Cyber Kill Chain-Based Hybrid Intrusion Detection System for Smart Grid

Vivek Kumar Singh and Manimaran Govindarasu

Abstract Today's electric power grid is a complex, automated, and interconnected cyber-physical system (CPS) that relies on supervisory control and data acquisition (SCADA)-based communication infrastructure for operating wide-area monitoring, protection, and control (WAMPAC) applications. With a push towards making the grid smarter, the critical SCADA infrastructure like power system is getting exposed to countless cyberattacks that necessitate the development of state-of-the-art intrusion detection systems (IDS) to provide comprehensive security solutions at different layers in the smart grid network. While considering the continuously evolving attack surfaces at physical, communication, and application layers, existing conventional IDS solutions are insufficient and incapable to resolve multi-dimensional cybersecurity threats because of their specific nature of the operation, either a data-centric or protocol-centric, to detect specific types of attacks. This chapter presents a hybrid intrusion detection system framework by integrating a network-based IDS, model-based IDS, and state-of-the-art machine learning-based IDS to detect unknown and stealthy cyberattacks targeting the SCADA networks. We have applied the cyber-kill model to develop and demonstrate attack vectors and their associated mechanisms. The hybrid IDS utilizes attack signatures in grid measurements and network packets as well as leverages secure phasor measurements to detect different stages of cyber-attacks while following the kill-chain process. As a proof of concept, we present the experimental case study in the context of centralized wide-area protection (CWAP) cybersecurity by utilizing resources of the PowerCyber testbed at Iowa State University (ISU). We also describe different classes of implemented cyber-attacks and generated heterogeneous datasets using the IEEE 39 bus system. Finally, the performance of the hybrid IDS is evaluated based in terms of detection rate in real-time cyber-physical environment.

V. K. Singh (✉) · M. Govindarasu
Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA
e-mail: vsingh@gmail.com

M. Govindarasu
e-mail: gmani@iastate.edu

H. Haes Alhelou et al. (eds.), *Wide Area Power Systems Stability, Protection, and Security*, Power Systems, https://doi.org/10.1007/978-3-030-54275-7_22

Keywords Cyber-physical system · Intrusion detection systems · Centralized wide-area Protection · Smart grid · Cyber kill chain · PMUs · WAMs · Cyber-attack

1 Introduction

Today's energy infrastructure is undergoing a massive transformation across all generation, transmission, and distribution systems to provide reliability, efficiency, and sustainability to the power system network. With a high dependence on advanced communications, as well as the increasing integration of smart meters and sophisticated controls, electric power systems have evolved into densely interconnected cyber-physical systems and the existing information technology (IT)-based cybersecurity measures are often ineffective at preventing them. In recent years, several WAMPAC applications, such as state estimation, wide-area protection scheme (WAPS), wide-area voltage controller (WAVC), etc., are developed to provide real-time monitoring and control as necessary to maintain the stability and reliability of the power system [1]. Since these WAMPAC applications are not conventionally designed to handle unexpected cybersecurity threats, any unusual malfunction or signicant operational delays, triggered through cyber-attacks, can affect the system observability, reliability, and stability of power system. This motivates the need to go beyond the traditional paradigm of "security by obscurity" and "bolt-on" security measures of retrofitting the existing system with conventional security solutions and develop a suite of layered innovative security solutions to enhance the grid resiliency against possible cybersecurity threats. Several efforts, such as the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 [2], DOE Cyber Security Roadmap for Energy Delivery Systems [3], DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [4], North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Standards [5], and National Electric Sector Cybersecurity Organization Resource (NESCOR) reports [6], have provided an in-depth understanding to identify cybersecurity vulnerabilities and develop mitigation and preventive strategies. Further, the IEEE guide published by the Power System Relaying Committee [7] recommends strong cybersecurity practices and measures, including access controls, firewalls, cryptography; however, poor security key management, weak cryptography, and misconfigured firewall rules can degrade the secure operation of the power system. Therefore, it is highly imperative to thoroughly investigate the cybersecurity vulnerabilities and develop state-of-the-art detection and defense techniques to neutralize possible threats and make the grid *attack-resilient*.

1.1 Challenges for IDS in Smart Grid

The current IDS solutions in the power system face several challenges in detecting anomalies accurately and timely by analyzing multi-dimensional data at physical, network, and application layers, which are elaborated in greater detail below.

(1) ***Detection Latency***: Several WAMPAC applications have a stringent timing requirement to perform their optimal control operations. Therefore, in order to support the seamless integration of IDS with the grid infrastructure, detection latency has to be minimized so that it does not affect the normal operation of the power system. Also, the operational timing requirement of different applications varies widely. For example, the centralized wide-area protection scheme (CWAPS) has a strict timing requirement, typically in the order of 50–150 ms, AGC operates in approximately 4–8 s, and economic dispatch operates every 5 min. Further, the development of attack-resilient infrastructure requires an immediate incident response that can quickly restore the grid condition to the normal state.

(2) ***Robustness and Consistency***: Since cyber-attacks vary from a nave level to a sophisticated level, it is not justified to completely rely on the specific types of IDS to detect all classes of attacks. Although the SIDS shows a high accuracy without signaling false alarms as compared to the ABIDS, it is only able to detect known cyber-attacks, and thus it has to be updated regularly with newly discovered attack signatures. The current existing ABIDS and SIDS show good accuracy; however, it is difficult to obtain detailed information from them about different classes of attacks. Further, the advanced persistent threat (APT) actors can leverage their skill sets, expertise knowledge, intellectual capabilities, and operational tools resources to perform sophisticated and coordinated cyber-attacks by manipulating cyber and physical information in spatial and temporal domains. These stealthy cyber-attacks are difficult to be detected by a signature or anomaly-specific IDS at the network or host level.

(3) ***Data Management***: The current operational technology (OT) environment is inundated with an overload of network information and power measurements that frequently lead to the challenge of Big data, which is difficult to handle from the conventional IDS perspective. The current big data challenge is driven by volume, velocity, and veracity of data. Volume in the smart grid environment includes line flows, relay status, phasor measurement, network packets, etc. that significantly contribute to the large volume of data. Velocity refers to the sampling rate at which data is processing at substation and control center networks; and variety refers to the complex data problem, including multi-dimensional structure data, high dimensional data, and data from multiple independent sources. Further, since the current grid infrastructure depends on multiple hardware and software resources for handling grid measurements and network traffic, there exists no real-time sensing platform that can allow the processing of heterogeneous datasets to facilitate the operation of different types of IDSs.

1.2 Related Work

In recent years, there has been a strong urge in the development of IDS pertinent to the cyber-physical security in the smart grid environment. Several researchers with different backgrounds have proposed different types of IDSs, such as model-based, rule-based, protocol-specific, machine learning or data-mining-based IDS, etc. for the smart grid cyber-physical security. In [8] and [9], the authors have proposed a model-based IDS using real-time load forecast information to detect faulty SCADA measurements in the context of automatic generation control (AGC) in the power system. In [10], a decision tree-based supervised machine learning algorithm is applied to detect malicious tripping of relays. In [11], the authors have shown how the model-based IDS can be developed in a centralized manner using load forecasts and secure phasor measurements for the state estimation. Although the centralized IDS is developed pertinent to the energy management system (EMS) applications like state estimation, automatic generation controller (AGC), etc., the multi-agents-based distributed IDS is also proposed in [12] to avoid a single point of failure while detecting anomalies in the decentralized protection scheme. Apart from the anomaly-based IDSs, several signature-based IDSs [13]–[16] are also proposed that perform deep packet inspection on the SCADA and synchrophasor communication protocols to detect cyber intrusions in real-time. Further, in [14], the authors show how two open-source IDS tools-Snort and BRO, can be utilized in detecting a data integrity attack using the timing information of two consecutive network packets and compared their performances in terms of accuracy and latency rates. Although the rules-based IDS works well in detecting malicious network traffic using cyber logs, it requires an intensive knowledge and rigorous analysis for developing rules and is apposite for the big-data problem. Meanwhile, several research efforts have shown the application of machine learning algorithms and data mining techniques in detecting malicious and non-malicious events like line faults. Pan et al. presents a learning-based IDS using the common path mining technique to classify cyber-attacks, normal operations, and physical disturbances [17]. The common path mining technique learns temporal patterns for different scenarios using synchrophasor measurements and audit logs in an automated way.

2 Intrusion Detection System in Smart Grid

2.1 Smart Grid Communication Architecture

The smart grid network consists of multiple communication architectures that are interconnected through physical and application layers to facilitate real-time monitoring of the grid network and protect the grid's health on spatial and temporal levels. These communication architectures can be classified into three major cate-

gories: SCADA network, synchrophasor network, and advanced metering infrastructure (AMI) network.

(1) **SCADA Network**: Consists of a remote terminal unit (RTU), as a substation gateway that receives measurements from sensors, transducers, and instruments, which are located at remote grid stations as field devices and transmit data to the control center for real-time monitoring and control of generation, transmission, and distribution systems every few seconds. Several communication protocols like IEC 61850, IEC 60870, Modbus, Distributed Network Protocol 3 (DNP3), etc. are utilized to support SCADA-based wide-area applications.

