Snort alerts by alert type using Logstash and Kibana

number of clients if there are more than the intended number of clients. At certain times, we observe more than 10 active connections, as some clients lose connection and re-initate a new connection with a different source port number due to the MiTM attacks. A higher variance of connections is observed in 10 master cases due to higher retransmissions.

The Kibana Query Language (KQL) filters help us filter traffic, based on the source IP of the DNP3 master (i.e., 172.16.0.2) and the destination port in the DNP3 outstations (i.e., 20,000) as shown in Figure 20. A separate Logstash index is created in Elasticsearch to store real-time Snort alerts. Figure 21 shows the histogram in Kibana for Snort alerts such as ICMP flood, ARP spoof, and DNP3 operate during one of the scenarios from the use cases.

6.6 | Discussion

These results validate the integration of emulators, simulators, hardware, and software tools including visualisation and IDS in RESLab by performing DoS and MiTM attacks on the power system. Through four use cases, RESLab shows how such attacks can cause contingencies in the electric grid.

To understand the dynamics of the DoS attack, the results present the impact on RTT and throughput due to different attack intervals and payload sizes of ICMP injections in DoS. For understanding the dynamics of the MiTM attack, we analyse the strategies adopted by the intruder to cause the desired contingencies. We analysed MiTM attacks' practicality based on the attack success probability of each kind of traffic under each kind of different polling intervals and the number of polled outstations. The intrusions performed in *UC3* and *UC4* provide a platform to create and mitigate FDI attacks on state estimation which involves an intruder tampering with the measurements.

The simulations performed for the substation network in CORE consisted of one broadcast domain. This caused the intruder to observe the traffic related to all the substations. The number of DNP3 masters is limited to 5 or 10 in our scenarios which is enough to enable the intruder to accomplish its $N - x$ contingencies such that its x components are in these 5 or 10 substations. However, they are modelled through a single substation network in CORE. Hence, the intruder's capacity to inject modified traffic is resource-limited due to having a single substation LAN in CORE, as the intruder can only process traffic on the single network buffer.

7 | CONCLUSION

A cyber-physical testbed provides a platform to understand security threat events and their impact on the power grid. This will help to facilitate grid resiliency to cyber intrusions. In this work, we present our testbed RESLab, where its architecture makes use of components, such as vSphere, CORE, PWDS, Snort, RTAC and different automation tools for experiment orchestration, data collection, and visualisation, for emulating the physical and cyber component of a synthetic large-scale electric grid and for demonstrating the use of DNP3-based control and measurement traffic to and from substation field devices. The methodology and mechanics behind our testbed are demonstrated through four use cases of MiTM intrusions and varying impact of DoS intrusion strength. The dynamics of the intrusions are validated by implementing use cases targeting specific parts of a large-scale grid. These intrusion events are evaluated from their respective characteristic features, including latency (RTT), throughput, and goodput in the emulated WAN network. We additionally provide a rigorous analysis on MiTM attack practicality by empirically computing the attack probability and validating it from experiments and theory.

By providing a safe proving ground for cyber-attack experimentation, RESLab is a platform to study defence mechanisms where its ability to generate real-time datasets and customise monitoring, visualisation, and detection will play a major role in developing cyber-physical state estimation, situational awareness, optimal response etc. to prevent impending contingencies.

ACKNOWLEDGEMENTS

This research is supported by the US Department of Energy's (Doe) Cybersecurity for Energy Delivery Systems programme under award DE-OE0000895.

