CPS Testbed Architectures for WAMPAC using Industrial Substation and Control Center Platforms and Attack-Defense Evaluation

Gelli Ravikumar, *Member, IEEE*, Burhan Hyder, *Student Member, IEEE*, Jeyanth Rajan Babu, Kush Khanna, *Member, IEEE*, Manimaran Govindarasu, *Fellow, IEEE*, and Manu Parashar

***Abstract*—Advanced persistent threats and cyberattacks can impact wide-area monitoring, protection, and control (WAMPAC) system operation. Many cyber-physical system (CPS) testbeds have been developed for attack-defense experimentation and attack-resiliency tools evaluation for WAMPAC, but they are limited to a simulation-and-emulation based environment. This paper presents a quasi-realistic CPS attack-defense testbed-based framework for WAMPAC applications using the industrial substation and control center platforms such as eTerra integrated with the hardware-in-the-loop CPS smart grid testbed available at Iowa State University. The proposed framework includes various combinations of industry-grade substation and control center platforms, communication topologies, realtime digital simulators, and a novel cyber-physical distributed intrusion-and-anomaly detection system (D-IADS) for WAMPAC applications. The D-IADS includes a *master* at the control center and geographically distributed *sensor* devices at each substation. Each D-IADS sensor deployed at a substation or control center network monitors ingress and egress traffic, detect intrusions, and dispatch alerts to the D-IADS master. The D-IADS master centrally monitors and analyze the alerts and controls D-IADS sensors. We considered an EMP60 synthetic CPS grid as a case study to demonstrate the framework and proposed D-IADS for WAMPAC applications against cyberattack vectors such as Man-in-the-Middle DNP3 attack, denial-of-service, and data-integrity attacks.**

***Index Terms*—Cyber-physical testbed, WAMPAC, smart grid.**

I. Introduction

THE modern electric power system is a complex and interdependent cyber-physical system (CPS). The reliable, secure, and resilient operation of CPS smart grid is of paramount importance to national security and is vital to other interdependent critical infrastructure sectors [1]. With the growing cybersecurity challenges across the CPS smart grid critical infrastructure, it is essential to carry out cyber attack-defense experimental studies to evaluate their impact on the power systems and smart grid applications. It becomes prohibitively expensive to replicate a real-world CPS smart grid environment for attack-defense experiments. Various CPS smart grid testbed platforms have been attempted to develop impact characteristics on the inter-dependent dynamics of power and cyber systems, and for the consolidated analysis on the performance of the CPS smart grid applications subject to various cyber system impacts [2]–[5]. Hardware-in-the-Loop testbed-based evaluations have been carried out for various CPS WAMPAC applications [6]–[9]. While simulation-and-emulation-based testbeds provide a flexible environment, they have limitations in the cyber-physical attack-defense experiments. They do not capture the essential behaviors and interactions of industry-grade control center applications, WAMPAC and energy management systems (EMS), substation applications, and supervisory control and data acquisition (SCADA). This shortcoming motivates the need to include an industry-grade control center platform such as eTerra for EMS and WAMPAC applications, industry-grade substation platforms such as SICAM PAS Siemens substation automation system (SAS), SEL protection relays (SEL 421 and SEL 351), and SEL Real-time automation controller (SEL-3530). We discussed efficient modeling of the substation platform including Siemens SAS, industry-grade relays, and RTAC, and real-time digital simulator for small-scale to large-scale power grid models, and attack-defense applications [10]–[12] using the CPS smart testbed available at Iowa State University. This paper presents the testbed integration to the industry-grade eTerra control center platform (SCADA, EMS, and WAMPAC applications), realistic multistage cyberattack scenarios, and a defensive solution D-IADS.

The paper is organized as follows: Sections II and III propose CPS attack-defense framework for WAMPAC applications and D-IADS. Section IV discusses testbed-based validation and evaluation to demonstrate efficacy of the proposed methodology, followed by, conclusions in Section V.

