# On the Detection of Cyber-Attacks in the Communication Network of IEC 61850 Electrical Substations

Zur Erlangung des akademischen Grades einer

**Doktorin der Ingenieurwissenschaften**

von der KIT-Fakultät für Informatik des
Karlsruher Instituts für Technologie (KIT)

genehmigte

**Dissertation**

von

M.Sc. Ghada Elbez

| | |
|---|---|
| Tag der mündlichen Prüfung: | 05. Mai 2022 |
| Referent: | Prof. Dr. Veit Hagenmeyer |
| Korreferentin:: | Prof. Dr. Klara Nahrstedt |

# Abstract

The availability of the data within the network communication remains one of the most critical requirement when compared to integrity and confidentiality. Several threats such as Denial of Service (DoS) or flooding attacks caused by Generic Object Oriented Substation Event (GOOSE) poisoning attacks, for instance, might hinder the availability of the communication within IEC 61850 substations. To tackle such threats, a novel method for the Early Detection of Attacks for the GOOSE Network Traffic (EDA4GNeT) is developed in the present work.

Few of previously available intrusion detection systems take into account the specific features of IEC 61850 substations and offer a good trade-off between the detection performance and the detection time. Moreover, to the best of our knowledge, none of the existing works proposes an early anomaly detection method of GOOSE attacks in the network traffic of IEC 61850 substations that account for the specific characteristics of the network data in electrical substations.

The EDA4GNeT method considers the dynamic behavior of network traffic in electrical substations. The mathematical modeling of the GOOSE network traffic first enables the development of the proposed method for anomaly detection. In addition, the developed model can also support the management of the network architecture in IEC 61850 substations based on appropriate performance studies. To test the novel anomaly detection method and compare the obtained results with available techniques, two use cases are used.

**Keywords:** anomaly detection, communication network, cyber-security, electrical substations, GOOSE, IDS, IEC 61850, IEC 62351.

# Acknowledgment

The present thesis carried out at the institute of Automation and applied Informatics, was initially supported by the Energy System Design (ESD) and KASTEL projects within the Helmholtz Association (HGF).

I would like to thank to my supervisor Prof. Dr. Veit Hagenmeyer, director of the Institute of Automation and applied Informatics (IAI), for his valuable scientific advice and support throughout my thesis. I am also very grateful to Prof. Dr. Klara Nahrstedt, Grainger Distinguished Chair of Engineering Professor in the Department of Computer Science at the University of Illinois at Urbana-Champaign (UIUC) and director of the Coordinated Science Laboratory (CSL), for the fruitful discussions and numerous suggestions that helped improve the quality of the present work. Special thanks to Prof. Dr.-Ing. Anne Koziolek, head of the Architecture-Driven Requirements Engineering group for accepting to be part of the examination community that helped evaluate the present thesis.

I would like also to express my acknowledgment to Dr. Hubert Keller and apl. Prof. Dr. Jörg Matthes for their support and their assistance throughout the work which was greatly appreciated. My special thanks to my colleagues, Kai, Kathrin, Qi, Oli, Sine, Aneeqa, Grushika, Hoomaan and Harun for the great scientific exchange and the excellent work culture. I wish to extend my thanks to our administrative and technical staff, particularly Andreas Hofmann and Bernadette Lehmann. A special thanks goes also to Dr.-Ing. Michael Kyesswa whose feedback and support helped significantly with the administrative procedure through the doctoral process.

I am very grateful for the rich scientific exchange with Dr. Atul Bohara and Dr. Alfonso Valdes during my research stay at the Information Trust Institute (ITI). Special thanks to Jonas, Hedi, Balint and Karuna for their active participation and commitment in setting up the software testbed where some of the experiments and the attack scenarios were performed.

Mostly, I want to express my very profound gratitude and love to my parents, my sister Syrine and my husband David for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of the present research work. This accomplishment would not have been possible without them. Thank you. I would like also to express my deep gratitude to my parents in-law Cecilia and Luis as well as to Tatiana, Kelly and Luigi for their kind words and the unforgettable moments shared together.

Eggenstein-Leopoldshafen, Mai 2022 Ghada Elbez

# Contents

# List of Figures

# List of Tables

# Acronyms

| Notation | Description |
|---|---|
| ACF | Auto-Correlation Function |
| AD | Anomaly Detection |
| AEG | Attack Execution Graph |
| APDU | Application Protocol Data Unit |
| ARFIMA | Auto-Regressive Fractionally Integrated Moving Average |
| ARIMA | Auto-Regressive Integrated Moving Average |
| CB | Circuit Breaker |
| CPS | Cyber-Physical Security |
| CUSUM | cumulative sum |
| DER | Distributed Energy Resources |
| DoS | Denial of Service |
| DPI | Deep Packet Inspection |
| DR | Detection Rate |
| EM | Expectation Maximization |
| FA | False Alarm |
| FDIA | False Data Injection Attack |
| FNR | False Negative Rate |
| FPR | False Positive Rate |
| GLRT | Generalized Likelihood Ratio Test |
| GOOSE | Generic Object Oriented Substation Event |
| HMI | Human-Machine Interface |
| i.i.d | independent and identically distributed |

| Notation | Description |
|---|---|
| ICS | Industrial Control System |
| ICT | Information and Communication Technology |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IPS | Intrusion Protection Systems |
| IT | Information Technology |
| KF | Kalman Filter |
| LAN | Local Area Network |
| LN | Logical Node |
| LRD | Long-Range Dependency |
| MITM | Man-In-The-Middle |
| ML | Machine-Learning |
| MLE | Maximum Likelihood Estimator |
| MMS | Manufacturing Message Specification |
| MU | Merging Unit |
| NRMSE | Normalized Root Mean Square Error |
| NSM | Network and System Monitoring |
| OT | Operational Technologies |
| P&C | Protection and Control |
| PDF | Probability Density Function |
| PLC | Programmable Logic Controller |
| ROC | Receiver Operating Characteristic |

| Notation | Description |
|---|---|
| RSA | Rivest-Shamir-Adleman |
| RT | Real-Time |
| SAS | Substation Automation System |
| SCADA | Supervisory Control And Data Acquisition |
| SCL | Substation Configuration Language |
| SCN | Substation Communication Network |
| SG | Smart Grid |
| SLD | Single Line Diagram |
| SNTP | Simple Network Time Protocol |
| SRD | Short-Range Dependency |
| SS | state space |
| SV | Sampled Values |
| TNR | True Negative Rate |
| TPR | True Positive Rate |
| WGN | White Gaussian Noise |

