

Kummerow, André; Schäfer, Kevin; Gupta, Parul; Nicolai, Steffen;  
Bretschneider, Peter

**Combined network intrusion and phasor data anomaly detection for secure  
dynamic control centers**

---

<i>Original published in:</i>	Energies. - Basel : MDPI. - 15 (2022), 9, art. 3455, 16 pp.
<i>Original published:</i>	2022-05-09
<i>ISSN:</i>	1996-1073
<i>DOI:</i>	<a href="https://doi.org/10.3390/en15093455">10.3390/en15093455</a>
<i>[Visited:</i>	2023-05-03]



This work is licensed under a [Creative Commons Attribution 4.0 International license](https://creativecommons.org/licenses/by/4.0/). To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/>

---

## Article

# Combined Network Intrusion and Phasor Data Anomaly Detection for Secure Dynamic Control Centers

André Kummerow , Kevin Schäfer, Parul Gupta, Steffen Nicolai and Peter Bretschneider

Fraunhofer IOSB, IOSB-AST, Fraunhofer Institute of Optronics, System Technologies and Image Exploitation, 98693 Ilmenau, Germany; kevin.schaefer@iosb-ast.fraunhofer.de (K.S.); parul.gupta@iosb-ast.fraunhofer.de (P.G.); steffen.nicolai@iosb-ast.fraunhofer.de (S.N.); peter.bretschneider@iosb-ast.fraunhofer.de (P.B.)

\* Correspondence: andre.kummerow@iosb-ast.fraunhofer.de

**Abstract:** The dynamic operation of power transmission systems requires the acquisition of reliable and accurate measurement and state information. The use of TCP/IP-based communication protocols such as IEEE C37.118 or IEC 61850 introduces different gateways to launch cyber-attacks and to compromise major system operation functionalities. Within this study, a combined network intrusion and phasor data anomaly detection system is proposed to enable a secure system operation in the presence of cyber-attacks for dynamic control centers. This includes the utilization of expert-rules, one-class classifiers, as well as recurrent neural networks to monitor different network packet and measurement information. The effectiveness of the proposed network intrusion and phasor data anomaly detection system is shown within a real-time simulation testbed considering multiple operation and cyber-attack conditions.

**Keywords:** cyber-security; dynamic control centers; network intrusion detection; anomaly detection; cyber-physical systems; phasor measurement units



**Citation:** Kummerow, A.; Schäfer, K.; Gupta, P.; Nicolai, S.; Bretschneider, P. Combined Network Intrusion and Phasor Data Anomaly Detection for Secure Dynamic Control Centers. *Energies* **2022**, *15*, 3455. <https://doi.org/10.3390/en15093455>

Academic Editor: Piotr Kosowski

Received: 13 April 2022

Accepted: 7 May 2022

Published: 9 May 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

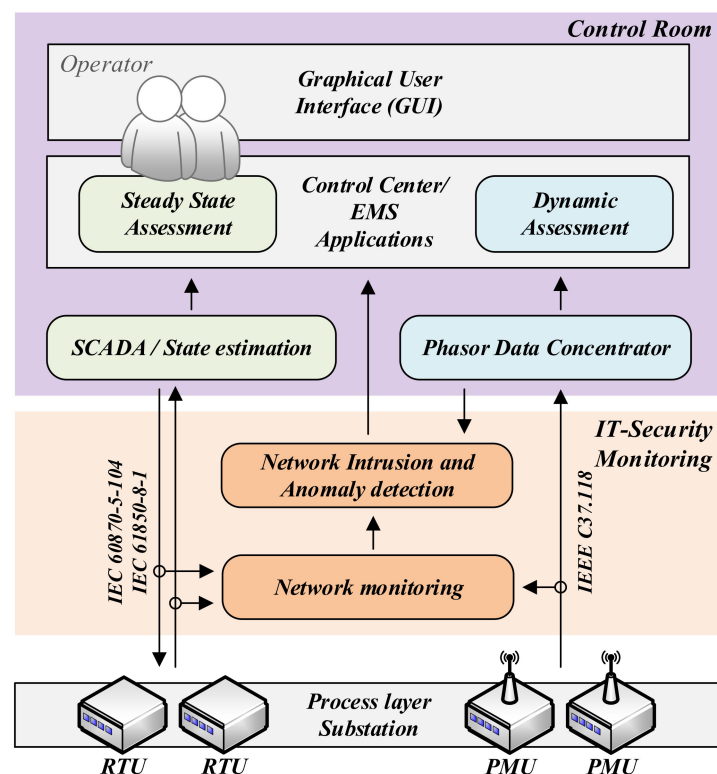
## 1. Introduction

### 1.1. Motivation

As introduced in [1–4], dynamic control centers extend traditional SCADA-based system architectures with new assistant functionalities (e.g., DSA, WAMS) to increase the situational awareness and to improve the grid operation to handle critical grid situations or disturbed system states. This requires the integration of additional monitoring and control components (e.g., PMUs, HVDC, FACTS), and an increased utilization of TCP/IP-based transmission protocols as well as automation processes. From a cyber-security perspective, new system threats arise in these architectures and can severely endanger the reliable operation of power transmission systems, especially during transient system states. This may include malfunctions (e.g., failures in protection devices), outages, violations of operational limits, or large-scale power supply interruptions with high financial impact [2,4]. Dynamic control center functionalities rely on secure communication links and trustworthy measurement and control data, which can be achieved by integrating efficient active and passive cyber-security measures.

### 1.2. Main Contributions

In contrast to conventional cyber-security solutions, special requirements have to be fulfilled to enable cyber-secure dynamic control centers. These include the inspection of specific protocols and data types as well as a combined monitoring of relevant network and process data. This study proposes an active cyber-security solution to enhance the reliability and robustness of control center functionalities for the steady state and dynamic assessment, as shown in Figure 1.



**Figure 1.** Basic concept of a cyber-secure dynamic control center architecture.

For this purpose, various detection algorithms have been developed within this study for the automatic online-monitoring of SCADA and PMU data transmission between the dynamic control center and substation level. This includes a combination of rule-based and machine-learning-based intrusion detection methods to analyze different information in the exchanged network packets at all protocol layers. Additionally, a novel recurrent-neural-network-based autoencoder and forecaster model is proposed to detect and correct data manipulations in high-resolution phasor measurements.

### 1.3. Paper Organization

The paper is organized as follows. Section 2 gives a brief overview of current network intrusion detection approaches for the relevant communication protocols IEC 61850 and IEEE C37.118. Then, Section 3 starts with a general overview of the proposed network intrusion and anomaly detection system. Afterwards, the different monitoring applications are explained in detail, including a specification- and anomaly-based NIDS as well as a recurrent-neural-network-based autoencoder and forecaster model. The evaluation in Section 4 describes the experimental setup based on a real-time simulation system with integrated communication links and different attack scenarios to assess the performance of the network and anomaly detection applications. Section 5 summarizes the results and gives a short outlook for necessary improvements and possible future work.

## 2. Cyber-Attack Detection in Power Transmission Systems

As already investigated in [2,4–9], dynamic control center architectures are faced with a wide range of possible active and passive cyber-attacks, which endanger different power system assets, including RTUs, PMUs, protection systems, or relays, as well as control room servers. Typical active or passive attack types comprise MITM attacks, data spoofings (e.g., insert fake commands to trip lines or manipulate PMU measurement information), eavesdropping, or reconnaissance attacks. As a common defense approach, intrusion detection systems (IDSs) enable the detection of malicious activities or events in ICT systems and mitigate cyber-attacks on critical infrastructures [10–12]. Specification-

based NIDS with various stateful or stateless deep packet inspections are proposed to detect cyber-attacks within the PMU data transmission based on the IEEE C37.118 protocol. These expert rules typically check IP addresses, TCP ports, device IDs, time or quality flags, measurement values, message sizes, and other meta information, which can be compared to derived nominal values from the CONFIG frame [13–15].