II. Proposed CPS Attack-Defense Framework for SCADA, EMS, and WAMPAC Applications

We consider integrating an industrial-grade eTerra control center platform to advance our existing Hardware-in-the-Loop (HIL) CPS testbed [10], [13], [14] for realistic testing and evaluation of data-integrity cyberattacks and their effect on the real-world SCADA, EMS, and WAMPAC applications. To achieve scalability, ability to execute small-scale to large-scale power grid models and cyber system models, we consider three critical CPS WAMPAC testbed architectures – **Design-1** integrates the eTerra platform directly to Real-Time Digital Simulator (RTDS), **Design-2** integrates the eTerra to RTDS via Siemens SICAM PAS substation remote terminal unit (RTU) and substation automation system (SAS), and **Design-3** integrates the eTerra to RTDS via Substation RTUs and substation field devices such as Relays, PMUs, and Real-Time Automation Controller (RTAC). Fig. 1 shows these three CPS WAMPAC testbed-based designs, including RTDS, industrial-grade field devices, substation RTUs/SAS, and eTerra control center platform. We consider widely-used virtual and real (physical) communication network topologies in these designs

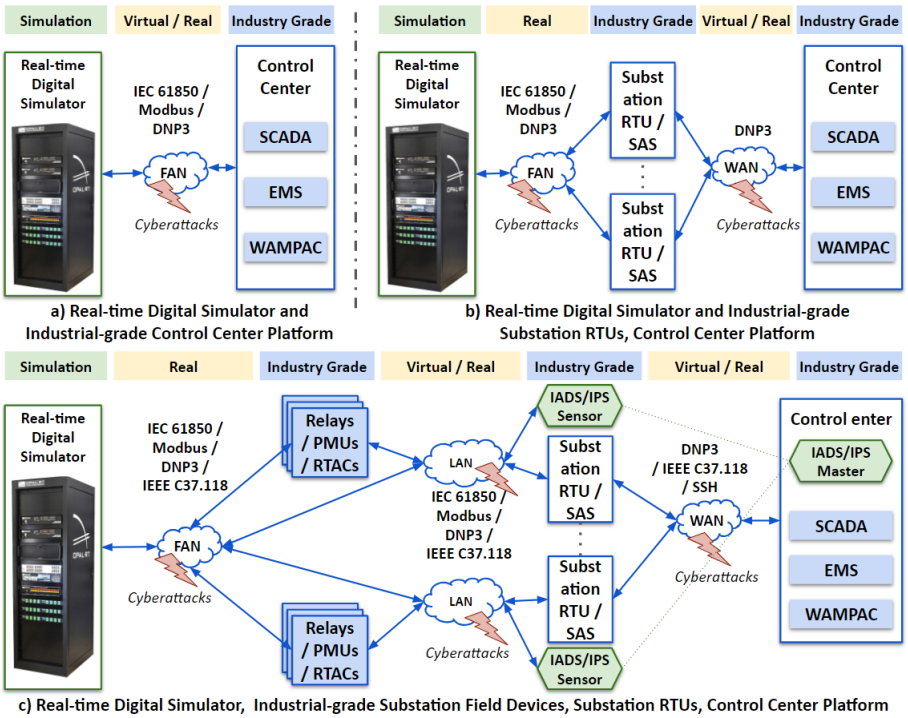

Fig. 1. Proposed CPS WAMPAC Framework using Industrial-grade platforms integrated with real-time digital simulator

– i) field-area network (FAN) by physical communication networks, switches, and routers, ii) local-area network (LAN) by virtual communication networks, switches, and routers, and iii) wide-area network (WAN) by virtual communication networks, switches, routers, and routing topologies.

We consider **Design-1** shown in Fig. 1a, to simulate large-scale power grid and cyber system models. However, it does not provide the capabilities to test, validate, and evaluate data-in-transit network-based defense-in-depth CPS security tools. The **Design-2** shown in Fig. 1b provides realistic SCADA interactions between industrial-grade substation RTU/SAS and control center platform. We consider this design to test and evaluate multistage cyberattacks, including data-integrity cyberattacks and evaluate their impact on the SCADA and WAMPAC applications in the industrial-grade control center environment. The **Design-3** shown in Fig. 1c further extends it to the intra-substation environment to capture substation-wide SCADA interactions across substation field devices such as protection relays, PMUs, and RTACs. In Section IV, we discuss the demonstration of **Design-3**, which is a superset of both designs 1 and 2, for various multistage cyberattacks and the proposed D-IADS under CPS WAMPAC environment.