(2) **Synchrophasor Network**: Includes phasor measurement units (PMUs), phasor data concentrators (PDCs), global positioning system (GPS) clocks, Transmission Control Protocol/Internet Protocol (TCP/IP) network infrastructure, and data storage and collection system. The traditional SCADA system fails to provide faster and high-resolution measurements that are necessary for wide-area dynamic monitoring and control of the power system. These limitations can be overcome by deploying PMUs in the field-area network (FAN) that provides phasor measurements at a sampling rate of 30 to 120 samples/second to support mission-critical applications. Further, there has been a rapid shift in extending the SCADA EMS to incorporate synchrophasor-based wide-area control applications like a wide-area voltage controller (WAVC), oscillation damping, etc. [18]. The authors of [19] present the design and architecture of synchrophasor-based WAPS for different types of applications, including voltage instability, oscillation monitoring, thermal overloading, etc.

(3) **AMI Network**: Includes smart meters, data aggregator, data manager, and communication network that facilitates the bi-directional communication between smart meters and grid utilities for exchanging information related to power consumption, outage reporting and awareness, and price updates. During normal operation, data aggregators (DAs) receives real-time consumption information from smart meters and sends necessary commands through the neighborhood-area network (NAN). Further, smart meters also communicate with devices, located on the customer's premises, through the home-area network (HAN). ANSI C12 series is the most commonly used communication protocol in the US, while IEC62056 protocols dominate the AMI market in the EU to support the information exchange in a wide-area network (WAN), NAN, and HAN of AMI [20].

Fig. 1 clearly illustrates attack surfaces, as shown by lightning bolt symbols, in the grid network that can be exploited by attackers based on the existing vulnerabilities at device, network, and application levels. Since the communication protocols in the grid network are not encrypted, there is numerous possible scope of cyber-attacks, despite the existing defense mechanisms, such as firewall, a virtual private network (VPN), etc. For example, an attacker can sniff the clear text communication packets going between the control center and substation networks to perform data integrity attacks over WAN. An attacker can also sniff wide-area communication packets to develop a network footprint, and later perform Man-in-the-Middle (MITM) or denial of service (DoS) attacks to undermine the system observability and controllability. In AMI, the deployed smart meters operate as an interface between the utility's network and HAN or NAN, which makes them an ideal target for cyber-attacks.

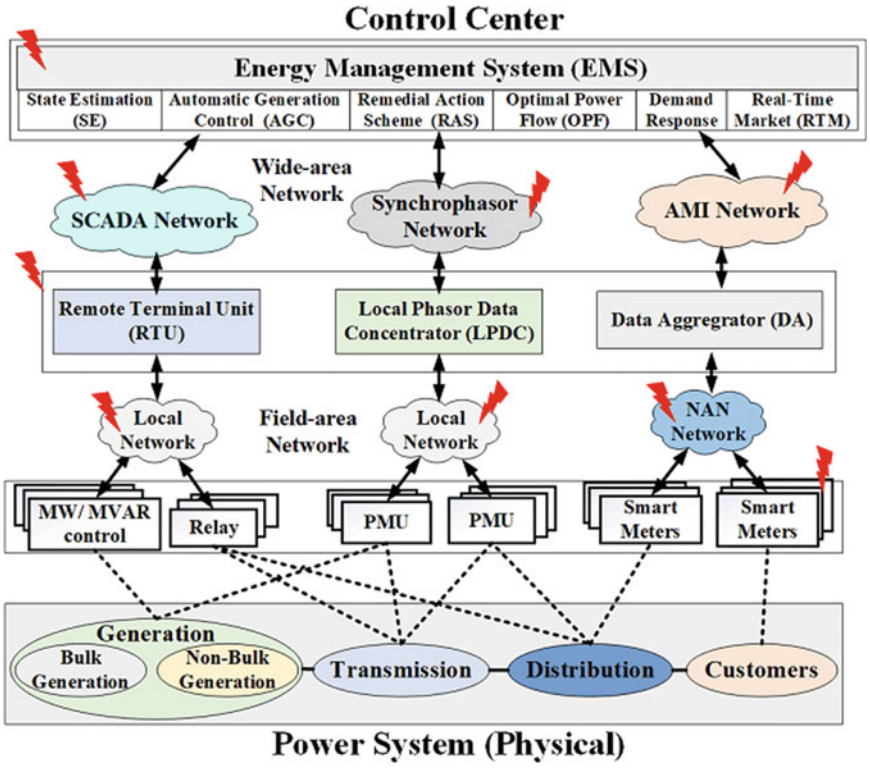

Fig. 1 High-level schematic architecture of the smart grid

Also, several vulnerabilities have been reported in smart meters installation. For example, a control unit system in smart meters is subjected to reverse engineering, side-channel, and data-integrity attacks. Further, at the national level, the advanced and nation-sponsored attackers can perform stealthy and coordinated cyber-attacks, such as compromising control centers that are difficult to detect using conventional security methods.

2.2 Intrusion Detection System Taxonomy

IDS is based on the notion that the system behavior during cyber-attacks would be different from legitimate behavior. Several types of IDSs are developed to detect anomalies accurately and timely at physical, cyber, and application layers in the power system. Fig. 2 shows the taxonomy of IDS based on their locations and the nature of operations in the grid network. Based on the location-based taxonomy, it can be classified into two different types: Network and Host-based IDSs.

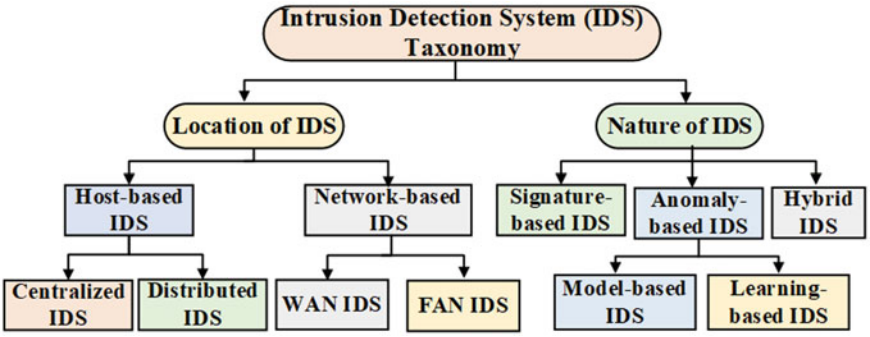

Fig. 2 Taxonomy of intrusion detection system (IDS) in the power system

(1) **Network-based IDS (NIDS)**: This IDS inspects the communication traffic to detect security breaches in the grid network. Different techniques like port-mirroring, network taps, switched port analyzer, etc. are developed by the network infrastructure vendors to facilitate packet sniffing in the context of NIDS. It can be classified into two broad categories: WAN IDS and FAN IDS.

- WAN IDS (WIDS): This IDS is deployed over WAN that sniffs the network traffic and detects anomalies using the statistical or baseline models and attack signatures. Potential challenges related to the WIDS are network data overload, quality of service (QoS), and encryption, and signature lag time.
- FAN IDS (FIDS): This IDS passively monitors network traffic of smart meters and actuators in a local area network (LAN), FAN, or NAN and detects anomalies in real-time. It is generally deployed at the field level, made tamper-resistant, and supported extra computational power and memory to forward the detected alerts to gateways and central IDS deployed at the utility control center.

(2) **Host-based IDS (HBIDS)**: It is deployed at operating and application systems and operated through an internal computing system to monitor and analyze traffic patterns at the system level. Based on its location in the grid network, it can be classified into broad categories: Centralized IDS and distributed IDS.

- Centralized IDS (CIDS): It requires global measurements to analyze cyber and physical events; and hence, it is deployed at the control center level and provides much accurate and consistent detection performance because of its global view of the grid network. It can also be utilized to develop application-specific IDS for the EMS like bad data detection in the synchrophasor network [21] by monitoring incoming measurements and outgoing control signals. However, it is also an ideal target for cyber-attacks and can lead to a single point of failure, if compromised that can render the whole EMS control center vulnerable to cyber threats.
- Distributed IDS (DIDS): It overcomes the limitation of a *"single point of failure"* by introducing multiple autonomous IDS agents that are deployed at the substation levels. In DIDS, it is crucial to consider an efficient communication topology like a

mesh network and communication standard with an anomaly detection algorithm for optimal and reliable performance of DIDS. A recent survey in [22] has shown the efficiency of a mesh network topology and communication standard like Zigbee [23] can be efficiently utilized to provide low-cost and low power-standard communication within the wireless network.

According to the nature-based taxonomy, we have classified IDS into different types: signature and anomaly-based IDSs.

(1) **Signature-based IDS (SIDS)**: This IDS detects anomalies based on the notion of comparing incoming network traffic to the known trails of malicious packets that are stored in the attack signature database. Since it relies solely on the database of known attack signatures, it cannot detect unknown or new attacks that do not match with the existing attack signatures. Several IDS tools, such as Snort, BRO (Zeek), Firestorm, Spade, etc., can be utilized in developing signature-based IDS in real-time based on the defined rules.

(2) **Anomaly-based IDS (ABIDS)**: It identifies malicious events based on deviations in the normal system behavior instead of looking into the library of known attack patterns. Based on the statistical profiling, it develops a baseline of normal cyber and physical activities and sends alert messages in real-time to the control center operators if the system deviates from the defined baseline. Different types of IDSs, such as model-based IDS, machine learning-based IDS, multi-agents-based IDS, etc. can be an integral part of anomaly-based IDS for detecting attacks in the power system.