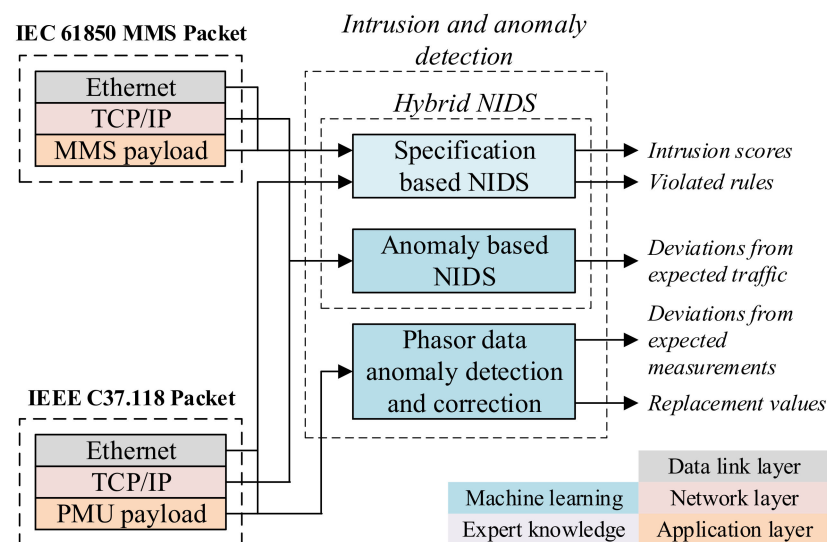
For the IEC 61850 data transmission, anomaly-based NIDS and specification-based NIDS approaches have been investigated. This includes the application of machine learning (e.g., neural networks) to analyze network traffic information such as round-trip times, packet sizes, or IP addresses as well as the derivation of expert rules from SCL files to check IP addresses, TCP ports, IDs, sequence numbers, and state numbers. Most of these approaches focus on the process bus communication within the substation, including sampled values and GOOSE messages [16–21].

The majority of existing cyber-attack detection algorithms focus only on the analysis of process information to recognize anomalies in the field measurements using well-known feature extraction and classification techniques (e.g., Bag-of-Patterns, SVMs, decision trees). In general, these solutions can be categorized as anomaly-based NIDS; however, they ignore important network information and limit the detection capabilities to specific cyber-attack types (e.g., DoS-attacks) [22–27].

### 3. Intelligent Monitoring and Analysis of Heterogeneous Network and Process Data

#### 3.1. System Overview

The proposed network intrusion and anomaly detection system for secure dynamic control centers consists of the following main applications: a specification- and anomaly-based NIDS, combined as hybrid NIDS application, and an anomaly detection and correction application for phasor data. Each application focuses on different information of incoming PMU and MMS network packets to detect different cyber-attacks by using expert knowledge and machine learning techniques. A general overview of the network intrusion and anomaly detection system is given in Figure 2.



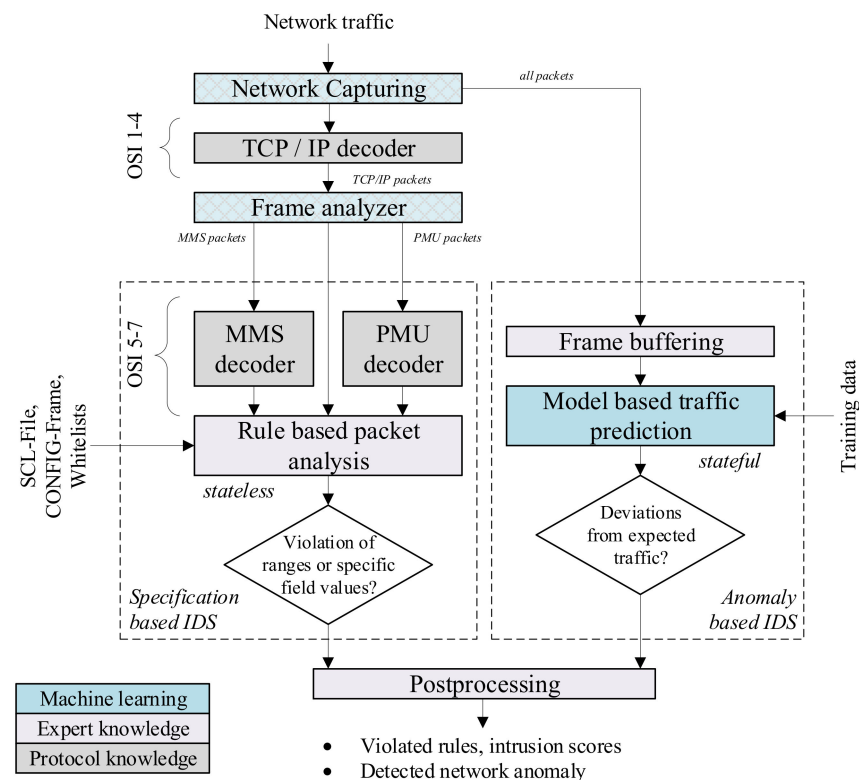
**Figure 2.** Main workflow and components of the network intrusion and anomaly detection system.

The *specification-based NIDS* uses expert rules to check specific protocol fields in all OSI layers of IEC 61850-8-1 (MMS) and IEEE C37.118 (PMU) network packets. The *anomaly-based NIDS* trains a one-class classification model using examples from normal and noncorrupted MMS and PMU network traffic. Representative features are derived from a stateful analysis of the data link and network layer of current and past network packets. More information regarding the network traffic processing as well as the integration of expert knowledge is given in the following subsections.

The application *phasor data anomaly detection and correction* (PADC) uses a recurrent-neural-network-based autoencoder and forecaster model to detect and replace the manipulated phasor data. In contrast to the previous applications, only the measurement data from the last layer of the incoming PMU network packets are analyzed. Several inputs are required for the different detection applications, including the extraction of CONFIG frames and SCL files, the incorporation of expert knowledge, as well as sufficient training data of noncorrupted network traffic. A detailed explanation of the applications is given in the subsequent subsections.

### 3.2. Hybrid Network Intrusion Detection System (Hybrid NIDS)

The basic architecture of the hybrid NIDS, which includes the specification-based NIDS and the anomaly-based NIDS applications, is shown in Figure 3.

