Investigating Man-in-the-Middle-based False Data Injection in a Smart Grid Laboratory Environment

Ömer Sen*, Dennis van der Velde*, Philipp Linnartz†, Immanuel Hacker*
Martin Henze‡, Michael Andres*, Andreas Ulbig†
*Digital Energy, Fraunhofer FIT, Aachen, Germany
Email: {oemer.sen, dennis.van.der.velde, immanuel.hacker, michael.andres}@fit.fraunhofer.de
†High Voltage Equipment and Grids, Digitalization and Energy Economics, RWTH Aachen University, Aachen, Germany
Email: {philipp.linnartz, andreas.ulbig}@iaew.rwth-aachen.de
‡Cyber Analysis & Defense, Fraunhofer FKIE, Wachtberg, Germany
Email: martin.henze@fkie.fraunhofer.de

***Abstract*—With the increasing use of information and communication technology in electrical power grids, the security of energy supply is increasingly threatened by cyber-attacks. Traditional cyber-security measures, such as firewalls or intrusion detection/prevention systems, can be used as mitigation and prevention measures, but their effective use requires a deep understanding of the potential threat landscape and complex attack processes in energy information systems. Given the complexity and lack of detailed knowledge of coordinated, timed attacks in smart grid applications, we need information and insight into realistic attack scenarios in an appropriate and practical setting. In this paper, we present a man-in-the-middle-based attack scenario that intercepts process communication between control systems and field devices, employs false data injection techniques, and performs data corruption such as sending false commands to field devices. We demonstrate the applicability of the presented attack scenario in a physical smart grid laboratory environment and analyze the generated data under normal and attack conditions to extract domain-specific knowledge for detection mechanisms.**

***Index Terms*—Cyber-Physical System, Smart Grid Cyber Security, Man-in-the-Middle Attack, False-Data-Injection**

I. Introduction

The ongoing transformation of electric power systems in smart grids (SGs) is driven primarily by the increasing penetration of volatile distributed energy resources (DERs) and new load situations created by prosumer entities [1]. Thus, grid operators face new challenges, including congestion and bidirectional power flow situations, which require timely active grid operation through the increased use of information and communication technology (ICT) [2], [3]. Consequently, the increasing dependence on the ICT infrastructure and system complexity therefore generates new threats. For example, the secure operation of the power grid is at risk due to incorrect configuration of communication links, faulty grid automation algorithms, or cyber attacks [2], [4]. In this new threat landscape for SGs, cyber-attack vectors that exploit the vulnerabilities of advanced ICT infrastructures occupy a central position in power supply threat scenarios [1], [5], [6]. Severe cyber-attacks aim to compromise the integrity, confidentiality, and availability of grid operations to distort operational decisions, obtain sensitive information, or delay or disrupt the functioning of services [7]. As cyber-attacks become more diverse and sophisticated [6], and information and operational technologies continue to converge, novel cross-domain security strategies are needed to ensure a reliable power supply. For instance, intrusion detection systems (IDS), next-generation firewalls, role-based access control, and encryption methods aid to address system vulnerabilities, detect various cyber-attacks, take the appropriate countermeasures, and identify the entities involved within the attack [8]. The development and validation of such cross-domain security strategies depends on the availability and quality of information from all relevant attack scenarios [9]. However, insights and information from real cyber incidents in power grids that provide characteristics and signatures of the attack are limited to the scientific community for privacy and security reasons [5] and are usually generated by studying synthetically replicated attack scenarios [9]. Since it is difficult to replicate attack scenarios that have severe consequences in a productive, operating power grid for investigation purposes, an isolated, secure and controllable environment is required that provides valid properties not only within the energy domain but also of the ICT. Consequently, a test environment of an energy information system with its primary and secondary technology components is required, in which attack scenarios affecting both the ICT and the electrical grid are deployed and investigated to extract useful characteristics for the development of appropriate countermeasures. Therefore, in order to gain useful insights from experiments that can be used to develop and validate data-driven countermeasures such as IDS, detailed documentation of the underlying infrastructure and attack scenarios, including both ICT and process views, is essential for meaningful adoption of experiment results for security measures. In this paper, we present a structured and comprehensive approach to conduct experiments under normal operating and attack conditions in a cyber-physical SG lab environment and gain useful knowledge for countermeasures such as process-aware IDS from a targeted analysis. The