- Model-based IDS (MIDS): This IDS leverages protocol information and historical and redundant measurements for developing a prediction model, and malicious and unknown attacks are detected based on behavior-based rules that are defined during the statistical and temporal correlation analysis of incoming data streams. Behavior-based rules include timing-based rules, range-based rules, transmission line status-based rules as well as rules defined based on the coordination and correlation of different events.
- Learning-based IDS (LIDS): This IDS applies several state-of-the-art machine learning algorithms like supervised and unsupervised algorithms, and data mining techniques to detect unknown, stealthy, and coordinated cyber-attacks. It relies on an immense volume of power system data to develop a non-linear complex relationships as necessary to distinguish between natural disturbances, malicious, and non-malicious events. This IDS involves data pre-processing, input feature selection, training, and real-time testing of different participating classifiers, and based on their performances, the best classifier is selected for optimal decision making.

(3) **Hybrid IDS (HIDS)**: This IDS integrates the conventional signature-based IDS with anomaly-based IDS on a common platform to provide better accuracy in detecting multi-level intrusions by utilizing both network and power system information while exhibiting a minimum detection latency. This IDS also overcomes the weakness of other previously discussed IDSs by leveraging the best qualities of other

IDSs while simultaneously monitoring physical, network, and application layers to minimize the attack surface in the grid network.

3 Hybrid Intrusion Detection System: A Potential Solution

Since it is imperative to thoroughly investigate possible cyber-attacks in the grid network to minimize attack surfaces, it is imperative to develop a comprehensive and robust IDS that can provide an optimal detection performance with a minimum detection latency while addressing the discussed IDS challenges. The HIDS provides one of the promising solutions that incorporates both grid measurements and network traffic information to minimize blind spots from the traditional IDS and capture possible intricacies at physical, cyber, and application layers [24]. In particular, the mechanism of HIDS combines network logs-based and data-driven approaches to detect different types of malicious events in the system operations.

Figure 3 shows the high-level schematic architecture of HIDS that integrates the existing conventional SIDS with the state-of-the-art LIDS and MIDS to accurately detect multi-level intrusions at physical, network, and application layers in real-time, and also minimize detection latency by assessing the network integrity in real-time. It consists of four layers: Layer 1 presents a SIDS that detects anomalies based on

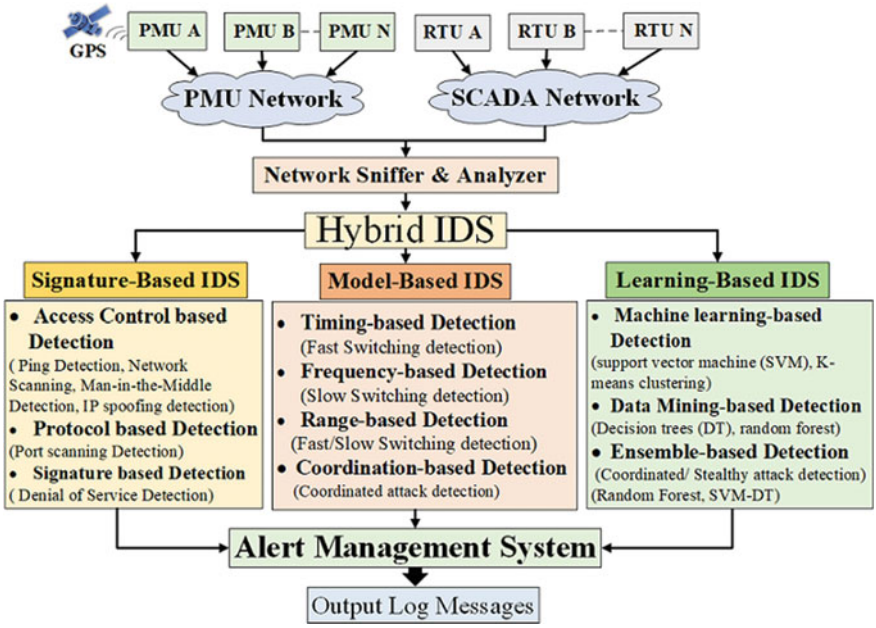

Fig. 3 High-level schematic architecture of HIDS in the smart grid

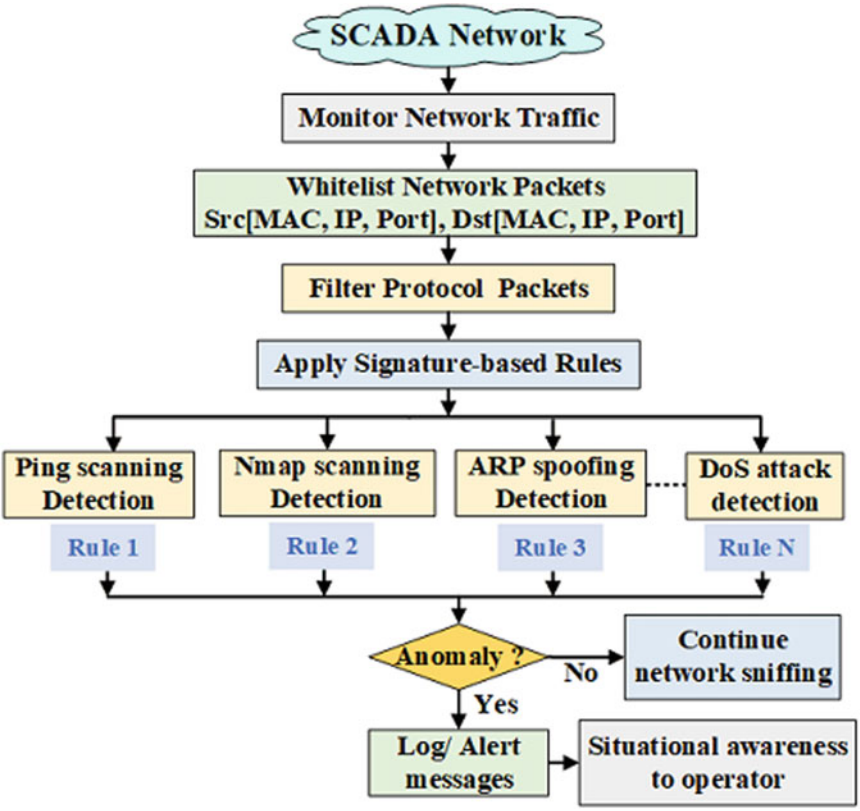

Fig. 4 Methodology of signature-based IDS

the known attack signatures using cyber logs; Layer 2 presents a MIDS that relies on the spatio-temporal behavior of power system to develop threshold-based rules to detect anomalies, and Layer 3 is a LIDS that applies the state-of-the-art machine learning approaches and data-mining techniques to detect stealthy and coordinated cyberattacks and provide a detailed classification of different events; Layer 4 presents an alert management system (AMS) that manages alerts, coming from all three intrusion detectors, and provides a final event identification to the control center operator.

(a) ***Signature-based IDS***: This layer monitors and analyzes SCADA network traffic and consists of several components that analyze various levels of communications traffic to detect anomalies in the grid network, as shown in Fig. 4. Access-control white-listing ensures legitimate traffic in the SCADA network by white-listing media access control (MAC) addresses, internet protocol (IP) addresses, and port numbers in the hardware, network, and transport layers. The protocol white-listing filters specific SCADA protocols and related function codes. Further, signature-based rules are applied to detect anomalies based on the known attack signatures like ping scanning

detection, Nmap scanning detection, address resolution protocol (ARP) spoofing detection, denial of service (DoS) attack detection, etc., which are publicly available in open-source IDS databases. Finally, the generated alert messages during network intrusions are directly forwarded to the AMS to provide situational awareness about network intrusions to the control center operator.

(b) ***Model-based IDS***: This layer performs an in-depth analysis of SCADA communication protocols and analyzes spatio-temporal behaviors of power systems to define normal and legitimate behavior models. In particular, it filters the SCADA communication packets, computes incoming packet rate, and extracts digital and analog values to develop behavior-based rules. Several behavior-based rules can be developed based on the timing of packets, range of power system variables, relays status, and a combination of behavior-based rules in a coordinated fashion, as shown in Fig. 5, to detect malicious and unknown threats. In this layer, once an anomaly is detected, the generated alert messages are fed to the machine learning classifiers as input features to accurately detect and classify cyber-physical events, including cyber-attacks and line faults.

(c) ***Learning-based IDS***: This layer applies machine-learning algorithms and data mining techniques to detect stealthy and coordinated cyber-attacks using multi-source heterogeneous system data and also differentiates cyber-attacks from natural disturbances like line faults, to provide intelligent decision support to the control center operator. For building the classification model, the SCADA and synchrophasor measurements, along with the cyber logs, are collected from the grid network and forwarded to the data aggregator at the control center. Fig. 6 shows the high-level methodology for developing machine learning-based IDS that includes two phases: offline process and online process. During the offline process, a library of heterogeneous datasets from a multi-source system has been generated for different events that are labeled later in the integer format to facilitate the supervised learning process. Afterward, data pre-processing steps are carried out to improve the data quality by formatting and sampling it to develop approximate models with data cleaning to filter inconsistent values and eliminate rows with a missing data. Further, the data transformation module is applied to normalize datasets for enhancing smoothness and homogeneity among samples followed by features selection and extraction, which filter irrelevant information and unreliable data that may affect the learning process and events prediction. Several feature selection techniques, such as filter (Pearson Correlation, Chi-Square, etc.), wrapper (best-first search method, backward elimination, etc.), and embedded methods (decision tree, L1 (LASSO) regularization) can be applied for selecting relevant features. The selected input features are utilized for developing, training, and updating machine learning models with new scenarios or cases when models are not online. Finally, during the online process, the trained model is deployed for testing multi-events classification, detecting malicious and benign events, and sending output logs to the AMS for final events identification and visualization.