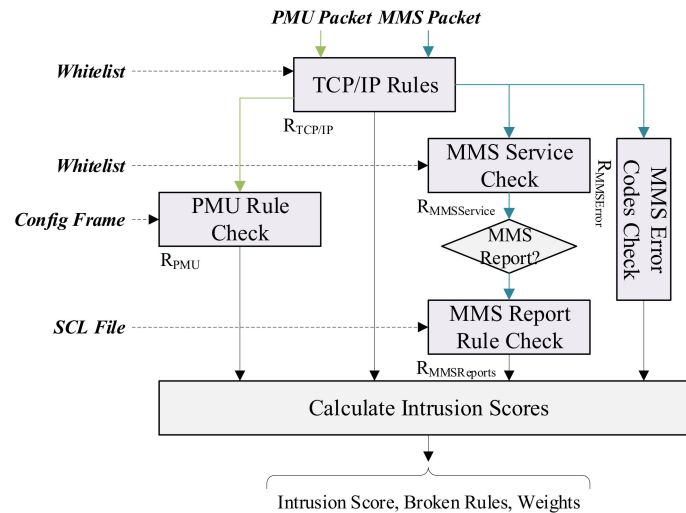


**Figure 3.** Basic architecture and workflow of the hybrid NIDS application.

In the first step, a *network interface* is defined to capture network traffic (online) or to read historical network records (offline) for a predefined set of machines (e.g., via the corresponding MAC addresses) within the network. The full network traffic is then passed to the *model-based traffic prediction module* within the anomaly-based NIDS for further processing and analysis. The necessary training data are provided as additional PMU and MMS network records. In case of the specification-based NIDS, only TCP/IP-based network packets are decoded and forwarded to the *rule-based packet analysis*. The *frame analyzer* explores the packet structure and checks for existing PMU or MMS application layers at OSI level 5 to 7, which are further decoded for the deep packet inspection in the specification-based NIDS. For the rule-based NIDS, additional expert knowledge is required, including whitelists (as user-defined text files with a specific format.), the IEC 61850 SCL description (as XML files usually created during the configuration of IEC 61850 communication links), as well as the PMU CONFIG frames (extracted and stored as object files at the start of the PMU communication). All three files are automatically loaded and parsed with the rule-based NIDS application. A final postprocessing step calculates the intrusion scores and collects the results from both NIDS applications.

### 3.2.1. Rule-Based Deep Packet Inspection

The main part of the specification-based NIDS is a multilevel and stateless deep network packet inspection of incoming PMU and MMS frames. The basic structure of the proposed expert rule system is given in Figure 4.



**Figure 4.** Basic architecture and workflow of the specification-based NIDS.

The rule system uses multiple rule sets,  $R$ , which are composed of different expert rules,  $r \in R$ , to inspect protocol information at different OSI layers. In the first step, all incoming PMU and MMS packets are passed to the *TCP/IP rule check* by applying the rule set  $R_{TCP/IP}$ . Thus, OSI layers 3 and 4 are inspected with the incorporation of a user-defined whitelist. Depending on the protocol type, all PMU packets are further processed in the *PMU rule check* by applying the rule set  $R_{PMU}$ , whose rules are automatically derived from the CONFIG frame. Various protocol information of the transmitted DATA frames is checked, including the checksum, the DATA frame size, the seconds of century (SOC) timestamp, the time quality flag, as well as the stream source ID-code. On the other hand, the MMS packets are passed to the *MMS service check* with the rule set  $R_{MMSService}$  using a user-defined whitelist as well as to the *MMS error codes check* with the rule set  $R_{MMSError}$ . In case of MMS reports, an additional rule set  $R_{MMSReports}$  is applied within the *MMS report rule check* incorporating IEC 61850 data model information from extracted SCL/SCD files. An overview of the different rules and associated rule weights is given in Table 1.

**Table 1.** Rule overview of the specification-based NIDS.

Rule Set	Rule Object	Rule Weight	Reference Value
TCP/IP	Protocol type	0.3	
TCP/IP	Source IP address	0.25	
TCP/IP	Destination IP address	0.25	defined in a whitelist
TCP/IP	Source TCP port	0.1	
TCP/IP	Destination TCP port	0.1	
PMU	Checksum	0.2	recalculated checksum
PMU	DATA frame size	0.2	derived from the CONFIG-Frame
PMU	SOC timestamp	0.2	current system time and user-defined delay
PMU	Time quality flag	0.2	time quality indication MSQ_TQ is "0" or "Normal operation"
PMU	Stream source ID codes	0.2	derived from the CONFIG-Frame
MMS service	MMS service type	[0, 1]	defined in a whitelist
MMS error	MMS error code	[0 ... 1]	
MMS reports	Integrity period	1/3	derived from SCL file
MMS reports	Transmission time	1/3	system time
MMS reports	Number of active report instances	1/3	derived from SCL file



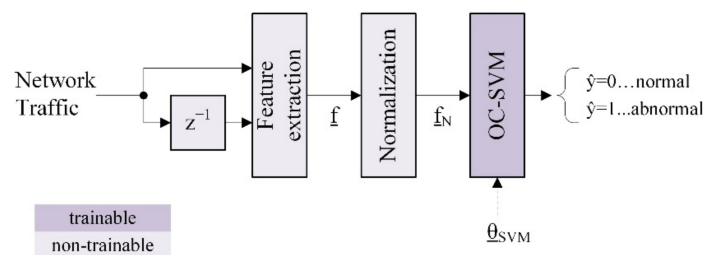
The rule weights  $w_r$  are specified by the expert to account for the relative importance of each rule within a given rule set  $R$ . In case of the MMS service type, only one specific service is possible for a given MMS message, which leads to a weight  $w = [0; 1]$ . In case of the MMS error codes, a weight  $w = [0 \dots 1]$  is associated with each possible error code (13 in total). A detailed description is omitted at this point. Within the postprocessing step, the inspection results  $\hat{y}$  ( $\hat{y} = 0$ : no violation;  $\hat{y} = 1$ : rule violation) of all rules  $r$  within a rule set  $R$  are summarized using the predefined weights  $w \in [0, 1]$  to create an intrusion score  $S_R$ :

$$S_R = \sum_{r \in R} w_r \cdot \hat{y}_r \text{ with } S_R \in [0 \dots 1]. \quad (1)$$

The computation of intrusion scores allows an aggregation of expert rules with different severity levels and impacts on the power system reliability.

### 3.2.2. Classification-Based Prediction of Network Traffic Anomalies

The traffic-prediction module uses a *one-class classification* approach to differentiate between normal and abnormal network packets. This is achieved with a one-class support vector machine (OC-SVM), which in contrast to binary SVMs uses a special optimization procedure to maximize the distance between a hyperplane and the zero point of the feature space [28]. For a given training dataset, the OC-SVM computes a closed decision boundary, such that observations or network packets with a high distance to that decision boundary are classified as abnormal, and vice versa. The basic structure of the proposed classification model is given in Figure 5.