Author's version of a paper accepted for publication in Proceedings of 2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe).

structure as well as the contribution of this paper are:

1) We provide an overview of relevant cyber-security issues in SGs, as well as current challenges in legacy-compliant security measures for traditional power grids (Section II).
2) We show and describe a laboratory environment that replicates an SG use case with high ICT penetration for conducting cyber-security investigations (Section III).
3) We present and discuss a structured and traceable setup for performing Man/Machine-in-the-Middle (MITM)-based False Data Injection (FDI) attacks in SG lab environments to gain insights into complex attack techniques (Section IV).
4) We demonstrate the feasibility of the developed attack tool and investigate communication- and process-level characteristics for detecting such attacks using novel IDS approaches. (Section V).

II. Cyber Security in Smart Grids

As a basis for our work, we provide a brief overview of the core components and their security issues in SG utilities and highlight existing challenges in prominent security measures.

A. Cyber Security in Power Process Networks

Process networks in SGs provide interconnectivity between control centers, field devices, and assets on which Supervisory Control and Data Acquisition (SCADA) systems are responsible for monitoring and controlling automatic operations in transmission or a distribution substation [10]. In particular, communication standardized via industrial protocols such as IEC 60870-5-104 (IEC-104) or DNP3 is carried out via Master Terminal Units (MTUs) with the logical controllers such as Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs), which in turn are responsible for monitoring the processes in the industrial environment by interacting with the sensors and actuators. Initially designed for use in narrowly defined networks, IEC-104 as a legacy industrial protocol does not provide any security functionalities, in particular neither encryption nor authentication [11]. This means that process data is transmitted unencrypted, allowing unauthorized third parties to monitor and analyze data traffic (e.g., reading out certain memory locations), which can have severe consequences for the provision of a reliable power supply. In addition, many commands of the protocol, such as reset command, query commands, and read commands, do not have authentication mechanisms built in, allowing unauthorized access. One exploit of the aforementioned protocol vulnerability would be the MITM-based FDI, which refers to an attacker who could intercept the logical connection between communicating devices (e.g., between MTU and RTU) [12] and inject their messages (e.g., a false command) through an MITM attack [13]. Given the lack of security mechanisms in the IEC-104 protocol, the attacker would then be able to read, modify, inject, or discard sent or new messages between the intercepted endpoints [14].

B. Security Measures and Challenges

In view of the prominent security issues in process networks, various research and discussions are being conducted to secure IEC-104 communications based on the security principles of the IEC 62351 standard [15]. In particular, the integration of cipher suites, as used in the Transport Layer Security (TLS) protocol, is mandated by the IEC 62351 standard to secure end-to-end communication between two connection terminals through secure key exchange, encryption, and authentication [16]. However, traditional process networks usually consist of performance-limited devices, so the trade-off between security and performance can result in critical real-time requirements not being met [17]. An approach which does not actively interfere with the process network is an IDS, which typically monitors network traffic with passive sniffing and detects attack indicators over the monitored network [18]. Known detection methods in this area include identifying attack indicators by comparing captured traces to a specification or model representing either system behavior under normal operating conditions (i.e., anomaly-based) or attack scenarios (i.e., misuse-based), with any discrepancy or match resulting from this comparison leading to the generation of an alert [9]. However, these detection approaches require a comprehensive, robust, and diverse data foundation and understanding in terms of attack signatures from real-world cyber incidents or system behavior under normal operating conditions [19]. In this paper, we present a MITM-based FDI attack scenario in a real laboratory setup and study the observations during the experiment to provide useful insights and information that can be used within a process-aware detection mechanism to effectively detect such attacks.