(d) ***Alert management system (AMS)***: It receives alert messages from all three IDSs: NIDS, MIDS, and LIDS, and manages them through log parsers by performing real-time logical processing based on defined logic rules to prioritize alert types.

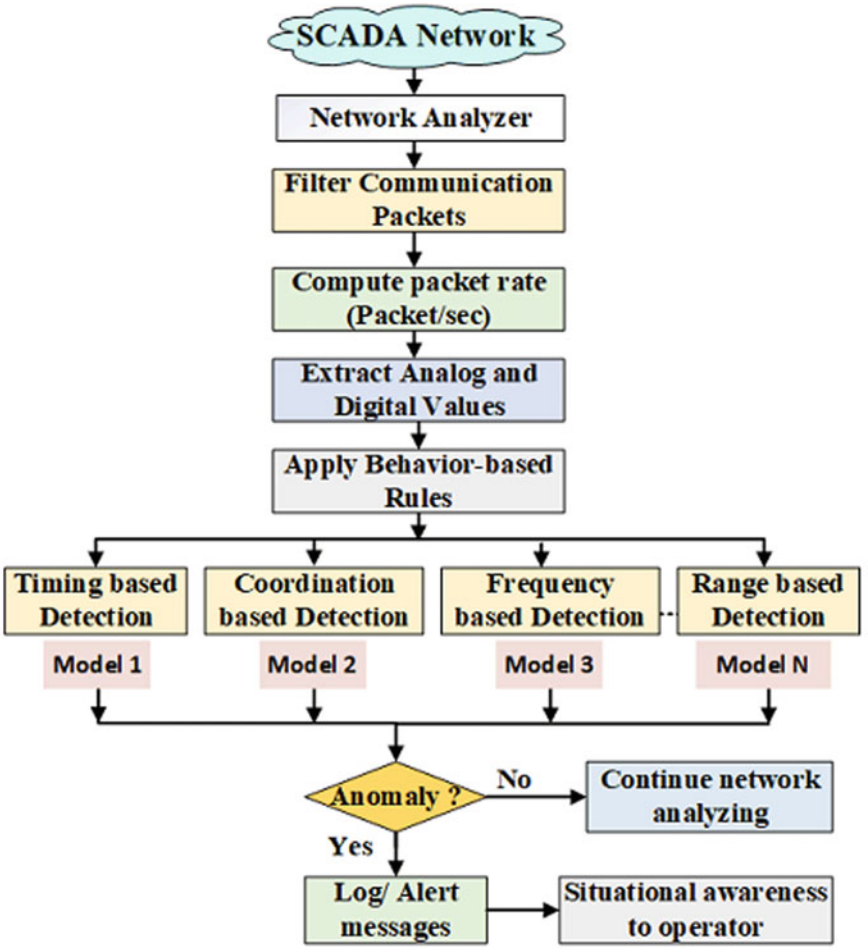

Fig. 5 Methodology of model-based IDS

Fig. 7 shows the log publishers X, Y, and Z, which are generated from network-based, model-based, and learning-based IDSs, and fed to the decision logic. The decision logic consists of two rules, i.e. rule 1 and rule 2.

Rule 1: It receives alerts from the Log Publisher X for SIDS and forwards them to the aggregator (B, C) as an output B. For example, if the output of rule 1 is $x1$, then B is also set to $x1$.

Rule 2: It receives alerts from the Log Publishers Y and Z for MIDS and LIDS and compares their alert logs to provide a final identification of events. If the alert outputs are conflicting, then LIDS is given a higher preference because of its advanced capability and sophistication in learning different types of events. For example, if Y is $y1$ and Z is $z1$, if $y1 = z1$, then C is set to $y1$ or $z1$. If $y1$ is not equal to $z1$, then C is set to $z1$ and $z1$ alert log is forwarded to the aggregator (B, C).

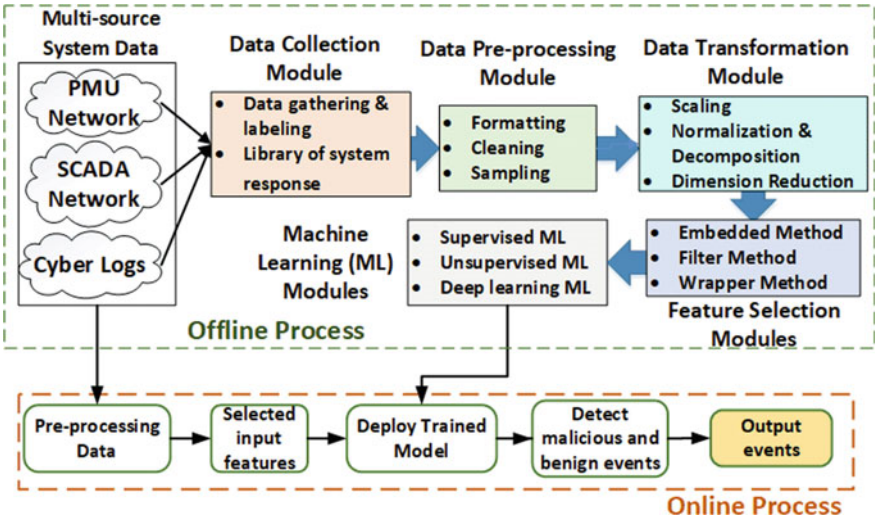

Fig. 6 Methodology of learning-based IDS

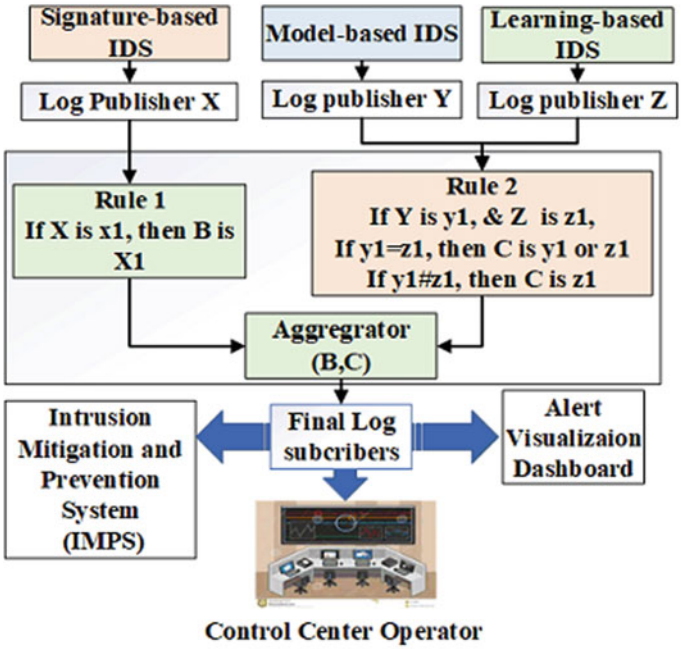

Fig. 7 High-level methodology of alert management system

The final alert logs that are coming from the aggregator (B, C) are displayed through real-time visualization dashboard and it can also be utilized for developing intrusion mitigation and prevention system (IMPS). The visualization dashboard also supports different sets of features to provide comprehensive visibility of the aggregated datasets and support event analysis based on the aggregated logs in real-time.

3.1 Cyber Kill Chain Mapping with HIDS

Since the attacker's skills, intellectual capabilities, and operational resources vary from a nave to a sophisticated level, it is imperative to have a comprehensive understanding of several attack processes and mechanisms. The cyber kill-chain model presents possible footsteps that can be utilized by attackers to successfully execute severe and stealthy cyber-attacks. For example, the real cyber-attack on Ukraine's power grid in 2015 [25] followed a similar cyber kill chain model, where the attackers performed a sequence of steps to understand the operational technology (OT) network and SCADA distribution system followed by shutting down multiple online distributed substations. Therefore, the development of the cyber kill chain model reduces the likelihood of adversary success while optimizing available resources and minimizing investments in cybersecurity. Further, it assists to better understand the end-to-end decision-making process from the adversary's perspective while engaging them to create desired effects; hence it is possible to develop a robust intrusion detector that can provide consistent and accurate performance in detecting cyber-attacks. Figure 8 shows an abstract-level presentation of the cyber kill chain in the context of SCADA cyber-physical security. Several tools, tactics, and procedures (TTP) can be utilized in a sequence of steps as per the attack mechanism to perform successful stealthy cyber-attacks. The model consists of various processes or stages that are elaborated here, as discussed in [13].