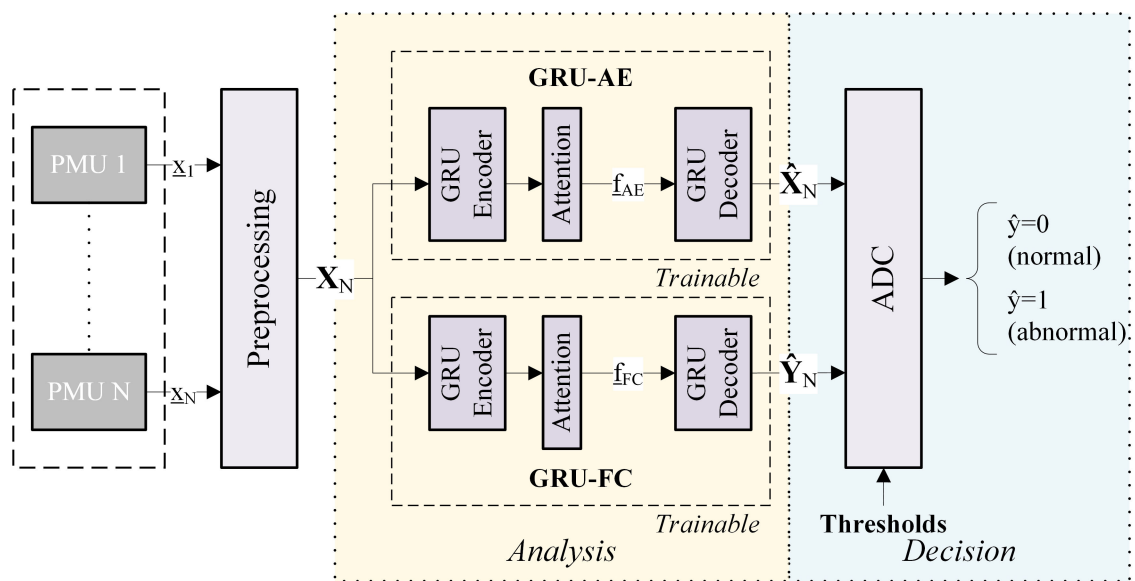


**Figure 5.** Basic architecture of the anomaly-based NIDS using an OC-SVM.

The anomaly-based NIDS takes the actual and last network packet to derive representative features to distinguish between normal and abnormal network packets. These features comprise the total packet length ( $f_1$ ), the size of the TCP payload ( $f_2$ ), and the time difference between two subsequent packets ( $f_3$ ). In case of non-TCP network packets, the size of the TCP payload is set to  $f_2 = 0$ . The resulting feature vector  $\underline{f} = [f_1, f_2, f_3]$  is standardized and passed to the OC-SVM with an RBF kernel to compute the class affiliation  $\hat{y} = 0$  (normal packet) or  $\hat{y} = 1$  (abnormal packet). Additional hyperparameters include the coefficient of the RBF kernel  $\gamma$  and a calibration factor for the learned class boundary  $\nu$ . In contrast to the rule-based NIDS from Section 3.2.1, a training phase is required to optimize the model parameters of the OC-SVM using PCAP files from historical and uncorrupted network traffic records. To mitigate data imbalances during the training, the samples are additionally weighted according to the frequency  $h_P$  of each of the  $N_P$  protocol types with  $w = 1/(N_P \cdot h_P)$ .

### 3.3. Recurrent-Neural-Network-Based Phasor Data Anomaly Detection and Correction (PADC)

The detection of data manipulations in PMU frequency, voltage magnitude, and voltage angle measurements is based on a combination of gated recurrent units (GRUs)-based autoencoder (GRUs-AE) and forecaster (GRUs-FC) models. The basic architecture of the PMU anomaly detection and correction (PADC) application is illustrated in Figure 6.



**Figure 6.** Conceptual overview and workflow of the PADC application.

The frequency, voltage magnitude, and voltage angle signals from  $N$  PMU sensors are acquired as input data over a fixed time period  $T$ . For each measurement type, an individual autoencoder–forecaster combination is trained on a normalized input matrix

$$X_N = [x_k]_{k=0}^{k=N} \text{ with } X_N \in \mathbb{R}^{T \times N}. \quad (2)$$

The GRU-AE and GRU-FC models are implemented as Seq2Seq-models with additional attention mechanisms to learn the normal system behavior based on the latent representations  $f_{AE}$  and  $f_{FC}$  for various contingencies and transient system states using uncorrupted PMU signals. The GRU encoder computes the hidden state vectors from the input signals and passes them to the attention model to extract the latent representations—as introduced in [3]. The GRU decoder uses these latent representations as well as the last hidden state of the encoder to compute the reconstructions or forecasts. The GRU-AE model  $f_{AE}$  reconstructs the input matrix  $X_N$  minimizing a reconstruction error

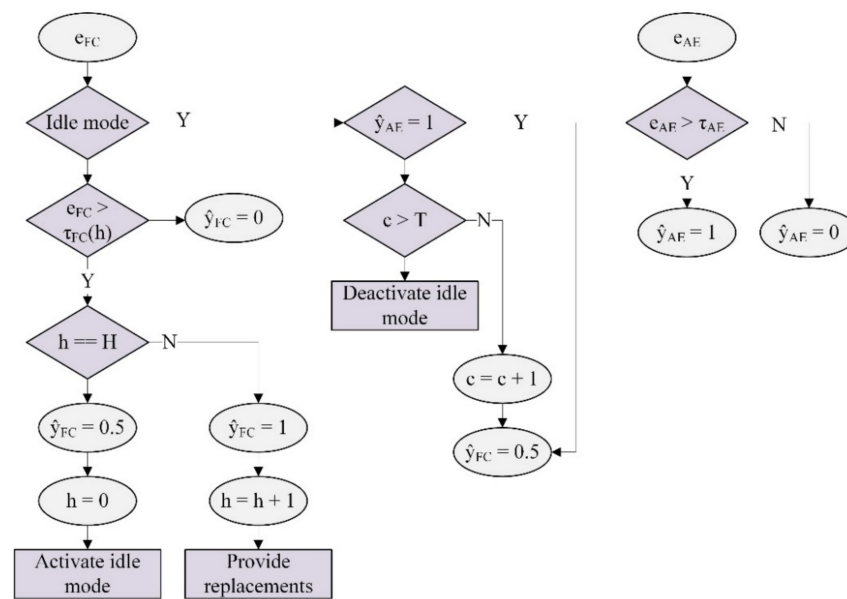
$$E_{AE} = |f_{AE}(X_N, \theta_{AE}) - X_N| = |\hat{X}_N - X_N|. \quad (3)$$

From the same input matrix, the GRU-FC model  $f_{FC}$  predicts the next  $H$  time steps by minimizing a forecast error

$$E_{FC} = |f_{FC}(X_N, \theta_{FC}) - Y_N| \text{ with } Y_N \in \mathbb{R}^{H \times N}. \quad (4)$$

The model parameters  $\theta_{AE}$  and  $\theta_{FC}$  are learned via backpropagation through time (BPTT). To distinguish between corrupted and noncorrupted measurement values, threshold values are derived from the unnormalized reconstruction and forecast error distributions after completion of the training phase. For this, a histogram-based error analysis is used based on the relative cumulative sums and the definition of a specific error tolerance to account for bad training examples. As a result, the sensor-dependent threshold values are extracted from the reconstruction errors; similarly, the sensor- and forecast-horizon-dependent threshold values are extracted from the forecast errors. In the application phase, these threshold values and the error results of the GRU-AE and GRU-FC models are passed to an *anomaly detection and correction (ADC) model* to achieve a time- and sensor-specific detection of abnormal PMU measurements and to provide additional replacement values. The principal workflow is given in Figure 7.





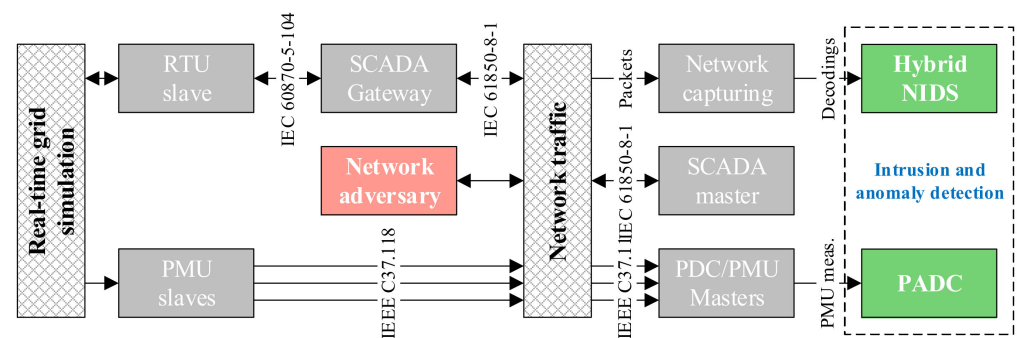
**Figure 7.** Principal workflow of the anomaly detection and correction (ADC) model.