ORCID

Abhijeet Sahu https://orcid.org/0000-0002-7647-3758
Ana Goulart https://orcid.org/0000-0001-7184-7485

REFERENCES

1. CBR Staff Writer: High Voltage Attack: EU's Power Grid Organisation Hit by Hackers. TECH MONITOR, Online (2020) [Online]. https://www.cbronline.com/news/eu-power-grid-organisation-hacked
2. Robert M., Lee, Michael J., Assante: Tim, Conway, Background. Analysis of the cyber attack on the Ukrainian power grid (E-ISAC, Online 2016). https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf
3. Streltsov, L.: The system of cybersecurity in Ukraine: Principles, actors, challenges, accomplishments. European Journal for Security Research. 2(2), 147–184 (2017)
4. Langner, R.: Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy. 9(3), 49–51 (2011)
5. Pan, S., Morris, T., Adhikari, U.: Developing a hybrid intrusion detection system using data mining for power systems. IEEE Transactions on Smart Grid. 6(6), 3104–3113 (2015)
6. Adhikari, U., Morris, T., Pan, S.: Wams cyber-physical test bed for power system, cybersecurity study, and data mining. IEEE Transactions on Smart Grid 8(6), 2744–2753 (2016)
7. Poudel, S., Ni, Z., Malla, N.: Real-time cyber physical system testbed for power system security and control. International Journal of Electrical Power & Energy Systems. 90, 124–133 (2017)
8. YangSezer, Y.: Multidimensional intrusion detection system for iec 61850-based networks. IEEE Trans. 32(2), 1068–1078 (2017)
9. Fovino, I.N.: An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. In: 3rd International