# List of Symbols

| Notation | Description |
|---|---|
| $a_i$ | An element of the $\mathbf{A}$ matrix |
| $\mathbf{A}$ | The state transition matrix $\in \mathbb{R}^{n \times n}$ |
| $B$ | Backshift operator |
| $\boldsymbol{B}$ | base rate representing the probability that there is an intrusion in the observed data set |
| $C$ | The ratio of the cost of an IDS failing to detect an intrusion and its cost when it generates a false alarm |
| $\mathbf{C}$ | The measurement matrix $\in \mathbb{R}^{g \times n}$ |
| $C_{exp}$ | The expected cost metric |
| $C_{ID}$ | The intrusion detection capability metric |
| $d$ | The difference coefficient |
| D | A selection term for the measurement equation |
| $\mathsf{e}[k]$ | Value of the sequence $\{\mathsf{e}[k]\}$ at discrete-time $k$ |
| $g$ | The CUSUM decision function |
| $\mathbf{H}$ | A selection matrix for the state equation |
| $H$ | Hurst parameter |
| $k$ | Discrete time index |
| $\mathbf{K}$ | The Kalman filter gain |
| $l$ | Delay order of the back-shift operator |
| $L$ | Length of non-overlaping intervals composing a time-series |
| $m$ | The level of aggregation |
| $N$ | Size of a time-series |
| $p$ | The order of the autoregressive polynomial |

| Notation | Description |
|---|---|
| $q$ | The order of moving the average polynomial |
| $\mathbf{Q}$ | A $n \times n$ covariance matrix of the states or process noise |
| R | The variance of the measurement or signal noise |
| $s[k]$ | Log-likelihood ratio increment |
| $S_i$ | The standard deviation of a subset x calculated over the interval $[i,u]$ |
| $S[k]$ | The novel score function |
| $W_{i,u}$ | The partial sum of a subset x calculated over the interval $[i,u]$ |
| $\mathit{x}$ | A stochastic time-series |
| $\mathit{x}^{(m)}$ | The aggregated sequence by $m$ of $\mathit{x}$ |
| $\boldsymbol{\alpha}[k]$ | The state vector at sample $k$ |
| $\beta$ | The signature of additive change on the estimates |
| $\Gamma(.)$ | The gamma (generalized factorial) function |
| $\gamma$ | The threshold for the statistical detector |
| $\Gamma_{\mathit{x}}$ | Gain matrix for $\Upsilon_{\mathit{x}}$ |
| $\delta$ | The signature of additive change on the states |
| $\boldsymbol{\varepsilon}$ | Model residuals |
| $\boldsymbol{\eta}[k]$ | A state disturbance vector $\in \mathbb{R}^{g \times 1}$ |
| $\Theta(B)$ | Moving average (MA) polynomial operator of an ARFIMA model |
| $\boldsymbol{\Theta}$ | The parameter vector |
| $\boldsymbol{\mu}$ | The conditional mean of the state vector |
| $\Xi_{\alpha}$ | Gain matrix for $\Upsilon_{\alpha}$ |
| $\rho$ | The signature of additive change on the innovations |

| Notation | Description |
|---|---|
| $\sigma_k$ | Variance matrix of the innovations |
| $\boldsymbol{\sigma}$ | The conditional variance of the state vector |
| $\sigma_e^2$ | Variance of a white Gaussian noise process |
| $\Upsilon_\alpha$ | Term to represent additive change in the states |
| $\Upsilon_x$ | Term to represent additive change in the observations |
| $\phi(B)$ | Autoregressive (AR) polynomial operator of an ARFIMA model |
| $\psi_j$ | Parameters of the MA part of the ARFIMA model for $j = 1,...,m$ |

# CHAPTER 1

## Introduction

The concept of Smart Grid (SG) refers to the enhancement of the existing power grid with "valuable technologies that can be deployed in the very near future or are already deployed today" according to the US Department of Energy (DoE) [69]. The definition proposed by the European Standards Organization CENELEC refers to the SG as "an electricity network that can integrate in, a cost-efficient manner, the behavior and actions of all users connected to it" [14].

Some of the objectives of the SG are to offer an economical efficiency, a sustainable power system with high levels of quality and safety of supply and to make the consumer a prosumer i.e. an informed and active agent or a factor and possibly a producer. In fact, one of the major promises of SGs is to enable companies as well as households to generate electricity and to sell it on to other consumers [14]. Integration of renewable resources such as wind turbines and solar panels in the energy production imply design and development of adequate solutions for the generation and storage such as DER.

To guarantee an efficient and optimal operation of the grid, securing those critical infrastructures is a top priority. Security concerns related to modern SGs are receiving an increasing attention within the research community. When taking up the challenge of enhancing the security of the SG, it is clear that improvement in the system is required as different parts including the transmission and the distribution grid system were not developed with security as a primary concern [29]. In the present chapter, the context of the work as well as a collection of some definitions laying the foundations for the next chapters will be set.

## 1.1 The Next Generation of Energy Systems - Smart Grids

The electric power infrastructure is based on an installation of components and equipments that enable the generation, transmission and use of electricity. To allow an efficient management of this resource, the power industry has been growing into an interconnected and complex system based on a two way communication i.e. grid operator receive consumers' information and the energy consumers get real-time

prices and bills. Ensuring a secure and reliable transmission of the information flow help maintain an optimal and efficient operation of the power grid.

The integration of ICT in the control, protection and monitoring of power systems helps increase the efficiency of the production, transmission and distribution operations. The new generation of energy systems uses ICT to meet the ever-growing demand on electricity [91].

The combination of smart components with well-designed Substation Communication Network (SCN), according to specific norms and recommendations, shall ensure an optimal operation of the power systems with a significant economic efficiency.