C. Related Work

The security issues regarding the study of the impact of MITM-based FDI attacks in SGs have been investigated in several directions. In particular, research has been conducted in this regard to investigate FDI-based attack scenarios in narrowly defined power system testbeds [20], also emulating MITM-based attacks for IEC-104 security and risk assessments [10]. Moreover, further work is being done to present an approach to providing a data generation framework focused on DNP3 MITM-based injection attacks [21] and data and control manipulation attacks over IEC 61850 in secondary substations [22]. In addition, studies have been conducted on synthesis frameworks for specific attack vectors [23] as well as on an automated marking process for deployed protocol-specific attack [13]. In this context, research on stealthy MITM attacks for FDI in DNP3 or Profinet is also conducted in a cyber-physical test environment to analyze the impact on latency [24] or generate datasets for data-driven detection approaches [25]. Many of the related works involve the study of cyber-attacks on power grids for data generation and consequence analysis. However, most of them lack sufficient coverage of the generated data within the experiments themselves, especially from a process perspective,

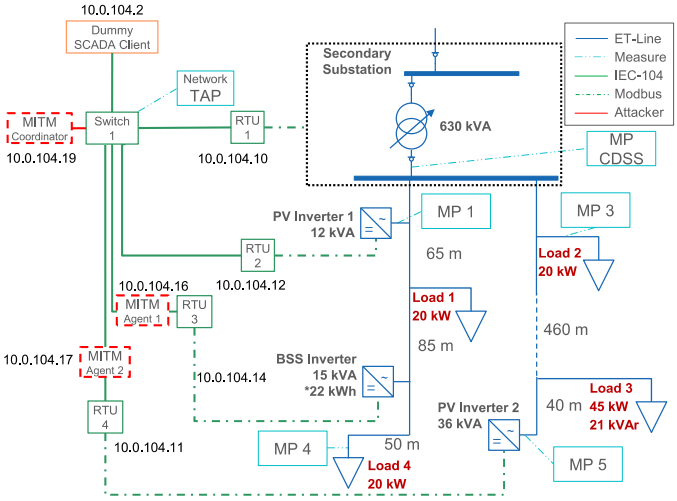

Fig. 1. Our SG testbed setup replicates an MV/LV distribution grid and consists of multiple DER assets, resistive/inductive loads, and a controlling field device within a SCADA network.

and the majority of experiments are conducted in a (partially) virtualized testbed. In this work, we provide insight and analysis of MITM-based FDI attack experiments in terms of their ICT and process data components performed in a physically deployed IEC-104 SG laboratory environment consisting of typically used components.

III. Laboratory Environment

To replicate MITM-based FDI attack scenarios, we present and describe an SG lab environment and experiment setup in this section. Due to the homogeneous structure of process networks in the energy sector and the selectively chosen assets in our testbed setup, our experimental results provide high applicability for security measures in this domain. Our experiment aims to cover later stages of cyber-attacks, assuming that physical access to the network perimeter has already been gained in worst-case scenarios.

A. Smart Grid Testbed Setup

The SG testbed replicates an medium voltage (MV) / low voltage (LV) distribution grid equipped with networked assets. All components in our cyber-physical testbed are physically deployed with no virtual simulation of equipment. We present the underlying ICT and electrical topologies in Figure 1. Within the testbed setup, the electrical assets consist of a 10 kV / 0.4 kV controllable distribution secondary substation (CDSS) with a 630 kVA transformer, 22 kWh battery storage system (BSS), 12 kVA and 36 kVA photovoltaic inverters (PVs), and several resistive/inductive loads. The LV grid is configured with a radial topology consisting of two strings, the first of which is equipped with a 200 m, and resp. 500 m NAYY cable. In addition, the MV/LV grid is equipped with five integrated three-phase current and voltage measuring points (MPs) with built-in power analyzers for current and voltage measurements as well as power quality measurements (e.g., harmonics). The DER assets are commercial inverters with adjustable feed-in profiles and programmable reactive power control (Q(U), Q(P), cos ϕ) fed from DC sources. These assets are controlled and monitored via RTUs with Modbus. In addition, the testbed's process network consists of an ICT switch that connects the RTUs to the Dummy SCADA Client (DSC). In this regard, the DSC in our testbed is replicated by an IEC-104 MTU that sends control and query commands to RTUs. Consequently, our testbed setup provides realistic behavior of secondary and primary technology components in terms of communication and electrical energy exchange, enabling cross-domain investigation of MITM-based FDI attack scenarios.

