A Novel Architecture for Attack-Resilient Wide-Area Protection and Control System in Smart Grid

Vivek Kumar Singh and Manimaran Govindarasu
Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011
Email:vsingh@iastate.edu, gmani@iastate.edu

***Abstract*—Wide-area protection and control (WAPAC) systems are widely applied in the energy management system (EMS) that rely on a wide-area communication network to maintain system stability, security, and reliability. As technology and grid infrastructure evolve to develop more advanced WAPAC applications, however, so do the attack surfaces in the grid infrastructure. This paper presents an attack-resilient system (ARS) for the WAPAC cybersecurity by seamlessly integrating the network intrusion detection system (NIDS) with intrusion mitigation and prevention system (IMPS). In particular, the proposed NIDS utilizes signature and behavior-based rules to detect attack reconnaissance, communication failure, and data integrity attacks. Further, the proposed IMPS applies state transition-based mitigation and prevention strategies to quickly restore the normal grid operation after cyberattacks. As a proof of concept, we validate the proposed generic architecture of ARS by performing experimental case study for wide-area protection scheme (WAPS), one of the critical WAPAC applications, and evaluate the proposed NIDS and IMPS components of ARS in a cyber-physical testbed environment. Our experimental results reveal a promising performance in detecting and mitigating different classes of cyberattacks while supporting an alert visualization dashboard to provide an accurate situational awareness in real-time.**

I. Introduction

Today's power grid has evolved into a densely interconnected, computerized, and autonomous cyber-physical system (CPS) with more dependence on communication infrastructure and technology to make the grid smarter. During the past 10 years, there has been a remarkable enhancement in developing wide-area protection and control (WAPAC) applications, such as automatic generation control (AGC), wide-area protection scheme (WAPS), synchrophasor-based wide-area voltage control system (WAVCS), etc., in the energy management system (EMS) that serve as a backbone for stable, reliable, and resilient power grid. It facilitates real-time monitoring to gain an adequate situational awareness of grid operations and performs optimized, automated, and coordinated responses to mitigate transient instability in real-time. Further, with the recent advancements in synchrophasor technology and its significant growth in the industry deployment, there has been a rapid shift in incorporating PMU measurements to develop mission-critical applications, including WAPAC, as it can provide dynamic stability assessment and assist in developing intelligent controllers. In general, these close-loop applications utilize wide-area supervisory control and data acquisition (SCADA) and synchrophasor measurements from remote and geographically-dispersed substations to mitigate or prevent small and large-scale disturbances that are difficult to resolve using traditional and local control schemes [1]. Since WAPAC applications rely on data sharing devices and communication network to provide the timely control operations, the security of cyber and physical infrastructures is very crucial. These applications are vulnerable to numerous cyber-attacks due to rapid digitization, unencrypted communication, and insecure data-sharing devices. Since these state-of-the-art solutions are not conventionally designed to handle unexpected cybersecurity threats, any unusual malfunction, triggered through cyber-attacks, can compromise their normal operations [2]. The National Institute of Standards and Technology Interagency Report (NISTIR) 7628 [3] has highlighted the key challenges to developing end-to-end attack-resilient solutions to neutralize the cybersecurity threats and enhance the grid resiliency. Further, the National Electric Sector Cybersecurity Organization Resource (NESCOR) cybersecurity report [4] discusses the existing nested vulnerabilities, interoperability requirements, and standards in the context of WAPAC cybersecurity.

The significant challenges to developing an attack-resilient system (ARS) for WAPAC involve detailed analysis of attack-surfaces and providing cyber-physical security of wide-area measurement and control signals without affecting its normal operation. The IEEE guide published by the Power System Relaying Committee [5] recommends strong cybersecurity practices and measures, including access controls, firewalls, and cryptography; however, poor security key management, weak cryptography, and misconfigured firewall rules can degrade the secure operation of the power system. Also, the past cybersecurity incidents, including Stuxnet Worm [6] and Ukraine's grid hack in 2015 and 2016 [7], have highlighted that the normal power system operation can be compromised through stealthy and sophisticated cyber-attacks with a severe impact on grid stability, market, and power system economics. Therefore, it is imperative to think outside the box and develop an innovative solution that encompasses a synergy of defense-in-depth and defense-in-breadth approaches at infrastructure and application layers of the EMS to make WAPAC applications resilient to a wide-class of cyber-attacks in inside and outside grid environment.

In general, a cyber-physical ARS is defined as a combination of an intrusion detection system (IDS) and intrusion mitigation and prevention system (IMPS) that can quickly detect cyber-attacks, happening at physical, communication, and applications layers, at an early stage and initiate intelligent and effective mitigation and preventive strategies, tailored to these events, to restore the normal grid operation after disturbances. In this paper, we proposed an ARS pertaining to the cybersecurity of WAPAC applications. In particular, the proposed generic architecture of ARS consists of two components. The first component includes a network-based IDS (NIDS) that relies on wide-area network (WAN) traffic to detect network reconnaissance, data integrity, and communication failure attacks based on the defined behavior and signature-based rules. The second component includes mitigation and prevention measures that are triggered based on state transition diagram-based operation states of the power system during attacks. As a proof of concept, we present the experimental case study in the context of a wide-area protection scheme (WAPS) cybersecurity. Several hardware and software resources available at the PowerCyber testbed at Iowa State University (ISU) are utilized to perform a hardware-in-the-loop (HIL) experimental testing and evaluation in real-time cyber-physical environment for different types of cyber intrusions.