In fact, integration of renewables together with a dynamic management of the demand-response system was shown to support a balance between energy consumption and demand to avoid overloads on the providers' side and shift consumers' consumption from peak loads [39].

Despite the considerable improvements in facilitating the management of supply and demand of electric power in the next-generation energy systems, there is still room for improvement especially with respect to the cyber-security of the SGs.

### 1.1.1 Cyber-Security Challenges in Modern Energy Systems

Use of networking technologies is essential to allow a real-time demand response and management strategies as well as an inclusion of distributed micro-generation based on renewable energy sources.

However, a major challenge of the increased ICT interconnection is the larger exposure to malicious cyber-attacks. Several works in this field (e.g. [47], [28] and [107]) has shown the different vulnerabilities of SGs.

To counter the cyber-physical threats, the required security solutions shall meet the multiple performance requirements including the time-critical operation of the physical power system as well as the high availability and reliability of the communication network. In order to secure the next-generation of energy systems, several aspects shall be considered including a reliable and safe software for control systems [59] and a secure communication network traffic.

SGs are based on a heterogeneous structure including several agents and stakeholders resulting in a high-level of integration between the physical system and IT. Consequently, one of the main challenges in guaranteeing a safe and secure operation of the modern energy systems is to combine Operational Technologies (OT) and Information Technology (IT) cyber-security.

Researchers and experts in this field agree, however, that there are considerable differences between conventional IT security mechanisms and OT cyber-security.

### 1.1.2 Main Differences with Conventional IT Security

Cyber-security solutions for the next-generation of energy systems need to be specifically tailored for the features of the present heterogeneous and complex system. Direct transfer and application of security solutions used in conventional IT systems would not be possible due to several factors summarized in Table 1.1.

First, the underlying physical system needs to be accounted for which often implies time criticality conditions. In fact, a low latency is crucial to guarantee a high performance of the SG or any other industrial environment. For instance, some specific trip signals in electrical substations require an end-to-end transfer time of 3 ms at most, whereas the requirement on the delay for multimedia services is of the order of 100 ms.

Secondly, the lifetime span of solutions in energy systems and in ICS is, in general, considerably longer that the one in the IT field. In the IT sector, a renewal cycle of 3 to 5 years is expected contrarily to the power plants where software and hardware have typically a lifetime of 15 to 20 years. This leads to the presence of legacy systems that are part of the power grid and which need to be considered in the design of cyber-security solutions. A patch management program shall be considered according to the EU comission recommendation on cyber-security in the energy sector in the EU cyber-security Act that took effect in June 2019 [30].

Thirdly, cascade effect of vulnerabilities that might be also encountered in IT systems, shall be considered. Indeed, exploit of exposure points in the network, software or firmware used in ICS would result in cascading effects that might lead to disturbances in the physical system as already experienced in some of the major cyber-attacks against critical infrastructures reported in Section 2.1.

**Table 1.1:** Main characteristics of SGs [26]

| **Differences from conventional grids** | **Differences from IT systems** |
|---|---|
| Small-scale distributed resources | Industrial process connected to IT and cascade effects of vulnerabilities that might lead to vulnerabilities on physical process |
| Smart devices to access timely information | Difficult long-term and well-tested mechanisms in legacy systems |
| Challenges modeling the cyber and physical parts | Different communication protocols but Network with simpler dynamics (fixed topology, stable user population) |
| Incompatibilities between legacy systems and smart devices | Limited resources with respect to computational power and memory |

Fourthly, the differences in resources in SGs is another aspect to be taken into account. In fact, most industrial devices have limited computational power and memory resources. The particular nature of the industrial environments impose limitations on the CPUs. Controllers, PLCs and IEDs have embedded processors that are encapsulated in closed cases to avoid dust, water or insects. This results in a lower ventilation thus power dissipation capabilities, which make the previously mentioned processors generally slower [47]. Considerations on the limited resources in industrial systems are particularly relevant for security studies as authentication and encryption options need to account for those limitations as discussed further in the present work.

Additionally, conventional security attributes shall be considered differently when it comes to industrial or energy systems. In order to secure the network traffic in SGs, several aspects shall be considered. From an information security perspective, confidentiality, integrity and availability of the data transmitted within the communication network shall be tackled.

Approaches including access control to ensure the protection of the data against unauthorized access, disclosure or theft are commonly used to guarantee the data confidentiality.

Data integrity refers to protecting the data against any improper modification or alteration to guarantee its accuracy and consistency. Techniques used to ensure the integrity of the data within ICS or next generation energy systems shall account for the strict time criticality requirements expected in such environments. Some authentication methods adapted for these particular conditions have been proposed in literature such as [29], [100] and [84]. Another characteristic of ICS and SGs is the necessity of granting real-time reliability of the communication networks [12] to ensure an optimal operation of the physical system.

Contrarily to conventional IT systems, the most critical requirement in modern energy systems is to ensure the availability of data [80]. Attacks against SGs might exploit security vulnerabilities to attempt to deny legitimate communications within the network traffic that would result in blocking legitimate information and services to allowed users.

## 1.2 Intrusion Detection Systems (IDSs) in Energy Systems

Extensive research works ([8, 19, 57, 67, 78, 87, 105]) have been developed in the field of IDS in ICS and SCADA systems. However, in the present work there will be a focus on efforts aiming at detecting anomalies in modern energy systems.

One of the most common and relevant ways to cluster the different IDSs, is based on their ability to detect unknown or zero-day attacks.

### 1.2.1 Signature-based Approaches

Signature or rule based methods are the first class of IDSs. They are based on comparing collected data with a database of attacks' signatures. This type of method is very efficient in detecting anomalies with few FAs under the condition that meaningful and relevant signatures are defined. One of the pioneer studies on IDS in electrical substations was conducted by [87]. A Snort rule-based IDS for IEDs in IEC 61850 substations was developed through applying blacklisting of rules described with an experimental setup.

In [78], detection of anomalies in Modbus/TCP traffic was achieved through the use of a preprocessor of Snort developed by Digital Bond namely Quickdraw.

Niventhan and Papa [81] presented a framework for dynamic rules generation and DPI for use on top of Snort and Suricata. Several rules based on specifications for Modbus/TCP, DNP3 and Ether/IP protocols are developed.