B. Experiment Setup

Within this work, the described testbed will be the subject of MITM-based FDI attack experiments performed with a specially developed MITM tool (cf. Section IV). As shown in Figure 1, two MITM agents are placed to intercept one or more communication channels, i.e., placed between RTU 3 and Switch 1 and between Switch 1 and RTU 4. To capture the traffic of different communication channels within the process network, we also place network taps on the ICT switch and MITM agents. The MITM coordinator is directly connected to Switch 1 and uses the existing ICT infrastructure of the testbed to communicate with the MITM agents. We perform the following experiment:

(a) Testbed operation with MITM deployment, but no active interference with systems. During this phase of the experiment ($t < 500$s), the DSC sends stepwise power reduction control commands with set-points of 30% and 50% nominal power to the PV Inverter 2 (PVI2) via RTU 4 at approximately 360s. At about 480s, the DSC sends 21% and 42% of the rated power discharge command to the Battery Storage System Inverter (BSSI) via RTU 3.

(b) Testbed operation with an active MITM performing FDI. Within this experimentation phase ($t > 500$s), the MITM coordinator sends action packets to MITM Agent 2, instructing it to send a set-point command of 100% at about 600s to the PVI2. MITM Agent 1 is instructed at approximately 750s to issue a control command with a set-point of -42% nominal power to the BSSI.

IV. Man-in-the-Middle-based False Data Injection

As a basis for our FDI attack experiments, we developed a special MITM tool for IEC-104 for transparent physical interception. The implementation is based on worst-case assumptions, where the attacker surreptitiously intercepts the communication on already layer 1. Our MITM-attack tool, as shown in Figure 2, follows a coordinator-agent architecture, where the coordinator remotely controls the behavior of agents (located between two target endpoints) via certain action packets (cf. Figure 3). The action packets received via TCP connections are used to determine which actions the agent has to perform (e.g., manipulate measured values or inject new control commands). They also contain application rules, such as for the inject action a collection of parameters needed for local IEC-104 package forgery. To bridge the

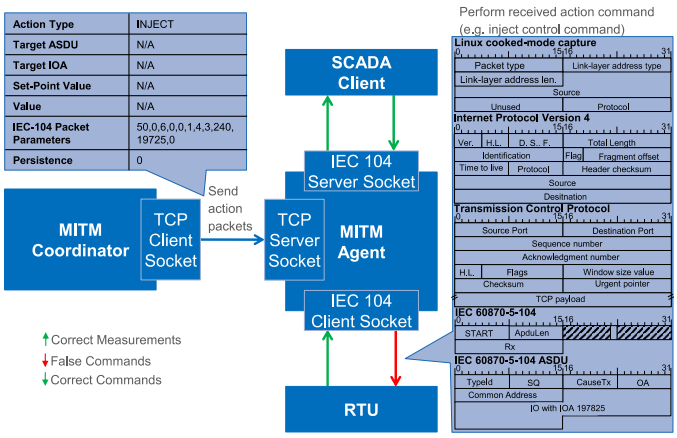

Fig. 2. The MITM agent sits on the communication path between a RTU and the MTU (e.g., on a compromised network switch) and is instructed by the MITM coordinator to perform actions such as manipulating, injecting, or collecting transmitted or new data.

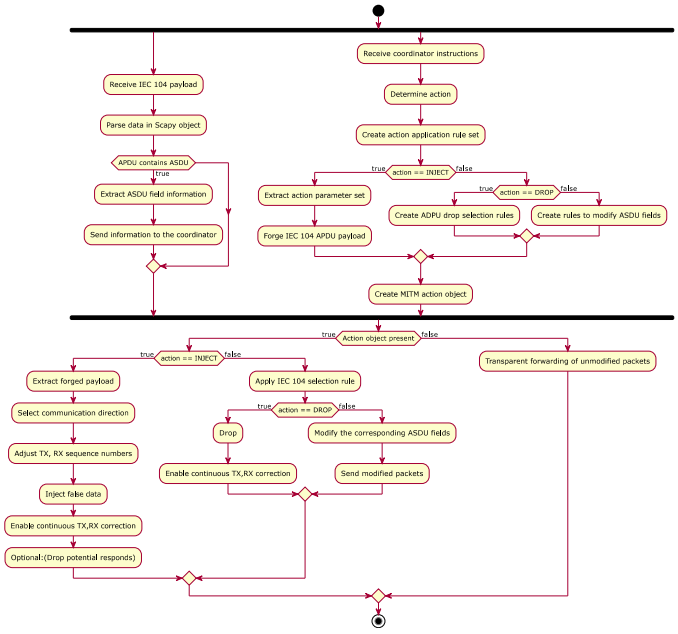

Fig. 3. High-level representation of MITM agent logic interacting with MITM coordinator to execute remotely received instructions.