We consider an e-terra control center platform for the Designs 1, 2, and 3. Hence, these three designs support both small-scale and large-scale power system applications. The purpose for proposing the three designs is to increase granularity at the middle-layer between a control center and the real-time grid simulator. Design-1 has Zero middle-layer components, Design-2 has industrial substation RTU/SAS as middle-layer components, and the Design-3 has both industrial substation RTU/SAS software and industrial field devices such as Relays, PMUs, and RTACs. We follow the communication topologies similar to what the power utilities use in-practice to operate electric power grids. Hence, we used WAN for control center and substation communication, LAN for substation RTU/SAS and field device communication, and FAN for field devices and grid simulator communication.

III. Proposed Distributed Intrusion-and-Anomaly Detection System (D-IADS) for SCADA & WAMPAC

To achieve cyber-physical situational awareness and monitor the network intrusions and anomalies, we proposed a D-IADS algorithm for CPS WAMPAC, as shown in Fig. 2. The D-IADS includes a *master* at control center and geographically distributed *sensor* devices at each substation. The D-IADS master centrally monitors and analyzes the alerts and controls D-IADS sensors. Each D-IADS sensor deployed at a substation or control center network monitors ingress and egress traffic, detects intrusions, and dispatches alerts to the D-IADS master. A D-IADS sensor uses an Intrusion Detection System (IDS) engine such as Snort, Suricata, or Zeek to process the ingress and egress traffic and matches them with the IDS rule sets. There are well-known IDS rules for detecting many IT-based cyberattacks. There were some attempts to build DNP3-specific IDS rule sets, but they are limited to IP-based signatures [15]–[17]. We analyzed the SCADA and WAMPAC traffic using the testbed as shown in Fig. 1c and defined DNP3-function-specific and threshold-based more in-depth packet inspection IDS rules to detect intrusions and anomalies on analog and digital measurements.

The proposed D-IADS rule algorithm uses the IDS_{rule} function as defined in (1).

$$IDS_{rule} = f(R_a, R_p, S_{IP}, S_{Port}, D_{IP}, D_{Port}, R_{Body}) \quad (1)$$

The R_a denotes rule action such as $alert$, the R_p denotes rule protocols such as ICMP, TCP, UDP, FTP, SSH, and DNP3.

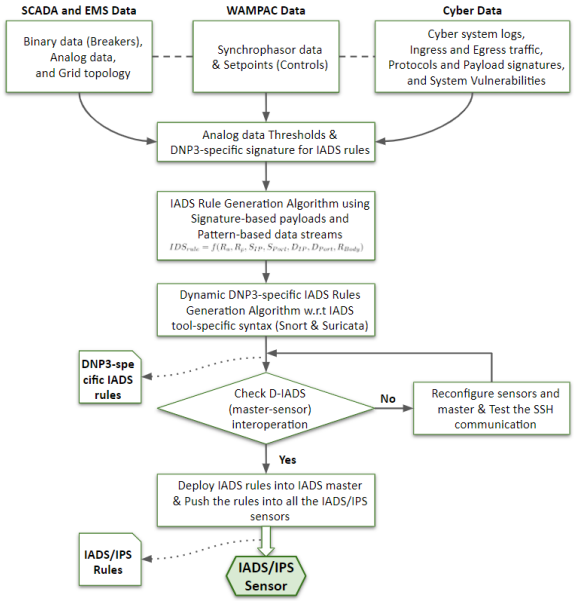

Fig. 2. Proposed D-IADS Algorithm for CPS SCADA, EMS, and WAMPAC

The S_{IP} denotes source IP address of the packet, the S_{Port} denotes source Port number of the packet, the D_{IP} denotes destination IP address of the packet, and the D_{Port} denotes destination Port number of the packet. The R_{Body} denotes the rule-body, which includes various parameters to conduct deep packet inspection, threshold count bands, and threshold bands for analog data points. Fig. 3 shows an example list of four rules, where **R1** and **R2** detect violations on the analog data against data-integrity cyberattacks, **R3** detects port scanning, and **R4** detects network reconnaissance.