1. ***Reconnaissance***: In this stage, an attacker tries to collect substantial and relevant information of the target to develop the blueprint of network architecture. The attacker can perform ping scanning, port scanning, service scanning, etc. as attack mechanisms to complete this stage. Several scanning tools like Ping Scanner, Nmap, Zenmap, etc. can be leveraged to identify alive hosts, map network addresses, and figure out the up-to-date network architecture.
2. ***Access and Exploitation***: In this stage, an attacker tries to communicate or connect to a target to discover potential vulnerabilities. Later, the obtained information about the existing vulnerabilities can be exploited to gain a foothold or the privilege escalation to launch a successful attack. The vulnerability assessment or penetration testing can be used as an attack mechanism; and tools like OpenVAS, Metasploit, Nessus, etc. can be utilized to complete this stage.
3. ***Attack Launch/ Execution***: Before reaching this stage, an attacker must ensure that he has obtained the necessary privileges to execute or launch different types

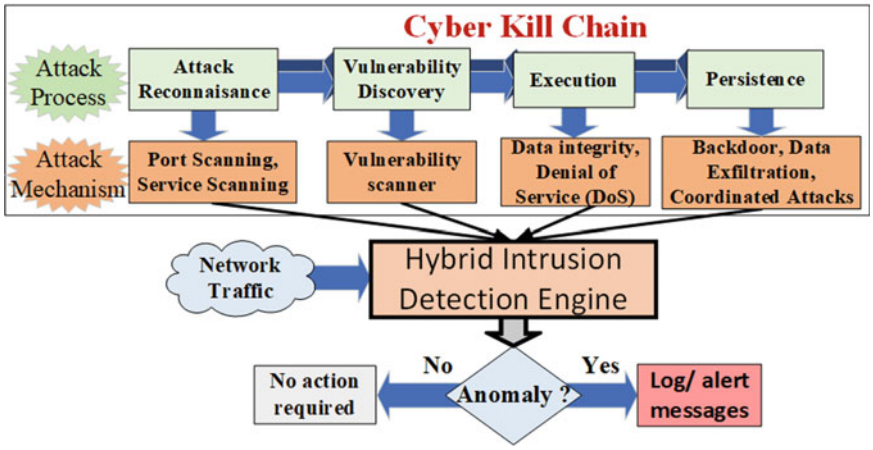

Fig. 8 Cyber kill-chain mapping with the hybrid IDS

of attacks on system measurements, control signals, wide-area communication network or operating field devices to disrupt the grid stability.

4. ***Persistence***: This is the final stage where an attacker creates an additional backdoor or access channel to maintain his persistence access to the compromised system that can be exploited later for attack repetition or launching multiple attacks in a coordinated fashion.

Since our main objective is to detect all kinds of attacks, irrespective of the attacker's intelligence, different components of HIDS are developed around the kill chain and mapped with its different stages to detect attackers at an initial stage and predict their next move. Note that any disruption in the process/stage can break the chain process, and thus, it may interrupt the attacker's objective of destabilizing the grid network. Also note that the sequence of chain model can be modified, changed, and expanded depending upon the scenario, security investigation, and OT organization.

4 Case Study: Hybrid IDS for Wide-Area Protection Scheme

4.1 Problem Formulation

A centralized wide-area protection scheme (CWAPS), also known as a remedial action scheme (RAS), is an automatic protection system that performs corrective actions to prevent widespread outages and maintain the system's stability and reliability during disturbances. The corrective actions, as defined by the NERC guideline

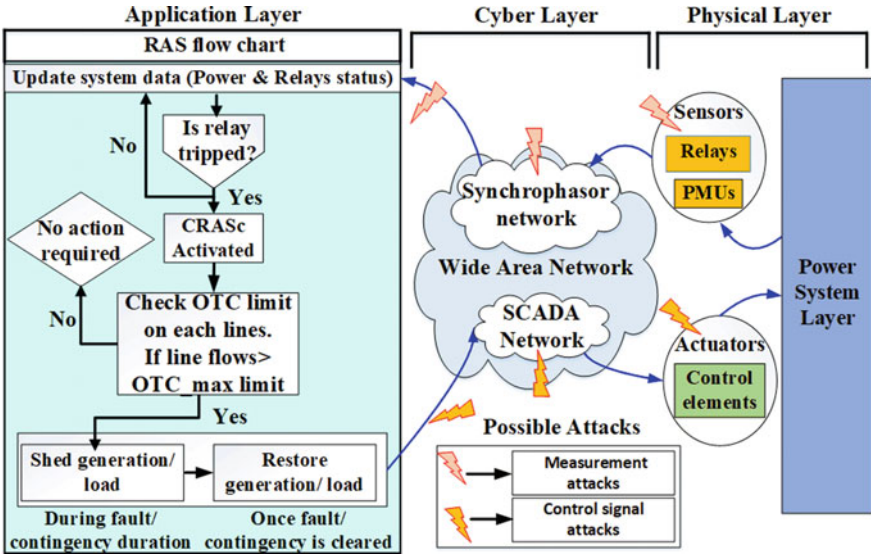

Fig. 9 Attack surface representation in the CWAPS

[26], include a change in generation and load (MW or MVAR) and system configuration. Seethalekshmi et al. presents the requirements of WAPS and explains how the WAPS overcomes the major drawbacks of the SCADA-based localized protection scheme [27]. According to the 2008 design guide of the Western Electricity Coordinating Council (WECC), RAS is divided into four different types: event-based, parameter-based, response-based, and a combination of the above [28]. The event and parameter-based schemes are open-loop faster schemes, which take inputs as relays status, line currents, voltages, etc. and perform corrective actions by shedding the load, generation, and other pre-defined actions. The response-based scheme is a close-loop slower scheme that examines the dynamic behavior while performing corrective actions. In particular, the RAS is mainly utilized during transient instability, voltage instability, and thermal overloads.

Fig. 9 shows possible attack surfaces in CWAPS architecture at physical, cyber, and application layers, as well as measurement and control sides. Since the CWAPS relies on the SCADA and synchrophasor communication networks that are interacting with data sharing devices for normal operation, the existing cybersecurity vulnerabilities can be exploited by attackers to launch simple or elaborated classes of cyber-attacks like denial of service (DoS), data integrity, etc. [29]. Moreover, it cannot prevent themselves from legitimate users who misuse their privileges to perform malicious activities. Therefore, there is a compelling urge to develop a HIDS for CWAPS that can detect attacks at an earlier stage to break the life-cycle of cyber-attacks.

In this work, we have implemented an event and parameter-based CWAPS that consists of a centralized RAS controller (CRASc). The CRASc, initially at an armed

stage, collects phasor data at a regular interval in terms of relays status, power line flows, and generator output. During a single line outage, the CRASc is triggered, it checks the operational transfer capability (OTC) of the remaining adjacent lines that are directly connected to the generator. If the current line flows exceed its maximum operational transfer capability (OTC_max) limit, it performs corrective action by shedding generation to prevent the thermal overloading in other adjacent lines. Note that we have considered a thermal overload limit while computing the OTC_max, other factors like voltage and angular stabilities are ignored in this work. The OTC_max limit of each transmission line is provided through the predefined action table that also provides information about how much generation has to be reduced for the specific line contingency. Apart from the generation shedding, it is also allowed to restore the generation once the fault/contingency is cleared, as mentioned in [26].

4.2 Scenarios and Data Generation

This subsection presents several types of events, including malicious (cyber intrusions) and non-malicious events (line faults), which are considered to develop a robust hybrid IDS that can provide accurate and consistent results. Moreover, a library of the system database is generated for different scenarios for testing, validation, and evaluation.

4.2.1 Physical Line Faults

It involves different types of faults, including symmetrical and asymmetrical faults that can happen on transmission lines. In this case, we have considered 5 different types of faults: line to ground (L-G), double line to ground (LL-G), three phases to ground (LLL-G), line to line (L-L), and 3 phase faults (L-L-L). The unsymmetrical faults, (L-G), (LL-G), (L-L) are more frequent and cause uneven flows of current and phase shifts in a 3-phase power system. The symmetrical faults, (LLL-G) and (L-L-L) cause the short-circuiting of three phases and often to the ground. These faults are very rare but have a severe impact on the system's stability.

4.2.2 Cyber Attacks

We have considered several types of cyber intrusions around the kill-chain model, irrespective of the attacker's intelligence that can have a potential impact on system stability. We have classified attack vectors into two different types: IT-based attacks and SCADA-based attacks. Both are discussed in details in the remainder of this section

1. ***IT-Based Attacks***: IT-based attacks include traditional host and network-based attacks-including scanning attacks (e.g., ping and Network Mapper (NMAP) scanning), DoS attacks, and spoofing attacks (e.g., IP spoofing, ARP poisoning)–that can be deployed in the SCADA environment to develop a blueprint of the network architecture and compromise power system devices.
2. ***SCADA-Based Attacks***: SCADA-based attacks include those attacks that are defined in the OT environment pertinent to the SCADA power system. These attack vectors target insecure SCADA communications protocols, field devices, computers, and several other digital access points to inflict severe damage on the grid infrastructure. We consider three different attack vectors:
   (a) **Malicious tripping attack**: This attack vector involves the malicious tripping of a physical relay that can be performed in several ways, such as unauthorized access to the control center, altering the setting of physical relays, etc. During a MITM attack between substation and control center networks, the false tripping command packets are injected to trip a circuit breaker and disconnect power system components.
   (b) **Pulse attack**: This attack vector involves periodically changing an input control signal by adding the pulse attack parameter, λ_{pulse}, for a small-time interval, $(t1)$. It retains the original input for a remaining interval, $(T - t1)$, for the given time period, (T), as shown in Eq. 1.
   (c) **Ramp attack**: This attack vector involves adding a time-varying ramp signal to the input control signal based on a ramp signal parameter, λ_{ramp}, as shown in Eq. 2.

$$P_{pulse} = \begin{cases} P_i(1 + \lambda_{pulse})(t = t_1) \\ P_i(t = T - t_1) \end{cases} \tag{1}$$

$$P_{ramp} = P_i + \lambda_{ramp} * t \tag{2}$$

4.3 Hybrid IDS Components

This subsection presents the three components of HIDS where SIDS is utilized to detect IT-based attacks, and MIDS and LIDS are deployed to detect SCADA-based attacks as well as physical disturbances.

