Energy Informatics

RESEARCH Open Access

On specification-based cyber-attack detection in smart grids

Ömer Sen[1,2*], Dennis van der Velde[1,2], Maik Lühman[1], Florian Sprünken[1], Immanuel Hacker[1,2], Andreas Ulbig[1,2], Michael Andres[1,2] and Martin Henze[3,4]

From The 11th DACH+ Conference on Energy Informatics 2022
Freiburg, Germany. 15-16 September 2022

*Correspondence:
o.sen@iaew.rwth-aachen.de

[1] High Voltage Equipment and Grids, Digitalization and Energy Economics, RWTH Aachen University, Schinkelstraße 6, 52062 Aachen, Germany
[2] Fraunhofer Institute for Applied Information Technology FIT, Schloss Birlinghoven, Konrad-Adenauer-Straße, 53757 Sankt Augustin, Germany
[3] Security and Privacy in Industrial Cooperation, RWTH Aachen University, Ahornstraße 55, 52074 Aachen, Germany
[4] Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, Fraunhoferstraße 20, 53343 Wachtberg, Germany

Abstract

The transformation of power grids into intelligent cyber-physical systems brings numerous benefits, but also significantly increases the surface for cyber-attacks, demanding appropriate countermeasures. However, the development, validation, and testing of data-driven countermeasures against cyber-attacks, such as machine learning-based detection approaches, lack important data from real-world cyber incidents. Unlike attack data from real-world cyber incidents, infrastructure knowledge and standards are accessible through expert and domain knowledge. Our proposed approach uses domain knowledge to define the behavior of a smart grid under non-attack conditions and detect attack patterns and anomalies. Using a graph-based specification formalism, we combine cross-domain knowledge that enables the generation of whitelisting rules not only for statically defined protocol fields but also for communication flows and technical operation boundaries. Finally, we evaluate our specification-based intrusion detection system against various attack scenarios and assess detection quality and performance. In particular, we investigate a data manipulation attack in a future-orientated use case of an IEC 60870-based SCADA system that controls distributed energy resources in the distribution grid. Our approach can detect severe data manipulation attacks with high accuracy in a timely and reliable manner.

Keywords: Cyber security, Cyber physical systems, Intrusion detection systems

Introduction

The paradigm shift that is taking place in the energy sector as part of the energy transition due to the increasing penetration of Distributed Energy Resources (DERs) poses new challenges for grid operators, especially at the distribution grid level (Ourahou et al. 2020). To meet these challenges, a more active role of the distribution grid operator is required through increased expansion of sensors and actuators, which provide telecontrol connections via Information and Communication Technologies (ICTs) to resources such as controllable DERs (Bernd et al. 2021). This transformation from traditional grid structures to intelligent networked energy information systems—Smart

Grids (SGs)—using ICTs not only opens up new opportunities and solutions to master the energy transition, but also new dangers that threaten resilience and cyber-security (van der Velde et al. 2020).

Reliable and secure grid operation increasingly depends on properly functioning communication technologies and processes due to the high penetration of ICTs, making it more vulnerable to failures and cyber-attacks (Klaer et al. 2020). In particular in the context of Industrial Control System (ICS), which also includes process networks of power grids, a threat landscape against cyber-attacks becomes apparent, which is essentially characterized by a long lifetime of assets and the use of legacy components with limited security mechanisms (Eder-Neuhauser et al. 2017): in 2015, unauthorized third parties exploited these vulnerabilities to gain control of remotely controlled equipment, such as circuit breakers, to disrupt the power supply of more than 225,000 customers (Case 2016).

To counter new threats such as cyber-attacks, and to protect basic security objectives, i.e., confidentiality, availability, and integrity, cyber-security countermeasures are required, which are divided into preventive and reactive or active and passive measures. Various guidelines and standards, e.g., the IEC 62531 series of standards (IEC 2016), specify countermeasures such as the use of cryptography and authentication procedures in the telecontrol protocols. However, given the long-standing legacy devices with performance and resource constraints, countermeasures with high performance overhead involve high expenditures and costs to implement upgrades or workarounds (Tanveer et al. 2020). More passive and reactive security measures are network-based Intrusion Detection Systems (IDSs), which passively record communication traffic and perform attack detection within the process networks at selected points (Wolsing et al. 2022).

Intrusion detection methods can be broadly divided into blacklisting, in which observations are compared with known attack signatures, and whitelisting, in which observations are compared with the established understanding of the system's characteristics under normal conditions (Krause et al. 2021). For process networks with deterministic network structures and physically plausible verifiable payloads, whitelisting is a promising methodology to detect attacks or anomalies without prior knowledge of patterns and signatures (Eckhart and Ekelhart 2018). Furthermore, the impact of missing or hard-to-access data on attacks against power grids on the effectiveness of detection methods can be reduced, as whitelisting approaches do not primarily require such data.

A challenge in applying a whitelisting approach is the need for a holistic capture of the characteristics of the system and its formalism, which includes technical and operational specifications of the infrastructure, as well as the behavior of the devices under normally defined states. Possibilities for this capture can be machine-learning-based or domain-specific knowledge-based approaches (Krause et al. 2021). The first approach is essentially characterized by the automated generation of a model in defined learning periods, which is trained and generated from recorded communication data (Baraneetharan 2020). In particular, in combination with Deep Packet Inspection (DPI), industrial protocols such as IEC 60870-5-104 (IEC-104) are decomposed into relevant fields to collect training data for models to detect the derivation of a standard pattern and suspicious processes in the form of anomalies (Mochalski 2020). However, this may imply a potential vulnerability to data manipulation during the learning phases and incompleteness of non-observable legitimate situations such as maintenance in the training datasets. In the second approach, specifications are defined that are used as a set of rules to define the characteristics of the system under normal conditions to detect anomalies. E.g., the IEC 61850 standard, which is mainly used in substations, describes data models and communication parameters in a format known as Sub-station Configuration Language (SCL), which can provide the Specification Base (SB) for normal conditions (Hokama and de Souza 2020). However, the thoroughly available data prescribed by the standard's data model is not applicable to all industrial protocols, such as IEC-104. Thus, the Specification-based IDS (SIDS) approach requires proper domain knowledge deposited and validated, but potentially achieves higher precision rates compared to machine-learning-based IDS approaches (Verma and Ranga 2020; Kus et al. 2022).

However, the holistic capture of infrastructure specification and behavior of components in normal states requires high manual efforts in bundles of cross-domain knowledge and their maintenance, resulting in technically complex implementations without suitable accessible formalization. We identify the following challenges:

- Concentration of dispersed domain-specific knowledge in a holistic SB description of the infrastructure.
- Automated extraction of detection rules from infrastructure knowledge to detect anomalies and suspicious events.
- Provision of explanations for issued alerts through coherent rule matching of infrastructure knowledge and alert generation.
- Maintain high flexibility in detection capabilities through modular enrichment of infrastructure knowledge.

To address these challenges, we propose an approach for a SIDS, which, supported by an infrastructure specification and Automata Models (AMs) for component behavior w.r.t. communication flows, captures characteristics of the SG for cyber-attack detection. More precisely, our contributions are:

1. We identify relevant domain knowledge for the SIDS of cyber-attacks and intrusions in SGs by extracting domain-specific data based on a Graph-based Infrastructure Model (GIM) approach (Specification Basis).
2. We present and describe a structured approach for detecting anomalies in communication behavior in SGs process networks that uses a holistic GIM as a SB and AMs for flow consistency checks (Deep Packet Inspection).
3. We demonstrate and discuss the performance of our proposed approach against different attack scenarios in a physical testbed by evaluating the detection quality and performance within the scenarios (Evaluation and Discussion).

Smart grid and process-awareness in detection

As the basis of our work, we describe the infrastructure specification of process networks based on Supervisory Control and Data Acquisition (SCADA), discuss their security and related research work.