target communication channel, the agent must operate as an inline bridge [26], i.e., take a hybrid role and provide counterpoints to the respective MTU and RTU endpoints to establish and maintain the connection and perform transparent proxying. The design of our MITM tool is based on transparent proxying to enable consistent protocol-compliant and selective forwarding of intercepted traffic. Therefore, our MITM tool intercepts the connection between the MTU and RTU endpoints via a virtual network bridge based on a Linux operating system using the bridge utilities. Since our MITM agent intercepts directly on a Layer 1 basis, we assign the agent's two physical network interfaces, the incoming client-side interface and the outgoing origin-server-side interface, to the newly created bridge interface. The bridged interfaces share an IP address provided by the bridge interface, which the MITM coordinator uses to reach the MITM agent. Then, to selectively lift IEC-104 traffic for the FDI, incoming packets on a bridged interface that are to be forwarded to another bridged interface are instead intercepted and forwarded through the BROUTING chain of ebtables when the IEC-104 protocol is associated. Thus, when IEC-104 traffic is detected in the incoming packets arriving at a (forwardable) interface, the packet flow is marked and policy routing is used depending on the directionality of the bridged interfaces. In the following, transparent proxying via TPROXY for inbound packets is needed to force the acceptance of packets to foreign IP addresses, i.e., intercept connections between clients (MTUs) and servers (RTUs) without being visible. Hereby, inbound transparency describes being transparent to connections that enter the proxy, while outbound transparency describes being transparent to connections that originate from the proxy. To allow our FDI application to access the IEC-104 packets, the marked traffic is routed back to the localhost application of the MITM agent via a policy routing table through the loopback interface. In the Python-based FDI application, transparent TCP sockets are used to read the forwarded IEC-104 data, even if this data is not intended for the host itself. Consequently, to intercept the communication channel between the RTU and MTU endpoints, the MITM agent opens the sockets as a counter endpoint for connection establishment by first providing a server-side socket that listens for connection requests from the MTU. When the connection between the MTU and the MITM agent is established, the MITM agent acts as a client and continuously sends connection requests to the RTU. If the connection to the RTU is successful, the MITM agent forwards the data internally to the MTU passing through the MITM agent application. In this phase, Scapy [27] is used to manipulate the intercepted IEC-104 communications, allowing selective high-level manipulation of the Application Service Data Unit (ASDU) payload by parsing the packet bytes into an accessible structured Python object and converting them back into bytes for forwarding to the appropriate destination endpoints. In addition, the injection of new IEC-104 packets is also based on Scapy, which allows modular, protocol-compliant packet forgery according to external parameter sets. However, actively changing the payload size of packets or transmitted frames in the communication channel, e.g., for inject or drop actions, requires stateful continuous correction of certain protocol fields such as checksum or sequence numbers. By converting the socket instances into Scapy socket streams, no adaptation within the underlying Ethernet/IP/TCP protocol layers is required, as Scapy takes care of the consistent correction. However, at the IEC-104 application level, the transmitted - TX, received - RX sequence numbers within the Application Protocol Control Information (APCI) must be continuously corrected, depending on the security functions within the IEC-104 endpoint applications. This correction is done at the level of the FDI script, where the amount of sent and received Application Protocol Data Unit (APDU) packets of each communication direction is counted and adjusted according to

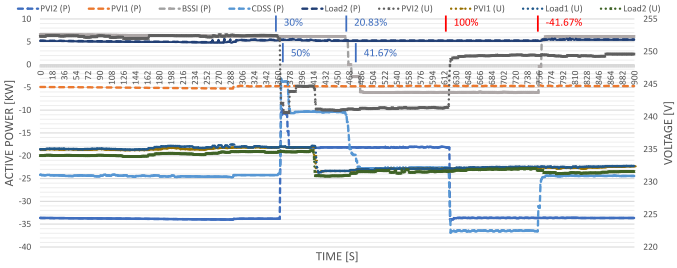

Fig. 4. Recorded power and voltage measurements at MP sites and commands sent by DSC and MITM agents are shown, with the actions of FDI occurring at 600s with 100% and 750s with −41.67% set-point value.