4.3.1 Signature-Based IDS Component

For SIDS, we have defined several rules for detecting IT attacks, as shown in Table 1. Table 1 shows detailed information about IDS rules corresponding to different stages of attacks based on the kill chain model. In this table, rule 1 and rule 2 belong to the reconnaissance (stage 1), rule 3 belongs to the access (stage 2), and rule 4 belongs to

Table 1 Snort rules for signature-based IDS

Rules	Attack	Snort IDS Rules
Rule1	Ping Scanning (Reconnaissance)	*Alert icmp* $ *EXTERNAL_NET any -> (IP of your substation RTU) any (msg:ICMP to Substation; content:*| 10 11 12 13 14|; *sid: 9000547; rev:1;)*
Rule 2	Nmap Scanning (Reconnaissance)	*alert tcp any any -> (IP of your substation RTU) 22 (msg:NMAP TCP Scan;sid:10000005; rev:2;)*
Rule 3	Telnet Access (Access)	*Alert tcp* $ *EXTERNAL_NET any-> (IP of your substation RTU) 23 (msg:Incoming Telnet ; content; root; nocase; sid: 9000546; rev:1;)*
Rule 4	DOS Attack (launch)	*Alert tcp* $ *EXTERNAL_NET any -> (IP of your substation RTU) 20000 (msg:Warning DoS attack incoming; threshold:type threshold, track by src, count 100, seconds 5; sid: 9000547; rev:1;)*

the launch stage (stage3). Note that we have utilized the Snort IDS tool to analyze the SCADA traffic through network interfaces and later develop these rules as discussed in [13].

Rule 1: It detects the ping scanning attack on the substation network by capturing incoming network traffic on the specified network internet protocol (IP) address for the Internet Control Message Protocol (ICMP) protocol.

Rule 2: This rule detects the Nmap scanning attack whenever an attacker performs TCP-based Nmap scanning on the substation RTU on port 22.

Rule 3: This rule detects an unauthorized Telnet session through a root login to the substation RTU at port 23.

Rule 4: This rule detects a DoS attack on the substation network targeting the distributed network protocol 3 (DNP3) communication on port 20000. In this rule, an alert is generated after the first 100 SYN packets (SYN flood) within a sampling period of 5 s.

4.3.2 Model-Based IDS Component

For MIDS, we have considered three behavior-based rules: range-based detection, status-based detection, and timing-based detection, by defining thresholds in the Zeek (BRO) analyzer function and Snort IDS for the DNP3 communication to detect pulse attack, tripping attack, and ramp attack, as shown in Table 2 and 3, also discussed in [13, 14, 24].

Table 2 Zeek scripts for model-based IDS in DNP3

Alert ID	Model-based Rules (Attack)	Zeek IDS Scripts
Alert ID 1	Range-based Detection (Pulse Attack)	*event dnp3_analog_input_SPwFlag(c: connection, is_orig: bool, flag: count, value: count){ if (value* != 0 && *value* < 3000000000 && *value* != 1065353216) { *if (value* < 1123679256 ‖ *value* > 1200000000){ *c* $*dnp3*$*alert* = 1; } } }

Table 3 Snort rules for model-based IDS in DNP3

Alert ID	Model-based Rules (Attack)	Snort IDS Rules
Alert ID 2	Status-based Detection (Tripping Attack)	*Alert tcp !(IP from your control center) any -> (IP of your substation RTU) 20000 (msg:Unauthorized Relay Trip; content :*|00 81| *;rev:1;)*
Alert ID 3	Timing-based Detection (Ramp Attack)	*Alert tcp (IP from your control center) any -> (IP of your substation RTU) 20000 (msg:Ramp attack ; content :* |00 81|; *threshold:type threshold, track by src, count 2, seconds 0.3; sid: 9000547; rev:1;)*

Range-based detection: In this case, a minimum threshold value is defined based on the analog value that is extracted from the DNP3 SCADA communication protocol. Table 2 shows a range-based detection in the Zeek script that generates an alert with an alert ID 1 if the generated output power goes below the defined initial generation. For example, if the output power of generator 1 is 135.4 MW, then an alert is triggered if the generation reduces to the minimum threshold of 108.32 MW (0.8 *135.4) that is equivalent to 1123679256 as an unsigned 32-bit integer, one of the few available data types in Zeek (Bro) IDS [23].

Status-based detection: It triggers an alert in Snort IDS with an alert ID 2 if the line status changes from 1 to 0 to notify the control center operator that the specific relay is tripped.

Timing-based detection: This rule is defined based on the statistical analysis of two consecutive control signal packets. We assign the minimum threshold value to 0.3 seconds for two consecutive normal DNP3 packets based on the high-speed auto-reclosing time, as discussed in [14], and an alert ID 3 is triggered in the Snort IDS.

4.3.3 Learning-Based IDS Component

This component of hybrid IDS applies machine-learning algorithms and data mining techniques to detect the last stage (Persistence) of kill chain model that includes stealthy and coordinated cyber-attacks. This approach utilizes secure phasor measurements that are communicated over a separate WAN like the NASPI network (NASPInet) with inherent cybersecurity features, and alert logs, obtained from the model-based IDS, to accurately detect attacks and provide the detailed classification of them while distinguishing them from natural disturbances like line faults. The detailed classification and clarification of cyber-physical events provide a comprehensive understanding of incidents and also assist the control center operator to take intelligent decisions.

Fig. 10 shows the methodology for developing LIDS to perform multi-events classification. For building the classification model, the phasor measurements, including generator bus voltage magnitude (Vm_g) and line bus voltage magnitudes (Vm_i, Vm_j), where subscripts i and j represent the sending and receiving ends of the transmission lines, are collected from the deployed PMUs. Apart from PMU measurements, the learning-based IDS also receives the generated alert logs (Y) from model-based IDS as input features. The offline process is applied, as outlined in Fig. 10 from connector A to B, for training and updating model and developing the final machine learning model. During the offline process, a library of the dataset has been generated for different events, including cyberattacks, line faults, and nor-

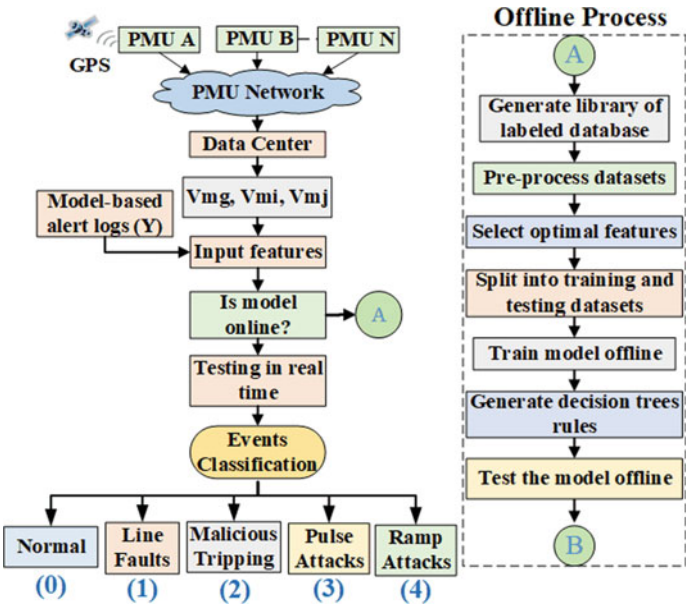

Fig. 10 Machine learning-based IDS using PMU measurements

mal events, which are labeled later in the integer format, as part of the supervised learning. Afterward, data preprocessing steps are carried out that involve normalization, transformation, and features selection and extraction, which filter out the irrelevant information and unreliable data that may affect the learning process and events prediction. Further, the Pearson Correlation-based feature selection technique is applied to select the relevant features. The obtained dataset is split into training and testing datasets. It is appropriate to note that due to the space limitation, we are not discussing the details of different scenarios required for generating the labeled datasets. Overall, we have generated datasets for the five events: normal (0), line faults (1), malicious tripping attack (2), pulse attack (3), and ramp attack (4). Finally, the trained model is deployed for performing multi-events classification and sending output logs to the operator.