SCADA-based process networks

Based on the Purdue reference model (Williams 1994), process networks based on SCADA in SGs can be described as hierarchical control structures consisting of primary technology, secondary technology, and ICT (Bernd et al. 2021) as presented in Fig. 1. Divided into several levels, the primary technology, such as circuit breaker switches, is monitored and controlled utilizing secondary technology, such as sensors and actuators.

At the lowest level of the control hierarchy, the infrastructure is divided into the Operational Technology (OT) network [(equipment and systems with telecontrol connection through Wide Area Network (WAN)]. Directly connected to the OT network is the SCADA network (control systems and communication stations with operator stations). Connected via firewalls, a security-controlled level, the Demili-tarized Zone (DMZ), is present (logically segmented area between corporate office and SCADA network). Finally, the corporate network is connected to DMZ.

The primary facilities are connected to the OT network through Intelligent Electronic Devices (IEDs) used for control and measurement tasks, aggregated within the control hierarchy by Remote Terminal Units (RTUs). Data are then forwarded to the SCADA system through the OT network using appropriate OT protocols such as IEC-104 (IEC 2016) or Modbus (MICIE 2020). Within the OT network, the Master Terminal Unit (MTU) counterpart to the RTU acts as a gateway for the SCADA system.

Cyber-security in process networks

In the European energy sector, the IEC-104 protocol is often used to monitor and control geographically widely distributed processes (Matoušek 2017). IEC-104 as a legacy industrial protocol does not provide security features such as encryption or authentication (IEC 2016). Therefore, without an encryption or authentication mechanism, unauthorized third parties can intercept critical IEC-104 traffic and potentially endanger the grid. E.g., the attacker can intercept existing communication channels by a

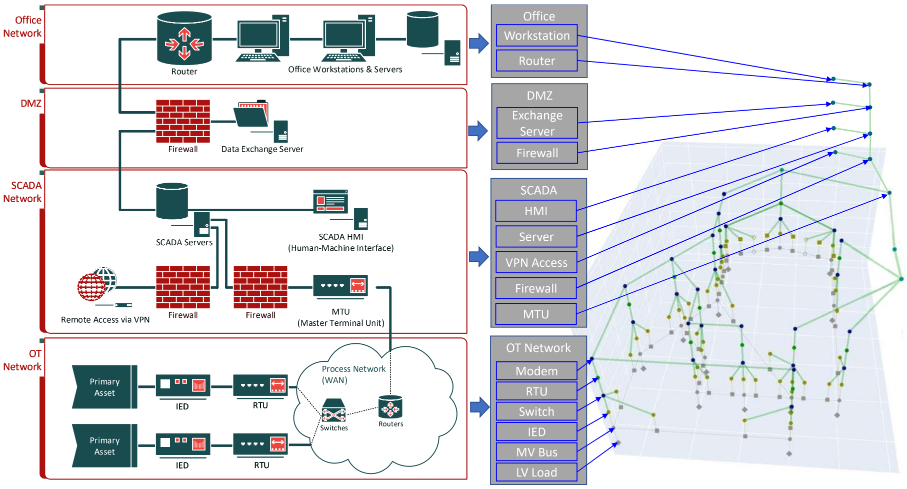


Fig. 1 Illustration of the SG infrastructure based on the Purdue reference model, representing a future-oriented SCADA system that is connected to the primary equipment via dedicated and/or public communication infrastructure (van der Velde et al. 2021). The right side represents the graph-based formalism of the infrastructure as a SB (Klaer et al. 2020)

Man-in-the-Middle (MITM) attack or establish new connections to manipulate the traffic. Thus, the attacker would be able to read, modify, inject, or discard new or sent messages between the intercepted or newly connected endpoints (Yang et al. 2012).

To address the critical security issues within the process network, especially the legacy protocols, the IEC 62351 standard discusses new security principles and requirements. E.g., the IEC 62351 standard requires secure end-to-end communication using the Transport Layer Security (TLS) protocol, which provides secure key exchange, encryption, and authentication (IEC 2018). However, large-scale implementation and adaptation of the new standards in traditional process networks are hampered by the large number of resource-constrained devices, which may jeopardize service availability. These approaches can overwhelm resource-limited field devices such as RTUs or IEDs and cause higher communication latency, preventing SCADA applications from meeting real-time requirements (Tanveer et al. 2020).

Different studies investigated the performance issues caused by TLS protocol integration, and negative impacts on the performance of industrial protocol communications (e.g., IEC 61850, IEC-104) have been observed (Todeschini and Dondossola 2020). Power grids often contain performance-limited assets with long depreciation periods that cannot be replaced or upgraded without high costs, which require legacy compliant solutions (Castellanos et al. 2017). IDS can provide passive security via detective capabilities to identify possible attack indicators or anomalies that do not actively interfere with the process network (Fernandes et al. 2019). There are several IDS approaches to identify potentially suspicious events, either by comparing observation with knowledge that represents normal system behavior, or by directly comparing the signature with known classified attacks (Zuech et al. 2015).

However, the latter approach requires attack data for detection, which limits flexibility in detecting unknown attacks such as zero-days (Akshaya 2019). Moreover, comparing observations with known normal conditions based on trained models using data-driven machine learning approaches also has the disadvantage of low accuracy and limitation due to the scenarios included in the training data (Khraisat et al. 2019). Therefore, a specification-based approach that relies on verified expert knowledge has the potential to provide high accuracy in detection and reduce the flexibility constraint by relying on domain-specific knowledge. The challenge with SIDS approaches is to provide a standardized SB for different SG use cases, based on which anomaly detection conditions can be automatically derived. Therefore, in this paper, we present a SIDS that uses a defined GIM to automatically derive the set of rules.

Related work

Many studies and research works have investigated detection mechanisms based on process-awareness of Cyber-Physical System (CPS) for their suitability as IDS.

One of these research directions involves addressing process-aware IDSs that evaluates the attractiveness and criticality of ICS devices that underlie industrial processes that could be modified to achieve adversary goals (Cook et al. 2017). On this basis, the necessary signatures or heuristics that an adversary will leave as traces in its compromise attempt are identified. Another research approach uses the degradation and functionality features of control signals to extract the meaning of the process of commands and determine the nondegradation pattern of the control signal within the action chain (Escudero et al. 2018). The goal is to detect the unlegitimacy of the control signal issued by IED to the action chains before it controls the equipment.

Toward a holistic coverage of CPSs, there are approaches that replicate the program states from physical devices to their digital twins using passive data sources and system specifications (Eckhart and Ekelhart 2018). Using stimuli and replication in a virtual environment, detailed testing is enabled in the context of IDS. More advanced research approaches address cyber-attack classification prepared in laboratory experiments and performed in tests to design various IDS rules (Mohan et al. 2020). The approach is based on rule generation algorithms in a distributed architecture to accommodate SCADA traffic.

Another approach pursues process-aware IDS by modeling ICS/SCADA communication using probabilistic automata (Matoušek et al. 2021). The model represents normal communication with a small number of states and edges whose semantics are extracted from the headers of the protocol and detect state-based anomalies. In the context of state interpolations in the automaton, an approach is presented that uses a combination of fuzzy interpolation with fuzzy automata (Almseidin et al. 2019). Using automata theory and the fuzzy system for reasoning as part of the detection mechanism, a state transition rule base method is implemented to detect attacks.

Regarding the anomaly detection methods for IEC-104, some multivariate access control and outlier detection approaches have been proposed using extracted packet information and communication statistics through Scapy (Rohith et al. 2018) and CICFlowMeter (Lashkari et al. 2017) for anomaly detection (Grammatikis et al. 2020). In the area of statistically based anomaly detection on IEC-104, the work in Burgetová et al. (2021) presents a 3-value detection method that independently compares the number of packets transmitted in three consecutive time windows against a statistical profile and reports anomalies when a deviation from the specified range is detected. To address the problem of missing labeled data, the work of Anwar et al. (2021) explores the use of unsupervised machine learning on IEC-104, in particular, one-class support vector machines, isolation forest, histogram-based outlier detection, and k-nearest neighbor are investigated.