Conference on Human System Interaction, pp. 679–686. Human System Interactions (HSI), (2010)
10. Oyewumi, I.A.: Isaac: The Idaho cps smart grid cybersecurity testbed. In: 2019 IEEE Texas Power and Energy Conference (TPEC), pp. 1–6. IEEE, College Station, TX, USA (2019)
11. Chen, B.: Implementing a real-time cyber-physical system test bed in rtds and opnet. In: 2014 North American Power Symposium (NAPS), pp. 1–6. Pullman, USA (2014)
12. Nelson, A.: Cyber-physical test platform for microgrids: Combining hardware, hardware-in-the-loop, and network-simulator-in-the-loop. In: 2016 IEEE Power and Energy Society General Meeting (PESGM), pp. 1–5. IEEE, Boston, MA, USA (2016)
13. Mallouhi, M.: A testbed for analying security of control systems (tasscs). In: ISGT 2011, pp. 1–7. IEEE, Anaheim, CA, USA (2011)
14. Aghamolki, H.G., Miao, Z., Fan, L.: A hardware-in-the-loop SCADA testbed. In: 2015 North American Power Symposium (NAPS), pp. 1–6. IEEE, Charlotte, NC, USA (2015)
15. Sahu, A., Goulart, A., Butler-Purry, K.: Modeling ami network for real-time simulation in ns-3. In: 2016 Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 1–8. IEEE, Chicago, IL, USA (2016)
16. Raybourn, E.M., et al.: A zero-entry cyber range environment for future learning ecosystems. In Cyber-Physical Systems Security. pp. 93–109. Springer (2018)
17. Johnson, J., Jacobs, N.: Sceptre: power system and networking co-simulation environment Workshop on Co-Simulation Platforms for the Power Grid, Berkeley, CA, USA 07. (2018)
18. Palmintier, B.: Design of the HELICS high-performance transmission-distribution-communication-market co-simulation framework. In: 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), pp. 1–6. IEEE Pittsburgh, PA, USA (2017)
19. Yafen, S.: Reliability analysis of system-in-the-loop network platform based on delays. In: 2011 Seventh International Conference on Computational Intelligence and Security, pp. 750–753. IEEE, Sanya, China (2011)
20. Hong, J., et al.: Cyber-physical security test bed: a platform for enabling collaborative cyber defense methods. In: PACWorld Americas Conference 2015. Raleigh, NC, USA (2015)
21. Liu, R., et al.: Analyzing the cyber-physical impact of cyber events on the power grid. IEEE Transactions on Smart Grid. 6(5), 2444–2453 (2015)
22. Kezunovic, M.: The use of system in the loop, hardware in the loop, and co-modeling of cyber-physical systems in developing and evaluating new smart grid solutions. In: Proceedings of the 50th Hawaii International Conference on System Sciences HICSS, Manoa, Hawaii (2017)
23. Papaspiliotopoulos, V.A.: et al., Hardware-in-the-loop design and optimal setting of adaptive protection schemes for distribution systems with distributed generation. IEEE Trans. 32(1), 393–400 (2015)
24. Ashok, A.: Experimental evaluation of cyber attacks on automatic generation control using a cps security testbed. In: 2015 IEEE Power Energy Society General Meeting, pp. 1–5. IEEE PES, Denver (2015)
25. Zhang, Y.: Real time digital simulation for large power systems with embedded power electronics. IEEE PES, Portland (2018). http://site.ieee.org/pes-hpcgrid/files/2019/08/5_PESGM2019.pdf
26. Johnson, J., et al.: Interconnection standard grid-support function evaluations using an automated hardware-in-the-loop testbed. IEEE Journal of Photovoltaics. 8(2), 565–571 (2018)
27. Thornton, M., et al.: Internet-of-things hardware-in-the-loop simulation architecture for providing frequency regulation with demand response. IEEE Transactions on Industrial Informatics. 14(11), pp. 5020–5028 (2017)
28. Piesciorovsky, E.C., Schulz, N.N.: Fuse relay adaptive overcurrent protection scheme for microgrid with distributed generators. IET Gener. 11(2), 540–549 (2017)
29. BecejacO'Brien, T.: Prime: a real-time cyber-physical systems testbed: from wide-area monitoring, protection, and control prototyping to operator training and beyond. IET Cyber-Physical Systems: Theory Applications. 5(2), 186–195 (2020)
30. Azimian, B., et al.: Cross-platform comparison of standard power system components used in real time simulation. In: 2019 7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, pp. 1–6 IEEE, Montreal (2019)
31. Stifter, M., et al.: Real-time simulation and hardware-in-the-loop testbed for distribution synchrophasor applications. Energies. 11(4), p. 876 (2018)
32. Yang, Y., et al.: Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems. In: International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), pp. 1–8. IET Hangzhou (2012)
33. Birchfield, A.B., et al.: Grid structural characteristics as validation criteria for synthetic networks. IEEE Trans. Power. Syst. 32(4), 3258–3265 (2017)
34. Wlazlo, P.: A cyber topology model for the Texas 2000 synthetic electric power grid. In: 2019 Principles, Systems and Applications of IP Telecommunications (IPTComm), pp. 1–8. IEEE, Chicago (2019)
35. Onunkwo, I., et al.: Technical Report. Cybersecurity assessments on emulated der communication networks. vol. 03 (2019). https://www.osti.gov/biblio/1761846
36. Sahu, A., et al.: Data processing and model selection for machine learning-based network intrusion detection. In: 2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability. pp. 1–6. IEEE Virtual Conference (2020)
37. Adhikari, U., Morris, T., Pan, S.: Wams cyber-physical test bed for power system, cybersecurity study, and data mining. IEEE Transactions on Smart Grid. 8, 1 (2016)
38. Pan, S., Morris, T., Adhikari, U.: Developing a hybrid intrusion detection system using data mining for power systems. IEEE Transactions on Smart Grid. 6(6), 3104–3113 (2015)
39. Pan, S., Morris, T., Adhikari, U.: A specification-based intrusion detection framework for cyber-physical environment in electric power system. Int. J. Netw. Secur. 17, 174–188 (2015)
40. Sahu, A.: Cyber-physical dataset for attacks in power systems IEEE Dataport, Online (2021). https://doi.org/10.21227/e4dd-2163
41. Sahu, A., Mao, Z.: Multi-source data fusion for cyber intrusions in power systems. CodeOcean, Online (2021). https://codeocean.com/capsule/3327036/tree
42. Sahu, A.: Multi-source data fusion for cyberattack detection in power systems arXiv, Online (2021). https://arxiv.org/abs/2101.06897
43. Wlazlo, P.: Man-in-the-middle attacks and defene in a power system cyber-physical testbed arXiv, Online (2021). https://arxiv.org/abs/2102.11455
44. Kundu, A.: Attention-based auto-encoder anomaly detector for false data injection attacks. Elec. 189, 106795 (2020). [Online] http://www.sciencedirect.com/science/article/pii/S0378779620305988
45. Ozay, M., et al.: Machine learning methods for attack detection in the smart grid. IEEE Transactions on Neural Networks and Learning Systems. 27(8), 1773–1786 (2016)
46. Davis, C.M.: Scada cyber security testbed development. In: 2006 38th North American Power Symposium, pp. 483–488. IEEE, Carbondale (2006)
47. Gaudet, N.: Firewall configuration and path analysis for networks. In: 2020 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR), pp. 1–6. IEEE, Virtual Conference (2020)
48. Huang, H., Davis, K.: Extracting substation cyber-physical architecture through intelligent electronic devices' data. In: 2018 IEEE Texas Power and Energy Conference (TPEC), pp. 1–6. IEEE, College Station (2018)
49. Tan, S., et al.: Score: smart-grid common open research emulator. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp. 282–287. IEEE, Taiwan City (2012)