R1 is used to detect when a substation RTU (a DNP3 client) reports an analog measurement voltage violation greater than 1.04 p.u. on a specific substation. This rule utilizes the hex codes to measure the specific analog input voltage configured at a specific point in the DNP3 SCADA software. The rule checks specific byte codes at specific positions pointed by depth and distance keywords. The $|05\ 64|$ byte codes indicate the start of a DNP3 payload. $|81|$ represents the response function code. $|1e\ 05|$ represents the analog input DNP3 object group number 30 variation 05. *byte_test* keyword is used to detect the analog data represented as a 32-bit floating-point number, compared against the threshold value set in the rule.

R2 is used to detect when the substation RTU (a DNP3 client) reports an analog measurement system frequency violation occurring at Area $East$. Hex codes are again used to measure the specific analog input frequency configured at a specific point in the substation RTU DNP3 SCADA software.

R3 detects the port scanning operation being carried out on Substation Kincard using tools such as NMAP. Port scanning operation detects open ports by sending TCP SYN packets to all the ports of a device within the range (0-65535) in a short period of time, stopping at the reception of ACK packets without completing the 3-way handshake. The rule looks out for a bombardment (count: 500) of SYN packets within 30 seconds on a single host using the threshold snort keyword.

R4 flags reconnaissance attempts for host discovery made by adversaries as a part of the fingerprinting processes to detect

R1	`alert tcp $Substation_IP 20000 -> $ControlCenter_IP any (msg: "Voltage violation > 1.04 pu @ Richview"; content: "|05 64|"; depth: 2; content: "|81|"; distance: 10; content: "|1e 05|"; distance: 2; byte_test: 2,>,0xc842,40; sid: 96500161;)`
R2	`alert tcp $Substation_IP 20000 -> $ControlCenter_IP any (msg: "System frequency violation @ East Area"; content: "|05 64|"; depth: 2; content: "|81|"; distance: 10; content: "|1e 05|"; distance: 2; byte_test: 2,<,0x6c42,57; sid: 96500162;)`
R3	`alert tcp $EXTERNAL_NET any -> $Substation_IP $TCP_PORTS (msg: "Port scanning on Kincard RTU (East Area)"; flags:S; threshold: type both,track by_src,count 500,seconds 30; sid: 96500163;)`
R4	`alert icmp $EXTERNAL_NET any -> $Substation_IP any (msg: "Reconnaissance on Kincard RTU (East Area)"; sid: 96500164;)`

Fig. 3. D-IADS Rules (Example Rule Anatomy)

device vulnerabilities. This rule triggers when ICMP packet requests are made from an external network.

We consider these SCADA DNP3-specific rules, particularly **R1** and **R2** types, for all the analog and digital measurements of every substation to detect anomalies due to cyberattacks and power grid perturbations. The significant challenge is to define desirable thresholds and these can be derived by historical values, system operator domain knowledge, and grid analysis.

IV. Testbed-based Experiments and Evaluation

The implementation of the proposed framework is done on the HIL CPS testbed at Iowa State University [10]. The GE eTerra platform situated in the control center provided an open-loop and closed-loop SCADA, EMS, and WAMPAC applications to implement the proposed framework. These applications include Automatic Generation Control (AGC), Real-Time Contingency Analysis (RTCA), and Remedial Action Scheme (RAS) as closed-loop applications and State Estimation, Volt/VAR Dispatch, Short Circuit Analysis, etc. as open-loop applications. As described in Fig. 1, the three topologies are achieved by (a) Interfacing OPAL-RT (real-time power system model simulator – RTDS) directly with the eTerra platform wherein the OPAL-RT DNP3 I/O interface module is used to send and receive the required measurements and controls to and from the eTerra SCADA and EMS applications, and IEEE C37.118 I/Os to send to Phasorpoint; (b) Interfacing eTerra platform with Siemens RTU software which in turn is interfaced with the OPAL-RT allowing communication between OPAL-RT and the control center applications; (c) Interfacing eTerra platform with Siemens RTU software which is configured with industrial-grade hardware relays, PMUs, and RTACs, and OPAL-RT through these devices. For this study, we model the EMP60 (i) in OPAL-RT to closely mimic the actual grid in real-time; (ii) in the Siemens RTUs to relaying information between the grid and the control center utilizing DNP3 RTU mapping; (iii) in the eTerra platform which acts as a control center executing EMS applications like State Estimation. The EMP60 model shown in Fig. 4 consists of 30 substations, 136 buses, and 3 control areas: $ECAR$, $East$, and $West$ areas. For each substation in the system, various signals including bus voltage magnitudes, branch real and reactive power flows, and power injections from loads or generators are exchanged with the eTerra platform from the OPAL-RT. The e-terraEMP can send close and trip commands to breakers and ramp-up/down signals to the generators by closed-loop applications like AGC and RAS.