When addressing security issues within the protocol IEC-104, research in Scheben et al. (2017) examined the detection qualities of a machine learning-based detection system compared to a misuse-based system such as Snort (Caswell and Beale 2004). The result undermines the flexibility-accuracy dilemma described earlier, where the misuse-based system has high accuracy but low flexibility, whereas the machine learning-based system has higher flexibility but lower accuracy. Furthermore, the challenge with automated machine learning-based detection systems also lies in their explainability (Dang 2021), which challenges the plausibility check of the output (Holzinger et al. 2020).

Although the proposed approaches provide different mechanisms to combine process knowledge with cyber-security, they still require significant additional analytical resources to provide the necessary information for their functionality. E.g., in addition to the infrastructure specification for which the operator can provide necessary knowledge, additional efforts must be made to develop an understanding of likely attack targets, details about stimuli, statistical data, or vendor-specific technical specifications such as equipment degradation that are often inaccessible. Therefore, our approach is entirely based on the utilization of domain-specific knowledge, which is accessible from standards and infrastructure knowledge from grid operators. While the implementation of AMs enables the detection of inconsistencies within processes and flows, it does not take into account the semantics of the data points involved in the traffic. Therefore, the intrusion detection capabilities of our proposed SIDS rely not only on automata-based detection, but also on semantic verification of the data points. The Gim encapsulates the semantics of the data points, which is part of advanced detection. Through the holistic formulation of a graph-based specification foundation that provides the required overall understanding of the process, semantics, and communication of SG, we design a process-aware SIDS.

Specification-based intrusion detection

In this section, our approach of a SIDS for SGs is presented.

In general, our approach is based on SB derived from GIM that encapsulates domain-specific knowledge. Using SB, monitored network traffic is checked against SB, with a violation resulting in a specific and explainable alert. Furthermore, the consistency of communication behavior is checked against protocol-specific AMs to ensure that the industrial packet flows comply with the state transitions. Thus, intrusion detection is performed using a mixture of approaches leveraging the domain knowledge of a GIM.

Framework overview

Our proposed SIDS (cf. Fig. 2) is a network-based SIDS that checks for the presence of malicious content in the various layers of the network protocol. The SIDS detects anomalies based on the captured traffic by checking information from the packet headers and payloads within the industrial protocol stack (e.g., Ethernet/IP/TCP/IEC-104) and discrepancies in the packet flow using Mealy automata (Grigorchuk et al. 2000). The Mealy

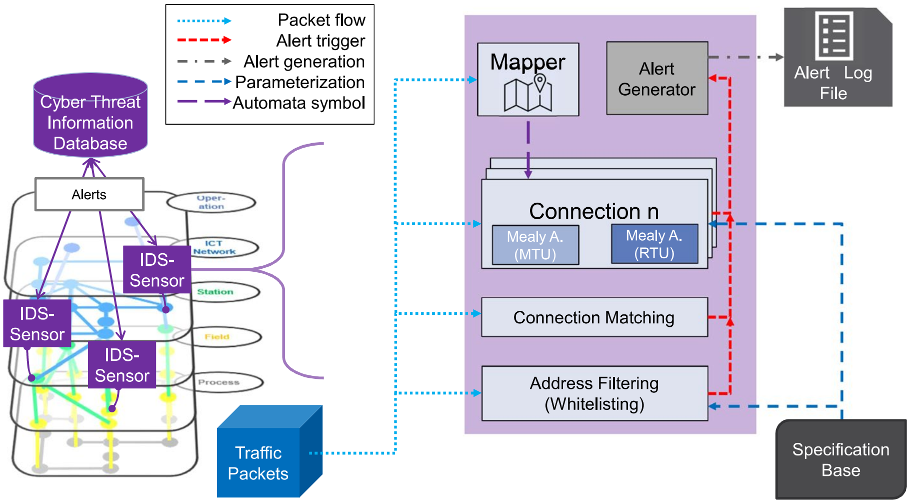


Fig. 2 This illustration presents the SIDS approach to observe network traffic based on specifications and indication of traffic, which is a hybrid approach of specification-based rule matching and behavior consistency checking via a Mealy automata

automaton has no accepting states, and the sequence of outputs from the sequence of transitions leads to a reactive system with transitions as its core and is therefore a more appropriate model for protocols (Bieniasz et al. 2016). Based on a variation of Angluin's L* algorithm that generates Mealy automata (Bollig et al. 2010), the state machine model is used to perceive the communication behavior.

In this paper, we focus on the IEC-104 protocol, which is a widely used standard in the European energy sector for monitoring and controlling tasks in TCP/IP-based networks (Matoušek 2017). However, the SIDS is not limited to the contents of the application layer of IEC-104 traffic, but considers all layers that are included in typical TCP/IP-based IEC-104 packets. In particular, packets that use IP at the network layer, TCP at the transport layer, and IEC-104 at the application layer.

To distinguish between illegitimate and legitimate traffic, the SIDS uses a set of rules defined in a machine-readable input file derived from the SB (cf. "Specification basis" section). Here, specifications are defined as sets of information that represent the known parameters and characteristics of the SG infrastructure to some extent. Anything specified in SB is considered valid; anything that does not conform to a specification is considered malicious traffic.

When observing network traffic, the SIDS examines each packet using DPI (cf. "Deep packet inspection" section). In this context, the conformance of the data packet to the SB, such as the protocols used, protocol fields, address validation, and payload consistency is checked. After the initial inspection of the packet, the next inspection step evaluates connection attributes and states. Each connection is defined in SB, specifying the properties of the connection, and two Mealy automata modeling the connection endpoints.

Regarding IEC-104 traffic within the SCADA network, the roles of endpoints are represented as MTU and RTU. For correct semantic mapping of packets, the mapper component is responsible for translating the packet contents into an input symbol for the Mealy automata (cf. "Automata model" section). After the mapper receives the corresponding input symbol, the connection object passes it to the instantiated AMs representing the connections. Because of the use of Mealy automata, it provides immediate feedback by returning an output symbol. If the output symbol indicates an error or suspicious behavior, the connection object triggers the alert generator with a specific alert reason to issue an alert (cf. "Alert generation" section). Alert generation is triggered by various components for different reasons. The cyber threat information database represents the collection of alerts combined with the specification of the infrastructure, which is part of a higher-level correlation as presented in our previous work (Sen et al. 2021a, 2022).

Specification basis

Based on a formal GIM of SG (Klaer et al. 2020), we extract the SB for the SIDS through the explicit data model definition. Thus, whitelists can be created from the data model and anomaly detection through the whitelist configurations. This includes communication (e.g., link quality, routing, packet flows), authentication (e.g., MAC/IP addresses), and process data (e.g., control, measurement, state—plausibility). Table 1 describes the domains and information fields of the SB.

Table 1 Domain-specific attribution of captured traffic

Domain	Field attribution
Communication	Address matching of packets (L2–L4, L7)
	Connection and established communication channel (client/server, protocol, port)
	Packet flow according to protocol (L4, L7)
Asset	Data point matching
	Integrity at data point level
	Role-based verified operations
Operation	Technical assets boundaries
	Technical command execution capability

The SB provides information on the behavior of communication, assets, and operating limits, from which rules can be derived. In the area of communication, e.g., the addresses of the relevant fields of the protocol layer (L2–L4, L7), such as the MAC address, the IP address, the Port number, and Information Object Address (IOA) of the IEC-104 protocol, are specified. Additionally, legitimate connection channels and routes are defined which specify allowed communication channels between the endpoints with protocol types and Port numbers. In the dynamic scope, the standards assigned to the application layers (L7) are defined accordingly, which then sets the corresponding predefined AMs for attack detection. E.g., for IEC-104, AMs are used that represent the data transaction process during communication initialization and confirmation of control commands.

The use of protocols is also considered in the SB. E.g., the use of certain protocols such as SSH can either be whitelisted or even restricted to certain periods such as maintenance times on weekends. Protocol behavior is observed with AMs that represent valid communication flows for specific protocols. Currently, there is only one model for IEC-104 traffic, but in general other state-full protocols can also be modeled through AMs. The SB can also be extended to include other criteria such as the maximum Round Trip Time (RTT) for TCP packets.