4.4 Experimental Setup

Fig. 11 shows the hardware in the loop (HIL)-based cyber-physical system (CPS) testbed for attack-detection experiments in CWAPS. We have modeled the IEEE 39

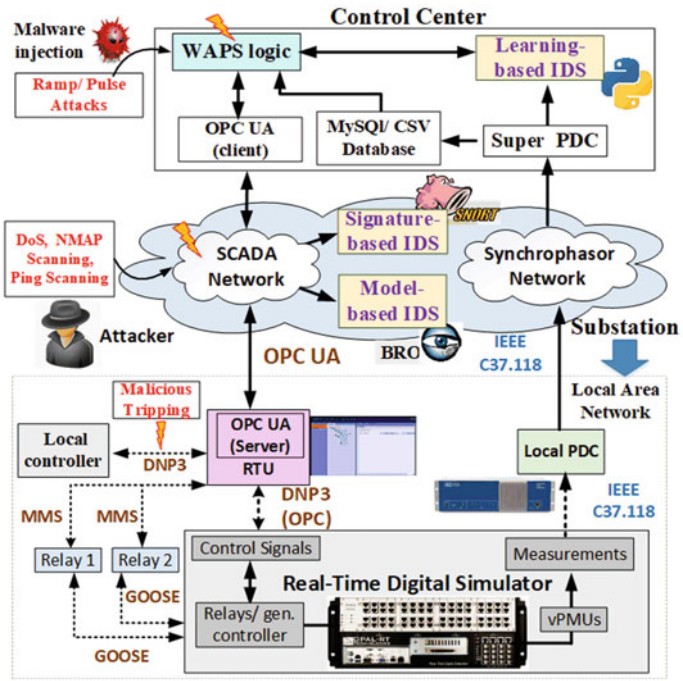

Fig. 11 Experimental setup for attack-detection experiments

bus system in ARTEMiS/SSN (eMEGASIM), and simulated in the real-time digital simulator (OPAL-RT). We have deployed virtual PMU models (vPMUs) to generate synthetic phasors, and computed the relevant features inside the simulator. The computed relevant features are sent to the hardware local phasor data concentrator (LPDC), deployed at the substation network, which forwards the data to the software-based super PDC (Open PDC) at the control center over the WAN. The super PDC saves the data in a local comma-separated values (CSV) historian as well as in the MySQL database. The stored data is used for generating the labeled database and further training and testing machine learning model, as a part of the LIDS. In this experiment, the CRAS controller is running in the python script, which is communicating with the substation RTU through the Kepserver's OPC Unified Architecture (UA) client-server interfaces. The substation RTU, as shown in a pink box, is communicating with a simulator using the DNP3 (OPC server) SCADA communication. The software OpenPDC collects the phasor measurements and forwards it to the LIDS. Also, the CWAPS controller receives phasor measurements through the MySQL in real-time, and sends the control signal back to the substation network through the SCADA communication to provide an appropriate response, if necessary, to close the loop. Also, SIDS and MIDS are deployed over the WAN that sniffs the SCADA traffic and detects possible anomalies.

Fig. 12 shows the CRAS-enabled modified IEEE 39 bus system that is divided into two major areas, where the area 2, working as a primarily generation area, is supplying generation to the area 1 through the tie-lines L15-16 and L16-17. During the tripping of line L16-17, the line L15-16 gets overloaded. Therefore, the CRAS controller sheds the generation at bus 35, as shown by black colored arrow, and the equal amount of load is shed at bus 18 to maintain the system frequency. To perform the HIL experiment, relay 1 and relay 2 is mapped to lines L15-16, and L16-17 [30].

For implementing IT-based attacks, the installed Kali Linux machine is listening to the network traffic between the control center and substation network. We have utilized the pre-installed tools, *Nmap*, and *ping* command, in the Kali machine to perform the attack reconnaissance. The DoS attack is performed by sending a huge number of random packets to the RTU through the TCP SYN flooding attack using *hping* tool.

For implementing SCADA-based attacks, we have performed the malicious tripping attack on the relay 2 to trip the line L16-17 by replaying the tripping packet using the python script through the MITM between the substation and local control center. For executing ramp and pulse attacks on generator 35 (G35), the malware, Trojan Horse, is installed in the OPC server-based substation RTU, which provides backdoor access to the attacker. The attacker closes the legitimate RTU program and initiates python script-based malicious logic, which periodically sends the control signal to the simulator targeting the generator (G35) to initiate ramp and pulse attacks. We have also simulated 3 phase to ground faults followed by the normal tripping of the line L16-17, and multiple simulations are performed for different cases as discussed in [6]. Note that in this work, we assume that the attacker is only looking to compromise insecure SCADA network and the synchrophasor network is

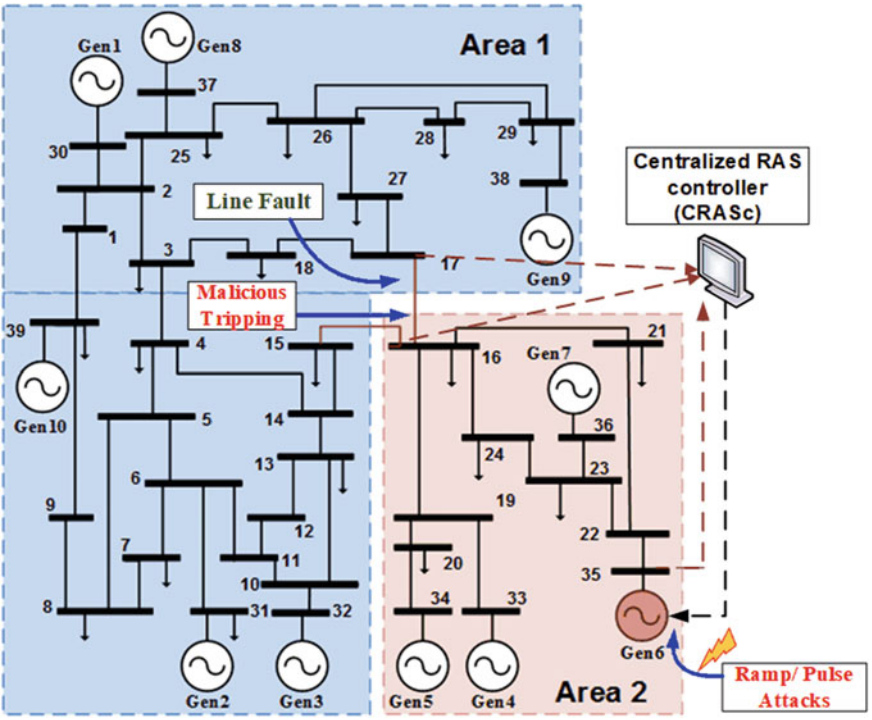

Fig. 12 CRAS enabled modified IEEE 39 bus system

secure with inherent cybersecurity features and the detection results are provided in the next section.

4.5 Results and Discussions

Table 4 shows the performance of HIDS as well as its comparison with an individual SIDS in terms of accuracy rate. It can be observed that the SIDS is able to detect IT attacks including ping scanning, Nmap scanning, DoS attack, and Telnet access attack with an accuracy rate of 100%; however, it fails to identify stealthy SCADA-related attacks and physical disturbances like line-to-ground faults. The HIDS merges LIDS with SIDS and MIDS to detect IT and OT attacks with an accuracy rate of 100% and 98.71%. Further, it is also able to detect physical disturbances with an accuracy rate of 97.94% using machine learning-based random forest classifier during 70% training and 30% testing datasets.

Note that while developing the LIDS, different machine learning classifiers were applied—such as decision tree (DT), random forest (RF), and support vector machine

Table 4 Accuracy Rate of several IDSs

IDSs	IT Attacks	OT Attacks	Line Faults
Network-based IDS (%)	100%	×	×
Hybrid IDS (%) (Network+Model+Learning)	100%	98.71%	97.94%

Table 5 Average accuracy rate for different classifiers during Case 1 and Case 2 experiments

Parameters	Case 1	Case 2
70% Training and 30% Testing		
Decision Tree (DT)	88.5	79.8
Support Vector Machine (SVM)	91.3	89.2
Random Forest (RF)	96.33	95.4

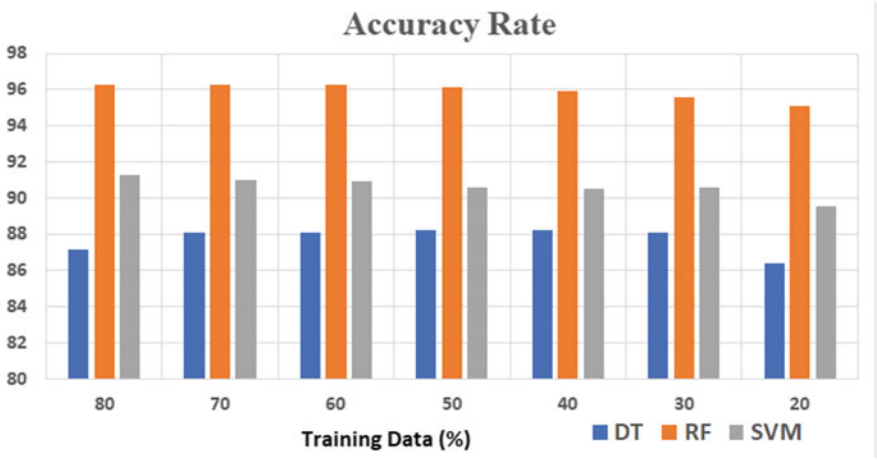

Fig. 13 Average accuracy rate for different classifiers during case 2

(SVM)—to select the best classifier. Table 5 shows the average accuracy rate of different classifiers during case 1 and case 2 experiments for 70% training and 30% testing datasets. Note that case 1 represents the scenario when PMU measurements and cyber alerts, generated from MIDS, are utilized as input features, whereas input features for case 2 include only PMU measurements. Table 5 also shows that the RF exhibits a higher accuracy rate as compared to other classifiers with an average accuracy of 96.33% in case 1 and 95.4% in case 2.

