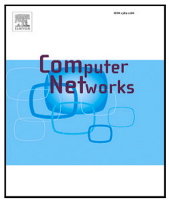
Computer Networks 184 (2021) 107679

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Survey paper

A survey on intrusion detection and prevention systems in digital substations

Silvio E. Quincozes [a,*], Célio Albuquerque [a], Diego Passos [a], Daniel Mossé [b]

[a] Computer Science Department, Universidade Federal Fluminense, Niterói, RJ, Brazil
[b] Computer Science Department, University of Pittsburgh, Pittsburgh, PA, USA

ARTICLE INFO

Keywords:
Smart grid
Cybersecurity
Intrusion Detection Systems
IDS
Survey
IEC–61850 standard

ABSTRACT

Smart Grids integrate the traditional power grid with information processing and communication technologies. In particular, substation intelligent devices can now communicate with each other digitally to enable remote information gathering, monitoring, and control. There have been many efforts to promote global communication standards. The IEC–61850 international standard addresses substation communication networks and systems. Despite the many benefits, this standardized communication poses new cyber-security challenges. Also, traditional Intrusion Detection Systems (IDSs) may not be suitable for digital substations, given their critical components and stringent time requirements. We present an in-depth analysis of attacks exploiting IEC–61850 substations and recent research efforts for detecting and preventing them. Our main contribution is an original taxonomy comprising design and evaluation aspects for substation-specific IDSs. This taxonomy includes IDS's architectures, detection approaches, analysis, actions, data sources, detection range, validation strategies, and metrics. Additionally, we present a compilation of the detection rules deployed by the state-of-art IDSs and assess their resiliency to five types of attacks. Our assessment reveals that some attacks are covered by currently-deployed IDSs, but, particularly, further advancement is necessary to deal with masquerade attacks. Finally, we discuss trends, open issues, and future research topics.

Digital substations have a critical role in the entire power grid, given their role of splitting, transforming, and combining the energy. Information technology solutions are used to provide easy data acquisition, remote control and monitoring of electrical infrastructure, services, and components. Integrating all these features and devices requires several new protocols and standards [1]. The IEC–61850 [2] is a global standard for substation automation that has revolutionized the way digital substations are configured and maintained [3].

Despite the many benefits from the IEC–61850 standard – such as the interconnection support for heterogeneous devices, protocols, and functionalities, as well the potential to reduce errors and misconfiguration – from a security perspective, the increased complexity and interconnection in digital substations have exposed them to a wide range of cyber-security threats. These threats are both external (*e.g.*, hackers, terrorists, and competitors) and internal (*e.g.*, employees and vendor maintenance team). In practice, attackers may exploit vulnerabilities to launch attacks such as eavesdropping, fake control and measurement messages, Denial-of-Service (DoS), flooding, poisoning. Hong et al. [4] points out hundreds of real attacks that caused outages to hundreds of thousands of people in the U.S. and Ukraine in recent years. Human life may also be at risk (*e.g.*, if a malicious command is injected during a programmed maintenance) [5,6].

Many digital substation network protocols do not cover security aspects and most substation devices (called Intelligent Electronic Devices, or IEDs) are designed to perform specific functions related to the electrical domain, without built-in security mechanisms. Therefore, deploying IDSs (Intrusion Detection Systems) to detect both traditional threats, inherited from information technology and network protocols and specialized attacks targeting IEC–61850 protocols became essential. Nevertheless, IDS research for substations is still at an early stage. In addition, any overhead imposed by security functions may harm proper system operation, because some IEDs have time-critical requirements. Accordingly, traditional mechanisms such as complex encryption algorithms are not supported by these devices [4]. In-depth investigations are still required for understanding the threat vector and, thus, for developing effective methods for intrusion detection and prevention, as discussed later in this work.

Whereas existing surveys already address IDSs in the overall Smart Grids [7] and SCADA (Supervisory Control and Data Acquisition) [8] contexts, this survey focuses specifically on IEC–61850 digital substations. It presents an original taxonomy based on an in-depth review of the security threats and state-of-the-art solutions for detecting and preventing intrusions in digital substations. Specifically, we address

* Corresponding author.
E-mail addresses: sequincozes@id.uff.br (S.E. Quincozes), celio@ic.uff.br (C. Albuquerque), dpassos@ic.uff.br (D. Passos), mosse@pitt.edu (D. Mossé).

https://doi.org/10.1016/j.comnet.2020.107679
Received 10 July 2020; Received in revised form 25 September 2020; Accepted 7 November 2020
Available online 21 November 2020

both design (*i.e.,* architecture, detection approach, type of analysis, and response action) and deployment aspects (*i.e.,* data sources, detection range, evaluation and metrics) of the current state-of-the-art IDSs. Among these aspects, three main groups of detection approaches are discussed and the most popular of them, named specification-based IDSs, is assessed through a compilation of 24 specification rules and five types of attacks to IEC–61850 network protocols — we do not consider physical attacks on devices, only through messages. Our evaluation shows that further improvement is necessary for state-of-the-art IDSs, especially to deal with masquerade attacks. Finally, open issues and future research directions for efficiently detecting threats within IEC–61850 digital substations, considering both time and cost requirements, are highlighted.

The remaining of this paper is organized as follows. In Section 1, we present a brief overview of the IEC–61850 standard. In Section 2, we discuss the security and threats in digital substations. In Section 3, we present an in-depth analysis of the existing state-of-the-art IDSs proposals. In Section 4, we perform a study involving current IDSs based on specification rules. Then, in Section 5, we address open issues and future directions. Finally, Section 6 presents the conclusions and ideas for future work.

1. Overview of the IEC–61850 standard

Legacy substation automation protocols defined communication conventions between hard-wired electrical devices and monitoring/control components [2]. In contrast, the IEC–61850 standard [9] was defined with the following goals: (i) interoperability; (ii) long term stability; and (iii) simplified configuration. Besides the structure of transmitted data and interoperability aspects, the IEC–61850 standard specifies the physical topology (*e.g.*, ring topology, redundant LANs), network protocols, and object modeling [9,10].

1.1. Physical topology

A typical substation infrastructure is composed of three levels: *station, bay*, and *process* (or *field*). Two communication channels are used in these levels, allowing both horizontal (*i.e.*, between devices of the same level) and vertical (*i.e.*, between devices of different levels) communication [11–13].

The *station level* provides the interface for humans managing the substation, and includes monitoring systems, engineering workstations, SCADA systems, and the *Remote Terminal Unit* (RTU). The RTU includes remote access, opening an entry point for remote attackers. Thus, it is imperative to employ security mechanisms to deal with potential threats [11].

The *bay level* consists of an intermediate level where automatic functions with real-time requirements are performed without the need for human intervention. It includes IEDs for control and metering, protection, and time synchronization [14]. These devices are connected to both the *substation* and *process busses* that link, respectively, the station and bay levels and the bay and field levels, enabling station level devices to perform operations, such as reading and writing from bay level IEDs [11].

The lowest level, the *process level*, includes both conventional and non-conventional switchyard equipment[1] from the electrical domain. Because conventional equipment supports only dedicated wired data, additional elements may be employed to act as an interface between the cyber and physical domains, such as *Merging Units* (MU) and *Intelligent Terminals* (ITs).

In particular, MUs play a significant role in digital substations. They provide synchronized phase, voltage, and current measurements collected from primary conventional equipment. These devices use the process bus to communicate, thus increasing the data availability and reducing wiring, as Ethernet replaces hard-wired connections. Note that this level carries extremely sensitive and time-critical applications [15] and thus cybersecurity is one of the most crucial challenges, especially considering the limited processing power of MUs that turn simple security measures, such as data encryption, impracticable [13]. Future power grid systems are expected to have non-conventional equipment (*e.g.*, modern switchgear) capable of supporting communication protocols without depending on intermediate sensors and actuators [9]. A typical infrastructure topology involving both conventional and non-conventional devices is illustrated in Fig. 1.

1.2. Network communication protocols

In addition to traditional protocols, such as FTP (File Transfer Protocol) and HTTP (Hypertext Transfer Protocol), the IEC–61850 standard introduces two new protocols, namely (a) GOOSE (Generic Object Oriented Substation Events) for inter-IED communication and (b) SV (Sampled Values) for the communication between MUs and IEDs. IEC–61850 also specifies mappings of abstract objects and services in substations to MMS (Manufacturing Message Specification) , formally categorized by the ISO (International Standards Organization) as a part of ISO 9506 [16].

1.2.1. SV

SV [15] enables digitized current and voltage samples to be transferred to IEDs using Ethernet. Such measurements are collected through analog signals from electrical equipment and converted to digital signals by MUs. Once converted, SV messages are transmitted to subscriber devices (*i.e.*, control and/or protection IEDs). In particular, protection IEDs consume these messages to detect faults based on their protection schemes [4]. SV messages are sent at a high transmission rate both for protection (80 samples per cycle[2]) and measurement (256 samples per cycle [4,17]). The number of samples per cycle also reflects on the number of *Application Service Data Units* (ASDUs) generated for each SV message. While eight ASDUs are sent for measurement purposes, only one ASDU is needed for protection messages [18].

In Fig. 2, the Ethernet frame structure and the internal structure of the Application Protocol Data Unit (APDU) of an SV message are illustrated. Each transmitted message may contain multiple ASDUs within the `Sequence of ASDU` field — each with the same structure illustrated in ASDU 1. Current and voltage measures are embedded into the `Sequence of Data` ASDU field. Each ASDU carries four current and four voltage measurements, corresponding to the four electrical phases (A, B, C, and Neutral). These values are illustrated as I_a, I_b, I_c, I_n and V_a, V_b, V_c, V_n, respectively, in Fig. 2, and are potential targets for attackers (*i.e.*, for fake electrical measurement injection).