Inside the ADC model, an “idle” mode is used to activate or deactivate the GRU-FC model depending on the currently used forecast horizon  $h$ , the GRU-AE prediction results  $\hat{y}_{AE}$ , and the time- and sensor-specific forecast error  $e_{FC}$ . An internal counter  $c$  checks if the number of currently processed observations reaches the sample window  $T$ . The GRU-FC model is deactivated (“idle” mode is active) if the maximum forecast horizon  $H$  has been reached, and activated (“idle”-mode is deactivated) if the GRU-AE model has not detected anomalies  $\hat{y}_{AE} = 0$  over the last  $T$  observations. Consequently, the GRU-AE model is primarily used to recognize the duration of the data manipulation, whereas the GRU-FC model recognizes the beginning of the data manipulation and distinguishes between corrupted and noncorrupted PMU sensors. Additionally, the forecast values of the GRU-FC model are used as replacement values.

## 4. Evaluation Studies

### 4.1. Experimental Setup and Attack Implementation

To evaluate the different applications of the proposed network intrusion and anomaly detection system, a transmission power system model based on [29] was implemented in a real-time simulation engine using HYPERSIM (OPAL-RT). The grid topology consisted of 6 machines, 17 busbars, and 26 branches divided into a southern and a northern subgroup and interconnected by 5 inter-area transmission lines. The overall experimental test setup is given in Figure 8.



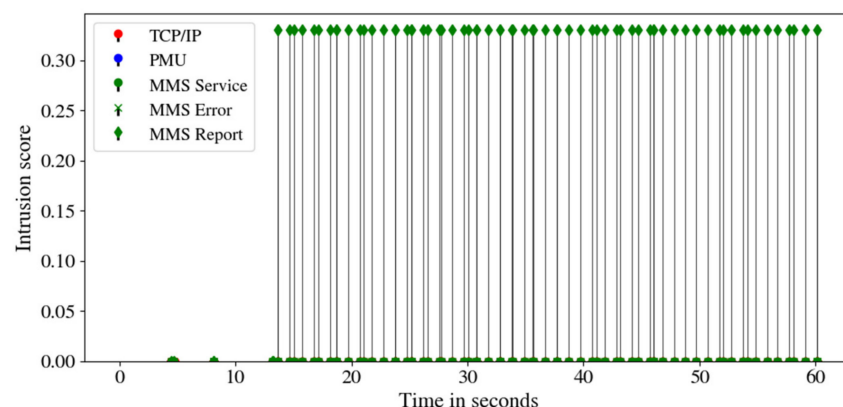
**Figure 8.** Overview of the experimental setup to evaluate the network intrusion and anomaly detection system.

The PMU slaves were implemented at all busbars to transmit frequency and voltage measurements using the IEEE C37.118 protocol at a fixed reporting rate of 25 f.p.s. One additional RTU slave was implemented at a single station to transmit voltage, current, as well as active and reactive power measurements via the IEC 60870-5-104 protocol using a fixed reporting every 2 s. A commercial gateway was used to convert the SCADA telegrams into the IEC 61850-8-1 (MMS) reports.

On the adversary side, a MITM attack was implemented to eavesdrop and manipulate arbitrary protocol information of the exchanged PMU and MMS network packets. The MITM attack uses ARP spoofing to redirect the network packets between the control center and substation level to an adversary. The adversary decodes the network packets, overwrites specific protocol information (e.g., measurement values), and sends the manipulated network packets to corrupt important monitoring or control applications. For simplification, no detailed attacker model was assumed in this work and no prior information about the system topology or historical measurements was available for the adversary. For the IEEE C37.118 protocol, the implemented attacks include various manipulations of frequency information and voltage phasor information, SOC timestamps, time quality flags, as well as ID-codes or station names in transmitted DATA frames. This goes beyond related investigations [15,23,24,26], which focused on data replays, packet drops, and timing attacks. Regarding the IEC 61850-8-1 (MMS) protocol, the attacker can compromise integer-based data attribute values and the time of entry in transmitted MMS reports.

#### 4.2. Attack Detection via Expert Rules

Some exemplary results of the specification-based NIDS are shown in case of a corrupted MMS traffic excerpt over 1 min—see Figure 9.



**Figure 9.** Intrusion scores of the specification-based NIDS for a corrupted MMS report communication.

In this case, the MMS report time is changed by the attacker (−1 h), which violates the corresponding MMS report rule. Since no other rules (e.g. TCP/IP or PMU rules) are affected, the resulting intrusion score equals the rule weight  $w_r = 1/3$ . A statistical summary of the network traffic capture is given in Table 2 with a high amount of ARP packets, which were periodically sent by the adversary to maintain the ARP spoofing.

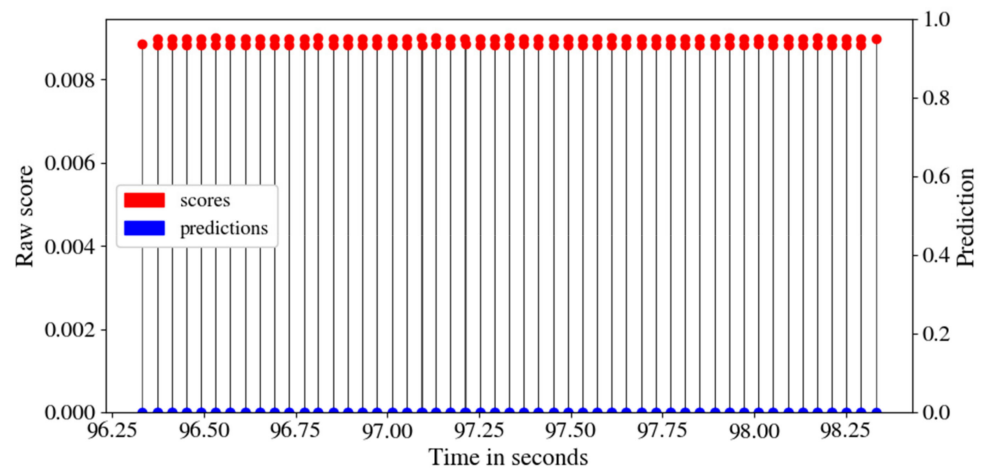
**Table 2.** Protocol counts and intrusion scores for the corrupted MMS report communication.

Protocol	Counts	$S_R$
ARP	40 (20.2 %)	-
TCP	82 (41.4 %)	0.00
MMS	76 (38.4 %)	0.33

#### 4.3. Attack Detection via Network Traffic Analysis

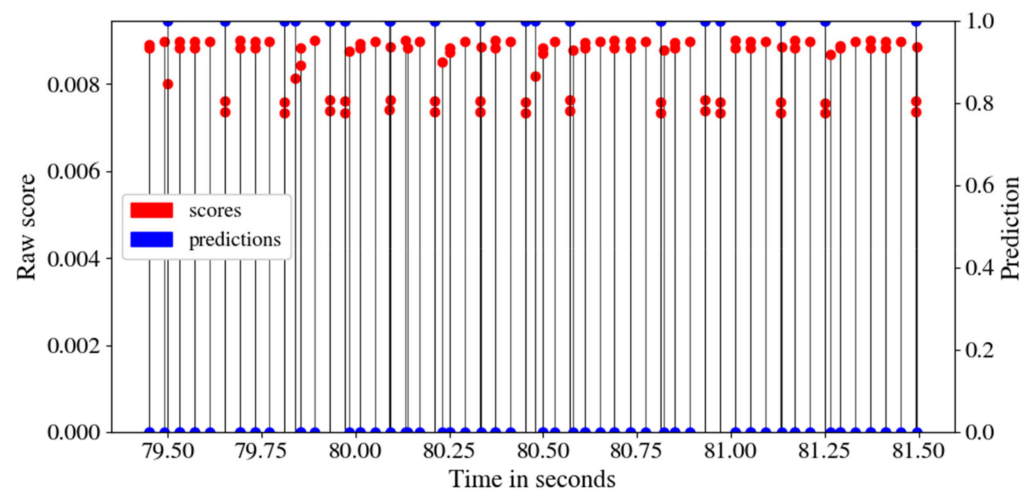
The evaluation of the anomaly-based NIDS focused on the amount of abnormal network packets, which were detected by the OC-SVM model during corrupted and

noncorrupted network traffic. Figure 10 shows the OC-SVM predictions  $\hat{y}$  and raw scores (results of the decision function) for an exemplary baseline network excerpt of about 2 s.