Fig. 13 shows the average accuracy rate of different classifiers during testing in case 2 where the training and testing datasets were varied from 80% training and 20% testing to 20% training and 80% testing datasets to analyze the robustness of different classifiers and it clearly illustrates the consistent performance of RF as compared

Fig. 14 Average accuracy rate of random forest (RF) for different training datasets

to DT and SVM. Fig. 14 represents the average accuracy rate of RF for different training datasets for both cases: case 1 and case 2. It clearly presents the consistent and reliable performance of RF, as its accuracy in detecting different events during testing is higher than 95% for case 1 and 93% for case 2, even when the training dataset is reduced to 20% in both cases. Further, we observed that the performance of each classifier improves by including power and cyber information for different datasets, as shown in case 1 with respect to case 2.

Fig. 15 shows the processing time of RF for different % of training datasets for both cases. It can be observed that the processing time (sec) for training the model was higher in case 1 as compared to case 2, which is amplified during the higher % of training datasets. Note that the RF exhibits a larger processing time in classifying events as compared to the DT because of a large number of associated decision trees in RF and the final prediction is made based on the majority vote, as discussed in [24].

5 Conclusion

Developing an intrusion detection system for the smart grid cybersecurity is a challenging task as it requires an in-depth understanding of power system related applications, grid network architectures, and comprehensive knowledge of cutting-edge technologies. In this chapter, we presented a systematic approach for developing a hybrid IDS by integrating conventional network security solutions with state-of-

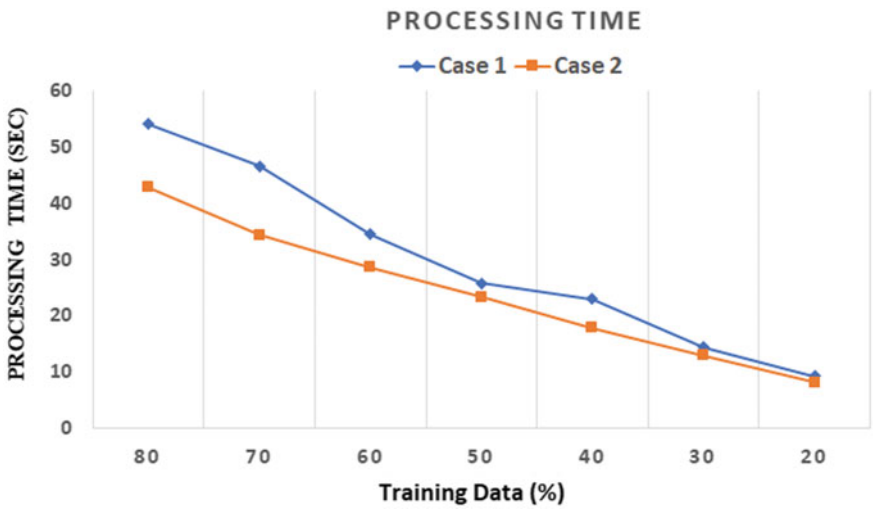

Fig. 15 Processing time of random forest (RF) for different training datasets

the-art machine learning and model-based intrusion detection approaches to detect advanced and persistent intruders at different stages while following the kill-chain model. Initially, this chapter discussed different types of IDSs and highlighted the existing challenges of developing IDS in the smart grid network. As a proof of concept, one case study was presented where hybrid IDS is applied in a centralized wide-area protection scheme to detect different types of cyberattacks, including IT- and SCADA-based attacks. In particular, Snort and Zeek IDS tools were applied in developing signature and model-based IDSs, and machine learning-based classification algorithms, including decision tree, random forest, and support vector machine, were applied for developing the learning-based IDS. Further, several steps were described to implement these cyber-attacks in the CPS testbed environment by utilizing the resources available at Iowa State University PowerCyber laboratory. Experimental results showed the superior performance of hybrid IDS to accurately detect different classes of anomalies and physical disturbances. Our case study also showed that the random forest-based classifier exhibited a higher accuracy rate as compared to the other machine learning classifiers, and a combination of grid measurements and alert logs, generated from model-based IDS, also assisted in providing a detailed classification of different events. The potential avenue for future work is to develop a library of novel IDSs for other SCADA protocols, such as GOOSE, Modbus, and smart energy profile (SEP) 2.0 protocols.

References

1. V. Terzija et al., Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. Proceedings of the IEEE **99**(1), 80–93 (2011)
2. National Institute of Standards and Technology (NIST), "NISTIR 7628 Revision 1: Guidelines for Smart Grid Cyber Security", September 2014
3. U.S. Department of Energy (DOE) Energy Sector Control Systems Working Group, 'Roadmap to Achieve Energy Delivery Systems Cybersecurity', Technical Report, 2011
4. U.S. Department of Energy (DOE) 'Cybersecurity Capability Maturity Model (C2M2)', February 2014
5. NERC, 'Critical Infrastructure Protection (CIP) Standards', 2015
6. National Electric Sector Cybersecurity Organization Resource (NESCOR), 'Wide Area Monitoring, Protection, and Control Systems (WAMPAC)-Standards for Cyber Security Requirements', 2012
7. U.S. Department of Energy (DOE) 'Cybersecurity Capability Maturity Model (C2M2)', February 2014
8. S. Sridhar et al., Model-Based Attack Detection and Mitigation for Automatic Generation Control. IEEE Transactions on Smart Grid **5**(2), 580–591 (2014)
9. S. Sarangan, V.K. Singh, M. Govindarasu, "Cyber Attack-Defense Analysis for Automatic Generation Control with Renewable Energy Sources,", North American Power Symposium (NAPS). Fargo, ND **2018**, 1–6 (2018)
10. V.K. Singh, M. Govindarasu, "Decision Tree Based Anomaly Detection for Remedial Action Scheme in Smart Grid using PMU Data,", IEEE Power & Energy Society General Meeting (PESGM). Portland, OR **2018**, 1–5 (2018)
11. A. Ashok et al., "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," in IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1636-1646
12. V.K. Singh, A. Ozen, M. Govindarasu, "A Hierarchical Multi-Agent Based Anomaly Detection for Wide-Area Protection in Smart Grid,", Resilience Week (RWS). Denver, CO **2018**, 63–69 (2018)
13. V.K. Singh, S.P. Callupe, M. Govindarasu, "Testbed-based Evaluation of SIEM Tool for Cyber Kill Chain Model in Power Grid SCADA System,", North American Power Symposium (NAPS). Wichita, KS, USA **2019**, 1–6 (2019)
14. V.K. Singh, H. Ebrahem, M. Govindarasu, "Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment,", North American Power Symposium (NAPS). Fargo, ND **2018**, 1–6 (2018)
15. V.K. Singh, E. Vaughan, J. Rivera, "SHARP-Net: Platform for Self-Healing and Attack Resilient PMU Networks,", IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Washington, DC, USA **2020**, 1–5 (2020)
16. Y. Yang et al., "Intrusion Detection System for network security in synchrophasor systems," IET International Conference on Information and Communications Technologies (IETICT 2013), Beijing, China, 2013, pp. 246-252
17. S. Pan et al., Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. IEEE Transactions on Smart Grid **6**(6), 3104–3113 (2015)
18. NERC, Reliability Guideline: PMU placement and Installation, December 2016
19. M. Begovic et al., Wide-Area Protection and Emergency Control. Proceedings of the IEEE **93**(5), 876–891 (2005)
20. Berthier, R., Sanders, W. H. (2011). Specification-based intrusion detection for advanced metering infrastructures. In Proceedings - 2011 17th IEEE PRDC 2011 (pp. 184-193)
21. M. Wu, S. Member, L. Xie, S. Member, Online detection of low-quality synchrophasor measurements: A data-driven approach. IEEE Trans. Power Syst. **32**(4), 2817–2827 (2016)
22. C.F. Garcia-Hernandez et al., "Wireless sensor networks and applications: A survey," IJCSNS Int. J. Comput. Sci. Netw. Security **7**(3), 264–273 (2007)
23. S. Safaric and K. Malaric, "ZigBee wireless standard," in Proc. 48th Int. Symp. ELMAR-2006, Zadar, Croatia, Jun. 07-09, 2006, pp. 259-262

24. V.K. Singh, E. Vaughan, J. Rivera, A. Hasandka, "HIDES: Hybrid Intrusion Detector for Energy Systems,", IEEE Texas Power and Energy Conference (TPEC). College Station, TX, USA **2020**, 1–6 (2020)
25. ICS-CERT, Cyber-Attack Against Ukranian Critical Insfrastructure
26. NERC,Remedial Action Development Definition Development project 2010-05.2 -Special Protection System
27. K. Seethalekshmi et al., "Wide-area protection and control: Present status and key challenges," in Proc. 15th Nat. Power Syst. Conf., Mumbai, India, Dec. 2008, pp. 169-175
28. WECC remedial action scheme catalog summary [Internet]; 2008
29. V. Kumar Singh, A. Ozen, M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid,", North American Power Symposium (NAPS). Denver, CO **2016**, 1–6 (2016)
30. V.K. Singh, "Evaluation of Anomaly Detection for Wide-Area Protection Using Cyber Federation Testbed,", et al., IEEE Power & Energy Society General Meeting (PESGM). Atlanta, GA, USA **2019**, 1–5 (2019)