1.2.2. GOOSE

GOOSE was introduced to enable the exchange of substation events, status change notifications, alarms, and control commands. Events of different components are exchanged by GOOSE messages, including temperature alarms, circuit breaker status, switch breaker interlocking. These data are put into a *GOOSE dataset* and transmitted in a publish/subscribe fashion to subscriber IEDs. Thus, IEDs can communicate with each other over multicast groups, where a publisher device transmits one message that is delivered to a group of subscriber IEDs. Each IED may subscribe to specific topics related to its domain, such as control, protection, or measurement.

In stable situations in which no events occur (*i.e.,* no changes are detected in the GOOSE dataset values), GOOSE messages are transmitted periodically at fixed $T0$ intervals. For each transmission, a sequence

[1] Switchyard refers to an enclosed area of a power system containing the switching equipment used in the transmission of electricity.

[2] A cycle is 16.6 ms for substations operating at 60 Hz or 20 ms for substations operating at 50 Hz.

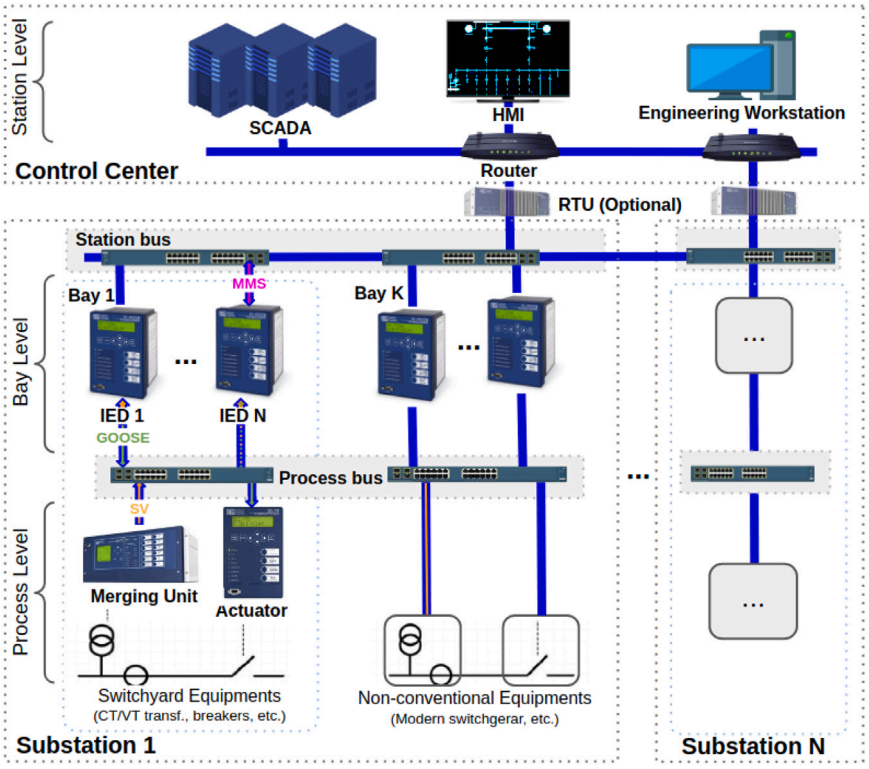


Fig. 1. IEC–61850 typical architecture.

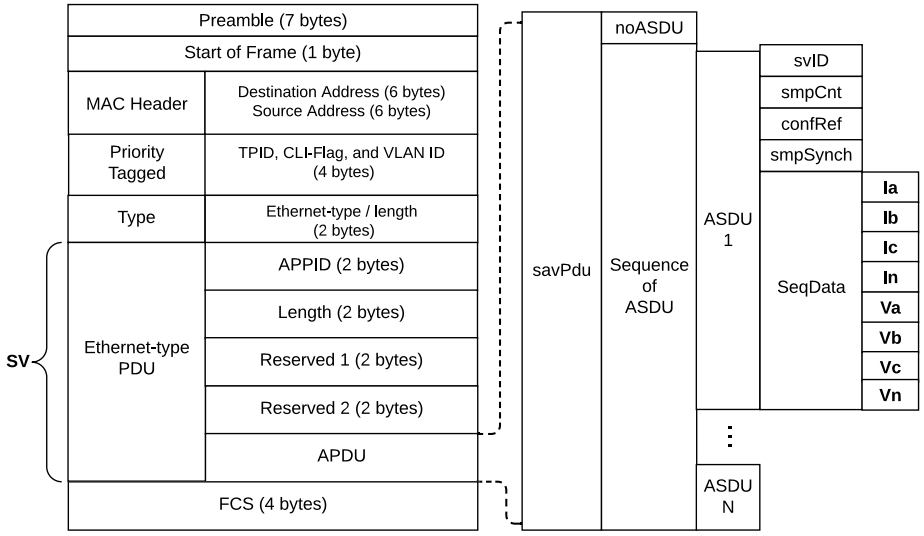


Fig. 2. Ethernet frames of SV messages.

number (SqNum) is increased. Once an event occurs, the SqNum field is set to zero, the status number (StNum) is increased, and a new GOOSE message is sent immediately. This message is retransmitted at increasingly larger intervals, starting with a short transmission interval ($T1$) and increasing at every retransmission ($T2$, $T3$, etc.), until reaching the original interval ($T0$), as illustrated in Fig. 3. Although this increasing function is not standardized, exponential backoffs are typically adopted.

Due to these standardized behaviors, different features may be analyzed by an IDS to distinguish legitimate and malicious activities. GOOSE packets carry a timestamp, which may help reveal a DoS attack since in normal conditions the interval between two received messages should not exceed $T0$. SqNum and StNum are potential indicators of fake message injection or message replay attacks. Accordingly, since changes in the equipment state informed at GOOSE's DatSet field should result in resetting SqNum and increasing StNum, these fields

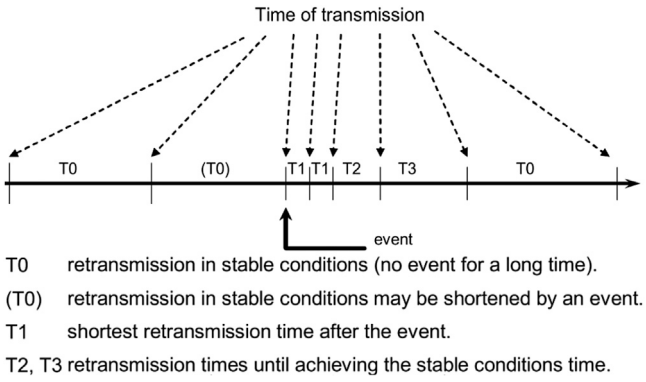


Fig. 3. GOOSE messages transmission.
Source: Extracted from [19].

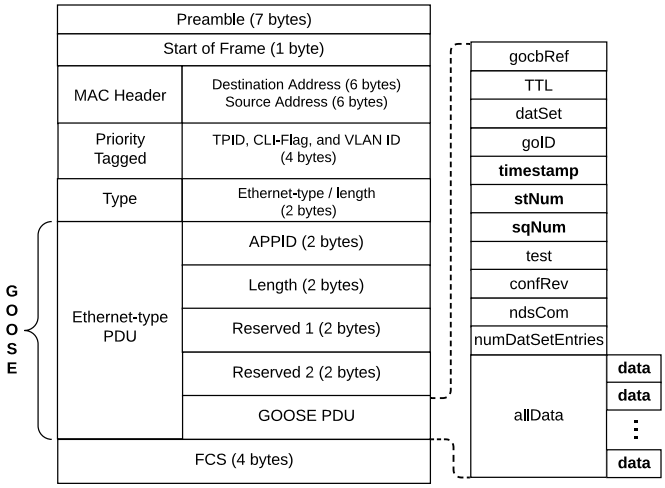


Fig. 4. Ethernet frame of GOOSE messages.

may be correlated to reveal undesired changes [20–22]. Fig. 4 shows a GOOSE message encapsulated into an Ethernet frame.

1.2.3. MMS

MMS enables the communication between the station level (*e.g.*, SCADA system) and IEDs over Ethernet. According to the IEC–61850-8-1 standard, each physical device (*e.g.,* IED) consists of logical devices, logical nodes, data objects, and data attributes. Access to each object is mapped to MMS services. This protocol executes on top of TCP/IP or OSI model, depending on the used profile. Hence, IEDs (MMS servers) may be accessed by their IP addresses, thus supporting read, write, and reporting operations by remote clients — either SCADA or any other device [19]. For example, the circuit breaker state may be requested through the MMS protocol to the physical device (*i.e.,* IED).

The MMS protocol stack is divided into Application Profile (A-Profile) and Transport Profiles (T-Profiles) [19]. As shown in Tables 1 and 2, they represent the protocols and agreements related to the upper 3 (A-profile) and lower 4 (T-Profiles) layers of the OSI Reference Model [23].

Note that MMS does not have any built-in security. However, since MMS is more complex than GOOSE and SV, the former can support more security mechanisms. For example, peer-entity authentication is possible at the setup of a connection between client and server [24]. Given its extra layers and functionality, MMS creates a larger attack surface (*e.g.*, due to the possibility of remote clients sending requests to the server). Note that, in contrast, it can support better security support as it may allow optional secure protocols in its protocol stack. More details are presented in Section 2.3.

Table 1
MMS A-Profile stack.
Source: Adapted from [19].

	A-Profile
Application	MMS ACSE
Presentation	Connection oriented presentation Abstract syntax
Session	Connection oriented session

Table 2
MMS T-Profiles stack.
Source: Adapted from [19].