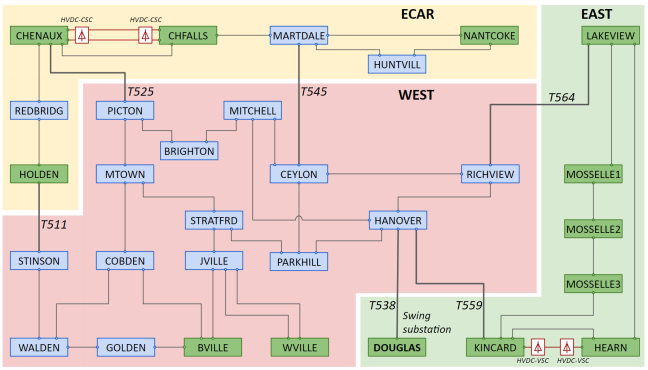

Fig. 4. Network Diagram for an EMP60 Synthetic CPS Grid. It has 3 areas and 30 Substations. Generation substations are highlighted in green colour.

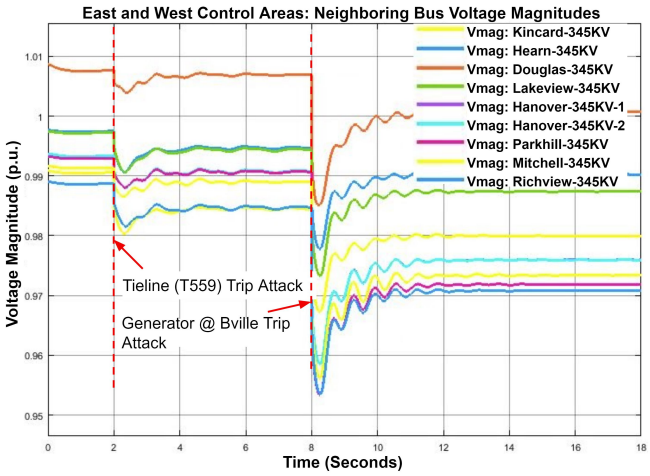

Fig. 5. Impact of coordinated DNP3 MITM attack on $East$ and $West$ control area voltage magnitudes, captured via IEEE C37.118 with 60 fps.

A. Modeling of Cyberattack Vectors

To demonstrate cyber attacks and defense tools for WAMPAC, we consider the following multistage cyberattacks – information technology (IT) intrusions and industrial control system (ICS) intrusions. The IT-intrusion stage includes Reconnaissance – Ping and Nmap attacks; Data Exploitation using Metasploit framework; Data Exfiltration; and Malware Installation. Upon successful IT-intrusion attacks, we carried out ICS-intrusion by DNP3 Man-in-the-Middle (MITM) attacks, including tieline trip and generator ramp-down cyberattacks. We discussed the modeling of these attacks in [12]. We carried out these attacks on multiple networks, including WAN, LAN, and FAN, as shown in Fig. 1. Further, we carried out MITM data-integrity attacks to manipulate measurement signals (e.g., Generation and Tie-Line measurements) and control signals.

B. Grid Impact Scenarios against Cyberattacks

We used e-terraSCADA platform for modeling the databases and connecting the SCADA data points of EMP60 bus grid model with the Siemens substation RTUs. We use e-terraEnergyManagementPlatform (EMP) for executing the network topology processor (NTP) and state estimator EMS applications. To capture grid impact characteristics, we used e-terraPhasorPoint software for the considered system events or attack events on the grid environment (as shown in Fig. 5 and Fig. 6). We launched DNP3-based MITM attacks on the SCADA environment and captured the grid impact characteristics from the WAMPAC environment using 60 frames per second (fps) synchrophasor data streams using IEEE C37.118.