II. Related Work

Over the recent decade, several researchers with different backgrounds have proposed several attack-resilient solutions to support WAPAC applications in the smart grid. The authors of [8] and [9] presented the attack-resilient synchrophasor architecture using software-defined networking (SDN) and dynamic network configuration. In [10], the authors proposed an event-triggered attack-resilient design for proportional integral-based load frequency control against denial of service (DoS) attacks by computing system stability criterion using Lyapunov theory and adjusting system parameters dynamically. The authors of [11] presented an attack-resilient automatic generation control (AGC) algorithm against data integrity attacks on measurement signals. In [12], the authors presented a multi-agent-based attack resilient solution that utilizes supervised machine learning algorithms to detect DoS attacks and applies adaptive load-shedding strategy to mitigate them using agents-based architecture for WAPS. In [13], the authors proposed a framework and methodology for detecting corrupt PMU measurements in wide-area damping control (WADC) using an online principal component analysis. In the same context, the authors of [14] proposed a cyber-attack resilient design of WADC using a hashed algorithm-based cryptography method to detect cyber-attacks and interpolation and extrapolation-based techniques are applied as mitigation strategies to predict signals during cyber-attacks. A literature review indicates that most of these efforts are based on the specific WAPAC applications that leverage signal processing, machine learning, and model-based approaches, which are not sufficient to develop a generic attack-resilient architecture that encompasses a wide range of WAPAC applications. This paper presents a generic architecture of ARS for WAPAC that consists of different modules, which are seamlessly integrated to address real-world implementation challenges while supporting its normal operation.

III. Proposed Attack-Resilient Architecture

Fig. 1 presents the conceptual architecture that consists of several components that are fused and seamlessly integrated to develop an attack-resilient WAPAC system in the smart grid. In particular, this architecture operates in two phases, where the first phase operates during cyber intrusions, and the second phase facilitates the regular operation of the power system. These two phases of operation are performed by controlling the switch S1 and switch S2 to mitigate possible intrusions in the grid network and maintain the system stability and reliability.

During the first phase of operation, the status of switch S1 is switched to 1 and the status of switch S2 is switched to 0. In this phase, the proposed NIDS module detects possible cyber intrusions and sends generated alerts to the alert management system (AMS). The AMS forwards these alerts to the alert visualization dashboard to provide situational awareness and support grid health monitoring in real-time for the control center operators. The IMPS module also receives these alerts and triggers necessary corrective and preventive measures while coordinating with WAPAC applications based on the nature of detected intrusions.

The second phase facilitates the regular operation of control center-based WAPAC Energy management system (EMS) by switching the status of switch S1 to 0 and switch S2 to 1. During this operation mode, these WAPAC applications receive grid measurements from field sensors over the wide-area SCADA & sychhrophasor network, perform data processing and analytical functions, and send control signals, if necessary, to close the loop. The two major components involved in the first phase of operation are discussed below.

1) ***Network Intrusion Detection System (NIDS) Module***: This module sniffs the network traffic between substation and WAPAC-based control center networks to capture attack signatures and analyze the spatio-temporal behaviors of power system using the extracted network packets to detect different classes of cyber-attacks, as defined in the cyber kill chain model [15]. It consists of two layers: signature and behavior-based IDSs.

a) **Signature-based IDS (SIDS)**: This layer consists of several components that analyze various levels of WAN traffic to detect attacks, as shown in Fig. 2. Specifically, it includes access-control whitelisting to filter media access control (MAC) addresses, internet protocol (IP) addresses, and port numbers (Port) in the hardware, network, and transport layers between source and destination targets. It also includes WAPAC-based protocol filtering and related function codes, and later applying signature-based rules using the database of known attack signatures. We have defined several IDS rules to detect attack reconnaissance, unauthorized network access, and DoS attacks.

- **Reconnaissance detection rules**: This category includes different IDS rules to detect cyber kill chain-based attack reconnaissance, access, and exploitation levels of attacks, such as ping scanning, Nmap scanning, and unauthorized Telnet access, as developed in earlier research effort [15].
- **DoS detection rule**: This rule detects a DoS attack that targets DNP3 communication on port 20000 on the