	TCP/IP T-Profile	OSI T-Profile
Transport	ISO transport ICMP TCP	COTP
Network	IP ARP	Connectionless network ES/IS
Data link	Ethernet standard [25] CSMA/CD	Logical link control CSMA/CD
Physical (Option 1)	10Base-T/100Base-T ISDN interface	
Physical (Option 2)	Fiber optic 100Base-FX Fiber optic basic connector	

1.2.4. Legacy substation protocols

Substation automation systems use a variety of specialized standards, technologies and protocols. Besides those proposed by the IEC–61850 standard, some frequently-used protocols include the IEC–60870-based, MODBUS, and DNP3 (Distributed Network Protocol) [26]. In particular, the IEC–60870 specifications cover the electric utility communication between master stations and remote units (*e.g.,* the interfaces between RTU and IEDs). DNP3 is used for interconnecting automation systems, typically connecting IEDs to SCADA. The MODBUS protocol is used in automation systems and supports multiple networking technologies, including optical or radio networks, serial communication, and TCP/IP. However, MODBUS has some disadvantages including the lack of timestamps for the sequence of events and the lack of polled reports. One of the goals of the IEC–61850 protocols is overcome those limitations [26].

Finally, even though this survey focuses on IDS implementations for protocols specified by the IEC–61850 standards (*i.e.*, GOOSE, SV, and MMS) [3,4,12,21,27–31], additional protocols may also be found in substation networks, such as PTP (Precision Time Protocol) and LLDP (Link Layer Discovery Protocol), which provide time synchronization for IEDs and enable network devices to be discovered, respectively [32].

2. Security and threats

The easier communication with IEDs achieved with the IEC–61850 standard also enables the manipulation of electrical equipment (*e.g.*, circuit breakers), making substations more vulnerable to a number of cyber threats [4,22]. There are many potential cyber vulnerabilities within the networks and devices of digital substations that can degrade confidentiality, availability, and data integrity [14]. However, cyber-security features are included in IEC–61850 [33].

Therefore, understanding these potential vulnerabilities is crucial for designing suitable security countermeasures and intrusion detection mechanisms to protect the substation. Once an attacker gains access to the substation networks, the physical protection of the substation is no longer sufficient for protecting the infrastructure from potential harm, thus allowing attackers to cause catastrophic damage [33]. This section covers IEC–61850 specific threats and traditional threats that may affect digital substations. Furthermore, the IEC–62351 standard for securing substation devices is analyzed.

2.1. Attacks to IEC-61850 multicast protocols

Since the IEC–61850 multicast protocols (GOOSE and SV) are assumed to run within the substations' local network isolated from the Internet, attackers need to gain access to an intranet interface to capture, spoof, modify or retransmit malicious messages. Attackers may gain physical access to protective IEDs or explore alternatives, such as placing malware in device software (*i.e.*, through update patches) or infecting other devices connected to the network (*e.g.*, technician's computers). Regardless of the method, from this point on we assume the attacker has the ability to analyze, spoof, inject, and transmit malicious frames containing IEC–61850 multicast messages [21].

According to Hong et al. [21], there are 9 main potential ways for an attacker to exploit vulnerabilities to cause damage and disrupt the power system components: (i) compromising the user-interface; (ii) interrupting the time synchronization process; (iii) compromising the station level communication bus; (iv) gaining access to bay level devices; (v) changing protective device settings; (vi) capturing and modifying GOOSE messages; (vii) compromising the process level communication bus; (viii) placing forged values in SV messages; and (ix) compromising the firewall to gain access to the substation network. From these entry points, attackers may perform different attack variations, such as message relay, injection, and poisoning to cause DoS. These attacks are summarized in Table 3, and detailed below.

2.1.1. Replay attack

This attack model is based on the resending of a previously sent message. Basically, the attacker captures and replays the message without modifying its content. Such retransmission may occur immediately after the message is captured or after a longer delay. Checking timestamp and sequence numbers is useful for detecting this malicious behavior [21]. In the IEC–61850 architecture presented in Fig. 1, a replay attack could be launched by an attacker connected to either the process or station bus.

Existing tools may be used to perform this kind of attack. The TCPreplay Suite [34] can read a variety of packet capture (pcap) files and use them as input to perform message replays. Additionally, in our previous work [35], we developed a GOOSE traffic generator that was used for capturing and injecting malicious GOOSE messages to the network. We show that an attacker can explore these functions to harm a targeted system. Replay attacks may be especially harmful if the attacker chooses the proper opportunity to mislead the system during a critical operation. Suppose a scenario where a message containing a "circuit breaker close" command is captured by an attacker. If this message is retransmitted (replayed) during an electrical fault or line maintenance, the circuit breaker may be improperly re-closed, causing severe damage.

2.1.2. Message injection

Message injection attacks build and transmit false and potentially malicious messages into the network. In Fig. 1, this attack could be launched by an attacker connected to the process bus. In the simplest form of message injection, a message is randomly created without observing its consistency with the rules of the IEC–61850 standard (*i.e.*, it may contain invalid field values). Clearly, a syntax-based IDS which works by simply checking message syntax can detect these fake-injected messages. Also, the combination of multiple syntax rules to generate more complex rules is a potential way to increase the accuracy in the detection of message injection attacks.

The second way is to create new messages or modify captured messages that do not violate basic syntax rules. Note that in contrast to reply attacks, injection/modification attacks are assumed to send a fabricated or modified message instead of simply retransmit a past message. A method for exploiting the GOOSE protocol semantic to launch fake data injection attacks is presented in [20], where legitimate messages are captured and their source and destination MAC (Media Access Control) addresses are spoofed by using legitimate addresses used to impersonate benign devices. Additionally, the payload data of the messages (*i.e.*, a boolean parameter) are adulterated to cause malicious actions in the target. Attackers have to send fake messages in the gap between two legitimate messages to avoid their behavior being detected by a context-oriented IDS which checks the consistency between messages.

2.1.3. Masquerade attack

This attack model is a specialization of the injection attack, with a particular improvement: after old messages are captured, they are adulterated to mimic a legitimate behavior. Therefore, masquerade attacks have an additional step between the capture and transmission phases to get fresh (and valid) values for `SqNum` and `StNum`. Attackers learn from observing past messages' content to mimic their behavior. This particular improvement based on the analysis of the previous messages makes it difficult to distinguish fake messages from legitimate ones [22].

Accordingly, both syntax-based (*i.e.,* that considers individual messages' syntax) and anomaly-based IDSs (*i.e.,* that considers the traffic behavior) are expected to fail to detect it. Instead, an IDS based on more sophisticated techniques, such as machine learning, analyzing multiple sources of information from various protocols may be promising for such a challenging scenario. In Fig. 1, this attack could be launched by an attacker connected either to the process or station buses.

Table 3
Summary of threats on IEC–61850 digital substation networks.

Target protocol	Attack class	Description	Countermeasure
GOOSE and SV	Replay [21,36]	Old messages are re-transmitted.	Attributes consistency checking.
GOOSE	Naive injection [20]	Fabricated messages are transmitted (*e.g.*, commands).	IEC–61850 standard consistency checking.
SV	Naive injection [20]	Fabricated messages are transmitted (*e.g.*, measures).	IEC–61850 standard consistency checking.
GOOSE	IEC–61850 injection[20]	IEC–61850 compliant commands are transmitted.	Context attributes consistency checking.
SV	IEC–61850 injection[20]	IEC–61850 compliant messages with fake measures.	Multiple sources measurements correlating.
GOOSE	Masquerade [22]	Messages that mimic real behavior are transmitted.	Attributes consistency and correlation checking.
GOOSE	Poisoning [37]	The *StNum* is excessively increased.	Attributes consistency checking.
GOOSE and SV	Modification [36]	Specific attributes are adulterated.	Attributes consistency checking.
GOOSE and SV	Flooding [36,37]	Many messages are transmitted at high frequency.	Message statistics checking.

A particular implementation of masquerade attack [22] changes three specific GOOSE message fields. The main field used to cause damage is the `state` field. This field describes the state of the circuit breaker as open (*e.g.*, under a fault) or closed (*e.g.*, under normal conditions). By changing this value, an attacker may cause the undesired operation of a circuit breaker. The attacker may also change additional fields, such as `StNum` and `SqNum`, to make the detection of this malicious action more difficult. Finally, the frequency in which false messages are transmitted is gradually changed to mimic the typical (and legitimate) bursty message transmission behavior observed in state changes. As a consequence, attackers can perform malicious operations such as opening a circuit breaker when it should be closed. This is worse still if an attacker closes a circuit breaker improperly (*e.g.*, during line maintenance), where human life may be in danger.

2.1.4. Poisoning attack

The main goal of poisoning attacks [37] is to harm the communication between publisher and subscriber devices by preventing the subscriber from processing subsequent legitimate GOOSE messages or forcing subscribers to process fabricated GOOSE messages. The consequences of this attack include both DoS and improper operation of the devices.Three poisoning attack variations are proposed in [37], as described below. In Fig. 1, all variations of this attack targeting GOOSE messages could be launched by an attacker connected to either the process or station buses.

- *High Status Number Attack* consists of capturing a GOOSE message and sending a new spoofed with a higher `StNum` than that of the legitimate messages. The subscriber devices discard any subsequent legitimate GOOSE messages with a lower `StNum` than the poisoned number.
- *Flooding Attack* sending multiple fake messages on the multicast channel. Each fake message will increase the status number expected at the subscriber devices, appearing legitimate, and increasing the difficulty of detection. Furthermore, the legitimate messages may be delayed due to contention in the network or devices during the flooding. This attack may be better detected by an anomaly-based IDS since it considers the overall behavior instead of analyzing messages in isolation.
- *Semantic Attack* consists of observing the legitimate traffic for learning/predicting the message content and spoofing realistic messages, increasing the status number every new fake message, at a high rate. Thus, legitimate messages are discarded since their `StNum` are lower than the recently received fake messages. Note that the expected effect is similar to High Status Number Attack, however, in semantic attacks the `StNum` is increased by multiple messages instead of only one. Thus, whereas High Status Number Attack may be detected by checking the anomalous `StNum` increasing between two consecutive messages, Semantic attack may be better detected by behavior analysis through an anomaly-based IDS.