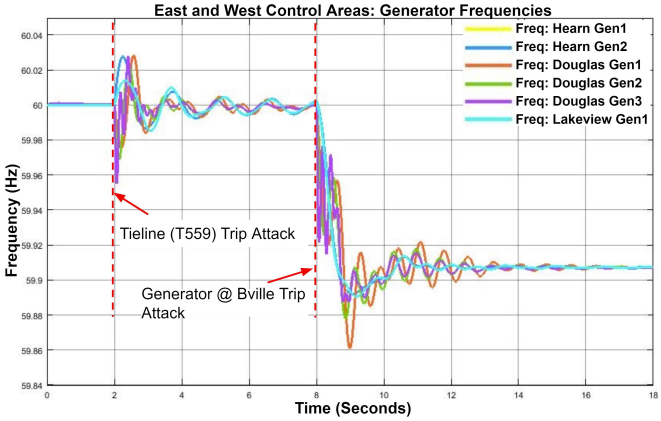

Fig. 6. Impact of coordinated DNP3 MITM attack on $East$ and $West$ control area generator frequencies, captured via IEEE C37.118 with 60 fps.

Fig. 5 shows the impact on voltage magnitudes of the buses (directly connected to substations $Hanover$ or $Kincard$) in the $East$ and $West$ control zones due to a coordinated cyberattack on the EMP60. Fig. 6 shows the impact of cyberattack vectors on the frequency of the system for each generator in the $East$ and $West$ control zones. The graphs depict two such attacks that are executed in sequence. The first attack represents a DNP3 MITM tieline trip attack on the tieline of $Hanover$ ($West$ zone) and $Kincard$ ($East$ zone) substations, namely, $T559$. The second attack is a DNP3 MITM generation trip attack where the attacker trips the generator in the $Bville$ substation. The system stabilizes after the attack vectors but the voltage magnitudes and frequency of the zones are reduced by about 2% and 0.1%, respectively. We have considered the system operating limits by the NERC [18] to define thresholds in D-IADS rules for detecting anomalies.

C. Detection of Cyberattacks using D-IADS

We implemented the D-IADS platform for both of the testbed designs shown in Fig. 1b and Fig. 1c. Fig. 7 shows the detected alerts acquisition from the geographically distributed D-IADS sensors deployed at each substation network. The alerts dashboard in the D-IADS master uses the Sguil engine to visualize alerts in real-time to system operators. These alerts also provide cyber-physical situational awareness to the system operators based on the IDS rules deployed at each D-IADS sensor. The alerts in the dashboard are categorized based on the **AlertID**. The *ST* shows cyber impact severity classification, wherin *RT* represents real-time. The *CNT* denotes number of intrusions, *Sensor* identifies the ID of each D-IADS sensor, and *Date/Time* provides timestamp to an intrusion event. The *Src IP* and *Sport* shows source IP and port of traffic flow, whereas *Dst IP* and *Dport* shows destination IP and destination port of traffic flow. The *Event Message* provides concise information about the detection of intrusion or anomaly.

The rule categories R3 and R4 are absolute, and have Zero false positives or false negatives. They can correctly determine if an NMAP or ping reconnaissance scanning attempt has been made. The R1 and R2 had a plenty of false positives during the initial deployment. We observed that the false positives were a result of the dynamic size of the DNP3 response payloads w.r.t