50. Schroder, C.: Dynamic routing with quagga. (2018). https://www.linux.com/topic/networking/dynamic-linux-routing-quagga/
51. Overbye, T.J.: An interactive, stand-alone and multi-user power system simulator for the PMU time frame. In: 2019 IEEE Texas Power and Energy Conference (TPEC), pp. 1–6. IEEE, College Station (2019)
52. Overbye, T.J.: An interactive, extensible environment for power system simulation on the time frame with a cyber security application. In: 2017 IEEE Texas Power and Energy onference (TPEC), pp. 1–6. IEEE, College Station (2017)
53. Mao, Z., et al.: W4IPS: A web-based interactive power system simulation environment for power system security analysis. InProceedings of the 53rd Hawaii International Conference on System Sciences Manoa, Hawaii (2020)
54. East, S., et al.: A taxonomy of attacks on the dnp3 protocol. vol. 311 (2009)
55. Packetbeat in elk stack. Elasticsearch B.V. (2021). https://www.elastic.co/beats/packetbeat
56. Zabbix for network monitoring. Zabbix LLC. https://www.zabbix.com/network_monitoring
57. Ortega, A.P.: Preventing arp cache poisoning attacks: proof of concept using openwrt. In: 2009 Latin American Network Operations and Management Symposium, pp. 1–9. IEEE, Punta del Este (2009)
58. Narimani, M., et al.: Generalized contingency analysis based on graph theory and line outage distribution factor. arXiv, Online (2020). https://arxiv.org/abs/2007.07009
59. Kalluri, R.: Simulation and impact analysis of denial-of-service attacks on power scada. In: 2016 National Power Systems Conference, pp. 1–5. NPSC, Bhubaneswar (2016)
60. Day, T.: Dnp3, distributed network protocol v3 an introduction. eventscloud, Online (2015). https://na.eventscloud.com/file_uploads/b68188f3ce5b22895a67b1afe5e51b6a_DNP3IntroductionHORS.PDF
61. Peterson, L.L., Davie, B.S.: Computer networks. In: A systems approach, 5th ed. Morgan Kaufmann Publishers Inc., San Francisco (2011)
62. Bertsekas, D., Gallager, R.: Delay Models in Data Networks. Data networks, 2nd. Prentice-Hall, Inc., USA (1992)

How to cite this article: Sahu, A., et al.: Design and evaluation of a cyber-physical testbed for improving attack resilience of power systems. IET Cyber-Phys. Syst., Theory Appl. 6(4), 208–227 (2021). https://doi.org/10.1049/cps2.12018