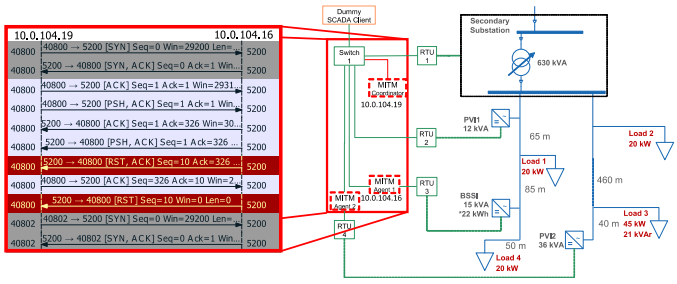

Fig. 5. Flowchart of observed communication within the C2 infrastructure between MITM coordinator (10.0.104.19) and MITM agent (10.0.104.16).

the amount of injected or discarded packets. Based on our approach, we are able to replicate Command and Control (C2)-based attack scenarios to deploy distributed MITM-based agents that perform transparent IEC-104 communication interception with remote control capabilities, forming the basis for coordinated attacks.

V. Analysis for the Detection of MITM-Based FDI

Using MITM-attack tool for IEC-104, we performed the experiment outlined in Section III-B and now present and discuss the corresponding experiment results. The sample data recorded during the experiment, i.e., active power and voltage measurements at the MPs and the transmitted set-point commands (marked with corresponding normalized set-point at trigger times as defined in Section III-B), is depicted in Figure 4. As these results show, our MITM tool can successfully inject control commands to the respective RTUs via the MITM agents. Thus, the FDI actions instructed by the MITM coordinator affect the electrical network of our SG laboratory in the same way as normal control commands sent by the DSC, but with reversed operational goals (e.g., counteracting the operation of DSC). In the following analysis, we investigate the possibilities of detecting FDI using a sophisticated MITM attack and exploit these insights for the development of process-aware IDS. In the communication traces recorded at the network tap of Switch 1, we can observe the control commands sent by the DSC, but not those sent by the MITM tool. However, depending on the technical sophistication of the implementation, other indicators of the attack can potentially be extracted from the traces in addition to meta-analysis of communication behavior such as RTT and MAC/IP/port (in)consistencies. For example,

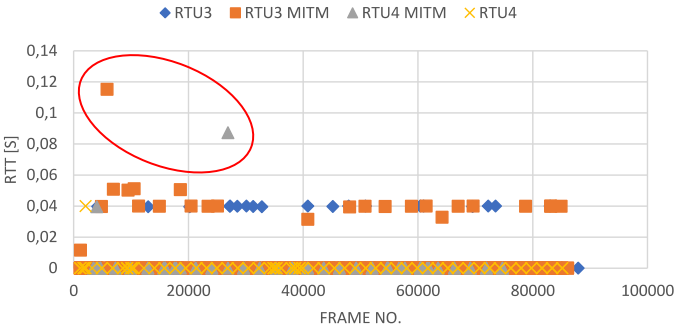

Fig. 6. RTT of IEC-104 traffic originating from RTUs 3 and 4, with and without interception by MITM agents, showing significant latency outliers.

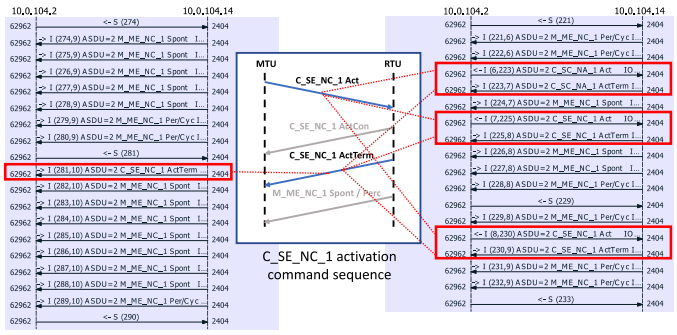

Fig. 7. Illustration of the sequence of activation of the set-point command C_SE_NC_1 between DSC and RTU 3 with MITM-based FDI (left) and the normal operation of DSC (right), showing anomalous flow behavior.