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	5	scadasiem...	11.42	2021-01-29 04:40:54	27.37.47.110		192.168.1.213		1	Reconnaissance on Kincard Substation RTU (East Area)
RT	1	scadasiem...	11.49	2021-01-29 04:41:05	27.37.47.110	36956	192.168.1.213	3306	6	ET SCAN Suspicious inbound to mySQL port 3306
RT	1	scadasiem...	11.50	2021-01-29 04:41:05	27.37.47.110	36956	192.168.1.213	5903	6	ET SCAN Potential VNC Scan 5900-5920
RT	1	scadasiem...	11.53	2021-01-29 04:41:05	27.37.47.110	36956	192.168.1.213	14441	6	Port scanning on Kincard Substation RTU (East Area)
RT	1	scadasiem...	11.74	2021-01-29 04:43:16	192.168.1.213	1067	27.37.47.110	4444	6	Data Exfiltration from Kincard Substation RTU (East Area)
RT	4	scadasiem...	11.75	2021-01-29 04:46:29	27.37.47.110	4444	192.168.1.213	1067	6	Malware installed into Kincard Substation RTU (East Area)
RT	4	scadasiem...	11.76	2021-01-29 04:46:29	27.37.47.110	4444	192.168.1.213	1067	6	TCP SYN flooding (DoS) on Kincard Substation RTU (East Area)
RT	1	scadasiem...	11.83	2021-01-29 04:49:39	27.37.47.110	52276	192.168.1.213	20000	6	DNP3 unauthorised Trip on T559 - Kincard Substation RTU (East Area)
RT	1	scadasiem...	11.87	2021-01-29 04:50:47	27.37.47.110	52284	192.168.1.213	20000	6	Tieline power flow violation @ T559
RT	1	scadasiem...	11.88	2021-01-29 04:55:10	27.37.47.110	52286	192.168.1.213	20000	6	Generation output violation @ Bville Substation
RT	1	scadasiem...	11.89	2021-01-29 04:55:28	27.37.47.110	52288	192.168.1.213	20000	6	Voltage violation > 1.04 pu @ Richview Substation
RT	1	scadasiem...	11.90	2021-01-29 04:55:43	27.37.47.110	52290	192.168.1.213	20000	6	System frequency violation @ East Area

Fig. 7. D-IADS Intrusion and Anomaly Detection Alerts for Multistage IT-intrusion and ICS-intrusion Cyberattacks

the total number of DNP3 change events reported and CRC checksums that inhibited indexing the DNP3 header objects precisely. We conducted DNP3 packet SCADA traffic analysis and carefully designed and modified R1 and R2 categories with the correct position of data points in the DNP3 payload for the EMP60 synthetic CPS grid environment. With these new IADS rule sets, we observed the D-IADS system correctly captured the anomalies with Zero/Less false positives or false negatives for the attack vectors.

The *AlertID*s 11.42, 11.49, 11.50, and 11.53 provided intrusion detection of reconnaissance, Emerging Threat (ET) scan, ET Virtual Network Computing (VNC) scan, and port scanning of network devices such as Substation RTUs/SAS. Upon monitoring the network, we made several attempts for successful TCP reverse bind attack establishing a communication channel with the targeted network devices such as RTU/SAS using the Metasploit framework. The *AlertID*s 11.74 and 11.75 showed the detection of data exfiltration from a substation RTU/SAS and Malware installation into a substation RTU/SAS. These alerts provided detection of real-time IT-intrusion multistage cyberattacks. Upon IT-intrusion, adversaries may launch MITM data-integrity cyberattacks to manipulate analog and digital measurements at a compromised substation RTU/SAS. The *AlertID*s 11.76 and 11.83 showed a Denial of Service (DoS) attack on the RTU and a DNP3 MITM trip attack on T559. The *AlertID*s 11.87, 11.88, 11.89, and 11.90 showed the detection of anomalies or threshold violations on Tieline power flow, generation output, voltage violation, and system frequency violation. These experimental results showed the detection of multistage IT and ICS cyber-attacks and provided CPS situational awareness to the grid.

V. Conclusion

This paper proposed a design and testbed-based implementation of CPS SCADA, EMS, and WAMPAC framework using industrial-grade substation and control platforms, substation field devices, and a real-time digital simulator. We demonstrated D-IADS on the **Design-3**, which is a superset of both the designs 1 and 2, for the multistage IT-intrusion and ICS-intrusion cyberattacks and the grid impact characteristics. The D-IADS master showed the real-time detection of intrusion-and-anomaly alerts and exhibited better performance with low latency. We demonstrated first-of-its-kind grid impact characteristics using synchrophasor data against data-integrity under a realistic ICS-intrusion cyberattack environment. We demonstrated these attack-defense scenarios for an EMP60 synthetic CPS grid. Future work includes evaluating closed-loop WAMPAC applications such as AGC and RAS-integrated RTCA, and open-loop applications such as state estimation.

VI. Acknowledgement

This research is funded in part by US DOE Grant # DE-OE0000830, and US DOE Grant # DE-EE0008773.