In the context of resource behavior, data points are taken from SB and verified for legitimacy within industrial telecontrol protocols, that is, regarding known data points with correct addressing. Consequently, the integrity of the data points is defined according to SB, if the data characteristics within the data points (e.g. IOA in IEC-104) are correctly assigned to the asset in the right communication direction. This provides the base for role-based verification of asset operations, in which the legitimacy of operation options of assets is also defined by the data points (e.g., sensors can send measurements but not commands).

In the scope of operational behavior, the technical operating boundaries of assets (e.g., maximum power rating for setpoints), and the execution plausibility of commands are also extracted from the domain-specific knowledge of the SB (e.g., nominal power-dependent plausibility range for the $\cos\phi$ setting of inverters (Scheben et al. 2017)].

Deep packet inspection

The functionality DPI is a key feature of SIDS and is anchored in the central organizer and forwarder of all internal intrusion detection processes (cf. Fig. 2). After a packet is received, it is categorized depending on the packet layers it contains. Relevant packets are those that correspond to one of the protocols described in the SB, e.g., IEC-104 or SSH packets.

The categorization determines the checks that are performed on each packet. Packets that are classified as irrelevant are ignored, while the contents of packets containing industrial protocols such as IEC-104 are checked more thoroughly. Although basic address detection and verification are performed at the first level of DPI, advanced and contextual checks are performed as part of connection-related checks. Each packet associated with a particular connection object is forwarded to the corresponding checks. Connection objects represent a connection between two endpoints. Each of the endpoints is assigned specific addresses for each network layer, including the application layer, e.g., the IEC-104 protocol, for which an AM is assigned. For IEC-104 traffic, this means that each connection contains two AMs, an MTU model, and an RTU model.

When a packet is assigned to a connection by the DPI component, all addresses are checked for consistency, both on the sender and the receiver side. In addition, the flow control of the IEC-104 layer is also checked. For this task, connections store the current packet sequence control counters for each endpoint individually. When a connection receives a packet containing sequence control information, namely packets containing Application Protocol Control Information (APCI) frames in I-frame and U-frame format, the connection objects are checked. They are checked for both endpoints whether the sequence numbers match the current counters and transmission direction. In addition, an I-framed APCI indicating an Application Service Data Unit (ASDU) is checked for technical specification conformity.

After all addresses, traffic sequence, and technical specifications are checked, the packet is passed to the packet mapper. The mapper maps the packet to an input symbol of the automata alphabet as an automata input. If any of the checks of DPI fails, e.g., the contained address information is unknown or the packet cannot be assigned to a connection, an alert is issued.

The automated process of generating the SB based on the infrastructure model is broken down into several components as shown in Fig. 3. The input consists of an GIM, which describes the infrastructure in the respective domains of power grid, IT, and OT devices. Each of these domains contains domain-specific information, such as asset data points, component networking, and their operational function in the process. In addition, a configuration is required that specifies the rules that will be used later to detect attacks. The rule configuration specifies the type of devices of interest for which rules are to be created that contain attributes and their environmental constraints.

To achieve the desired detection quality, the SIDS must be correctly configured by the given input. The prerequisite for this is SB, which is to be generated by the rule generator. The task of the rule generator is to convert a GIM into a SB based on a given configuration. This SB represents the set of rules that the SIDS uses to decide which communication and payload content is valid.

The rule generator consists of three modules, each serving a different purpose. The importer is used to read the respective inputs—the GIM and the configuration—and prepare them for further use. The rule manager is the main module of the rule generator and is responsible for reading the relevant attributes from the GIM and converting them

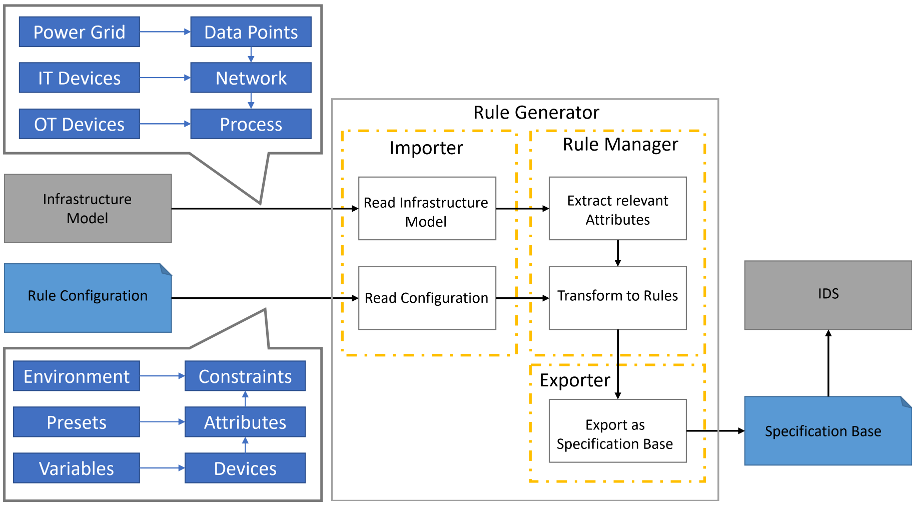


Fig. 3 Illustration of the rule generation process to automatically generate the SB based on the infrastructure model

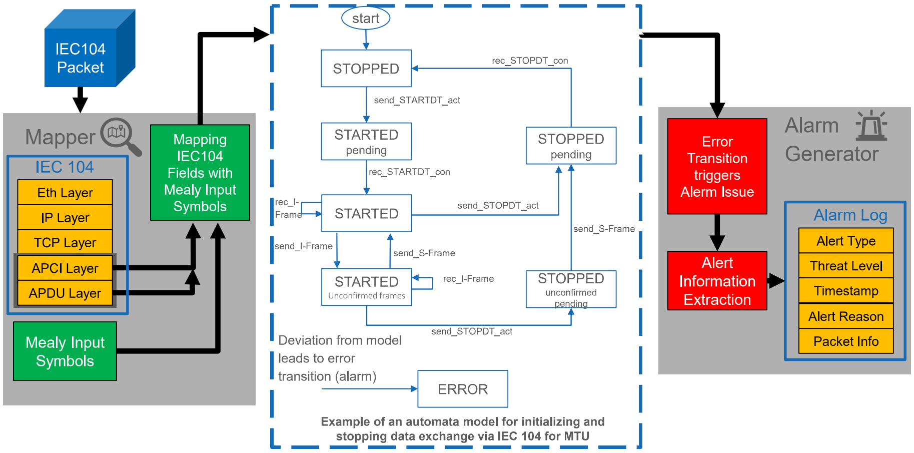


Fig. 4 Exemplary illustration of the mapper, that maps IEC-104 data packets to input symbols for the automata, which here, in an example for the MTU endpoint connection, generates according to the protocol standard a Mealy AM to stateful monitor e.g., the data transaction

into rules based on the specifications in the configuration. Finally, the exporter summarizes the generated rules in a SB that can be read by the SIDS. After generating the SB, the SIDS can apply the previously generated specifications to the packets of the captured network communication. As soon as the given specifications are violated or the recorded communication deviates from the expected normal behavior, alarms are triggered.

Automata model

AMs are used to dynamically check multiple packets within industrial protocol traffic (cf. Fig. 4). The goal of AMs is to model flow-based processes within the communication process according to the selected protocol, such as IEC-104. The states of the AM represent, e.g., the start of a connection and data transmission, the tracking of pending acknowledgments of commands and measured values, and the stop of the data transmission. Packets identified as industrial protocol traffic are processed by the mapper component, which maps the packets to their corresponding input alphabet counterparts for the AM.