**Figure 10.** OC-SVM predictions and raw scores of the anomaly-based NIDS for a baseline network traffic.

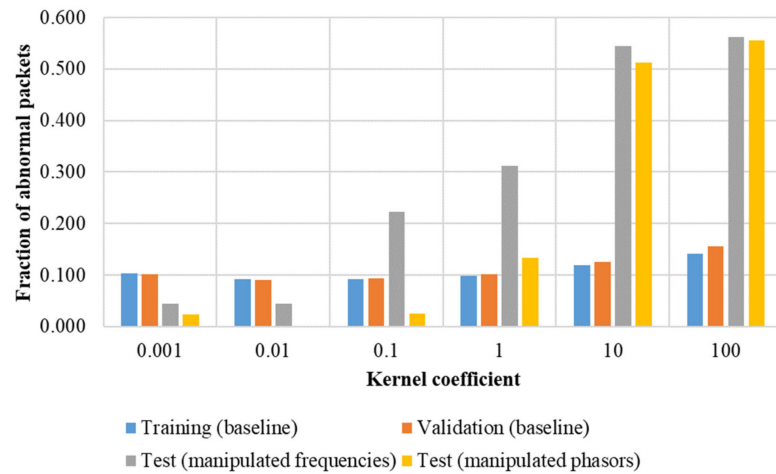
As can be seen, no network anomalies were detected for the baseline traffic, so  $\hat{y} = 0$  for all network packets. In contrast to that, Figure 11 shows the OC-SVM prediction results in case of corrupted network traffic by manipulating PMU frequency values within the MITM attack.



**Figure 11.** OC-SVM Predictions and raw scores of the anomaly-based NIDS for a corrupted PMU communication.

In that case, some of the network packets were detected as abnormal such that  $\hat{y} = 1$  and the corresponding score values decreased. The fraction of detected network anomalies in the total traffic  $\eta_A$  mainly depends on the chosen hyperparameters of the OC-SVM. This is illustrated in Figure 12 by comparing the  $\eta_A$  values for the baseline traffic during training/validation and the manipulated traffic during testing for different RBF kernel coefficients  $\gamma$ .

As it can be seen, high kernel coefficient values led to an increase in the number of abnormal network packets detected in both test data sets, while the number of detected normal network packets during training/validation remained almost constant. For kernel coefficients  $\gamma > 10$ , a good separation between normal and abnormal network packets was achieved.



**Figure 12.** Number of detected normal and abnormal network packets by the OC-SVM for baseline and corrupted PMU traffic datasets.

#### 4.4. Attack Detection via Phasor Measurement Analysis

To evaluate the PMU anomaly detection and correction application that was introduced in Section 3.3, the frequency and voltage phasor measurements were derived from the dynamic simulations (RMS) of the CIGRE TB 536 reference model (see Section 4.1). The training data included noncorrupted PMU signals with a fixed reporting rate of 25 f.p.s. and a window size of  $T = 25$  timesteps from the busbars of all 16 substations. The dynamic simulation was carried out for three operational points and 20 different contingencies (e.g., short-circuits, generator trips) taking the RMS signals until 20 s after the disturbance (approximately 30,000 training and validation samples). During testing, the data manipulations were created with arbitrary amplitudes, starting times, and durations for the simulated frequency, voltage magnitude, and voltage angle signals. Based on a simplified attacker model (see Section 4.1), the naïve attack patterns comprised positive and negative signal steps as well as the addition of Gaussian white noise. Additionally, the data manipulations could affect a single PMU or a randomly chosen subset of PMUs (concurrent or shifted manipulations).

To assess the performance of the GRU-AE and GRU-FC models, special evaluation metrics were defined based on the F1-score. In case of the GRU-AE model, the true positives  $t_{p,max}$ , false positives  $f_{p,max}$ , and false negatives  $f_{N,max}$  were calculated as maximum values over all  $N$  PMUs and summed up over all  $t$  time steps:

$$t_{p,max} = \sum_{t=0}^{t=T} \mathbb{I} \left( \max_{0 \leq n \leq N} \hat{y}_n(t) = 1, \max_{0 \leq n \leq N} y_n(t) = 1 \right), \quad (5)$$

$$f_{p,max} = \sum_{t=0}^{t=T} \mathbb{I} \left( \max_{0 \leq n \leq N} \hat{y}_n(t) = 1, \max_{0 \leq n \leq N} y_n(t) = 0 \right) \text{ and} \quad (6)$$

$$f_{N,max} = \sum_{t=0}^{t=T} \mathbb{I} \left( \max_{0 \leq n \leq N} \hat{y}_n(t) = 0, \max_{0 \leq n \leq N} y_n(t) = 1 \right). \quad (7)$$

The resulting F1-score follows with

$$\eta_{F1}^{AE} = \frac{t_{p,max}}{f_{p,max} + 0.5(f_{p,max} + f_{N,max})}. \quad (8)$$

In case of the GRU-FC model, the true positives  $t_p$ , false positives  $f_p$ , and false negatives  $f_N$  were calculated for all PMUs and time steps within the forecast horizon  $H$  without an additional aggregation, such that

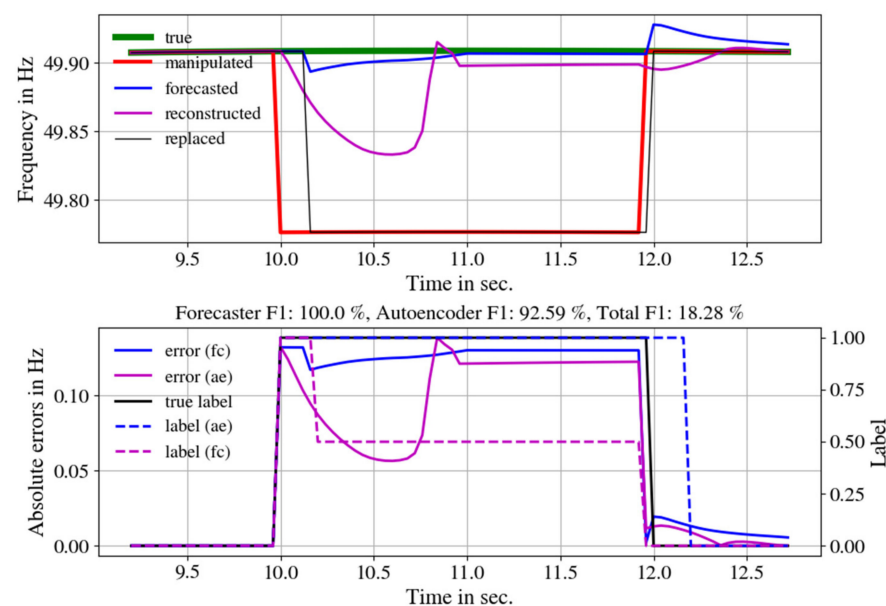
$$\eta_{F1}^{FC} = \sum_{n=0}^{n=N} \sum_{t=0}^{t=H} \frac{t_p^n(t)}{t_p^n(t) + 0.5(f_p^n(t) + f_N^n(t))}. \quad (9)$$

Table 3 lists the selected hyperparameters of the GRU-AE and GRU-FC models, which were derived from comprehensive training and validation runs.