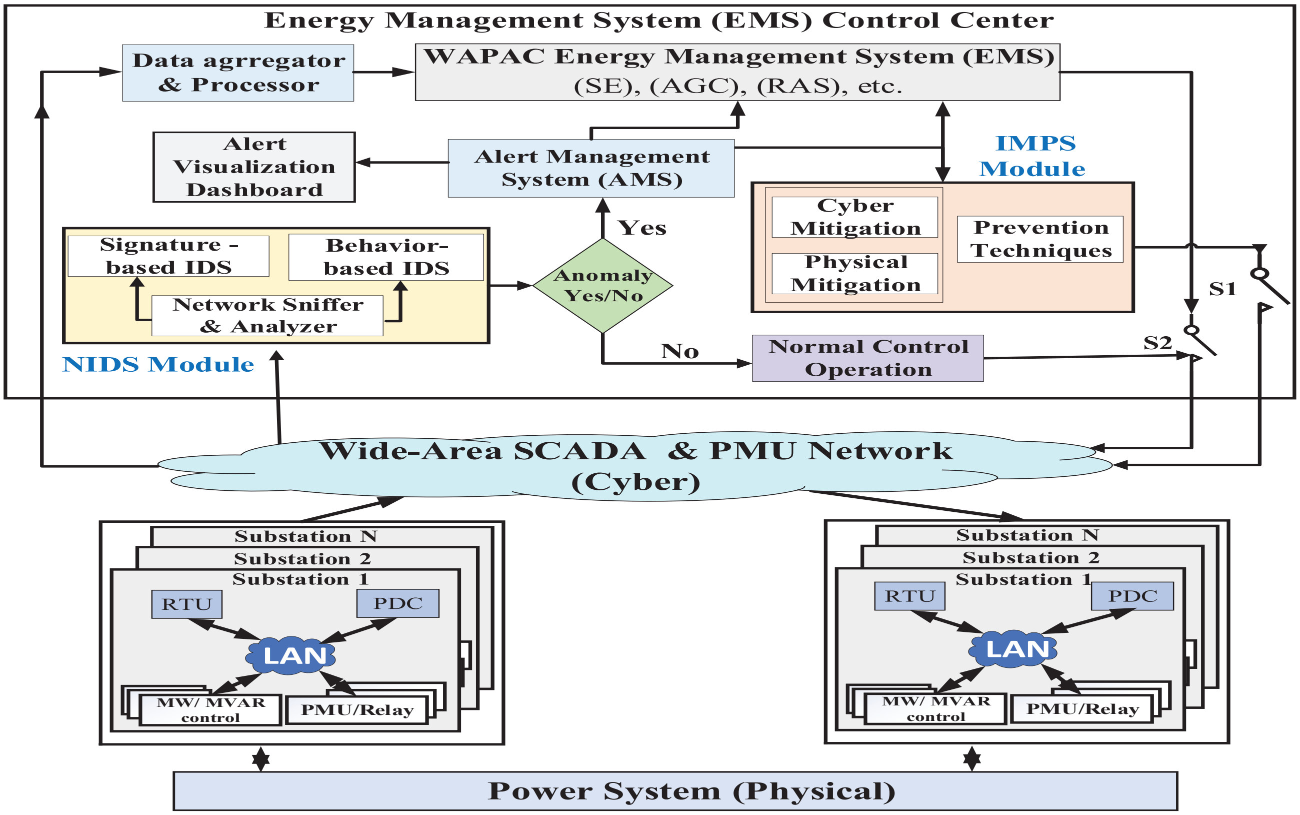


Fig. 1: Proposed attack-resilient architecture for WAPAC in smart grid.

substation network by counting the number of SYN flood packets within the given sampling period. In this work, an IDS alert is generated after the first 100 SYN packets (SYN flood) within a sampling period of 5 seconds.

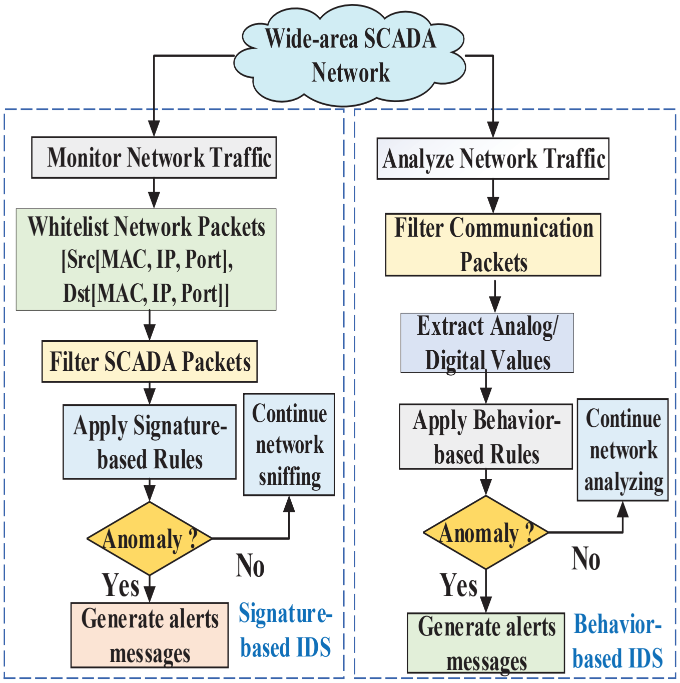

Wide-area SCADA Network
Monitor Network Traffic
Whitelist Network Packets [Src[MAC, IP, Port], Dst[MAC, IP, Port]]
Filter SCADA Packets
Apply Signature-based Rules
Continue network sniffing
Anomaly ?
No
Yes
Generate alerts messages
Signature-based IDS
Analyze Network Traffic
Filter Communication Packets
Extract Analog/ Digital Values
Apply Behavior-based Rules
Continue network analyzing
Anomaly ?
No
Yes
Generate alerts messages
Behavior-based IDS

Fig. 2: Overview of signature and behavior-based IDSs.

b) **Behavior-based IDS (BIDS)**: This layer performs an in-depth analysis of communication protocols and analyzes spatio-temporal power system behaviors to develop a baseline of normal cyber and physical activities. Based on the statistical profiling and comparative analysis of incoming data streams, behavior-based rules are defined using packets timing, analog and digital values, and a combination of them. In particular, we have defined two behavior-based rules in open-source IDS tools, such as Snort and Zeek (Bro), to detect malicious tripping and generation altering-based ramp attacks, which are discussed here.

- **Status-based Detection**: This rule, as defined in [15] and [16], triggers an action (alert, log) if the transmission line status $St(n)$ changes from 1 to 0 to detect the malicious tripping of an intelligent electronic device (IED).

$$St(n) \neq 1 \rightarrow Actions(alert, log) \qquad (1)$$

- **Timing-based detection**: This rule triggers an action (alert, log) if the time between two consecutive network packets $T_c(n)$ and $T_c(n-1)$ is less than the defined threshold T_{thr}.

$$T_c(n) - T_c(n-1) < T_{thr} \rightarrow Actions(alert, log) \qquad (2)$$

3) ***Intrusion Mitigation and Prevention System (IMPS) Module***: This module provides an appropriate mitigation and prevention strategies depending on the nature, severity, and location of cyber-attacks to ensure the resilient operation of WAPAC. To define an appropriate corrective actions, we have applied the state transition diagram [12] to classify the power system operation into four different states: *"Normal"*, *"Pre-alert"*, *"Alert"*, and *"Critical" states*. While considering the interaction between cyber and physical layers in the power system, several mitigation and preventive measures are defined,

as illustrated in Fig. 3, to restore the grid to normal state from other defined states during different types of attacks.