References

[1] The Department of Homeland Security of the United States of America, "Critical Infrastructure Sectors," 2020. [Online]. Available: https://www.dhs.gov/critical-infrastructure-sectors

[2] I. A. Oyewumi, A. A. Jillepalli, P. Richardson, M. Ashrafuzzaman, B. K. Johnson, Y. Chakhchoukh, M. A. Haney, F. T. Sheldon, and D. C. de Leon, "ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed," in *2019 IEEE Texas Power and Energy Conference*, Feb 2019, pp. 1–6.

[3] G. Elbez, H. B. Keller, and V. Hagenmeyer, "A Cost-efficient Software Testbed for Cyber-Physical Security in IEC 61850-based Substations," in *IEEE SmartGridComm*, Oct 2018, pp. 1–6.

[4] J. Fei, Y. Ma, X. Huang, Z. Liu, Q. Wang, and Y. Tang, "The Research on Cyber-Attack Testbed with Hardware-in-Loop," in *IEEE EI2*, 2017.

[5] G. Ravikumar, G. Ramya, S. Misra, S. Brahma, and S. A. Khaparde, "iPaCS: An Integrative Power and Cyber Systems Co-simulation Framework for Smart Grid," in *2017 IEEE PESGM*, July 2017, pp. 1–5.

[6] C. Konstantinou, M. Sazos, A. S. Musleh, A. Keliris, A. Al-Durra, and M. Maniatakos, "GPS Spoofing Effect on Phase Angle Monitoring and Control in a Real-Time Digital Simulator-based Hardware-in-the-Loop Environment," *IET CPS: Theory Applications*, vol. 2, pp. 180–187, 2017.

[7] A. S. Musleh, S. M. Muyeen, A. Al-Durra, I. Kamwa, M. A. S. Masoum, and S. Islam, "Time-Delay Analysis of Wide-Area Voltage Control Considering Smart Grid Contingencies in a Real-Time Environment," *IEEE Trans. on Industrial Informatics*, vol. 14, pp. 1242–1252, 2018.

[8] G. Ravikumar and M. Govindarasu, "Anomaly Detection and Mitigation for Wide-Area Damping Control using Machine Learning," *IEEE Transactions on Smart Grid*, 2019.

[9] M. Weiss, Y. Li-Baboud, D. Anand, P. Boynton, K. G. Brady, and M. Burns, "A Calibration of Timing Accuracy in NIST Cyber-Physical Systems Testbed," in *IEEE ISPCS*, 2018, pp. 1–6.

[10] G. Ravikumar, B. Hyder, and M. Govindarasu, "Efficient Modeling of HIL Multi-Grid System for Scalability Concurrency in CPS Security Testbed," in *2019 North American Power Symposium*, 2019, pp. 1–6.

[11] Gelli Ravikumar, Burhan Hyder, and Manimaran Govindarasu, "Efficient Modeling of IEC-61850 Logical Nodes in IEDs for Scalability in CPS Security Testbed," in *in IEEE T&D*, Oct 2020.

[12] G. Ravikumar, B. Hyder, and M. Govindarasu, "Next-Generation CPS Testbed-based Grid Exercise - Synthetic Grid, Attack, and Defense Modeling," in *2020 Resilience Week (RWS)*, 2020, pp. 92–98.

[13] G. Ravikumar and M. Govindarasu, "On-Premise Cloud-based HIL CPS Security Tesbted for Smart Grid," 2020. [Online]. Available: https://powercybertestbed.ece.iastate.edu/

[14] G. Ravikumar, B. Hyder, and M. Govindarasu, "Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications," in *IEEE Texas Power and Energy Conference*, 2020, pp. 1–5.

[15] Nivethan, Jeyasingam and Papa, Mauricio, "Dynamic rule generation for SCADA intrusion detection," in *IEEE Sympo. on Tech. for HST*, 2016.

[16] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, and H. Wang, "Rule-based Intrusion Detection System for SCADA Networks," 2013.

[17] IDS Signatures, "Digital bond," 2007.

[18] North American Electric Reliability Corporation, "Project 2015-09 SOL Definition and Exceedance Clarification White Paper," 2020.