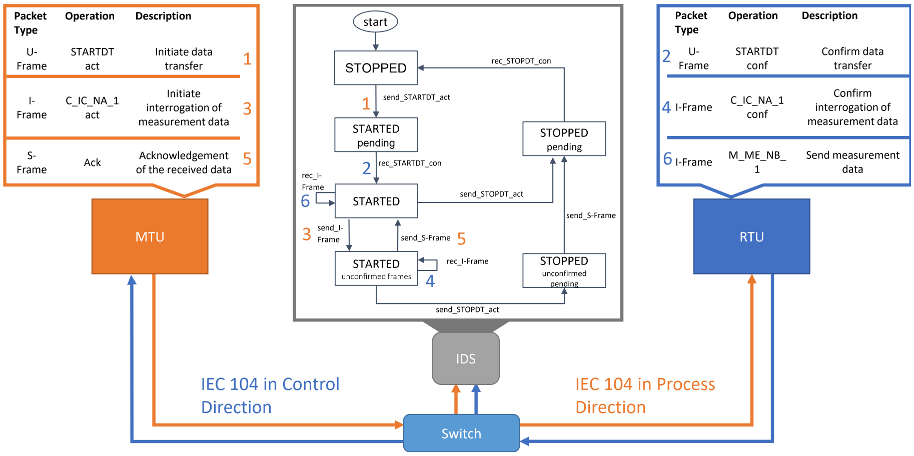
The mapper translates the contents of the IEC-104 layers into input symbols for the MTU and RTU automata used within the connection object. A data packet may contain multiple instances of IEC-104 layers. The mapper then returns an ordered list of symbols mapped from these packets. The symbol is mapped based on the contents of the decoded IEC-104 layer. Within this process, the format of the observed APCI frame is determined, where the APCI frame can have three different formats: U-frame, I-frame, and Sframe. Depending on the determined format, the frames are checked for additional flags that indicate membership in specific groups of packets mapped to special input symbols. Subsequently, these input symbols represent the set of possible input symbols for the IEC-104 automata. Additionally, an error symbol is used to indicate that the packet does not match any of the criteria used to assign it to one of the known input symbols.

According to the IEC-104 protocol standard, two transition systems are modeled, one representing the MTU stations of SCADA networks and one modeling RTU station for each connection. The use of this role-based modeling approach allows the states within the AMs to be sufficiently differentiated, such as the states of connection establishment and valid data transmission. To define the processes within the connection procedure of communication more accurately, the models must also be able to determine whether an input is sent or received. To this end, each packet categorization is extended to include a prefix indicating whether the packet was sent or received. Both automata use the same input alphabet and state sets, but differ slightly in some transitions.

After receiving an input symbol and using a transition, the automata returns an output indicating whether the input results in a suspicious state or whether this packet type is invalid for the current protocol procedure. Internally, this is done by a status variable within the automaton object. When certain transitions are used, they trigger functions that change the internal state, which is always given as a return value after processing the input. E.g., the AM requires the generation of 15 different input symbols for seven different packet types. The packets are recognized by the mapper and then extended by a prefix indicating the direction of transmission and an error input. These transitions do not change the internal state variable, so the output would be valid in the sense of Mealy automata.

All other transitions that trigger a change in the internal state variables of AMs are undefined behavior, i.e., a violation of the protocol procedure. Therefore, the output for each of these transitions is invalid. The error input indicates that the packet was not recognized as belonging to one of the defined packet types, therefore cannot be processed, and thus leads to an alert.

Figure 5 illustrates an example of how AMs works to check the consistency of normal traffic flow in the monitored communication channel. As an example, a data transmission sequence is used that contains an interrogation operation, where the MTU initiates the data transmission. After starting the data transmission, both automata reach the “STARTED” state, which allows I-frames to be sent. The MTU sends an interrogation command to RTU, which is acknowledged with the first I-frame back to MTU. After



Packet Type	Operation	Description	
U-Frame	STARTDT act	Initiate data transfer	1
I-Frame	C_IC_NA_1 act	Initiate interrogation of measurement data	3
S-Frame	Ack	Acknowledgement of the received data	5

	Packet Type	Operation	Description
2	U-Frame	STARTDT conf	Confirm data transfer
4	I-Frame	C_IC_NA_1 conf	Confirm interrogation of measurement data
6	I-Frame	M_ME_NB_1	Send measurement data

Fig. 5 Example illustration of packet flow conformance checking based on the MTU automaton model, showing a simple MTU and RTU communication scenario

Table 2 Alert output from SIDS

Alert field	Description
Alert type	The type of alert indicates what type of alert has occurred
Threat level	Low, medium or high threat levels
Timestampy	Each warning issued contains the timestamp when the warning was created
Alert reason	A textual reason that triggered the creation of this warning message
Packet content information	Detailed information about which data packet content is related to the issued alert

the first I-frame to the MTU, the RTU sends several I-frames containing the measurement data. The MTU acknowledges the packet reception with an S-frame indicating that all previous frames have been sent correctly and that both automata should now be in the "STARTED" state, since both have no unacknowledged frames. Since the traffic flow conforms to the automaton model, the conformity of the packet flow in this example is therefore also classified as correct by SIDS.

Alert generation

Alerts are the notifications of the SIDS that are triggered when certain packets violate the specification. They are issued by the alert generator component of SIDS and recorded in a machine-readable log file.

All alerts are written to a log file that assigns a unique running ID to each new alert. Each alert begins with an ID tag, followed by the attributes specified in Table 2.

To illustrate how alert messages are generated, we provide an example in Listing 1. We use Metasploit's IEC-104 Client Utility Module as the basis for this sample scenario (https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/client/iec104/iec104). Therefore, the scenario underlying this example is that a new endpoint with unknown IP and MAC address acts as a MTU and attempts to establish a IEC-104 connection to a RTU. In doing so, the new MTU also sends a control command specifying a new setpoint, such as a new power injection for a Photovoltaic (PV) inverter. In this example, the generated alarms cause anomalies regarding the IP and MAC addresses of the new endpoint, as these are not specified in the SB. In addition, the connection is also not valid because the communication channel between the new endpoint and the RTU is also not specified. Thus, any commands sent from the new endpoint to the RTU are also considered invalid. Furthermore, the control command contained a setpoint that also violates the specified allowable range of valid setpoints. Thus, all active interactions between the new endpoint and the RTU are classified as anomalies and output as alerts.

```
[ALERT_0]
alert_type = IP_MISMATCH
threat_level = high
timestamp = 14.04.2022 10:47:09
alert_reason = IP of this packet is
     unknown: 173.24.0.3
packet_info = ETH / IP / TCP /
    IEC104−U

[ALERT_1]
alert_type = PORT_MISMATCH
threat_level = high
timestamp = 14.04.2022 10:47:09
alert_reason = One of the Ports of
    this packet is unknown: 59478
packet_info = ETH / IP / TCP /
    IEC104−U

[ALERT_2]
alert_type = NO_SUCH_CONNECTION
threat_level = high
timestamp = 14.04.2022 10:47:09
alert_reason = Connection does not
    exist in whitelisting data!
packet_info = ETH / IP / TCP /
    IEC104−U

[ALERT_3]
alert_type = INVALID_OPERATION
threat_level = high
timestamp = 14.04.2022 10:48:00
alert_reason = Send packet contains
     invalid operation for the
    endpoint!
packet_info = ETH / IP / TCP /
    IEC104−I

[ALERT_4]
alert_type = INVALID_SETPOINT
threat_level = high
timestamp = 14.04.2022 10:48:00
alert_reason = Active control
    command contains invalid
    setpoint!
packet_info = ETH / IP / TCP /
    IEC104−I
```

Listing 1 Example of alert messages generated by the alert generator.

Overall, our SIDS, which automatically derives its SB based on a formal GIM, is designed to detect explainable anomalies from different domains. Specifically, the domain-specific knowledge used for anomaly detection is extracted as appropriate rules from the GIM, which represents the operator's existing knowledge of its infrastructure, without requiring the knowledge of cyber-security experts. Moreover, the dynamic nature of communication behavior is also validated by AMs with respect to protocol conformance and flow consistency. Subsequently, both the dynamic packet flow and attributes, as well as the protocol field values within the payload, are validated and checked for potential inconsistencies or specification violations. Thus, our SIDS detects critical violations of legitimate processes and infrastructure specifications at both the communication and operational levels, relying only on existing and available knowledge without requiring external expertise.