2.2. Other inter- and intra-substation threats

In addition to the attacks on the process and station busses, the attacks discussed below could be launched by an attacker connected to the control center network in Fig. 1.

A known issue since 1985 [38] to TCP protocol is the MITM (Man-In-The-Middle) attacks by impersonating a legitimate host (*i.e.,* using its IP address). A defense against this type of attack [39,40] improves the TCP protocol resistance to this vulnerability. However, an attacker that can observe the initial messages for a connection may still be able to launch MITM by impersonating that connection [40].

Therefore, the MMS communication protocol over TCP/IP is also vulnerable. Experiments exploiting MITM attacks [41] demonstrated the feasibility of causing physical effects on the electrical devices via malicious manipulation of IED parameters (*i.e.*, data attribute *MaxWLim*) through injected MMS commands (*i.e*, write requests). Aside from TCP, other protocols in the MMS stack may present vulnerabilities, such as TPKT and COTP [42].

Other auxiliary protocols used in digital substations may suffer from three types of attacks [36,43]:

- Password Crack: may target FTP, telnet, or HTTP;
- DoS attacks: high-rate data generated via PING tool;
- Packet sniffer: targets the ARP (Address Resolution Protocol) protocol.

Part of these attacks may be avoided by blocking such protocols when they are no longer used (*e.g.*, FTP may only be used for commissioning devices), reducing the risk of exploitation. On the other hand, some protocols (*e.g.*, MMS and PTP) may not be blocked, given their vital roles in the proper function of substation devices. In [32], authors describe two approaches to perform delay attacks that desynchronize the clocks of slave nodes and, then, delay the PTP synchronization messages: (i) adding a device to the network (called a delay box) that aims at delaying the synchronization messages; and (ii) retransmitting messages with a modified timestamp. In particular, the first approach requires physical access to the substation to insert such new device, whereas the second one requires compromising — through a malware installation (either by physical or remote access) — a device named grandmaster clock, which is responsible for disseminating the updated timestamp to other devices. Both approaches target the functionality of all the devices in the network, since their proper function relies on precise time synchronization, rather than a particular IED.

2.3. IEC–62351 standard

Except for IEC 61850–90-5, which only focuses on cybersecurity of Routable-GOOSE and SV (R-Goose and R-SV), the IEC–61850 standard does not specify security features to address these cyber-security vulnerabilities [22]. Thus, the IEC–62351 standard was published to specify security measures, such as cryptographic, for IEC–61850 applications.

Regarding the MMS, all TCP T-Profile implementations that claim conformance to IEC–62351-4 [44] shall support TLS (Transport Layer Security) to provide authentication, confidentiality and data integrity.

However, it is important to note that this standard also specifies that such implementations shall permit TLS to be disabled. OSI T-Profiles is outside the scope of this specification.

Because GOOSE and SV have strict timing requirements, IEC–62351 proposes the use of lightweight algorithms. However, IEC–62351 only recommends the adoption of techniques that may provide message integrity and node authentication. Note that TLS uses symmetric cipher after establishing the secure session, which can be performed quickly by secure and dedicated hardware. However, according to IEC–62351-6 [44], for applications using GOOSE and SV and requiring 4 ms response times, multicast configurations and low CPU overhead, encryption is not recommended. Instead, these messages are supposed to be restricted to a logical substation LAN.

IEC–62351 does not have full solutions geared toward mitigating certain attacks, including Masquerade attack [22]. Besides, IEC–62351 is not yet complete: it requires more evaluation to address other security aspects (*e.g.*, key management evaluation) [45].

3. Proposed taxonomy for digital substations intrusion detection systems

The existing IDS implementations are typically adapted to meet the requirements of the target scenario. Accordingly, a novel taxonomy is presented (see Fig. 5). We classify the existing IDSs considering both design and deployment aspects. Digital substations differ from traditional information technology systems in many perspectives, such as detection time requirements, specific hardware implementation and protocols, and other specific characteristics of the IEC-61850 standard. Each of them is addressed in the following subsections.

3.1. Design aspects

We subdivided the design aspects of an IDS into four main parts: architecture, approach, type of analysis (*i.e.*, online or offline), and actions (*i.e.*, detection only or prevention).

In terms of architecture, an IDS may be classified as centralized, distributed, or embedded. The centralized is the most common architecture since it requires only one additional network element. The goal is to capture and analyze data application logs or network packets in a central IDS component. The main problem of a centralized IDS is that it has a single point of failure, as well as a potential bottleneck. As such, it may compromise the services' availability. It may be prohibitive for an IDS to detect and prevent intrusions timely for substation time-critical applications. Despite that, most of the current IEC–61850 IDSs proposals are designed considering a centralized architecture [3,21,27,29–31,43,46,47].

The distributed approach avoids the aforementioned problems. A distributed mechanism [48] was proposed to detect data injection attacks collaboratively in digital substations based on the IEC–61850 standard. Similarly, there are other proposals [4,28] involving a distributed architecture to exchange information among IDSs regarding attack attempts. Their main idea is to introduce specification-based IDSs modules inside protective IEDs and Merging Units. Therefore, every GOOSE or SV message is analyzed before being processed. These internal modules communicate with each other to share the detected intrusions.

Embedded IDSs aim at integrating the IDS functionality into substations devices (*i.e.*, IEDs) [4,12,43]. The main drawbacks of this approach are the new hardware design requirements and the internal computational overhead. On the other hand, since intrusions are detected at the target device, this approach may detect and block malicious behavior of compromised devices before the attack has an effect (*e.g.,* malicious messages are discarded instead of processed).

In another categorization, according to Bostani and Sheikhan [49], an IDS can be categorized into three groups based on its detection approach: *signature-based, anomaly-based,* or *specification-based*. The same categorization is also employed in more specific Smart Grid scenarios, such as the AMI (Advanced Metering Infrastructure) [50]. Signature-based methods are characterized by containing a database with samples that represent known attack profiles, while anomaly- and specification-based methods attempt to profile the legitimate or "normal" behavior of network traffic or adjacent systems [49]. In particular, specification-based IDSs model a desirable behavior of a system through its functionalities and security policy [50]. However, unlike anomaly-based methods, specification-based methods are hard to design and generalize for various protocols (*i.e.*, different specification rules would be necessary for GOOSE, SV, MMS, and other protocols in the substation network) [49,50]. Currently, in the context of IEC–61850 digital substations, most IDSs are specification-based ones [3,4,7,12,21,27–29,46], while some IDSs are based on anomalies or are hybrid (*i.e.,* combination between multiple approaches) [31,43,47]. Among the methods categorized in [49], the signature-based approach is still the least explored [30].

To the best of our knowledge, there are no proposals that employ real-time analysis to detect intrusions on IEC–61850 digital substations within a specified time requirement (deadline). On the other hand, there are preliminary studies that address this issue for other Smart Grid domains, and these may be adapted for digital substations in the future. The MOA (Massive Online Analysis) library [51] was used to detect intrusions in devices from different AMI layers: smart meters, data concentrators, and control centers [1]. Recently, on online intrusion detection using MOA to detect traditional attacks were explored [52]. However, from our analysis of the literature, there is a dearth of studies employing such algorithms for detecting intrusions in substation networks.

Finally, IDPSs (Intrusion Detection and Prevention Systems) have the capability of responding to the attack to block the intruder right after the intrusion detection. The capacity for preventing an attack is closely related to real-time detection since the latter enables a quick response. Current IDSs designed for digital substations are typically focused only on detecting, and do not prevent attacks. Some existing efforts include the proposal of IDSs embedded into IEDs [4,12], and traffic blocking in network switches [53]. These may be potential alternatives to mitigate malicious activities before they cause undesirable effects, such as operating improperly an electrical equipment. Currently, there are only a few works proposing IDPSs and this research field needs to be better explored.

Note that real-time IDS and IDPS are not synonymous. While the former refers to the use of real-time processing tools for detecting intrusions, the latter refers to the response/mitigation to a previously detected intrusion.

3.2. Deployment aspects

To deploy an IDS in a digital substation, it is important to define the range of attacks that will be considered and which data sources will be analyzed to detect them. Similarly, the proper evaluation methods and metrics should be considered.

As discussed in Section 2, there are multiple entry points in substation networks where attacks may take place. Therefore, each possible attack should be considered and different data may be required to address each of them. Detecting traditional attacks that may target the station level, such as control centers, requires analyzing different data sources (*i.e.*, FTP unauthorized access logs, TCP and UDP traffic statistics) from those used for detecting attacks to the process level, such as fake measurement injection.