- **Normal State (N)**: Both cyber and physical layers are intrusion free and grid is in stable mode.

- **Pre-alert State (P)**: Attack reconnaissance at the cyber layer, but the physical layer is not affected.
  Attack examples: Ping scanning, Nmap scanning, port scanning, etc.
  Prevention Techniques: Moving target defense (MTD), network-reconfiguration, firewall updates (whitelisting & blacklisting rules), dynamic routing, etc.

- **Alert State (A)**: Intrusions at the cyber layer to compromise the normal operation of WAPAC.
  Attack examples: DoS attack, ARP spoofing attack, etc.
  Cyber Mitigation: Cyber islanding, local/ distributed mode operation, multiple/ backup communication channels, etc.

- **Critical State (C)**: Intrusions at cyber and physical layers to compromise the WAPAC operation and affect the power sytem stability.
  Attack examples: generation altering attack, line/ load tripping attack, coordinated attack, etc.
  Cyber and Physical Mitigation: Cyber islanding, line/ load/ generation restoration, multiple/ backup communication channels, etc.

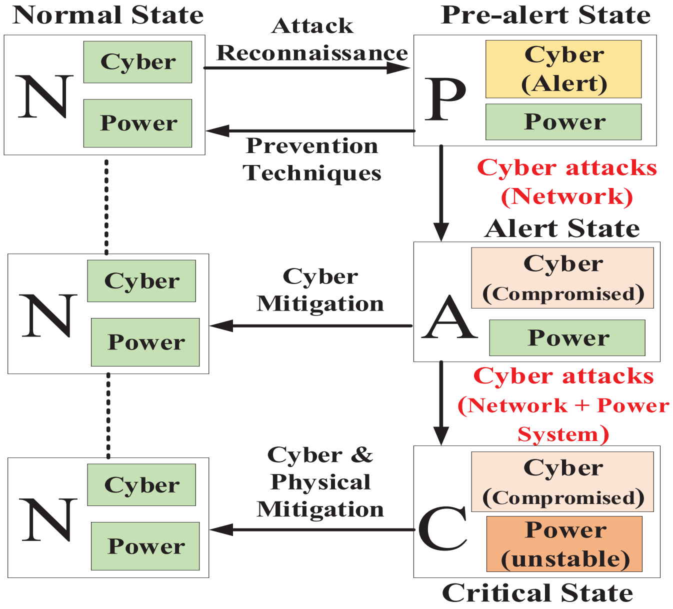


Fig. 3: State transition diagram-based mitigation and prevention measures of IMPS.

IV. Experimental Setup and Case Study

A. Case Study for WAPS

We have considered a SCADA-based WAPS [18] as a case study to validate the proposed architecture by experimental testing and evaluation. Fig. 4 presents the WAPS-enabled IEEE 39 bus system that is divided into two major areas: area 1 and area 2. Area 2 is operating as a major generation region that is supplying power to the area 1 through tie-lines L15-16 and L16-17. During the normal operation, the centralized controller of WAPS receives SCADA measurements regularly in terms of relays status and power line flows (analog measurements) of lines L15-16 and L16-17, and generator (Gen. 6) output to monitor disturbances. During a line outage of the tie-line L16-17, the WAPS controller is activated. It sheds the generation, as computed using the offline contingency analysis, at bus 35, as shown by black colored arrow, to prevent the thermal overloading at the line L15-16. Further, an equal amount of load is shed at the bus 18 to avoid an unbalance in system frequency during the generation shedding by this controller.

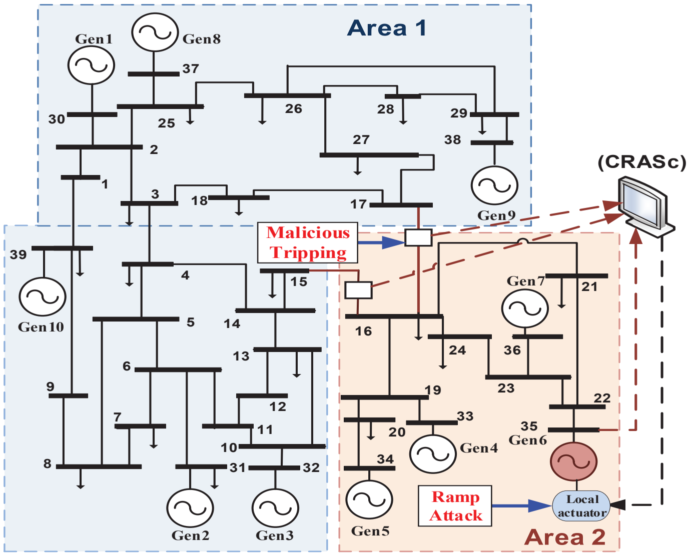


Fig. 4: IEEE 39 bus system with WAPS

B. Experimental Setup

Fig. 5 presents a HIL cybersecurity testbed at Iowa State University's PowerCyber (ISUPC) Laboratory that we have utilized to perform cybersecurity experiments in the context of WAPS cybersecurity. This testbed provides a coherent simulation environment by combining industry-grade hardwares, software, emulators, and real-time simulators that are interconnected through a multi-level communication network to emulate the grid network as close to the real world.