Other industrial tools such as StationGuard proposed by OMICRON are based on a similar principle of detecting erroneous packets in IEC 61850 substations with the help of a pre-defined set of rules.

Recent work developed in [8] proposes an efficient IDS primarily focus on the detection of GOOSE poisoning attacks. The network IDS is based on a comprehensive analysis of the GOOSE protocol specifications and implementation of the detection rules in the open-source network analyzer Zeek (previously Bro). Test results in terms of latency and jitter show an accuracy of the detection of poisoning attacks with a low-overhead that does not hinder the performance of the GOOSE communication.

Despite their high detection rate with few to none FAs, two main drawbacks are generally associated with specification and signature-based IDS. First, establishing a rule dataset is challenging. Indeed, the creation of a relevant set of rules is not sufficient as there is also the need to regularly update it and maintain it. Second, signature-based IDS are only able to detect known attacks. When considering the scarcity of attack databases in ICSs and energy systems due to the confidentiality of the data, signature-based IDS might not be an optimal choice for securing the network traffic within ICS and energy systems.

### 1.2.2 Anomaly Detection Approaches

Anomaly-based detection is another category of IDSs which is based on characterizing the normal behavior of a system. Thus, an anomaly is referred to as a deviation from the normal behavior. The main advantage of using AD methods is their ability to detect unknown attacks contrarily to signature-based techniques. Thus, AD methods in SGs and ICSs have been extensively used over the past few years: Indeed, model-based detection is commonly used in conventional IDSs and can be particularly relevant for monitoring unknown attacks in alike systems [19].

Barbosa et al. [3] analyzed the network traffic in ICS and assumptions about its periodicity was concluded to be further used to propose an AD method. The developed tool, PeriodAnalyser, whitelists the traffic including Modbus/TCP and MMS protocols according to a previously learned model.

Analysis of the communication patterns are also used for anomaly-based IDSs. An AD method based on One-Class Support Vector Machine (OC-SVM) technique is used to model communication patterns in [93]. Shang et al. [92] use OC-SVM to model normal communication and detect anomalies through the computation of a hyper-plane in the feature space to distinguish between normal and anomalous objects. The developed method is tested on communication traffic including only Modbus/TCP static exchanges between a client and a server. The work presented in [92] is telemetry-oriented and based on the assumption of the periodicity of the network traffic which is not always the case of MMS messages, for instance. Another limitation is the absence of any semantics' interpretation of the detected anomalous packets which gives no explanation on the cause of the detected traffic behavior.

Some AD methods presented in the literature use statistical techniques to detect intrusions or attacks. Indeed, the network traffic may exhibit several statistical properties that can be analyzed to establish a model of the traffic.

Several AD methods that are based on statistical techniques, have been used in the literature. In statistical approaches, AD methods are commonly expressed as a change point detection problem. The network traffic may exhibit several statistical properties that can be analyzed in order to detect intrusions or attacks.

To detect anomalies in IEC 61850 automation systems, Kwon et al. [63] use statistics of network telemetry metrics and protocol specifications of GOOSE and MMS. Metrics considered for GOOSE AD are GOOSE message frequency, counter of received GOOSE messages and timestamp of most recent GOOSE messages. Whereas for MMS, features are limited to the command type. The experiments are performed using a dataset of network traffic from a Korean SG testbed. In the model presented in [63], only periodic GOOSE traffic is considered while omitting legitimate fault events. Thus, the developed AD is only based on analyzing the mean and the standard deviation of network metrics which assumes that the network traffic can be simply modeled as a signal embedded in WGN. Such hypothesis can be hardly applied to the network traffic in IEC 61850 substations as demonstrated in the present work in Section 3. The main challenge that can be encountered by AD methods is to establish an accurate model of the analyzed system to decrease the rate of FAs.

### 1.2.3 Hybrid Approaches

To combine advantages of signature-based techniques and AD systems, another category of IDS adopts a hybrid approach.

An IDS based on three-level was proposed by Cheung et al. in [19]. The two first ones implement a rule-based check of the protocol specifications for Modbus/TCP and network segmentation and access policies. The rules were implemented in the open-source IDS software Snort. The third level is based on a learning-based approach.

An implementation of a DNP3 parser based on a set of rules to check the packets structure as well as the semantics was developed in [67]. To identify malicious commands, the state estimation of the simulated system was predicted and results were integrated within the IDS. The developed method was integrated to the open-source network analyzer Zeek. Some other works [88] and [21] use also Zeek for detection of intrusions in SCADA systems.

Yang et al. [104] proposed an IDS with a similar approach to [19], which is specifically designed for IEC 61850 electrical substations that is further extended to a multidimensional IDS [105]. A four-layer detection model is proposed that consists of an access control, protocol whitelisting, model-based detection for station and process bus and a multi-parameter based detection. Specific input features based on the standard definitions and the configuration system files for GOOSE and SV protocols, are included in the IDS. Other telemetry-based characteristics consisting in the packet transfer rate per second, transfer byte size per second, length and size of the packets are learned from the network traffic. The detection of deviations in the network communication that is based on a simple thresholding procedure. This is used to detect if any of the captured traffic characteristics goes beyond a minimum and a maximum value.

Few of previously mentioned works take into account the specific features of IEC 61850 substations and combine good detection performance with the robustness of the developed approach.

The limitations of the aforementioned available works are as follows:

- The works based on the network telemetrics ([62] and [103]) do not account for the specifities of the network data in electrical substations including the different types of communications.
- Most of the available works ([105], [62], [92] and [103]) consider simplification assumptions with respect to the modeling and do not include a good understanding and representation of the substation network.

- To the best of our knowledge, none of the existing works propose an early anomaly detection method of GOOSE attacks in the network traffic of IEC 61850 substations.

## 1.3 Contributions of the Present Work

The availability of the data transmitted within the communication network of the SG is the most critical requirement when compared with integrity and confidentiality as previously explained in Section 1.1.

Several threats such as DoS or flooding attacks caused by GOOSE poisoning attack, for instance, might hinder the availability of the communication within IEC 61850 substations. To tackle such threats, a well-adapted Early Detection of Attacks for GOOSE Network (EDA4GNeT) method is developed in the present work.