Besides the different devices, network segments, and protocols involved in the execution of each attack, particular features may be relevant to represent specific attackers' behavior. These features may include parameters from both network and application layers, ranging from specific field values (*e.g.,* `StNum`, `SqNum`, source IP address) to

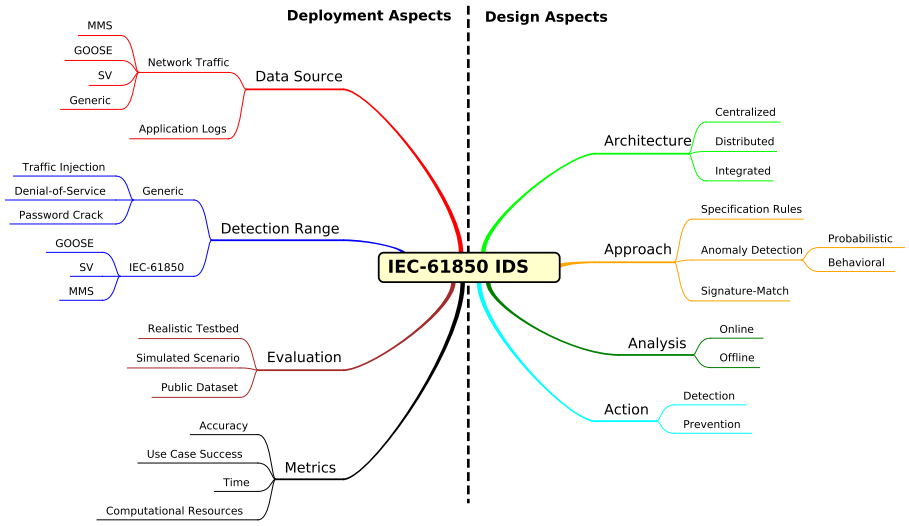


Fig. 5. Proposed taxonomy for intrusion detection aspects on IEC–61850 digital substations.

counters (*e.g.*, the number of transmitted bytes, the number of active connections, rate of packets per second).

Suppose that an IDS is deployed to detect GOOSE Poisoning, GOOSE Injection, and SV Flooding attacks. The key features for this IDS to analyze should include:

- `StNum`: it is typically excessively increased in GOOSE Poisoning attacks;
- `SqNum`: combined with *StNum*, this field may reveal modification of important parameters from the GOOSE dataset, such as circuit breaker state;
- `Timestamp`: this field allows computing the message transmission frequency, used to detect SV Flooding, where many messages are transmitted in a short time.

In fact, it is hard to predict manually all features related to each attack type. This procedure would require complete expert domain knowledge. This is a major issue of specification-based IDSs. Signature-based IDSs may support this process by automatic feature selection methods [54]. These methods may include filters, wrappers, and embedded algorithms. While filtering algorithms rely mainly on statistical methods to evaluate individual features, wrapper algorithms employ machine learning for evaluating different feature sets and identify which feature increases their accuracy. Typically, wrapping is slower but more accurate than filtering [55].

Once defined the attack detection range and data sources, proper evaluation strategies must be chosen to assess the IDSs. There are three main methods for evaluating an IDS. The first one is through realistic testbeds, where physical equipment is used to generate data. The second one consists of generating a synthetic dataset by capturing real or simulated data from the substation network and injecting attack samples. The third way is adopting existing labeled dataset containing normal and attack samples.

There are well-known datasets containing generic traffic which can be used for evaluating IDSs targeting traditional network protocols [47]. Unfortunately, to the best of our knowledge, there are no IEC–61850-based public datasets available, probably because of the proprietary or sensitive nature of the data. Therefore, acquiring real (or even realistic) traffic represents a big challenge.

In particular, Yoo and Shon [31] reported experiments based on a real digital substation, where GOOSE and MMS traffic is used to evaluate a specification-based IDS. However, most IDS proposals in the literature are evaluated in small test-beds and/or using simulation tools, as shown in Table 4.

Table 4
Summary of IDSs evaluation techniques.

Ref.	Year	Approach	Data source	Evaluation
[43]	2010	Anomaly	Generic	Testbed
[21]	2014	Specification	GOOSE and SV	Testbed
[28]	2014	Specification	GOOSE and SV	Testbed
[46]	2015	Specification	GOOSE and MMS	Testbed
[31]	2015	Anomaly	GOOSE and MMS	Real Subs.
[3]	2016	Specification	GOOSE, SV, and MMS.	Testbed
[30]	2016	Signatures	MMS	Testbed
[29]	2017	Specification	GOOSE, SV, and MMS.	Testbed
[27]	2018	Specification	GOOSE and SV	Prototype
[47]	2019	Anomaly	Generic	Dataset
[4]	2019	Specification	GOOSE and SV	Simulation

In terms of simulation tools, there is a specific hardware and simulation software named Real-Time Digital Simulator (RTDS). Although it has already been used for evaluating IDSs [4], it is a professional tool and typically too expensive for wide use in academic research.

Finally, it is necessary to choose the proper metrics to assess the IDS in light of the expected goals and requirements. From the basic indicators True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), different metrics can be derived. Important metrics include *Accuracy* (*i.e.*, the fraction of correct IDS classifications with respect to the total number of samples analyzed), *Recall* (*i.e.*, how many attacks are detected of the universe of attack samples), and *Precision* (*i.e.*, how many attack classifications are in fact attacks instead of false positives [56]). Formally, these metrics are defined as follows:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$Precision = \frac{TP}{TP + FP} \tag{3}$$

Also, considering use case success may be a simpler way to assess the specification rule IDSs. These metrics should be considered together with response-time and throughput metrics to ensure that attacks are detected timely.

4. Specification rules efficiency

Since the majority of the literature on detecting attacks on GOOSE and SV proposes specification rules, in this section, we present a

compilation and analysis of such rules employed by the state-of-the-art specification-based IDSs.

Both the attack models and the specifications rules are detailed in the following subsections.

4.1. Attack models

The attackers' behaviors are modeled after four different attacks presented in Section 2.1, namely *Replay*, *Injection*, *Masquerade*, and *DoS* attacks.

In particular, for injection attacks, two levels of attackers' expertise are considered. Whereas *Naive Injection* refers to a simple injection without observing the field format restrictions imposed by IEC–61850, *IEC–61850 Injection* assumes that the attacker has sufficient domain knowledge to abide by the standard, thus avoiding simple rule violations.

Replay and *Masquerade* attacks assume that the attacker already has access to listen, capture, and retransmit past messages into the network. As discussed in Section 2.1, we expect specification-based IDSs to have more difficulty in detecting Masquerade attacks, due to the careful analysis of the traffic standard carried out by the attacker before sending the masquerade messages.

DoS attacks are assumed to not violate the expected syntax of individual messages, but to violate behavioral rules (*e.g.,* increasing load through message flooding).

Note that each attack is assumed to be performed individually, separately from each other. Thus, one attack does not affect the detection performance for other attack models.

4.2. Specifications rules

Through a systematic review of the literature, we have compiled the following list of specification rules:

(#*R*1) GOOSE messages must have MAC address starting with *01-0c-cd-01* [3,4,21,28,29];
(#*R*2) GOOSE messages must have the `TPID` field with value *0x8100* [3,29];
(#*R*3) GOOSE messages must have the `ethertype` field equal to *0x88B8* [3,29];
(#*R*4) GOOSE messages must have `TimeAllowedToLive` equal to double of the value of `MaxTime` (*e.g.,* 5000 ms) [3,29];
(#*R*5) GOOSE messages must have the `APPID` field formatted as a 4-byte hexadecimal (*e.g,* 0000-3FFF) [3,29];
(#*R*6) Consecutive GOOSE messages must have consistent values for fields `gocbRef`, `timeAllowedToLive`, `datSet`, `goID`, `t`, `StNum`, `SqNum`, `test`, `confRev`, `ndsCom` and `numDatSetEntries` [4,21,28,29];
(#*R*7) GOOSE messages must have the `APPID` field matching the last two octets of the destination multicast address [29];
(#*R*8) The IED control block name must be consistent with the value of the `goID` field (*i.e.*, the LD/LN value in the `goCoRef` field must match the `datSet` field from the GOOSE APDU) [29];
(#*R*9) The size of frames containing GOOSE messages should be equal to 8 $bytes + APDU\ size$, and $APDU\ size$ should be less than 1492 bytes [3,29];
(#*R*10) The `SqNum` in GOOSE messages should be set to zero whenever the value of the `StNum` changes (w.r.t the previous message) [4,21,28,29];
(#*R*11) The number of messages captured in an interval must not exceed a predefined threshold (20% above the expected maximum) [4,21,28,46];
(#*R*12) The number of messages captured in an interval must not be equal to zero [4,21,28,46];
(#*R*13) The transmitter's timestamp should not be higher than the receiver's timestamp [4,21,28];
(#*R*14) The transmitter's timestamp from GOOSE messages should not be more than 4 ms apart from the receiver's timestamp [4,21,28];
(#*R*15) The *Recency* metric, represented by the last GOOSE message's arrival, must respect a minimum and a maximum threshold [46];
(#*R*16) The *Frequency* metric, represented by the average number of received GOOSE messages, must respect a minimum and a maximum predefined threshold [46];
(#*R*17) The *Monetary* metric, represented by the total number of received GOOSE messages, must be within a predefined threshold [46]. The difference from rule (#*R*11) is that this rule considers only received GOOSE messages;
(#*R*18) Only messages with specific source *port*, *IP* and *MAC* addresses are allowed [3,29];
(#*R*19) Only MMS, COTP, TPKT, and SNTP protocols are allowed on the station level network and only the GOOSE, SV, and IEEE 1588 protocols are allowed on the process level network [3,29];
(#*R*20) There must be consistency between the *GOOSE switch-in* messages (*e.g.*, breaker opening) and the value of the report sent by the MMS protocol (*i.e.*, MMS signal report) [3,29];
(#*R*21) The number of bytes that travel per second must not exceed a predefined threshold [29,46];
(#*R*22) The number of packets that travel per second must not exceed a predefined threshold [29,46];
(#*R*23) The length of the packet (specified in the packet header) must not exceed a predefined threshold [29];
(#*R*24) The total size of the packet must not exceed a predefined threshold [29].

If one or more specification rules are not satisfied, it is assumed that an anomaly has occurred. This anomaly may be either misbehavior (*e.g.*, as a consequence of high load or the improper function of some software or device) or an intentional violation caused by the malicious action of an attacker. For this analysis, we focus on the latter.