Evaluation and discussion

To demonstrate and discuss the performance of our proposed SIDS, we evaluate its detection quality in a physical testbed for attack and non-attack scenarios.

Smart grid testbed setup

We evaluate SIDS in a cyber-physical testbed as shown in Fig. 6 that is based on our previous work (Sen et al. 2021b). The testbed replicates an MV/LV grid consisting of physical components networked through a dedicated ICT infrastructure. Therefore, neither simulations nor virtualized components are involved. Since our SIDS is designed to monitor specific communication channels within defined network segments and thus acts more like a sensor with more than one entity deployment, the limited complexity of the testbed does not limit the scope of the study.

In our test setup, we use electrical equipment such as a 640 kVA secondary substation, 22 kWh Battery Storage System (BSS), 12 kVA and 36 kVA PVs, and several resistive/inductive loads. The power system topology consists of two strings to which the DERs and loads are connected, and on which we can measure current and voltage via integrated three-phase measuring points. We control the DER through their Modbus interface via RTUs, which is provided by their respective inverter. Following a SCADA network, the testbed also includes a process network consisting of the ICT infrastructure and the control room. The control room represents an MTU that sends IEC-104 control and query commands to RTUs.

We consider different attack scenarios based on attacks that have already gained access to the process network. The external attacker represents a new entity within the system with unknown IP and MAC addresses. Contrary, the MITM attack intercepts the communication between the control room and the selected RTUs.

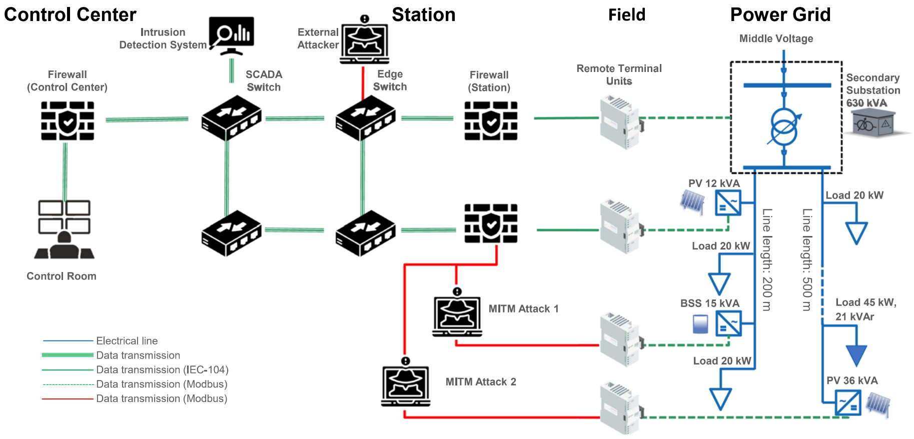


Fig. 6 Our setup of a SG testbed replicates a distribution grid with DERs and ICT infrastructure for control and monitoring

In addition, our SIDS approach is deployed in the process network at the SCADA switch, where traffic is monitored via a mirrored SPAN port or dedicated network taps. Active inline network taps are used between the SCADA node and switches to capture SCADA traffic and perform timestamping with a high resolution of 8 ns (https://www.profitap.com/wp-content/uploads/ProfiShark-1G-Plus-Datasheet.pdf). The mirrored SPAN port allows all traffic passing through the target switch to be captured, but with lower timestamp resolution and possibly more jitter. Preferably, dedicated network taps are used for the main communication channel between the MTU and RTU to be monitored. Thus, SCADA-related network traffic is continuously forwarded to SIDS for intrusion detection.

Methodology

We use the cyber-physical testbed and attack scenario described in Smart Grid Testbed Setup. In the first scenario without attack induction, all stations and traffic are within the specification, where normal protocol behavior of a system operation under normal conditions is replicated (Scenario 1). We use this scenario to examine the SIDS under normal operation conditions with an average traffic volume.

In the second scenario, we investigate the detection quality of SIDS under attack conditions. To this end, this scenario is divided into replicating an attack from outside the testbed with limited knowledge of the internal network and data points (Scenario 2-a) and an attack with sophisticated knowledge (Scenario 2-b).

Scenario 2-a contains a communication attempt with unknown addresses in L2 and L3 (e.g., MAC and IP address) to RTU, sending an interrogation command to query measurement values. Scenario 2-b is executed as a MITM-based False Data Injection (FDI) attack in which two different types of packet are injected. The first type of injected packet contains an IOA that is not associated with the corresponding asset in the specification (Scenario 2-b-I). In contrast, the second type contains an IOA included in the specification and also regularly used in the normal conversation of MTU and RTU with the correct mapping of devices (Scenario 2-b-II). However, the measurements transmitted with these packets contain measurements that are overlaid with small noise within the range of the technical specification.

We also measure the performance of SIDS in large traffic volumes per connection in a short time. An important requirement for this investigation is that SIDS always observes the beginning of the connection to use AMs for correct context and packet sequence tracking. Otherwise, it cannot find the correct initial state and therefore produces alerts for almost all data packets.

To evaluate the quality of detection, we rely on the confusion matrix and the performance metrics derived (Tharwat 2020). Thus, we measure the following metrics:

- True Positive (TP): event correctly classified as attack indicator.
- False Positive (FP): event incorrectly classified as attack indicator.
- True Negative (TN): event correctly not classified as attack indicator.
- False Negative (FN): event incorrectly not classified as attack indicator.

To evaluate the performance of our approach, we also use the following telemetry data of the captured network traffic in the scenarios.

- L2: MAC source and destination addresses.
- L3: IP source and destination addresses, checksum.
- L4: TCP sequence and acknowledge numbers, port number, checksum, RTT.
- L7: IEC 104 protocol fields of U- and I-frames.

Evaluation of performance and classification accuracy

Our results are presented in Table 3. Within Scenario 1, our results indicate that SIDS does not generate alerts caused by addressing, automata errors, or sequence number violations. The only parameter that may cause slight variations in the False Positive Rate (FPR) is the maximum RTT parameter, which in our experiments was parameterized in the range of 150 ms and 200 ms. Narrower ranges caused more FPs in our experiments due to varying RTT in the communication channels. With this adjustment, using a sufficiently large value for the maximum RTT (e.g., upper 95% confidence interval of the RTT variance), no FPs were produced.

In Scenario 2-a, the attacker mimics the normal behavior of a MTU by starting a conversation and sending a query command for the measurement data. The RTU responds with measurement data. All 115 malicious packets were correctly detected.

Within Scenario 2-b, we inject a total of 20 packets (10 packets from each of the subscenarios). SIDS was able to correctly classify the 10 packets from scenario 2-b-I (TP) due to incorrect addressing of IOA. Scenario 2-b-II represents an edge case where the attacker performs perfect spoofing and adheres to the legitimate specification of the system. Therefore, the 10 injected packets from Scenario 2-b-II were not correctly detected by SIDS, showing the limits of our approach (FN). However, limiting the range of attack actions so that the attacker can evade detection can shift the impact trajectory of the attack into a treatable scope. Subsequently, a larger scope of attack is required to cause more impact, imposing more actions on the attacker that can potentially reduce their stealthy movement.

To assess processing performance, we also evaluated the processing time of packets with and without specification compliance (Scenario 1 and Scenario 2). For compliance with the specification (Scenario 1), each packet monitored by SIDS is processed on average at 0.3 ms with an insignificant standard deviation. With invalid traffic (Scenario 2), each packet is processed in an average of 1.5 ms with also insignificant standard deviation. The reason for this discrepancy is that when a packet violates the specification,

Table 3 Confusion table of experiments

Scenarios	TP	TN	FP	FN
1	0	200	0	0
2-a	115	0	0	0
2-b-I	10	0	0	0
2-b-II	0	0	0	10

several steps are triggered in the reporting mechanism to extract alert-relevant information, which is written to the alert log.