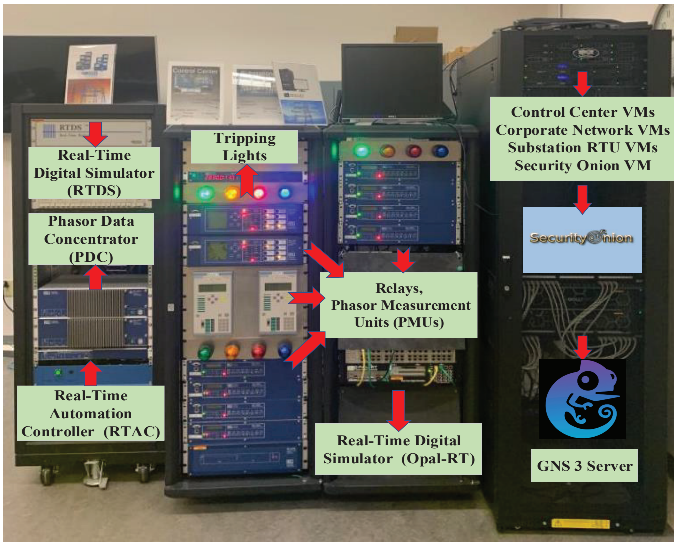


Fig. 5: Smart grid CPS testbed at Iowa State University

Fig. 6 presents the experimental setup where the IEEE 39 bus system is modeled in ARTEMiS/SSN (eMEGASIM), and simulated in the electromagnetic transient (EMT) domain in the real-time digital simulator (OPAL-RT). This simulator is also mapped to two physical SEL 421 relays (relay 1 and relay 2) with modeled transmission lines L15-16 and L16-17 using IEC 61850-8-1 GOOSE communication messages. We have utilized the DNP3 master-slave driver of the simulator to send SCADA measurements to the WAPS controller, deployed at the control center, through the substation remote terminal unit (RTU 1) that is SEL-3530 real-time automation controller (RTAC). The WAPS controller, running in the python script, sends control signals back to the simulator through the substation RTU 3 through the Kepserver's OPC Unified Architecture (UA) client-server interfaces. The substation RTU3, as shown in pink box, is communicating with the simulator using the DNP3 (OPC server) SCADA communication to provide an appropriate response, if necessary, to close the loop.

For implementing IT-related attacks, the pre-installed tools, *Nmap*, *ping*, and *telnet* commands are utilized to perform the attack reconnaissance. The DoS attack is performed by sending a huge number of random packets to the substation RTU 1 through the TCP SYN flooding attack using the *hping* tool, available in the Kali Linux machine. In case of SCADA related attacks, a malicious tripping attack is performed on the relay 2 to trip the line L16-17 by replaying the tripping packet using the python script through a man-in-the-middle (MITM) attack between the substation RTU 2 and EMS control center. For executing a ramp attack on generator 35 (Gen. 6), the malware, Trojan Horse, is installed in the OPC server-based substation RTU 3, which provides backdoor access to the attacker. The attacker closes the legitimate program in RTU 3 and initiates python script-based malicious logic, which periodically sends the ramping signal with a negative slope to decrease the generation at bus 35 gradually.

To facilitate attack detection experiments, we have deployed security onion (SecON) as NIDS that incorporates Snort and Zeek (BRO) IDSs to detect intrusions in real-time based on defined rules. The generated alerts are forwarded to the Python-based AMS that sends these alerts to rules-based IMPS. The IMPS interacts with the WAPS controller using the Python platform to provide necessary corrective and preventive measures. Further, the AMS is forwarding these alerts to the Sguil (SecOn) to provide a real-time visualization dashboard for alert monitoring using PyZMQ, a python binding for ZeroMQ.

V. Results and Discussions

A. Network IDS evaluation

In this section, we present the experimental evaluation of NIDS in terms of accuracy and latency rate in real-time; and also provide a comparative performance analysis of Snort and Zeek IDSs during attack detection.

1) Signature-based IDS evaluation

Fig. 7 shows the latency distribution for defined IDS rules in SIDS for ping scanning, Nmap scanning, Telnet unauthorized access, and DoS attacks. The green-colored diamond circles represent the mean of the computed latency corresponding to different attacks. The average computed latency for ping and Nmap scanning is 1.6 and 1.48 seconds that is higher than the computed average latency of telnet unauthorized access that is around 1.139 seconds. It can be observed that the latency for detecting DoS attack is more uniform as compared to ping and Nmap latencies with an average value of 1.47 seconds.

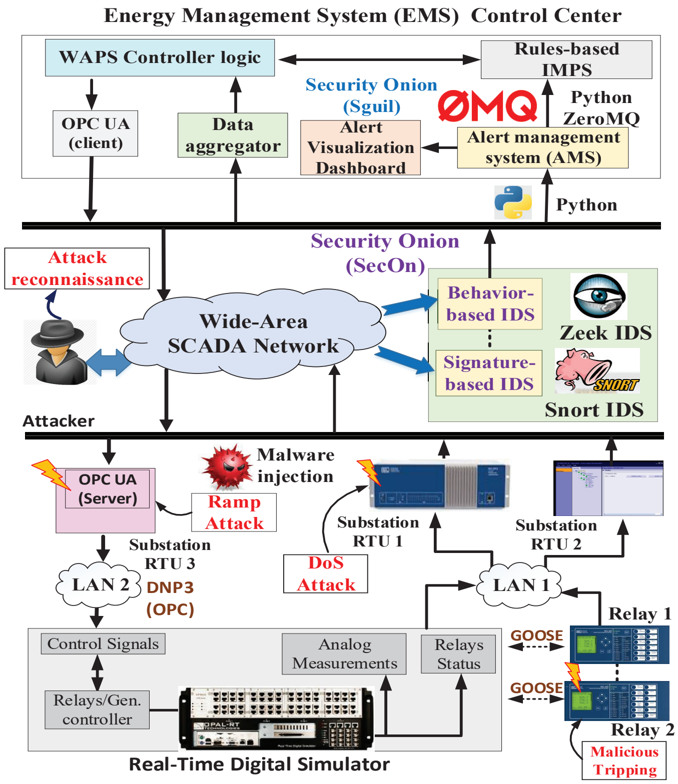


Fig. 6: Experimental setup for attack-detection experiments.