As discussed before, we found 24 specification rules in the literature [3,4,7,12,21,27–29,46]. Each rule is assessed by its ability to detect five different attacks. Specifically, we classified each rule's detection capabilities into four levels:

- `Detect`: the rule always detects all possible variations of the attack.
- `HProb`: there is a high probability that the rule detects most variations of the attack with .
- `Part`: the rule is partially successful, that it, it detects some of the attack variations, or under certain parameters (*e.g.*, a specific field should have a value in a known range). However, there are cases in which the same kind of attack is not detected.
- `Fail`: the rule always fails to detect the attack.

When deployed in digital substations, specification-based IDSs are typically configured based on specialized domain knowledge. Most of the specifications rules are defined by considering the consistency between message field values and the specifications established by the IEC—61850 standard.

Our first conclusion is that most of these rules are not able to detect *Replay attacks* since the values of malicious messages are the same as the legitimate ones. However, as shown in the second column of Table 5, rules #*R*6 and #*R*10 detect Replay attacks because these rules consider the consistency between multiple consecutive messages instead of considering only the parameters from a single message. In particular, the attributes `StNum` and `SqNum` allow them to detect messages out of context. Rule #*R*14 detects replay attacks only if there is a delay of at least 4 ms between the retransmitted and the

Table 5
Specification rules assessment results.

Rules	Attacks				
	Replay	Naive injection	IEC-61850 injection	Masquerade	DoS
#R1	Fail	HProb	Fail	Fail	Fail
#R2	Fail	HProb	Fail	Fail	Fail
#R3	Fail	HProb	Fail	Fail	Fail
#R4	Fail	HProb	HProb	Fail	Fail
#R5	Fail	HProb	Fail	Fail	Fail
#R6	Detect	HProb	HProb	Fail	Fail
#R7	Fail	HProb	Fail	Fail	Fail
#R8	Fail	HProb	HProb	Fail	Fail
#R9	Fail	HProb	Fail	Fail	Fail
#R10	Detect	HProb	Part	Fail	Fail
#R11	Fail	Fail	Fail	Fail	Detect
#R12	Fail	Fail	Fail	Fail	Part
#R13	Fail	Part	Part	Fail	Part
#R14	Part	HProb	HProb	Fail	Fail
#R15	Part	Fail	Part	Fail	Detect
#R16	Fail	Fail	Fail	Fail	Detect
#R17	Fail	Fail	Fail	Fail	Detect
#R18	Fail	HProb	Part	Fail	Fail
#R19	Part	Part	Part	Fail	Fail
#R20	Fail	Fail	Fail	Fail	Fail
#R21	Fail	Fail	Fail	Fail	Detect
#R22	Fail	Fail	Fail	Fail	Detect
#R23	Fail	Part	Fail	Fail	Part
#R24	Fail	Part	Fail	Fail	Part
[3]	Part	HProb	HProb	Fail	Fail
[4]	Detect	HProb	HProb	Fail	Detect
[21]	Detect	HProb	HProb	Fail	Detect
[28]	Detect	HProb	HProb	Fail	Detect
[29]	Detect	HProb	HProb	Fail	Detect
[46]	Part	Fail	Part	Fail	Detect
All	Detect	HProb	HProb	Fail	Detect

legitimate message, which might not always be the case. Similarly, rule #*R*15 may detect replay attacks exceeding a minimum or a maximum predefined time interval since the last received message. Also, #*R*19 only works if an IEC–61850 message is transmitted in an unauthorized communication bus (*e.g.*, MMS in the process bus [3,29]).

Regarding *Naive Injection* attacks, Table 5 shows that rules #*R*1 to #*R*10 may, individually, detect IEC–61850 standard violations on particular message fields. Whereas each stand-alone rule (*e.g.,* #*R*6) is limited to detect *Naive Injection* attacks only when specific fields are violated, we assume that this attack model has a high probability of containing multiple inconsistent fields — as it is not aware of the IEC-61850 standard. For example, $StNum$ may have 4,294,967,295 possible values[19], thus a naive injection attacker has a very small chance to correctly guess the proper value. Similarly, rules #*R*14 and #*R*18 are likely to detect these attacks based on the message context, but they fail if the SqNum of the fake message is eventually set to zero or if the transmitter's timestamp is within the 4 ms from the receiver's timestamp. There are other rules (*i.e.*, #*R*13, #*R*14, #*R*19, #*R*23, and #*R*24) with limited potential to detect this attack since they are based on parameters that may eventually be inconsistent with their specifications. Our conclusion is that even stand-alone rules have a high probability of detecting Naive Injection attacks. Besides, they can be still more easily detected when considering the combination of multiple specification rules (see bottom of Table 5).

IEC–61850 Injection attacks assume attackers have the knowledge to send syntactically correct fake messages that match the IEC–61850 standard (but not necessarily behavioral consistent); in this case, only 4 rules have a high probability of detecting such attacks. Both domain-based (*e.g.,* #*R*4 and #*R*8) and context-based (*e.g.,* #*R*6 and #*R*14) rules consider fields not known by attackers without access to the network traffic pattern and to the substation parameters. In particular, to bypass #*R*14, an attacker would need temporal synchronism with the target devices. Thus, these fields are not expected to be properly forged by this attack model.

Rule #*R*10 detects a single syntactically correct message if the attacker does not set the SqNum field to zero after a malicious StNum change. Moreover, rule #*R*18 detects some *IEC–61850 Injection* attacks if the used port, IP, and MAC addresses refer to an unauthorized device. The efficacy of rules #*R*13 and #*R*15 is limited to cases in which the fake message has an invalid timestamp or is transmitted in an excessively short interval, respectively.

It is worth noting that rule #*R*13 is able to detect in part both *Naive* and *IEC–61850 injection* attacks, *i.e.*, only when the fake timestamp is higher than the local time at the receiver. Both *replay* and *masquerade* attacks are not detectable by this rule because *replay* attacks do not change the timestamp (*i.e.*, it will not be higher than the local time at the receiver unless clocks are nor synchronized) and *masquerade* attacks have sufficient knowledge to insert a valid timestamp. Most DoS variations are not detectable by rule #*R*13 since they focus on resource overload. However, DoS attacks that operate by leading the system to an invalid status such as poisoning attacks are detected. In this case, this rule may be useful to detect messages with an incorrect timestamp.

The *masquerade* attack manages to circumvent all specification rules included in state-of-the-art solutions that have both syntax and behavioral consistency. The attacker profile indicates an advanced knowledge about the operation of the substation – potentially obtained through a historical analysis of the messages transmitted in the network. Therefore, it is important to note that further improvements to deal with this particular attack are necessary.

Rules *#R11*, *#R12* and *#R16* are suitable to detect *flooding* or other generic DoS attacks because they consider message counters capable of detecting anomalous behavior. In particular, *#R12* works only in an advanced stage of DoS, where no legitimate messages are being delivered. Similarly, rules *#R15*, *#R17*, *#R21*, and *#R22* allow the detection of anomalies in transmission time such as those caused by DoS attacks. Therefore, even though these rules may detect intrusion attempts, they are not effective in distinguishing malicious and legitimate messages. Finally, rules #*R*13, #*R*23, and #*R*24 are limited to detect DoS based on single malformed messages.

A complete and more accurate detection can be achieved by the composition of rules. This may enable IDSs to detect and distinguish the different attack variations as well as to measure the attackers' expertise. Also, the combination of rules may reveal possible correlations between events. For instance, #*R*18 may reveal a malicious IP connected to the network, while #*R*19 detects a malicious attempt to generate unauthorized traffic, and #*R*12 reports a compromised state causing the system to be unavailable. However, despite the potential of complex rules to detect more attacks, the combination of current state-of-art rules is still unable to detect all attacks.

Existing specification-based IDSs employ different combinations of the aforementioned rules. In [3] and [46], only a part of replay attacks are detected even after combining multiple rules. Also, they fail to detect *masquerade* attacks. Rules used in [3] present a high probability to detect Naive and IED–61850 injection, but fail to detect DoS. On the other hand, the rules used in [46] enable DoS detection but fail to detect Naive Injection and detect only part of IEC–61850 injection attacks. The combinations of rules presented in [4,21,28,29] provide a similar capability to detect all attacks: they detect replay and DoS attacks, and present a high probability of detecting Naive and IEC–61850 injection attacks. Finally, the last row of Table 5 shows that, even combining all rules, both Naive and IEC–61850 attacks are not always detected, although they provide a high detection probability. *Masquerade* attacks, on the other hand, still cannot be detected.

Although the compute of those metrics discussed in Section 3.2 requires numerical indicators (*i.e., TP, TN, FP, and FN*), it is possible to qualitatively estimate the expected level of *recall* to specification-based IDSs in detecting the five attacks analyzed in this section based on Table 5. In summary, *masquerade* attacks would present the lowest *recall* due to their high number of false negatives. Similarly, *replay* attacks may present a low *recall* by IDSs that do not employ rules

#R6 and *#R10*. On the other hand, *Naive Injection* and *DoS* attacks are expected to have a higher recall since there are more rules to detect them.

Since specification rules are designed by modeling specific malicious actions, it is reasonable to expect a high *precision* to all rules (*i.e.,* a low number of false positives) even if have poor recall. Estimating the *accuracy* without the knowledge of the number of samples analyzed would be not appropriate, because it may be affected by imbalanced datasets (*i.e.,* disproportional number of attacks and legitimate samples). However, assuming a balanced dataset and a similar *precision* for each attack, it would be expected that *accuracy* to be proportional to the *recall*.