In addition to the numerous differences between SGs and IT security presented in Section 1.1.2, the focus on the physical process as well as the use of several protocols among ICS increases the complexity of studying the network traffic behavior. The developed EDA4GNeT method accounts of the characteristics of the network traffic in electrical substations through a comprehensive analysis of the statistical characteristics of the communication features.

A better understanding of the characteristics of the SCN helps to define a well-adapted mathematical model to describe the network traffic in electrical substations. The designed model can accurately account for the SRD as well as the LRD in the network traffic data as shown by the reported results in Section 3. The mathematical representation of the network traffic in IEC 61850 substations developed in the present work has as primary use the basis for the detection method EDA4GNeT. The mathematical model can also considerably support the design of the network architecture of future electrical substations as well as the performance studies of the network communication.

The developed approach to the detection of attacks in the communication of electrical substations can be formulated as the well-known change point detection problem Chapter 4. Thus, to detect anomalies resulting from changes in the traffic patterns such as flooding attacks, statistical methods are adopted because of their increased reliability [4]. The detector used in EDA4GNeT is based on a novel score function presented in Section 5.2.2.

The EDA4GNeT method developed in the present work can account for dynamic changes in the model. It is also able to detect multiple anomalies at unknown change times while assuming unknown model parameters and different types of changes discussed in Chapter 4.

The developed method is based on a novel and robust score function that, on one hand suits the characteristics and the requirements of the mathematical model

representing the network traffic in IEC 61850 substations. And on the other hand, the experiments carried-out to test the performance of the EDA4GNeT approach show strong results in terms of detection accuracy and earliness of detection.

The different contributions of the present work will be clustered in major and minor contributions. The major contributions are as follows:

- An adequate mathematical model to describe the communication network of GOOSE network traffic in IEC 61850 electrical substations is presented. To this end, we develop a state space approximation of an ARFIMA model based on a structured analysis of the GOOSE network traffic. The modeling procedure includes efficient and suitable parameter estimation and prediction techniques. The developed mathematical model is primarily used, in the present work, for the detection of anomalies. However, it can also help design the network architecture of electrical substations as well as performance studies of the network traffic. It is worth noting that one of the remarkable characteristics of the selected model is that it can be easily extended to include more features of the communication in the form of time-series.
- An online method EDA4GNeT adapted to the detection of flooding attacks in the GOOSE network traffic in IEC 61850 substations is developed. Use of multi-step ahead prediction for SS approximation of an ARFIMA model for the EDA4GNeT method allow an early detection of anomalies. A quick detection of the attacks helps take corrective actions through response systems which considerably improves the overall cyber-security of the communication within energy systems.
- The novel AD method EDA4GNeT based on the designed mathematical model accounts for dynamic changes of the system which is shown to considerably decrease the rate of false alarms. Even though the presented case studies adopted in the present work are focused on availability attacks, the novel detection method allows detection of different types of changes (additive and non-additive). Additionally, for detection of several types of changes, the algorithm on which EDA4GNeT is based, enables the detection of multiple anomalies at unknown change times.

Besides the former major aspects, other contributions of the present research work are formulated in the following:

- A novel classification of attacks threatening the smart grid is developed. The proposed classification follows a methodical approach as it is based on the well-known SGAM model. Contrarily to the available classifications, the one developed in the present work takes into account the specific characteristics

of modern energy systems to give a comprehensive overview of the attacks threatening the cyber-physical security of smart grids.

- An investigation of the attack vectors targeting IEC 61850 substations is performed. The risks in a systematic approach using Attack-Execution Graphs (AEG) to describe the threats within an electrical substation are analyzed. The proposed approach allows a qualitative security assessment of a T1-1 substation.
- The performance of the novel detection method ED4GNeT is evaluated using two simulation case studies including different types of changes under different conditions.
- The accuracy of the suggested model using well-established criteria from the data-driven modeling field is evaluated including detection rate, FAs and earliness of detection.

## 1.4 Thesis Outline

The present work is composed of seven chapters where Chapter 2 introduces the motivation of the work as well as a detailed problem statement using established methods for presenting the different types of attacks as well as a risk assessment of possible attacks against IEC 61850 substations.

In Chapter 3, the characteristics of the GOOSE network traffic in IEC 61850 are analyzed. A statistical analysis of the considered time series is first conducted. The derived characteristics help select an appropriate regression model, in this case a state-space ARFIMA model to describe the data. Techniques for the estimation of the parameter vector to describe the model as well as the prediction of the dataset is then presented. The evaluation of the selected state-space model on the considered use cases is performed.

Chapter 4 is dedicated to introduce and discuss concepts necessary to the design of EDA4GNeT method. This chapter is mainly focused on formulating the AD as a statistical hypothesis testing for change detection. Introduction and extension of well-known techniques for our specific detection problem are presented.

Conclusions about the mathematical modeling of the SCN traffic data lead us to develop a novel early detection method EDA4GNeT based on an adapted score test introduced in Chapter 5. The description of EDA4GNeT method as well as a detailed explanation of the different steps for the estimation, prediction and detection procedures is presented.

Chapter 6 mainly focuses on the description of the developed use cases including normal operation of a T1-1 and a 66/11kV substation as well as the designed adversary

models. Relevant metrics derived from well-established criteria from the data-driven modeling field are used to evaluate the performance of the EDA4GNeT method.

The last Chapter 7, is dedicated to concluding remarks and an outlook to discuss promising future research opportunities.

## 1.5 Previous Publications

Some of the results of the present work were published in international peer-reviewed publications. In [28], an analysis of the cyber-security context for smart grids is first presented then a novel classification method for the different types of attacks is established. The tree-structured classification is based on the well-known SGAM model [13].

One of the use cases adopted to validate the developed EDA4GNET method was firstly published as a cost-efficient simulation testbed of the different network protocols used in IEC 61850 substations in [27].