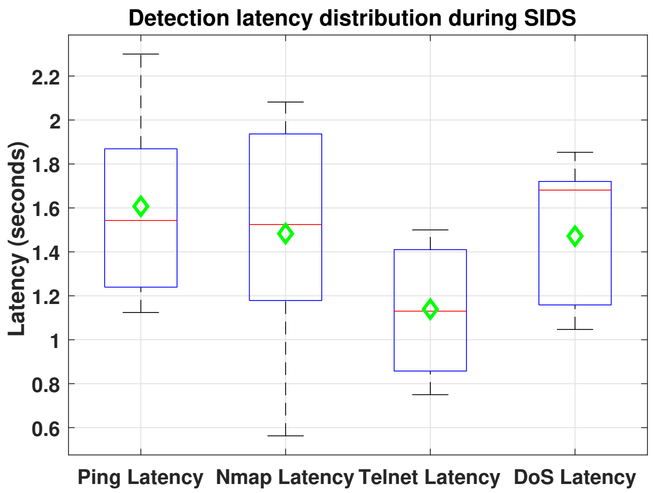


Fig. 7: Detection latency distribution for different attacks in SIDS.

2) Behavior-based IDS evaluation

We have evaluated the performance of BIDS using Snort and Zeek IDSs, available in the SecOn tool, in terms of latency and detection rate for detecting data integrity attacks in real-time. Fig. 8 presents the detection latency distribution for detecting malicious tripping and ramp attacks for several cases using Snort and Zeek IDSs. During the Snort IDS-based malicious tripping detection, we observe a latency varying from 0.446 seconds (minimum) to 2.27 seconds (maximum)

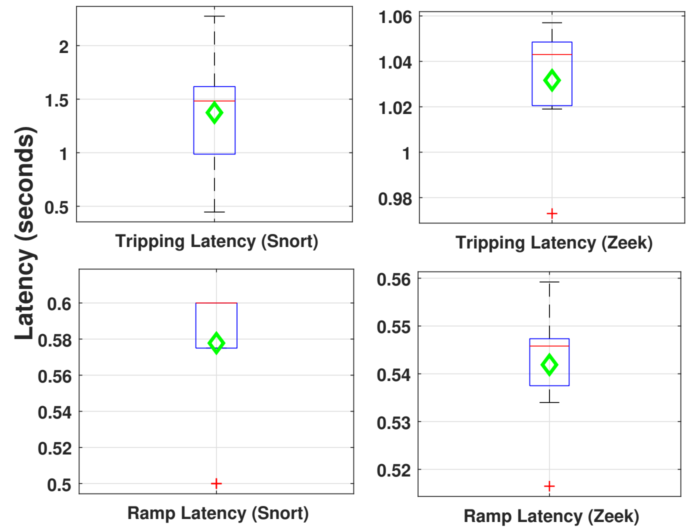


Fig. 8: Detection latency distribution for different attacks in BIDS.

with an average value of 1.374 seconds. However, the Zeek IDS shows a smaller latency with an average value of 1.037 seconds. During the ramp attack detection, the Snort IDS follows a similar trend with a relatively higher average latency of 0.557 seconds. In contrast, the Zeek IDS exhibits a slightly smaller latency with an average value of 0.541 seconds.

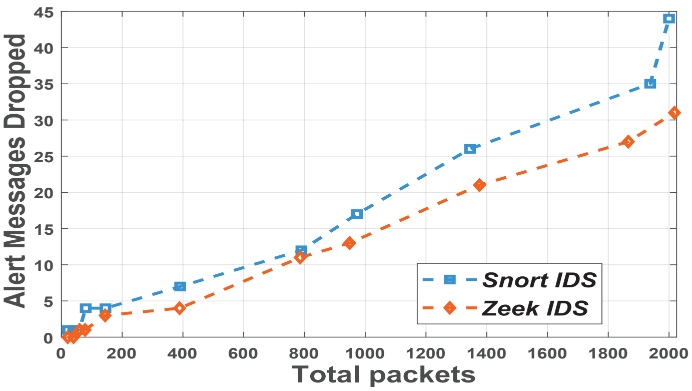
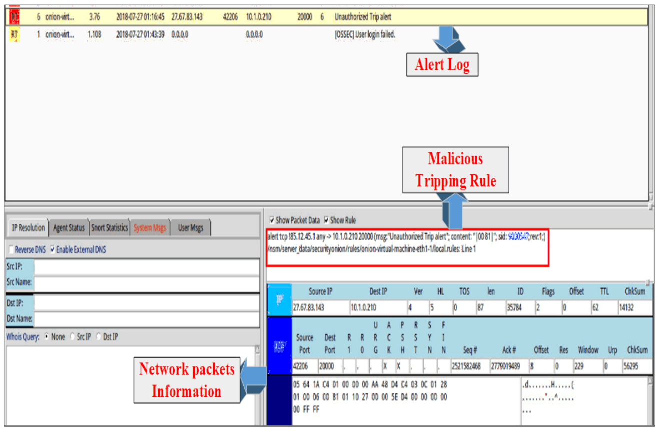