5. Trends, open issues and future directions

Although in the last years a few studies addressed IDSs in the context of Smart Grid, research on intrusion detection in digital substations is still at an early stage. Thus, several research topics remain open:

- *More general IDSs:* current IEC–61850-based IDSs rely on expert knowledge about the substation components, the standard, and its protocols. In particular, specification-based IDSs have limited attack detection capabilities [4,21,28,29]. As shown in Section 4, many detection rules fail to detect all or part of attacks due to their high specialization: they have low *Recall* (see Eq. (2)) and high number of false negatives;
- *Add Preventive Measures to IDSs:* traditional IDSs are focused on **detecting** malicious behavior. Accordingly, the intrusions attempts are logged or a warning is issued. However, due to the critical role of substation networks, it is important to replace them with IDPSs, which may take proper actions to **prevent** the attack instead of just detecting the intruders' behavior. Clearly, issues of cost, timeliness, performance, and overhead must come into play as well;
- *Big Data Issues:* improving the accuracy from current specification-based IDSs may require combining multiple and heterogeneous data sources (*e.g.*, SCADA-level logs, GOOSE commands, SV measures, MMS reports). On the other hand, the IDSs' processing time should be low enough to detect intrusions timely. Such data volume, variety, and velocity characterize a Big Data challenge [57], even though it is at the electric digital substation scale;
- *Lack of Evaluation Datasets*: as discussed in Section 3.2, the lack of datasets is a major challenge when evaluating novel IDSs proposals. Collaborative industry-academia-government efforts to build a public IEC–61850-based dataset containing attacks and normal traffic would allow the evaluation and comparison of current IDS solutions.

Based on the aforementioned open issues, we point out some potential future directions. These research topics are based on novel approaches that are still not well explored into substation networks and may be useful to address most of the existing issues on detecting and preventing intrusions in IEC–61850 substations.

- *Smart IDS:* an IDS based on more sophisticated techniques, such as machine learning, analyzing multiple sources of information may be promising for dealing with the most challenging scenarios in which anomaly and specification-based IDSs are ineffective (*e.g.*, for detecting masquerade attacks). El Mrabet et al. [58] adopted a deep learning architecture to automatically extract features and make a predictive classification in other Smart Grid environments (*i.e.*, AMI). Applying it to substation networks may also yield good results, but that approach has not been explored;
- *Proactive Blocking:* a promising approach to analyze the network traffic looking for malicious patterns in a timely manner consists of using additional hardware between the devices. This idea was previously introduced by Kim and Park [27]. They proposed an FPGA-based IDS to process IEC–61850 packets and detect intrusions by rule matching. This idea has the potential of blocking malicious traffic before it arrives at the target device;
- *SDN and IDSs*: Researchers have proposed building IDSs based on Software Defined Network (SDN) to enable general proactive flow blocking and forwarding suspicious traffic to IDSs [53]. Since SDN enables the flow forwarding through software applications, an implementation of this approach in digital substation networks may be interesting to handle suspicious traffic and blocking messages when they are detected as malicious;
- *Real-time IDS:* initial efforts of building a real-time IDS for Smart Grids were carried out by M. Faisal et al. [1]. They used the MOA Framework to process streaming data and detect malicious traffic. However, they did not consider substation networks, only addressing AMI communication. Employing similar techniques in IEC–61850 networks may be a promising research direction.
- *Real Datasets:* current researches rely mainly on simulated data, experimental testbeds, and prototype implementations. However, it should be noted that industry would play a key role by providing real data for academic research purposes. Hundreds of real attacks that caused outages in the U.S. and Ukraine were reported in recent years [4]. While this data can be potentially confidential and sensitive, data anonymization techniques can be applied before making it publicly available.

6. Conclusion

The IEC-61850 standard introduced many benefits for substation automation systems, including the interconnection of heterogeneous devices through new protocols and functionalities. On the other hand, the increased connectivity in digital substations has exposed them to a wide range of cybersecurity threats that can lead to catastrophic damage. Therefore, the adoption of IDSs is vital for protecting digital substations. Consequently, it is very important to understand the aspects of IDS for providing adequate intrusion detection measures.

To the best of our knowledge, this is the first work to present an in-depth survey on IDS aspects for digital substations based on the IEC–61850 standard. We covered intrusion detection approaches, data sources, architectures, evaluation methods, and metrics, and compared 12 existing proposals. Moreover, we assessed 24 specification rules for detecting five different attack types. Our evaluation shows that further advancement is necessary for state-of-the-art IDSs to deal with masquerade attacks. Although this attack does not violate the IEC–61850 standard, it is still able to inject fake messages and to cause catastrophic consequences including blackouts, damage to electrical equipment, and even expose human life to risks (*e.g.*, opening a circuit breaker during line maintenance).

Finally, we presented the trends, open issues, and future research directions in this field. More general IDSs can be developed to overcome the limitations of the current rule-based IDSs. They can become smarter by using both more elaborate rules and adopting artificial intelligence techniques. Future IDSs also require preventive actions to stop malicious actions. Indeed, adopting real-time techniques and software-defined networks (SDN) technologies are promising topics for building IDSs capable of responding to attacks in a timely manner. Furthermore, accurate IDSs require updated datasets to evaluate and improve the IDSs' performance. This can be an opportunity for the synergy between industry and academia to result in joint efforts with mutually relevant contributions.

CRediT authorship contribution statement

Silvio E. Quincozes: Conceptualization, Methodology, Writing - original draft, Investigation, Editing. **Célio Albuquerque:** Supervision, Conceptualization, Methodology, Writing - review & editing. **Diego Passos:** Supervision, Conceptualization, Methodology, Writing - review & editing. **Daniel Mossé:** Supervision, Conceptualization, Methodology, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

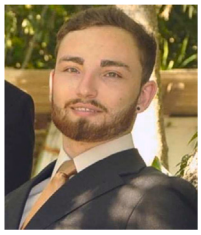
Acknowledgments

This work is supported in part by CAPES, Brazil, CNPq, Brazil, FAPERJ, Brazil, CGI/FAPESP, Brazil, TAESAP, Brazil and P&D ANEEL (PD-07130-0053/2018), Brazil.