To increase the cyber-security of electrical substations, two different techniques were proposed against integrity attacks such as FDIA or a particular type of GOOSE poisoning attacks. Both approaches were briefly discussed in Chapter 2. In [29], an authentication method based on the HMAC scheme for the time-critical GOOSE authentication was developed instead of the recommended RSASSA-PSS scheme proposed in the IEC 62351-6 standard. When implementation of an authentication algorithm of the communication is not possible, an additional security solution against integrity attacks and particularly GOOSE poisoning attacks was developed in [8]. An extension of the well-known IDS Zeek, previously bro, was suggested. In the two previous works, simulation case studies proved the performance of the developed techniques. Interested reader might refer to the previously mentioned publications for more details.

A first version of the developed anomaly detection approach was introduced in [25] where a statistical detection method was presented. An ARFIMA model was used to describe the network traffic in IEC 61850 substations which has been extended to state space model to include the dynamics of the traffic and propose an online detection method. The detection method presented in [25] was offline. Thus, in the present work, estimation and prediction approaches are adapted to develop a novel detection method EDA4GNeT that offers an early detection of attacks in the GOOSE communication within IEC 61850 substations.

# CHAPTER 2

## Problem Statement

Critical infrastructures are essential for the functioning of our modern society. Due to their vital role, critical infrastructures have been an attractive target for cyber-attacks [60]. To offer an optimal operation and an enhanced control and monitoring features, critical infrastructures are being equipped with IT capabilities. The interconnected nature of those essential assets, including for instance energy systems, introduces vulnerabilities, that when exploited by attackers, may result in catastrophic consequences [94].

In the present chapter, a general analysis of the different threats in energy systems is provided with listings of the most recent cyber-attacks against Industrial Control System (ICS) in general and Smart Grids (SGs) in particular. Due to the diversity of the attacks against SGs, a novel classification is proposed in Section 2.1.2. From this, it can be concluded that electrical substations are a critical part of the grid that can be targeted by several attacks. Thus a comprehensive security assessment of a typical IEC 61850 electrical substation is presented in Section 2.4. The risk assessment is based on a systematic tree-based approach presented in the form of an Attack Execution Graph (AEG).

## 2.1 General Analysis of Threats in Energy Systems

The main goal of energy systems is to ensure a stable and continuous electric power to consumers. Whereas the goal has remained the same, the structure of the future grid is facing a rapid change. Contrarily to conventional energy systems, SGs have a more complex and interconnected structure.

In the context of the ongoing energy transition, a major goal of the European Union's energy and climate policy objectives for 2020 and beyond is to integrate renewable Distributed Energy Resources (DER) [68]. This results in a two-way distributed flow of electricity instead of the traditional one-way hierarchical flow. To keep up with these new characteristics of the power grid, modernization of the Transmission System Operators (TSO) and Distribution System Operators

(DSO) maintaining and managing the transmission and the distribution substations, respectively, is required.

While the extensive deployement of IT solutions is necessary for the monitoring and control of modern energy systems, it increases considerably the exposure of the grid to cyber-attacks. Traditional protection schemes including "security by obscurity" and physical isolation are no more effective as several components of modern SGs are directly connected to the internet to allow, for instance, remote control actions. This makes them vulnerable to all the range of cyber-attacks in conventional IT systems.

In the next section, a collection of the reported simulated and real attacks against energy and SCADA systems is presented.

### 2.1.1 Simulated and Real Cases of Cyber-Attacks

One of the main challenges of the future power systems is to ensure their security against cyber-attacks. Multiple attacks targeting critical infrastructures such as SGs are perpetrated frequently for several reasons. Recent incidents have shown that adversaries have the required means and the motivation to perpetrate attacks against critical infrastructures [94]. The span of the motivation of attackers to target critical infrastructures is quite wide ranging from financial gain to political incentive. Those aspects are out-of-scope of the present work.

The damage caused by an attack on a critical infrastructure depends on one hand on the vulnerabilities inherent in the components and the communication within the facility, and on the other hand on the motivation, capabilities and interest of the attacker. Some of the major cyber attacks against critical infrastructures, in particular SGs, in the recent years are shown in Table 2.1 and discussed in the following:

- In 2003, a nuclear power plant in Davis-Besse in Ohio was infected by a slammer worm that exploited a Microsoft SQL vulnerability. The malware affected over

**Table 2.1:** Real and experimental attacks against SGs

| **Real Cases** | **Experimental Cases** |
|---|---|
| Slammer Worm (2003) | Aurora Attack (2007) |
| Stuxnet Worm (2010) | Erebos Trojan (2015) |
| Havex Remote Access Trojan (2015) | – |
| Ukraine Electric Grid Attack (2015) | – |
| Industroyer (2016) | – |

75000 machines causing a DoS of the safety system and the process computer for over 5 hours [89].

- In June 2010, a wide spread of the Stuxnet worm affected SCADA systems mainly in Uranium centrifuges in Iran. It targeted Siemens SCADA applications (PCS7, WinCC and STEP7) and hardware (Siemens S7 PLCs). After gaining access to the control system, attackers downloaded malicious code from a remote site. USB devices and zero-day vulnerability exploits were used to infect the plant. Physical damage to the plant was caused by the change of the rotational speed of the motors as Stuxnet periodically modifies the variable-frequency drives. More details about attacks against equipment are described in [28].
- In December 2015, an espionage campaign launched by Dragonfly using HAVEX malware targeted ICSs in different countries including the United States, Turkey and Switzerland. It mainly affected electric and petrochemical plants without causing physical harm [94] as its main goal was espionage and theft of information for potential future attacks. BlackEnergy 1-3 is another espionage malware that targeted HMIs connected to Internet through specific HMIs applications exploits including Siemens Simatic, GE Cimplicity and Advantech WebAccess [94].
- On December 23, 2015, the attack perpetrated on an Ukrainian power grid is considered to be the first known successful cyber-attack targeting a power grid. The attackers gained access to three energy distribution companies compromising their information system which resulted in causing an outage of 7 hours affecting more than 700.000 residents.
- In December 2016, another attack hit the electrical Ukrainian infrastructure. Hackers took control of a Remote Transmission Unit (RTU) at the substation Pivnichna which shutdown resulted in an outage of one hour. The two previous attacks were both benign even though according to [41] the consequences on the SG could have been more serious. It is believed that a modular malware, Crash Override (also refeered to as Industroyer), targeting ICSs, was used to perpetrate the attack. It enabled attacker to collect valuable information about the system process and even to take direct control of switches and circuit breakers [18]. The Industroyer malware was automatically able to gain knowledge about the targeted process without any manual commands. The main protocols that were targeted by the Industroyer malware are IEC 60870-5-101, IEC 60870-5-104 and IEC 61850 and it can be easily extended to other protocols [94]. During this second Ukranian attack, the Industroyer malware was able to scan the SCADA environment and deny service to local serial ports. It would be also possibly capable of wiping the Windows system platform as well as exploiting vulnerabilities such as the Siemens relay DoS.