Fig. 9: Performance evaluation of Snort and Zeek IDSs for ramp attack

Note that because of the static nature of attack reconnaissance (ping and Nmap scanning), Telnet access, DoS, and malicious tripping attacks, we are able to achieve 100 % accuracy rate in all cases; however, because of the dynamic nature of ramp attack, its accuracy varies with network packets. The Zeek IDS shows an average detection rate of 94.7% and a minimum of 90.9% whereas in case of Snort IDs, the detection rate varies from 93.5% to 75% with an average value of 88%, as discussed in our previous work [17]. To provide the comparative analysis of Snort IDS and Zeek IDS, we have analyzed the number of alert messages dropped concerning to the total alert messages, as shown in Fig. 9. We observe that the Snort and Zeek IDSs have similar performance for the small size of packets; however, the gap increases with the number of packets, and Zeek IDS exhibits a better performance than Snort IDS, especially during huge chunks of alert messages.



```
RT  6 onion-virt... 3.76  2018-07-27 01:16:45 27.67.83.143 42206 10.1.0.210 20000 6 Unauthorized Trip alert
RT  1 onion-virt... 1.108 2018-07-27 01:43:39 0.0.0.0            0.0.0.0              [OSSEC] User login failed.
```

```
alert tcp !85.12.45.1 any -> 10.1.0.210 20000 (msg:"Unauthorized Trip alert"; content: "|00 81|"; sid: 9000547;rev:1;)
/nsm/server_data/securityonion/rules/onion-virtual-machine-eth1-1/local.rules: Line 1
```

Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
27.67.83.143	10.1.0.210	4	5	0	87	35784	2	0	62	14132

Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
42206	20000	.	.	.	X	X	.	.	.	2521582468	2779019489	8	0	229	0	56295

```
05 64 1A C4 01 00 00 00 AA 48 D4 C4 03 0C 01 28     .d.......H.....(
01 00 06 00 B1 01 10 27 00 00 5E D4 00 00 00 00     .........'..^.....
00 FF FF                                             ...
```

Fig. 10: Alert visualization during a malicious tripping attack

B. Alert visualization dashboard

We have utilized the Sguil tool of security onion (SecOn), as the alert visualization dashboard, for monitoring network traffic, understanding and analyzing different alerts, and providing situational awareness in real-time. This tool provides information about raw data, session data, and events based on real-time packet analysis and network configuration. Fig. 10 shows an example of alert visualization during the malicious tripping attack that clearly illustrates the applied rule for detecting malicious tripping attack with an alert log and detailed network packets information, including Internet Protocol (IP) addresses, port addresses, function codes, etc.

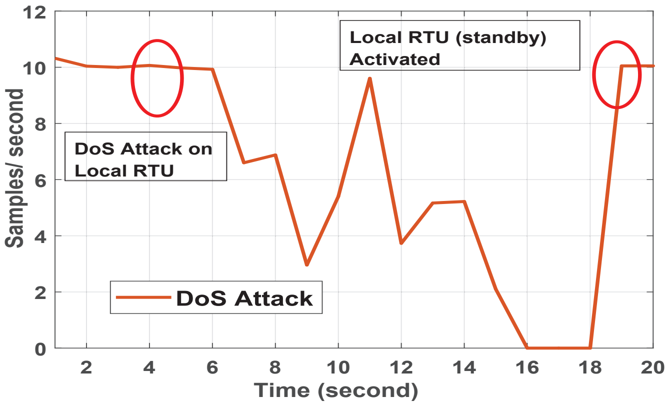


Fig. 11: Cyber mitigation during a DoS attack

C. Mitigation Evaluation

This section illustrates the application of proposed state transition diagram-based mitigation approaches through three example case studies. Fig. 11 presents the mitigation action during **A** state of power grid where a DoS attack is performed on RTU 1 at 4 second that reduces the DNP3 sampling rate from around 10 samples/ second to 2 samples/ second at 15 second, and the SCADA communication is disabled at 16 second. In this case, the SIDS detects this attack, and a backup communication is enabled manually by activating a standby local RTU to restore the communication at 19 second.

Fig. 12 presents the cyber and physical mitigation actions during the **C** state of power grid where a malicious tripping attack is performed on line L16-17 at 175.4 second that disconnects this line and injects transient instability on the generator at bus 35 (Gen. 6). In this case, the mitigation actions include restoring this transmission line at 182.8 second and