in our conducted experiments, we observed inconsistencies in MAC addresses between received packets from RTU 3 and sent packets from DSC in the recorded communication traffic within the process network. In terms of new network participants, we can also observe new inbound and outbound traffic generated by the C2 infrastructure of the built attack scenario by observing new IP addresses in the process network (cf. Figure 5). In addition, we can also observe the effect of MITM interception on the communication latency measured with the RTT, with clear outliers observed with MITM deployment (cf. Figure 6). Furthermore, anomalies in the communication flow may be observed based on the IEC-104 standard, which also dictates the communication behavior of, e.g., the IEC-104 server endpoint to return the received control commands to the IEC-104 client endpoint after successful processing with a cause of transmission (COT) of Activation Confirmation (ActCon) or Activation Termination (ActTerm). For example, as shown in Figure 7, in our experiment, we can observe that ActTerm packets are sent from RTU 3 without corresponding C_SE_NC_1 control commands with COT activation sent from DSC. In addition, the 15-bit sequence numbers in the I- and S-formatted APDU packets (TX, RX) can also reveal inconsistencies that can be used to indicate the MITM-based FDI. The receive sequence number RX of RTU 3 increases (approximately after 7000 frames) without the transmit number TX of DSC increasing, i.e., no I-frames are sent, indicating suspicious behavior at the protocol application level (cf. Figure 8). Consequently, our experiments provide several indicators of MITM-based FDI

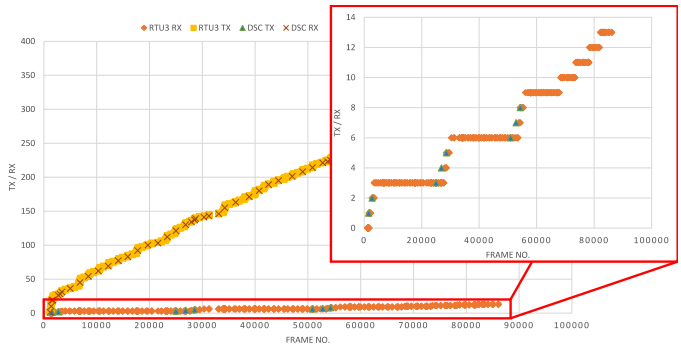

Fig. 8. Incremental sequence numbers of transmitted (TX) and received (RX) I-frames between RTU 3 and DSC indicating inconsistencies in tracked exchanged ASDU packets within the sequence numbers.

attacks, which can be detected by, e.g., stateful monitoring of communication flow, checking the consistency of IP and MAC addresses in bilateral communications, observing noticeable latency changes in communication traffic, checking new network participants with unknown IP addresses, and sequence number inconsistencies at the protocol application layer. In combination with plausibility and consistency checks of process data (e.g., consistency of measured values and operational plausibility of control commands), a cross-domain IDS approach with process awareness using knowledge from information and operational technology could be achieved. The experiments are based on worst-case assumptions for FDI via MITM, which can be successively relaxed to present additional attacker scenarios that provide further indications building on the discussed implications of this work. The findings presented in this paper have only emerged from a specific analysis of the communication and process data from the field experiments within our SG testbed.

VI. Conclusion

The development and validation of appropriate countermeasures against cyber-attacks in SGs require information and data from real attack scenarios. To lay a foundation to provide such data, we propose an SG laboratory environment consisting of primary and secondary technology components that enables a holistic investigation of cyber-security issues (Section III). In an effort to better understand the complex operations behind MITM-based FDI cyber-attacks, we have developed an MITM tool that uses basic FDI techniques to inject control commands into our SG lab environment (Section IV). We demonstrate the applicability and provide insights into our tool and environment by performing example attack scenarios consisting of a remote coordinator controlling multiple agents (Section V). Our results verify the functionality of the tool we developed and also provide insights into MITM-based FDI attacks that can be utilized in novel IDS approaches with domain-specific and stateful detection mechanisms. For instance, the MITM-based MITM was observed to produce inconsistencies in address fields within bilateral communications, application-level sequence numbers, and foreign network communications. Future work will address the modular extension of the ICT infrastructure to achieve greater diversity in terms of the components used, such as the extension of the process network with a meshed / ring topology, segmented into edge and SCADA networks. This also includes integrating security measures such as IDS, which use the results of this work in their detection mechanism to gain further insight into the applicability and effectiveness of novel detection approaches in practical environments.