In addition, we have also performed a comparison with other intrusion detection approaches, which is shown in Table 4. However, due to the lack of a standardized benchmark evaluation for countermeasures against cyber-attacks in SCADA systems, the comparison is qualitative.

The comparison compares our SIDS qualitatively with other approaches based on the following metrics:

- Tech.: describes the detection basis of the methodology.
- Proto.: describes which protocol is the main target of protection.
- Environ.: describes whether a simulated or physical testbed was used.
- Att.: describes on which basis the attack scenarios were designed.
- Mat.: describes the degree of readiness of the approach in likert-scale.
- Exp.: describes the flexibility to be adapted to other protocols in likert-scale.
- Det.: describes the degree of detection quality of the approach in likert-scale.
- Perf.: describes the performance level of the approach in likert-scale.

As the comparison shows, the conditions and environment under which the different approaches were evaluated are mostly different. The attack scenarios also diverge in their scope, vectors used, and interaction with operational equipment. The experiments conducted also differ within their respective environments where simulation was used with simplification and abstraction. Many of the approaches have a high degree of maturity and are capable of being deployed and operated in real grid environments. However, they lack the ability to be extended to other protocols. The performance of the approaches shows the recognition capabilities of packets within the time span 0.1 ms to 1 s, and the detection quality is also in the medium range, which is mainly due to the high FN. Thus, the evaluation suggests that our SIDS enables reliable detection of cyber-attacks within a reasonable time.

Discussion

The results show that for normal operation, our SIDS has not triggered any (false) alert messages. Deviations were only caused by a too narrow RTT range and should be considered when carefully setting this parameter for detection quality.

Table 4 Comparison with other intrusion detection approaches

Ref.	Tech.	Proto.	Environ.	Att.	Mat.	Exp.	Det.	Perf.
Al Balushi et al. (2016)	Ontology	Modbus TCP	Simulation	Mixed	M	L	M	L
Cruz et al. (2016)	Machine-learning	Modbus TCP	Testbed	Protocol	H	H	M	H
Udd et al. (2016)	Specification	IEC-104	Simulation	Channel	H	L	M	H
Yang et al. (2016)	Specification	IEC 61850	Testbed	Packet	H	M	L	H
Adepu and Mathur (2018)	Automata	Eth/IP	Testbed	Location	H	H	L	N/A
Lin et al. (2016)	Semantic	DNP3	Simulation	Control	H	L	M	L
Wang and Feng (2018)	Time series	IEC-104	Simulation	SCADA	L	L	M	N/A
our SIDS	Specification	IEC-104	Testbed	FDI	H	H	H	M

In the attack-induced scenario (Scenario 2-b-II), where the attacker knows which addresses and IOA entries are valid, SIDS will have difficulty detecting them if the manipulated values are within the technical specification. However, any deviation from the addresses defined in the specifications will lead to high detection rates. In general, the detection quality is very dependent on the provided SB. The given structure of the SB, which defines the exact addressing for each allowed connection, are very strict rules that detect all connections that are not explicitly allowed. Attacks from outside with limited knowledge of the technical specifications of infrastructures can thus be reliably detected.

To create perfect spoofing conditions, the attacker must maintain complete consistency and compliance with the specification, which requires extensive knowledge. Furthermore, the attacker must perform prior steps, such as reconnaissance and lateral movement, to persist in the process network, potentially leaving traces in the communication layer. In the context of situational awareness for intrusion detection, our SIDS can act as a low-level sensor that provides domain-specific indicators of multi-staged cyber-attacks. Alerts can be centrally processed with other indicators from other IDS sensors through a correlation system based on Security Information and Event Management (SIEM) to reconstruct the attack sequence (Sen et al. 2021a, 2022).

While our evaluation focuses on IEC-104, the proposed SIDS can also be used for other SCADA protocols such as IEC-61850. The semantics of SB is provided by GIM, where the adaptation of a new protocol requires the mapping process of the data and the fields of the protocol. Thus, an appropriate mapper must be developed to reference semantic data with protocol fields. In addition, AM can generally be adapted to stateful communication such as TCP-based protocols, where packet flows can be described with state transitions.

Conclusion

In the context of power grids transitioning to SGs, countermeasures against sophisticated cyber-attacks based on reliable detection mechanisms are required. To this end, we present a SIDS that uses a graph-based specification to holistically encapsulate the SG infrastructure to detect cyber-attacks. We discuss the design and subsequent implementation of our SIDS, which consists of a DPI component and an AM. Using our implementation, we evaluated the detection quality within a physical testbed for different scenarios under attack and normal conditions.

Our main findings are that our SIDS approach can reliably detect attackers injecting false data into intercepted IEC-104 channels. The performance and detection quality show the advantages of an approach SIDS and was validated in our study. Moreover, the disadvantage of high knowledge provisioning overhead is reduced by our novel approach of coupling infrastructure modeling with SIDS. Future work includes investigating different methods for detecting FDI in a cooperative, neighborhood-oriented manner. In addition, the generated alerts of the proposed SIDS will also be investigated in terms of providing a reliable basis for a higher-level correlation system for reconstructing complex attack campaigns.

About this supplement

This article has been published as part of Energy Informatics Volume 5 Supplement 1, 2022: Proceedings of the 11th DACH+ Conference on Energy Informatics. The full contents of the supplement are available online at https://energyinformatics.springeropen.com/articles/supplements/volume-5-supplement-1.

Author contributions

Conceptualization: ÖS; methodology: ÖS, ML, FS; validation: ÖS, ML, FS, MH; formal analysis: ML, FS, ÖS; investigation: ML, FS, ÖS, MH; resources: ML, FS, ÖS; data curation: ÖS, ML, FS; writing—original draft: ÖS; writing—review and editing: ÖS, ML, FS, MH, DvdV, IH, AU; visualization:ÖS, IH; supervision: ÖS, MH, AU; project administration: MA, DvdV; funding acquisition: MA. All authors read and approved the final maniscript.

Funding

This work has partly been funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK) under project funding reference 0350028.

Availability of data and materials

No data and materials are published.

Declarations

Competing interests

The authors declare that they have no competing interests.

Published: 7 September 2022

References

Adepu S, Mathur A (2018) Distributed attack detection in a water treatment plant: method and case study. IEEE Trans Dependable Secure Comput 18(1):86–99

Akshaya S et al. (2019) A study on zero-day attacks

Al Balushi A, McLaughlin K, Sezer S (2016) OSCIDS: an ontology based SCADA intrusion detection framework. In: SECRYPT

Almseidin M, Piller I, Al-Kasassbeh M, Kovacs S (2019) Fuzzy automaton as a detection mechanism for the multi-step attack. Int J Adv Sci Eng Inf Technol 9(2):575–586

Anwar M, Borg A, Lundberg L (2021) A comparison of unsupervised learning algorithms for intrusion detection in IEC 104 SCADA protocol. In: ICMLC. IEEE

Baraneetharan E (2020) Role of machine learning algorithms intrusion detection in WSNs: a survey. J Inf Technol 2(03):161–173

Bernd M, Buchholz S, Zbigniew A (2021) SMART GRIDS: fundamentals and technologies in electric power systems of the future. SPRINGER-VERLAG BERLIN AN, Axel-Springer-Strasse, Berlin

Bieniasz J, Sapiecha P, Smolarczyk M, Szczypiorski K (2016) Towards model-based anomaly detection in network communication protocols. In: ICFSP. IEEE

Bollig B, Katoen J-P, Kern C, Leucker M, Neider D, Piegdon DR (2010) libalf: the automata learning framework. In: CAV. Springer

Burgetová I, Matoušek P, Ryšavý O (2021) Anomaly detection of ICS communication using statistical models. In: CNSM. IEEE

Case DU (2016) Analysis of the cyber attack on the Ukrainian power grid. E-ISAC 388:1–29