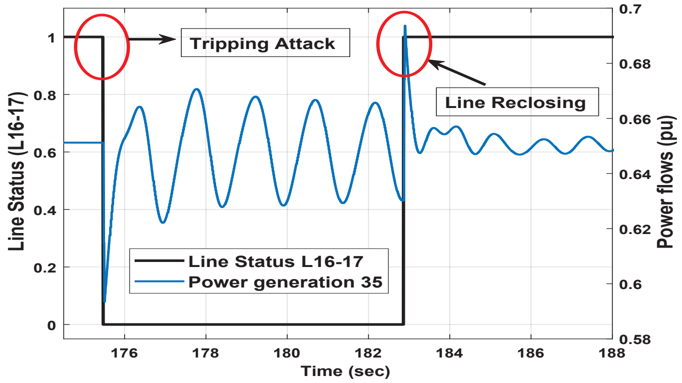


Fig. 12: Cyber and physical mitigation during a malicious tripping attack

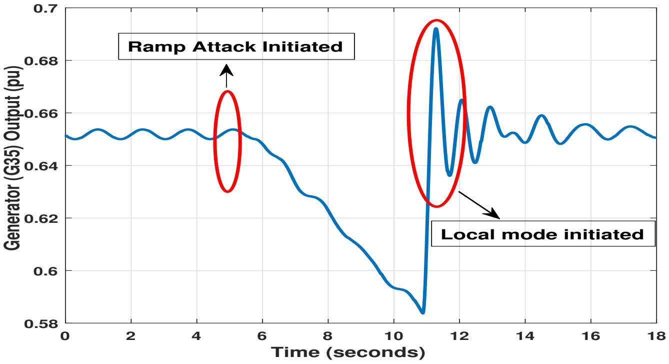


Fig. 13: Cyber and physical mitigation during a ramp attack

enabling the local-mode operation. The local mode operation disables the SCADA control signal from the WAPS controller to prevent unnecessary generation shedding. Finally, the system is restored to **N** state after 182.8 second. Fig. 13 presents the cyber and physical mitigation actions, including generation restoration and local mode operation, during the ramp attack that is performed at 5 second on generator (Gen 6) at bus 35. The BIDS detects this attack using the defined timing-based rule and triggers an alert. Once an alert is received to the IMPS module, the generation is restored to bring the system to **N** state after 11 second and local mode is activated, which disables the SCADA control signal from the WAPS controller to the generator.

VI. Conclusion

Developing an attack-resilient system (ARS) for WAPAC applications in the smart grid is a challenging task that requires an in-depth knowledge and in-breadth understanding of their operations, communication protocols, and network topology of the power system. In this paper, we presented a generic attack-resilient architecture for WAPAC applications that seamlessly integrates network-based IDS with mitigation and prevention strategies using an alert management system while supporting alert visualization and situational awareness n real-time. We described the proposed network IDS that utilizes attack-signatures and behavior-based rules to detect cyber-attacks at cyber and physical layers, followed by necessary mitigation actions based on the power system's operation states. To validate the proposed ARS architecture, we considered the SCADA-based WAPS as a case study and described several steps involved in implementing cyber-attacks and testing detection and mitigation components of ARS in a HIL cyber-physical testbed environment. Our experimental analysis reveals that the Zeek IDS tool demonstrates better efficiency in detecting cyber-attacks as compared to Snort IDS for different volumes of network traffic. We also analyzed several mitigation actions at cyber and physical levels that effectively restore the power system to a normal state after cyber intrusions. A potential avenue for future work is to develop a robust intrusion detection and mitigation system using machine learning and deep learning approaches to enhance the cybersecurity resiliency of WAPAC.

Acknowledgment

This research is funded in part by US NSF Grant # CNS 1446831 and US DOE Grant # DE-EE0008773.

References

[1] M. Begovic, D. Novosel, D. Karlsson, C. Henville and G. Michel, ”Wide-Area Protection and Emergency Control,” in Proceedings of the IEEE, vol. 93, no. 5, pp. 876-891, May 2005.

[2] A. Ashok et al., ”Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid,” in Proceedings of the IEEE, vol. 105, no. 7, pp. 1389-1407, July 2017.

[3] National Institute of Standards and Technology (NIST), ‘NISTIR 7628 Revision 1: Guidelines for Smart Grid Cyber Security’, September 2014.

[4] National Electric Sector Cybersecurity Organization Resource (NESCOR), ‘Wide Area Monitoring, Protection, and Control Systems (WAMPAC)–Standards for Cyber Security Requirements’, 2012.

[5] “IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems”, Power System Relaying and Substation Committee of the IEEE Power and Energy Society, 2014.

[6] N. Falliere et al., “W32.stuxnet dossier,” Technical report, Symantec, Feb. 2011.

[7] SANS (Mar. 2016). Analysis of the cyber attack on the Ukrainian Power Grid—Defense Use Case [Online].

[8] H. Lin et al., ”Self-Healing Attack-Resilient PMU Network for Power System Operation,” in IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1551-1565, May 2018.

[9] V. K. Singh, E. Vaughan and J. Rivera, ”SHARP-Net: Platform for Self-Healing and Attack Resilient PMU Networks,” 2020 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 2020, pp. 1-5.

[10] K. Lu, G. Zeng, X. Luo, J. Weng, Y. Zhang and M. Li, ”An Adaptive Resilient Load Frequency Controller for Smart Grids With DoS Attacks,” in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 4689-4699, May 2020,

[11] S. Sridhar and M. Govindarasu, ”Model-Based Attack Detection and Mitigation for Automatic Generation Control,” in IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 580-591, March 2014.

[12] P. Wang and M. Govindarasu, ”Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid,” in IEEE Transactions on Smart Grid, vol. 11, no. 4, pp. 3447-3456, July 2020.

[13] K. Mahapatra et al., ”Malicious Corruption Resilience in PMU Data and Wide-Area Damping Control,” in IEEE Transactions on Smart Grid, vol. 11, no. 2, pp. 958-967, March 2020.

[14] T. Prakash, V. P. Singh and S. R. Mohanty, ”Cyber-Attack Resilient Design of Wide-Area PSS Considering Practical Communication Constraints,” in IEEE Systems Journal, vol. 14, no. 2, pp. 2012-2022, June 2020.

[15] V. K. Singh, S. P. Callupe and M. Govindarasu, ”Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System,” 2019 North American Power Symposium (NAPS), Wichita, KS, USA, 2019, pp. 1-6.

[16] V. K. Singh, E. Vaughan, J. Rivera and A. Hasandka, ”HIDES: Hybrid Intrusion Detector for Energy Systems,” 2020 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2020, pp. 1-6.

[17] V. K. Singh, H. Ebrahem and M. Govindarasu, ”Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment,” 2018 North American Power Symposium (NAPS), Fargo, ND, 2018, pp. 1-6.

[18] V. K. Singh and M. Govindarasu, ”Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data,” 2018 IEEE Power Energy Society General Meeting (PESGM), Portland, OR, 2018, pp. 1-5,