Acknowledgments This work has partly been funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) under project funding reference 0350028.

References

[1] M. L. Tuballa *et al.*, "A Review of the Development of Smart Grid Technologies," *Renewable and Sustainable Energy Reviews*, 2016.
[2] D. van der Velde *et al.*, "Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures," in *IEEE ENERGYCon*, 2020.
[3] B. Klaer *et al.*, "Graph-based Model of Smart Grid Architectures," in *SEST*, 2020.
[4] D. U. Case, "Analysis of the Cyber Attack on the Ukrainian Power Grid," *E-ISAC*, 2016.
[5] L. Kotut *et al.*, "Survey of Cyber Security Challenges and Solutions in Smart Grids," in *CYBERSEC*. IEEE, 2016.
[6] J. Mendel *et al.*, "Smart Grid Cyber Security Challenges: Overview and Classification," *e-mentor*, 2017.
[7] X. Li *et al.*, "Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges," *IEEE Communications Magazine*, 2012.
[8] M. Henze *et al.*, "Poster: Cybersecurity Research and Training for Power Distribution Grids – A Blueprint," in *ACM CCS*, 2020.
[9] R. Zuech *et al.*, "Intrusion Detection and Big Heterogeneous Data: A Survey," *Journal of Big Data*, 2015.
[10] P. Radoglou-Grammatikis *et al.*, "Attacking IEC-60870-5-104 SCADA Systems," in *IEEE SERVICES*. IEEE, 2019.
[11] I. T. WG15, "IEC 62351 Security Standards for the Power system Information Infrastructure," 2016.
[12] M. Serror *et al.*, "Challenges and Opportunities in Securing the Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, 2020.
[13] N. R. Rodofile, "Generating Attacks and Labelling Attack Datasets for Industrial Control Intrusion Detection Systems." QUT, 2018.
[14] Y. Yang *et al.*, "Man-in-the-Middle Attack Test-bed Investigating Cyber-security Vulnerabilities in Smart Grid Scada Systems," 2012.
[15] M. G. Todeschini *et al.*, "Securing IEC 60870-5-104 Communications Following IEC 62351 Standard: Lab Tests and Results," in *AEIT*, 2020.
[16] I. I. 62351-3:2018/AMD1, "Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 3," 2018.
[17] A. Tanveer *et al.*, "Secure Links: Secure-by-Design Communications in IEC 61499 Industrial Control Applications," 2020.
[18] G. Fernandes *et al.*, "A Comprehensive Survey on Network Anomaly Detection," *Telecommunication Systems*, 2019.
[19] A. Khraisat *et al.*, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, 2019.
[20] S. Adepu *et al.*, "Epic: An Electric Power Testbed for Research and Training in Cyber Physical Systems Security." Springer, 2018.
[21] N. R. Rodofile *et al.*, "Framework for SCADA Cyber-attack Dataset Creation," in *Proceedings of the ACSW*, 2017.
[22] P. P. Biswas *et al.*, "A Synthesized Dataset for Cybersecurity Study of IEC 61850 Based Substation," in *IEEE SmartGridComm*. IEEE, 2019.
[23] V. Babu *et al.*, "Melody: Synthesized Datasets for Evaluating Intrusion Detection Systems for the Smart Grid," in *2017 WSC*. IEEE, 2017.
[24] P. Wlazlo *et al.*, "Man-in-the-middle attacks and defense in a power system cyber-physical testbed," *arXiv preprint arXiv:2102.11455*, 2021.
[25] M. Noorizadeh *et al.*, "A cyber-security methodology for a cyber-physical industrial control system testbed," *IEEE Access*, 2021.
[26] U. Böhme *et al.*, "Linux Bridge- Stp- Howto," *Revision 0.4. The Linux Documentation Project*, 2000.
[27] P. Biondi, "Packet Generation and Network Based Attacks with Scapy," *CanSecWest/core05*, 2005.