- The Aurora attack is a simulated vulnerability that was tested by the Homeland security department back in 2007 [108]. It exploits the coupling of two electrical generators. Causing an out of synchronisation by changing the operating frequency, results in an electrical and mechanical stress and thus to a damage to the equipment in the system.
- The Erebos attack is an experimental scenario based on a trojan malware that was used to remotely infect 50 generators in order to overload them causing a fictive blackout that would have affected a whole regional electric system in the northeast of the US [74].

The reader can find more details about incidents in SCADA systems and critical infrastructures in the survey of Miller and Rowe [77]. Considering the threats targeting SGs, a first step towards ensuring their cyber-physical security is to discern their specific features. In fact, the different specificities as well as the security requirements of the SG shall be taken into account to develop an adequate classification of the different threats.

### 2.1.2 Classification of Attacks in Energy Systems

Cyber security and privacy issues in the SG are relatively new areas in the field of power industry [70]. The highly-interconnected structure of SGs rises additional security challenges when compared with conventional power grids. A good understanding of the different threats and risks is essential to face those challenges and to guarantee an optimal operation of modern energy systems.

As an attempt to unveil the various threats that endanger the SG, a new classification of the different cyber-physical attacks was proposed by the author of this thesis in [28]. The suggested categories were based on the different layers of the Smart Grid Architecture Model (SGAM). We distinguish three categories of attacks. The first one groups attacks against power and energy layer. The second one consists of attacks against the computer/IT layer. Attacks against communication protocols are grouped in the third category. An overview of the specificities and the security requirements of the SG presented in [28] as well as a classification of the various attacks threatening the cyber-physical security of the SG is depicted in Figure 2.1

The new classification proposed in this paper provides a perspective on the cyber-physical security of the SG and forms the necessary knowledge basis for understanding the current security challenges . The classification of attacks against SGs introduced in [28] helps develop adequate countermeasures such as IDS, IPS, etc. towards protecting future energy systems against the investigated cyber-attacks.

Based on the attack classification presented in [28] and the different attacks targeting ICS and SCADA systems listed in Section 2.1.1, it was concluded that the

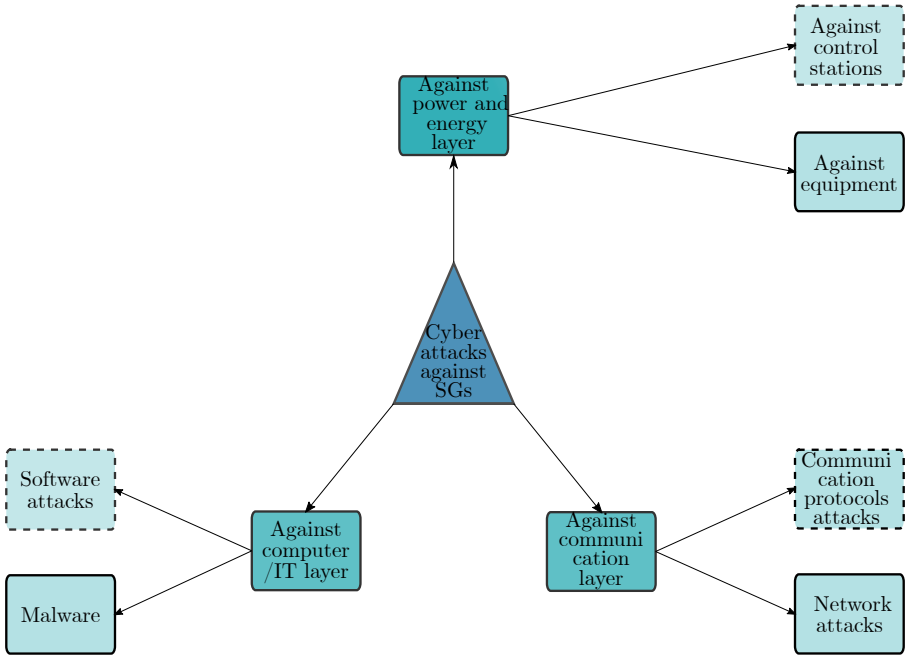



**Figure 2.1:** Classification of attacks against SGs [28] [b]

[b] This figure is based on one of our previous works that was published in [28]

IEC 61850 electrical substations, a critical component of energy systems, is one of the most exposed parts of modern energy systems.

## 2.2 Architecture of IEC 61850 Electrical Substations

Modern electrical substations are designed according to recommendations described in IEC 61850. The international IEC 61850 standard is proposed by the Technical Committee (TC) 57 Working Group (WG) 10 and was first issued in 2003. It is mainly focused on the communication networks and system within the Substation Automation Systems. A second edition of the standard was released in 2013 to include additional areas such as automation of wind power turbines, distributed energy systems and hydro-power systems.

### 2.2.1 The IEC 61850 Standard

The IEC 61850 standard describes the information model, the communication services and the architecture of the electrical substations. Electrical substations are an essential part of the SG. Depending on the type of the substation, its role is to transform voltage from high to low or vice-versa as well as distributing or switching functions. Each substation is controlled by an administrator via an automated structure called Substation Automation System (SAS).

#### Basic Concepts of IEC 61850

To offer such abilities, the model of the different functions and components of the substation should be defined. This is one of the main challenges met by the IEC 61850 standard. It suggests interoperability between different components thus the integration of devices and functions from different manufacturers is claimed to be possible when respecting the recommendations suggested in IEC 61850. Another objective of the standard is to reduce the number of protocols used in automation systems for electrical substations and to normalize their use in order to avoid problems of incompatibility between the different manufacturers.