**Table 3.** Selected hyperparameters of the autoencoder (GRU-AE) and forecaster (GRU-FC) models.

Hyperparameter	GRU-AE	GRU-FC
# of hidden units	40	40
Optimizer	RMSProp	RMSProp
Learning rate	0.001	0.001
Batch size	100	100
Forecast horizon	-	5 time steps

For a better understanding of the results, Figure 13 shows an exemplary negative frequency step manipulation for about 2 s at a single PMU.



**Figure 13.** Exemplary results of the GRU-AE and GRU-FC models for a frequency step manipulation.

The start of the data manipulation at 10 s simulation time was detected correctly by the GRU-AE and GRU-FC models, which can be seen in the sudden increase of the respective model errors as well as the change of the predicted labels. Additionally, the GRU-FC model successfully identified the corrupted PMU, leading to an F1-score of 100%. After exceeding the forecast horizon  $H$  at 100 ms, the GRU-FC model went into the “idle” mode (see also Section 3.3). The GRU-AE model failed to correctly predict the end of the data manipulation, such that the F1-scores decreased to approximately 92%. The total F1-score results of the GRU-FC model for different step and white noise manipulations as well as the number of corrupted PMUs are given in Table 4.

As it can be seen, the F1-scores only decreased slightly in case of a high number of corrupted PMUs. Larger differences arise when comparing the F1-scores between the step and white noise manipulations. Due to the stochastic behavior, white noise manipulations appear to be more difficult to be detected by the forecast model compared to step manipulations. This especially applies to the frequency and voltage angle signals. The corresponding GRU-AE model results are given in Table 5.

Compared to the GRU-FC model, higher drops of the F1-scores occur in case of a high number of corrupted PMUs but no significant differences arise between step and white noise components. Noticeably low F1-scores were achieved when performing step manipulations for the frequency or voltage angle signals of all PMUs.

**Table 4.** Total F1-scores of the GRU-FC model for different PMU step and noise manipulations.

Measurement Channel	1 PMU		6 PMUs		All PMUs	
	Steps	Noise	Steps	Noise	Steps	Noise
Frequency	0.84	0.65	0.91	0.65	0.81	0.62
Voltage magnitude	0.98	0.95	0.94	0.85	0.87	0.85
Voltage angle	0.93	0.73	0.88	0.78	0.82	0.71

**Table 5.** Total F1-scores of the GRU-AC model for different PMU step and noise manipulations.

Measurement Channel	1 PMU		6 PMUs		All PMUs	
	Steps	Noise	Steps	Noise	Steps	Noise
Frequency	0.85	0.87	0.89	0.88	0.26	0.74
Voltage magnitude	0.72	0.72	0.83	0.82	0.59	0.67
Voltage angle	0.86	0.75	0.87	0.85	0.50	0.75

#### 4.5. Real-Time Capability of the Proposed Applications

To evaluate the efficiency and applicability of the proposed hybrid NIDS (see Section 3.2) and phasor data anomaly detection and correction (PADC—see Section 3.3) application, comprehensive performance tests were performed to prove the real-time capabilities. Assuming a baseline network traffic, the average computational time for both applications is given in Table 6.

**Table 6.** Average processing time for the hybrid NIDS and PADC application.

Application	No. of Samples	Average Processing Time
Hybrid NIDS	55625	0.04 ms/sample
PADC	350	33.47 ms/sample

As it can be seen, the PADC application needs a lot more computational time due to the increased number of observations per sample and processing steps within the neural network models. Assuming a maximum data transmission rate of 25 f.p.s. for the PMU data communication, the real-time processing capability for both applications can be confirmed.

## 5. Conclusions and Outlook

This paper presents a novel network intrusion and phasor data anomaly detection system to protect dynamic control centers against cyber-attacks. Different algorithms have been developed, including a specification- and anomaly-based NIDS (hybrid NIDS) and a GRU-based autoencoder and forecaster model combination (PADC), to detect different adversarial network and measurement events within IEEE C37.118 and IEC 61850-8-1 (MMS) communication. For the evaluation, a real-time simulation engine was used to create network traffic for different steady-state and transient system states considering a 400 kV reference transmission grid. An adversary was integrated to implement MITM attacks for network infiltration and data manipulation purposes on both protocols. The results show the effectiveness of the proposed monitoring applications for different baseline and cyber-attack scenarios, including MMS report and PMU frequency and phasor measurement manipulations, during a steady and transient system operation.

Future work will include the implementation of a postprocessing algorithm to combine and assess the detection results of the different applications, which has been conceptually investigated in [30]. This can be a basis to further integrate comprehensive monitoring systems into existing decision processes of the system operation and to develop appropriate countermeasures against occurring cyber-attacks. Moreover, additional cyber-attack scenarios (e.g., DoS-attacks, timing-based attacks) including a more sophisticated attacker model should be integrated in the attack simulation, and additional MMS communication services (e.g.,



GETDATAVALUES) as well as existing benchmark methods should be considered in the experimental setup to further evaluate the detection capabilities of the proposed algorithms.

**Author Contributions:** Conceptualization, A.K. and K.S.; methodology, A.K., P.G. and K.S.; software, A.K. and K.S.; validation, A.K. and K.S.; formal analysis, A.K. and K.S.; investigation, A.K., P.G. and K.S.; resources, S.N. and P.B.; data curation, A.K., P.G. and K.S.; writing—original draft preparation, A.K. and K.S.; writing—review and editing, K.S., S.N. and P.B.; visualization, A.K.; supervision, S.N. and P.B.; project administration, A.K. and S.N.; funding acquisition, A.K., S.N. and P.B.. All authors have read and agreed to the published version of the manuscript.

**Funding:** This publication is a result of the project HyLITE (0350034) funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK).

**Conflicts of Interest:** The authors declare no conflict of interest.

## Nomenclature

### Abbreviations

ACSI	-	Abstract communication service interface
ADC	-	Anomaly detection and correction
ARP	-	Address resolution protocol
AE	-	Autoencoder
DSA	-	Dynamic security assessment
FACTS	-	Flexible AC transmission system
FC	-	Forecaster
GRU	-	Gated recurrent unit
ICT	-	Information and communication technology
ID	-	Identification
IP	-	Internet protocol
MITM	-	Man-in-the-middle
MMS	-	Manufacturing messaging specification
NIDS	-	Network intrusion detection system
PMU	-	Phasor measurement unit
RTU	-	Remote terminal unit
SCADA	-	Supervisory control and data acquisition
SCL	-	Substation configuration language
SVM	-	Support vector machine
TCP	-	Transmission control protocol
WAMS	-	Wide area monitoring system

### Variables

$c$	-	counter variable
$E_{AE}, e_{AE}$	-	Reconstruction error matrix or scalar
$E_{FC}, e_{FC}$	-	Forecast error matrix or scalar
$f$	-	Feature vector
$f_{AE}$	-	GRU autoencoder model
$f_{FC}$	-	GRU forecaster model
$H, h$	-	Forecast horizon
$N$	-	Number of PMU sensors
$S_R$	-	Intrusion score
$r$	-	Rule
$R_{MMSError}$	-	MMS error rule set
$R_{MMSReports}$	-	MMS report rule set
$R_{MMSService}$	-	MMS service rule set
$R_{PMU}$	-	PMU rule set
$R_{TCP/IP}$	-	TCP/IP rule set
$T$	-	Window size/sample size
$w$	-	Rule weight
$X_N$	-	(normalized) PMU signals
$\hat{y}, Y_N$	-	Prediction result