Castellanos JH, Antonioli D, Tippenhauer NO, Ochoa M (2017) Legacy-compliant data authentication for industrial control system traffic. In: ACNS. Springer

Caswell B, Beale J (2004) Snort 2.1 intrusion detection. Elsevier, Alibris, Emeryville

Cook A, Janicke H, Smith R, Maglaras L (2017) The industrial control system cyber defence triage process. Comput Secur 70:467–481

Cruz T, Rosa L, Proença J, Maglaras L, Aubigny M, Lev L, Jiang J, Simões P (2016) A cybersecurity detection framework for supervisory control and data acquisition systems. IEEE Trans Ind Inform 12(6):2236–2246

Dang Q-V (2021) Improving the performance of the intrusion detection systems by the machine learning explainability. Int J Web Inf Syst. https://doi.org/10.1108/ijwis-03-2021-0022

Eckhart M, Ekelhart A (2018) A specification-based state replication approach for digital twins. In: CPS-SPC

Eder-Neuhauser P, Zseby T, Fabini J, Vormayr G (2017) Cyber attack models for smart grid environments. Sustain Energy Grids Netw 12:10–29

Escudero C, Sicard F, Zamaï É (2018) Process-aware model based IDSs for industrial control systems cybersecurity: approaches, limits and further research. In: ETFA. IEEE

Fernandes G, Rodrigues JJ, Carvalho LF, Al-Muhtadi JF, Proença ML (2019) A comprehensive survey on network anomaly detection. Telecommun Syst 70(3):447–489

Grammatikis PR, Sarigiannidis P, Sarigiannidis A, Margounakis D, Tsiakalos A, Efstathopoulos G (2020) An anomaly detection mechanism for IEC 60870-5-104. In: MOCAST. IEEE

Grigorchuk RI, Nekrashevych VV, Sushchansky VI (2000) Automata, dynamical systems, and groups. Trudy Matematicheskogo Instituta Imeni VA Steklova

Hokama WS, de Souza JS (2020) Cybersecurity for smart substation. In: T&D LA. IEEE

Holzinger A, Carrington A, Müller H (2020) Measuring the quality of explanations: the system causability scale (SCS). KI-Künstliche Intelligenz
IEC (2006) Telecontrol equipment and systems—part 5-104: transmission protocols-network access for IEC 60870-5-101 using standard transport profiles. IEC Standard
IEC (2016) IEC 62351 security standards for the power system information infrastructure. Technical report, WG15, IEC TC57
IEC (2018) Power systems management and associated information exchange—data and communications security—Part 3: communication network and system security—profiles including TCP/IP. Technical report, IEC 62351-3
Infosecmatter: IEC104 client utility—metasploit. https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/client/iec104/iec104
Khraisat A, Gondal I, Vamplew P, Kamruzzaman J (2019) Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity 2(1):1–22
Klaer B, Sen Ö, van der Velde D, Hacker I, Andres M, Henze M (2020) Graph-based model of smart grid architectures. In: SEST. IEEE
Krause T, Ernst R, Klaer B, Hacker I, Henze M (2021) Cybersecurity in power grids: challenges and opportunities. Sensors 21(18):6225
Kus D, Wagner E, Pennekamp J, Wolsing K, Fink IB, Dahlmanns M, Wehrle K, Henze M (2022) A false sense of security? Revisiting the state of machine learning-based industrial intrusion detection. In: CPSS
Lashkari AH, Zang Y, Owhuo G, Mamun M, Gil G (2017) CICFlowMeter. Github
Lin H, Slagell A, Kalbarczyk ZT, Sauer PW, Iyer RK (2016) Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. IEEE Trans Smart Grid 9(1):163–178
Matoušek P (2017) Description and analysis of IEC 104 protocol. Faculty of Information Technology, Brno University o Technology, Tech. Rep
Matoušek P, Havlena V, Holík L (2021) Efficient modelling of ICS communication for anomaly detection using probabilistic automata. In: IM. IEEE
MICIE (2020) Modbus application protocol specification V1. 1b3. 2012. MICIE Consortium
Mochalski K (2020) Cybersicherheit der Netzleittechnik: Ergebnisse aus Stabilitäts-und Sicherheitsaudits. Realisierung utility 4.0, vol 1. Springer, Axel-Springer-Strasse, Berlin
Mohan SN, Ravikumar G, Govindarasu M (2020) Distributed intrusion detection system using semantic-based rules for SCADA in smart grid. In: T&D. IEEE
Ourahou M, Ayrir W, Hassouni BE, Haddi A (2020) Review on smart grid control and reliability in presence of renewable energies: challenges and prospects. Math Comput Simul 167:19–31
Profitap HQ BV ProfiShark 1G+ datasheet. https://www.profitap.com/wp-content/uploads/ProfiShark-1G-Plus-Datasheet.pdf
Rohith R, Moharir M, Shobha G (2018) SCAPY-A powerful interactive packet manipulation program. In: ICNEWS . IEEE
Scheben F, Genzmer K, Mohrdieck J-M, Möller J (2017) Status of the national implementation of the NC RfG in Germany. In: NEIS Conference 2016. Springer
Sen Ö, van der Velde D, Wehrmeister KA, Hacker I, Henze M, Andres M (2021a) Towards an approach to contextual detection of multi-stage cyber attacks in smart grids. In: SEST. IEEE
Sen Ö, Van Der Veldc D, Linnartz P, Hacker I, Henze M, Andres M, Ulbig A (2021b) investigating man-in-the-middle-based false data injection in a smart grid laboratory environment. In: ISGT Europe. IEEE
Sen Ö, van der Velde D, Wehrmeister K, Hacker I, Henze M, Andres M (2022) On using contextual correlation to detect multi-stage cyber attacks in smart grids. Sustain Energy Grids Netw 32:100821
Tanveer A, Sinha R, Kuo MM (2020) Secure links: secure-by-design communications in IEC 61499 industrial control applications. IEEE Trans Ind Inform 17(6):3992–4002
Tharwat A (2020) Classification assessment methods. Appl Comput Inform 17(1):168–192
Todeschini MG, Dondossola G (2020) Securing IEC 60870-5-104 communications following IEC 62351 standard: lab tests and results. In: AEIT. IEEE
Udd R, Asplund M, Nadjm-Tehrani S, Kazemtabrizi M, Ekstedt M (2016) Exploiting bro for intrusion detection in a SCADA system. In: CPS-SPC
van der Velde D, Henze M, Kathmann P, Wassermann E, Andres M, Bracht D, Ernst R, Hallak G, Klaer B, Linnartz P (2020) Methods for actors in the electric power system to prevent, detect and react to ICT attacks and failures. In: ENERGYCon. IEEE
van der Velde D, Sen Ö, Hacker I (2021) Towards a scalable and flexible smart grid co-simulation environment to investigate communication infrastructures for resilient distribution grid operation. In: SEST. IEEE
Verma A, Ranga V (2020) Machine learning based intrusion detection systems for IoT applications. Wirel Pers Commun 111(4):2287–2310
Wang D, Feng D (2018) Intrusion detection model of SCADA using graphical features. In: IAEAC. IEEE
Williams TJ (1994) The Purdue enterprise reference architecture. Comput Ind 24(2–3):141–158
Wolsing K, Wagner E, Saillard A, Henze M (2022) IPAL: breaking up silos of protocol-dependent and domain-specific industrial intrusion detection systems. In: RAID
Yang Y, McLaughlin K, Littler T, Sezer S, Im EG, Yao Z, Pranggono B, Wang H (2012) Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems
Yang Y, Xu H-Q, Gao L, Yuan Y-B, McLaughlin K, Sezer S (2016) Multidimensional intrusion detection system for IEC 61850-based SCADA networks. IEEE Trans Power Deliv 32(2):1068–1078
Zuech R, Khoshgoftaar TM, Wald R (2015) Intrusion detection and big heterogeneous data: a survey. J Big Data 2(1):1–41

Publisher's Note