References

[1] M.A. Faisal, Z. Aung, J.R. Williams, A. Sanchez, Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study, IEEE Syst. J. 9 (1) (2015) 31–44.
[2] R.E. Mackiewicz, Overview of IEC 61850 and benefits, in: 2006 IEEE Power Engineering Society General Meeting, IEEE, 2006, pp. 8–pp.
[3] Y. Yang, K. McLaughlin, L. Gao, S. Sezer, Y. Yuan, Y. Gong, Intrusion detection system for IEC 61850 based smart substations, in: 2016 IEEE Power and Energy Society General Meeting (PESGM), IEEE, 2016, pp. 1–5.
[4] J. Hong, C. Liu, Intelligent electronic devices with collaborative intrusion detection systems, IEEE Trans. Smart Grid 10 (1) (2019) 271–281.
[5] M. Popovic, M. Mohiuddin, D.-C. Tomozei, J.-Y. Le Boudec, IPRP—The parallel redundancy protocol for IP networks: Protocol design and operation, IEEE Trans. Ind. Inform. 12 (5) (2016) 1842–1854.
[6] A. Elgargouri, M. Elmusrati, Analysis of cyber-attacks on IEC 61850 networks, in: 11th International Conference on Application of Information and Communication Technologies (AICT), IEEE, 2017, pp. 1–4.
[7] P.I. Radoglou-Grammatikis, P.G. Sarigiannidis, Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems, IEEE Access (2019) 46595–46620.
[8] B. Zhu, S. Sastry, SCADA-specific intrusion detection/prevention systems: a survey and taxonomy, in: Proceedings of the 1st Workshop on Secure Control Systems (SCS), Vol. 11, 2010, p. 7.
[9] I. E. Commission, Communication Networks and Systems in Substations - ALL PARTS, IET, 2003.
[10] J. O'Raw, D.M. Laverty, D.J. Morrow, IEC 61850 substation configuration language as a basis for automated security and SDN configuration, in: Power & Energy Society General Meeting, IEEE, 2017, pp. 1–5.
[11] A. Ahmed, V.V. Krishnan, S.A. Foroutan, M. Touhiduzzaman, C. Rublein, A. Srivastava, Y. Wu, A. Hahn, S. Suresh, Cyber physical security analytics for anomalies in transmission protection systems, IEEE Trans. Ind. Appl. 55 (6) (2019) 6313–6323.
[12] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, E. Savary, Power utility automation cybersecurity: IEC 61850 specification of an intrusion detection function, in: 25th European Safety and Reliability Conference (ESREL 2015), CRC Press, 2015.
[13] M. El Hariri, T.A. Youssef, H.F. Habib, O. Mohammed, Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values, in: 2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), IEEE, 2017, pp. 1–5.
[14] A. Hahn, C.-C. Sun, C.-C. Liu, Cybersecurity of SCADA within substations, in: Smart Grid Handbook, Wiley Online Library, 2016, pp. 1–17.
[15] International Electrotechnical Commission, IEC 61850-9-2 Communication Networks and Systems in Substations – Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled Values over ISO/IEC 8802-3, first ed., IET, 2004.
[16] I. 9506, Industrial Automation Systems–Manufacturing Message Specification, International Standardization Organization, Geneva, 1991.
[17] S. Kariyawasam, A.D. Rajapakse, N. Perera, Investigation of using IEC 61850-sampled values for implementing a transient-based protection scheme for series-compensated transmission lines, IEEE Trans. Power Deliv. 33 (1) (2017) 93–101.
[18] E. Solomin, D. Topolsky, N. Topolsky, Arrangement of data exchange between adaptive digital current and voltage transformer and SCADA-system under IEC 61850 standard, Procedia Eng. 129 (2015) 207–212.
[19] I. E. Commission, Communication Networks and Systems in Substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, IET, 2003.
[20] J. Hoyos, M. Dehus, T.X. Brown, Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure, in: 2012 IEEE Globecom Workshops, IEEE, 2012, pp. 1508–1513.
[21] J. Hong, C. Liu, M. Govindarasu, Detection of cyber intrusions using network-based multicast messages for substation automation, in: Innovative Smart Grid Technologies (ISGT), IEEE, 2014, pp. 1–5.
[22] T.S. Ustun, S.M. Farooq, S.S. Hussain, A novel approach for mitigation of replay and masquerade attacks in smartgrids using IEC 61850 standard, IEEE Access 7 (2019) 156044–156053.
[23] I. 7498-1, Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model, International Standardization Organization Geneva, 1994.
[24] C. Ruland, N. Kang, J. Sassmannshausen, Rejuvenation of the IEC 61850 protocol stack for MMS, in: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2016, pp. 625–630.
[25] C. Hornig, RFC894: A Standard for the Transmission of IP Datagrams over Ethernet Networks, RFC Editor, 1984.
[26] J. Horalek, J. Matyska, V. Sobeslav, Communication protocols in substation automation and IEC 61850 based proposal, in: 14th International Symposium on Computational Intelligence and Informatics (CINTI), IEEE, 2013, pp. 321–326.
[27] J. Kim, J. Park, FPGA-based network intrusion detection for IEC 61850-based industrial network, ICT Express 4 (1) (2018) 1–5.
[28] J. Hong, C.-C. Liu, M. Govindarasu, Integrated anomaly detection for cyber security of the substations, IEEE Trans. Smart Grid 5 (4) (2014) 1643–1653.
[29] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, S. Sezer, Multidimensional intrusion detection system for IEC 61850-based scada networks, IEEE Trans. Power Deliv. 32 (2) (2016) 1068–1078.
[30] B. Kang, K. McLaughlin, S. Sezer, Towards a stateful analysis framework for smart grid network intrusion detection, in: Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research, 2016, pp. 124–131.
[31] H. Yoo, T. Shon, Novel approach for detecting network anomalies for substation automation based on IEC 61850, Multimedia Tools Appl. 74 (1) (2015) 303–318.
[32] B. Moussa, M. Debbabi, C. Assi, A detection and mitigation model for PTP delay attack in an IEC 61850 substation, IEEE Trans. Smart Grid 9 (5) (2016) 3954–3965.
[33] P.I. Radoglou-Grammatikis, P.G. Sarigiannidis, Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems, IEEE Access 7 (2019) 46595–46620.
[34] A. Turner, Tcpreplay: Pcap editing and replay tools for^* NIX, 2005.
[35] J. Noce, Y. Lopes, N.C. Fernandes, C.V. Albuquerque, D.C. Muchaluat-Saade, Identifying vulnerabilities in smart gric communication networks of electrical substations using geese 2.0, in: 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), IEEE, 2017, pp. 111–116.
[36] M.T.A. Rashid, S. Yussof, Y. Yusoff, R. Ismail, A review of security attacks on IEC61850 substation automation system network, in: Proceedings of the 6th International Conference on Information Technology and Multimedia, IEEE, 2014, pp. 5–10.
[37] N. Kush, M. Branagan, E. Foo, E. Ahmed, Poisoned GOOSE: exploiting the GOOSE protocol, in: Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Australian Computer Society, Inc., 2014, pp. 17–22.
[38] R.T. Morris, A weakness in the 4.2 BSD unix TCP/IP software, AT&T Bell Labs Tech. Rep. Comput. Sci. 117 (1985).
[39] S. Bellovin, RFC1948: Defending Against Sequence Number Attacks, RFC Editor, 1996.
[40] F. Gont, S. Bellovin, RFC6528: Defending Against Sequence Number Attacks, RFC Editor, 2012.
[41] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andrén, C. Seitl, F. Kupzog, T. Strasser, Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations, in: 20th Conference on Emerging Technologies & Factory Automation (ETFA), IEEE, 2015, pp. 1–8.
[42] S. Kim, W. Jo, T. Shon, A novel vulnerability analysis approach to generate fuzzing test case in industrial control systems, in: Information Technology, Networking, Electronic and Automation Control Conference, IEEE, 2016, pp. 566–570.
[43] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh, J.-C. Tan, An intrusion detection system for IEC61850 automated substations, IEEE Trans. Power Deliv. 25 (4) (2010) 2376–2383.
[44] I. E. Commission, IEC 62351-4 Power Systems Management and Associated Information Exchange Data and Communication Security, IET, 2007.
[45] M. Strobel, N. Wiedermann, C. Eckert, Novel weaknesses in IEC 62351 protected smart grid control systems, in: 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2016, pp. 266–270.
[46] Y. Kwon, H.K. Kim, Y.H. Lim, J.I. Lim, A behavior-based intrusion detection technique for smart grid infrastructure, in: 2015 IEEE Eindhoven PowerTech, IEEE, 2015, pp. 1–6.
[47] Q. Yang, W. Hao, L. Ge, W. Ruan, F. Chi, FARIMA model-based communication traffic anomaly detection in intelligent electric power substations, IET Cyber-Phys. Syst.: Theory Appl. 4 (1) (2019) 22–29.
[48] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, D. Ishchenko, Collaborative defense against data injection attack in IEC61850 based smart substations, in: 2016 IEEE Power and Energy Society General Meeting (PESGM), IEEE, 2016, pp. 1–5.

[49] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based IDS for internet of things using unsupervised OPF based on mapreduce approach, Comput. Commun. 98 (2017) 52–71.
[50] W. Tong, L. Lu, Z. Li, J. Lin, X. Jin, A survey on intrusion detection system for advanced metering infrastructure, in: 2016 Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC), 2016, pp. 33–37.
[51] A. Bifet, G. Holmes, R. Kirkby, B. Pfahringer, MOA: Massive online analysis, J. Mach. Learn. Res. 11 (May) (2010) 1601–1604.
[52] C. Nixon, M. Sedky, M. Hassan, Practical application of machine learning based online intrusion detection to internet of things networks, in: 2019 IEEE Global Conference on Internet of Things (GCIoT), IEEE, 2019, pp. 1–5.
[53] T. Ha, S. Yoon, A.C. Risdianto, J. Kim, H. Lim, Suspicious flow forwarding for multiple intrusion detection systems on software-defined networks, IEEE Netw. 30 (6) (2016) 22–27.
[54] G. Chandrashekar, F. Sahin, A survey on feature selection methods, Comput. Electr. Eng. 40 (1) (2014) 16–28.
[55] S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, A. Kannan, Intelligent feature selection and classification techniques for intrusion detection in networks: a survey, EURASIP J. Wireless Commun. Networking 2013 (1) (2013) 271.
[56] N. Tatbul, T.J. Lee, S. Zdonik, M. Alam, J. Gottschlich, Precision and recall for time series, in: S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, R. Garnett (Eds.), Advances in Neural Information Processing Systems 31, Curran Associates, Inc., 2018, pp. 1920–1930.
[57] H.-N. Dai, R.C.-W. Wong, H. Wang, Z. Zheng, A.V. Vasilakos, Big data analytics for large-scale wireless networks: Challenges and opportunities, ACM Comput. Surv. 52 (5) (2019) 1–36.
[58] Z. El Mrabet, M. Ezzari, H. Elghazi, B.A. El Majd, Deep learning-based intrusion detection system for advanced metering infrastructure, in: Proceedings of the 2nd International Conference on Networking, Information Systems & Security, 2019, pp. 1–7.



Silvio Ereno Quincozes received Software Engineer bachelors degree (2011) from the Federal University of Pampa (UNIPAMPA), a master's degree (2015) in Computer Science from the Federal University of Santa Maria (UFSM) and a Ph.D. student (from 2018) in Computing at the Fluminense Federal University (UFF). He is interested in researches topics related to Information Security, Computer Networks, Intrusion Detection Systems, Smart Grids, Digital Substation Systems, Internet of Things, Data Mining, and Software Engineering. He authored the best paper at the IX Latin American Network Operations and Management Symposium (LANOMS), in 2019.

Célio Albuquerque received the B.S. and M.S. degrees in electrical and electronics engineering from Universidade Federal do Rio de Janeiro, Brazil, in 1993 and 1995, and the M.S. and Ph.D. degrees in information and computer science from the University of California at Irvine in 1997 and 2000, respectively. From 2000 to 2003, he served as the networking architect for Magis Networks, designing high-speed wireless medium access control. Since 2004 he has been an Associate Professor at the Computer Science Department of Universidade Federal Fluminense, Brazil. His research interests include wireless networks, network security, Smart Grid communications, Internet architectures and protocols, multicast and multimedia services.

Diego Passos received his B.Sc., M.Sc. and D.Sc. degrees in Computer Science from Universidade Federal Fluminense (UFF), Rio de Janeiro, Brazil in 2007, 2009 and 2013, respectively. From 2013 to 2014, he worked as a postdoctoral fellow researcher at the same university. He is currently an associate professor at the Computer Science Department of UFF. His research interests include multihop wireless networks, network coding, and wireless routing.

Dr. Mossé received his B.S. (Mathematics, 1985) from the University of Brasilia, Brazil, and M.S. and Ph.D. degrees (Computer Science, 1990 and 1993) from the University of Maryland, College Park. He has been a professor at the University of Pittsburgh since 1992, including six years as department chair, and has co-founded HiberSense, a startup company in the area of Smart Homes. He has been involved in the design and implementation of a couple of distributed, real-time operating system. His main research interest is in the allocation of resources (computing, energy, and network resources) in the realm of sustainable computing, computing for sustainability, and real-time, with main concerns being power management, security, and fault tolerance. He bridges the gap between the operating systems and networking research fields, between practice and theory. For the last 20 years, most of his systems research has focused on power and energy management, and for the last decade on how to increase diversity and how to promote reproducible research in computing.