## References

1. Brosinsky, C.; Kummerow, A.; Naumann, A.; Kronig, A.; Balischewski, S.; Westermann, D. A new development platform for the next generation of power system control center functionalities for hybrid AC-HVDC transmission systems. In Proceedings of the 2017 IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017; pp. 1–5.
2. Kummerow, A.; Rösch, D.; Monsalve, C.; Nicolai, S.; Bretschneider, P.; Brosinsky, C.; Westermann, D. Challenges and opportunities for phasor data based event detection in transmission control centers under cyber security constraints. In Proceedings of the 2019 IEEE Milan PowerTech, Milan, Italy, 23–27 June 2019; pp. 1–6.
3. Kummerow, A.; Monsalve, C.; Brosinsky, C.; Nicolai, S.; Westermann, D. A Novel Framework for Synchrophasor Based Online Recognition and Efficient Post-Mortem Analysis of Disturbances in Power Systems. *Appl. Sci.* **2020**, *10*, 5209. [\[CrossRef\]](#)
4. Kummerow, A.; Rosch, D.; Nicolai, S.; Brosinsky, C.; Westermann, D.; Naumann, A. Attacking dynamic power system control centers—A cyber-physical threat analysis. In Proceedings of the 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 16–18 February 2021; pp. 1–5.
5. Huang, X.; Qin, Z.; Liu, H. A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis. *IEEE Access* **2018**, *6*, 69023–69035. [\[CrossRef\]](#)
6. Khan, R.; Maynard, P.; McLaughlin, K.; Laverty, D.; Sezer, S. Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research, Belfast, UK, 23–25 August 2016.
7. Zseby, T.; Fabini, J. Security Challenges for Wide Area Monitoring in Smart Grids. *E I Elektrotechnik Inf.* **2014**, *131*, 105–111. [\[CrossRef\]](#)
8. Ashok, A.; Govindarasu, M.; Wang, J. Cyber-Physical Attack-Resilient Wide-Area Monitoring, Protection, and Control for the Power Grid. *Proc. IEEE* **2017**, *105*, 1389–1407. [\[CrossRef\]](#)
9. Lin, H.; Deng, Y.; Shukla, S.; Thorp, J.; Mili, L. Cyber security impacts on all-PMU state estimator—A case study on co-simulation platform GECCO. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 587–592.
10. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecur* **2019**, *2*, 384. [\[CrossRef\]](#)
11. Buczak, A.L.; Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1153–1176. [\[CrossRef\]](#)
12. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. *IEEE Access* **2019**, *7*, 46595–46620. [\[CrossRef\]](#)
13. Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Pranggono, B.; Brogan, P.; Wang, H.F. Intrusion detection system for network security in synchrophasor systems. In Proceedings of the IET International Conference on Information and Communications Technologies (IETICT 2013), Beijing, China, 27–29 April 2013; pp. 246–252.
14. Sprabery, R.; Morris, T.H.; Pan, S.; Adhikari, U.; Madani, V. Protocol mutation intrusion detection for synchrophasor communications. In Proceedings of the Eight Annual Cyber Security and Information Intelligence Research Workshop: Federal Cyber Security R & D Program Thrusts, Oak Ridge, TN, USA, 8–10 January 2013; p. 1.
15. Khan, R.; Albalushi, A.; McLaughlin, K.; Laverty, D.; Sezer, S. Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid. In Proceedings of the 2017 IEEE Power & Energy Society General Meeting, Chicago, IL, USA, 16–20 July 2017.
16. Yoo, H.; Shon, T. Novel Approach for Detecting Network Anomalies for Substation Automation based on IEC 61850. *Multimed Tools Appl.* **2015**, *74*, 303–318. [\[CrossRef\]](#)
17. Yang, Y.; Xu, H.-Q.; Gao, L.; Yuan, Y.-B.; McLaughlin, K.; Sezer, S. Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks. *IEEE Trans. Power Deliv.* **2017**, *32*, 1068–1078. [\[CrossRef\]](#)
18. Ahmed, A.; Krishnan, V.V.G.; Foroutan, S.A.; Touhiduzzaman, M.; Rublein, C.; Srivastava, A.; Wu, Y.; Hahn, A.; Suresh, S. Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems. In Proceedings of the 2018 IEEE Industry Applications Society Annual Meeting (IAS), Portland, OR, USA, 23–27 September 2018; pp. 1–8.
19. Kreimel, P.; Tavalato, P. Neural Net-Based Anomaly Detection System in Substation Networks. In Proceedings of the 6th International Symposium for ICS & SCADA Cyber Security Research, Athens, Greece, 10–12 September 2019.
20. Hong, J.; Liu, C.-C.; Govindarasu, M. Integrated Anomaly Detection for Cyber Security of the Substations. *IEEE Trans. Smart Grid* **2014**, *5*, 1643–1653. [\[CrossRef\]](#)
21. Kwon, Y.; Lee, S.; King, R.; Lim, J.; Kim, H. Behavior Analysis and Anomaly Detection for a Digital Substation on Cyber-Physical System. *Electronics* **2019**, *8*, 326. [\[CrossRef\]](#)
22. Liu, L.; Esmalifalak, M.; Ding, Q.; Emesih, V.A.; Han, Z. Detecting False Data Injection Attacks on Power Grid by Sparse Optimization. *IEEE Trans. Smart Grid* **2014**, *5*, 612–621. [\[CrossRef\]](#)
23. Pan, S.; Morris, T.; Adhikari, U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. *IEEE Trans. Smart Grid* **2015**, *6*, 3104–3113. [\[CrossRef\]](#)
24. Adhikari, U. Event and Intrusion Detection Systems for Cyber-Physical Power Systems. Ph.D. Thesis, Department of Electrical and Computer Engineering, Mississippi State University, Starkville, MS, USA, 2015.

25. Pal, S.; Sikdar, B.; Chow, J. Detecting data integrity attacks on SCADA systems using limited PMUs. In Proceedings of the 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, Australia, 6–9 November 2016; pp. 545–550.
26. Ma, R.; Basumallik, S.; Eftekharijrad, S. A PMU-Based Data-Driven Approach for Classifying Power System Events Considering Cyberattacks. *IEEE Syst. J.* **2020**, *14*, 3558–3569. [[CrossRef](#)]
27. Zhu, R.; Liu, C.-C.; Hong, J.; Wang, J. Intrusion Detection Against MMS-Based Measurement Attacks at Digital Substations. *IEEE Access* **2021**, *9*, 1240–1249. [[CrossRef](#)]
28. Tax, D.M. One-Class Classification: Concept-Learning in the Absence of Counter-Examples. Ph.D. Thesis, Technical University of Delft, Delft, The Netherlands, 2001.
29. Cigre. Influence of Embedded HVDC Transmission on System Security and AC Network Performance: JWG C4/B4/C1.604. TECHNICAL BROCHURES. 2013. Available online: <https://e-cigre.org/publication/536-influence-of-embedded-hvdc-transmission-on-system-security-and-ac-network-performance> (accessed on 10 March 2022).
30. Kummerow, A.; Monsalve, C.; Rosch, D.; Schafer, K.; Nicolai, S. Cyber-physical data stream assessment incorporating Digital Twins in future power systems. In Proceedings of the 2020 International Conference on Smart Energy Systems and Technologies (SEST), Istanbul, Turkey, 7–9 September 2020; pp. 1–6.