The IEC 61850 standard is divided in several parts as presented in Table 2.2. Part 1 gives an overview of the IEC 61850 standard series, basic interface and reference model of a Substation Automation System (SAS). Part 2 and 3 provide an explanation of the terms used throughout the document and general requirements for electrical substation, respectively. A description of the system and project management structure including engineering and testing tools is presented in Part 4. Part 5 covers the communication requirements of the functions that are performed in the substation automation system. It also explains the Logical Nodes (LNs) for each function. In part 6, the IED related configuration languages based on the Extensible Markup Language (XML) including the Substation Configuration Language (SCL), IED Capability Description (ICD), System Exchange Description (SED), Instantiated IED Description (IID), System Specification Description (SSD) and Configured IED Description (CID) files are presented. The detailed communication architecture of

the substation including the explanation of the logical node names and data names for the communication, is defined from Part 7-1 to 7-4. Part 8-1 presents a data exchange method to MMS (ISO / IEC 9506-1 and ISO / IEC 9506-2) communication. The structure and the communication model using the SV protocol are described in parts 9-1 and 9-2. Lastly, part 10 focuses on recommendations for the conformance testing. It is, however, worth mentioning that besides some manufacturers' specific conformance tests, there is not yet a common certificate internationally acknowledged.

### Object Data Model

The IEC 61850 standard has a standardized object model for all the substation objects as shown in Figure 2.2 . Indeed, each physical device can be represented by different logical devices each of them grouping functions performed by the physical device. The different functions are, in fact, represented by a LN. The part IEC 61850-7-4 defines 13 logical groups in which the nodes are grouped in categories such as Protection, Control or Switchgear. The naming convention is, thus, defined according to the standard. The well-defined data model is independent from the method of

**Table 2.2:** Different parts of the IEC 61850 standard

| | |
|---|---|
| IEC/TR 61850-1 | Part 1: Introduction and overview |
| IEC 61850-3 | Part 2: Terms and abbreviations |
| IEC 61850-3 | Part 3: General requirements |
| IEC 61850-4 | Part 4: System and project management |
| IEC 61850-5 | Part 5: Communication requirements for functions and devices' models |
| IEC 61850-6 | Part 6: Configuration description language for communication in electrical substations related to IEDs |
| IEC 61850-7-1 | Part 7-1: Basic communication structure for substation and feeder equipment - Principles and models |
| IEC 61850-7-2 | Part 7-2: Abstract communication service interface (ACSI) |
| IEC 61850-7-3 | Part 7-3: Common data classes |
| IEC 61850-7-4 | Part 7-4: Compatible logical node classes and data classes |
| IEC 61850-7-410 | Part 7-410: Hydroelectric power plants - Communication for monitoring and control |
| IEC 61850-7-420 | Part 7-420: Basic communication structure- Distributed energy resources logical nodes |
| IEC 61850-8-1 | Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3 |
| IEC 61850-9-1 | Part 9-1: Sampled values over serial unidirectional multidrop point to point link |
| IEC 61850-9-2 | Part 9-2: Sampled values over ISO/IEC 8802-3 |
| IEC 61850-10 | Part 10: Conformance testing |

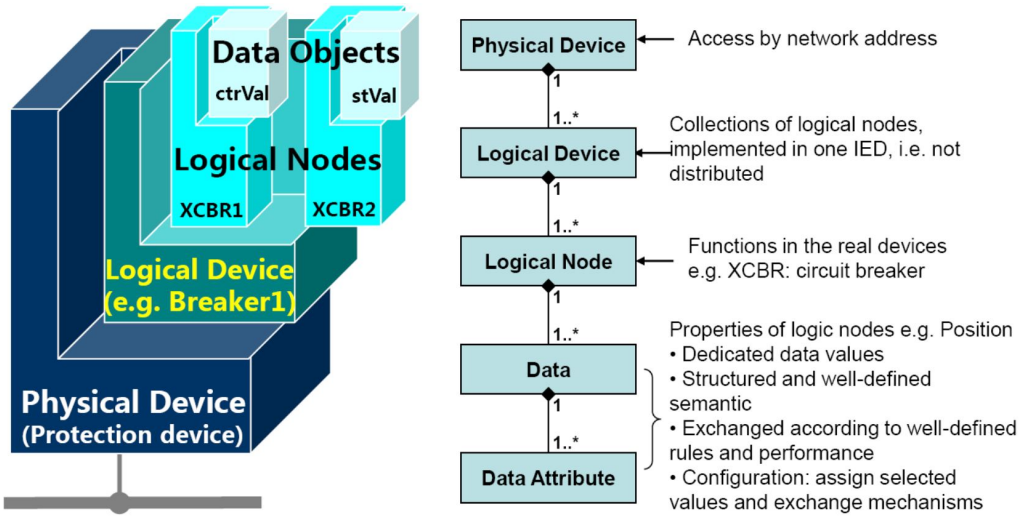



**Figure 2.2:** IEC 61850 Data Object Modeling [53]

communication which enables the use of new technologies and promotes vendors' independence. The object-oriented data model defined in IEC 61850 standard is based on an abstract level. The abstract model is currently mapped to the MMS, GOOSE and SV protocol. A set of logical nodes defines the mapping of the different protocols.

Each LN is composed of different data objects each of which comprises data attributes. The description of the properties of the different functions of a physical device are part of the device model. Each logical node contains a predefined set of data classes that includes data related to the different configurations. Such a modeling hierarchy reduces significantly the costs when it comes to the integration time and effort in power systems.

The configuration of the different IEDs is described using SCL which offers four file formats. The description of the capabilities of each IED is available in the IED Capabilities Description (ICD) files. The ICD is developed by the manufacturer and it has a generic description of the functions as well as the objects supported by a given device. Information concerning the configuration of the IEDs is part of the configured IED Description (CID). It is used internally by the device to be configured. The two other formats are the Substation configuration (SCD) as well as the Substation Specification Description (SSD) files.

### 2.2.2 Communication Network in Electrical Substations

Given the fact that services and objects defined in IEC 61850 are abstract, there is a need to map them into specific protocols. Theoretically, data models can be mapped to any protocol. However, due to their complexity, the mapping of the different abstract data models is currently available for the protocols presented in Figure 2.3.

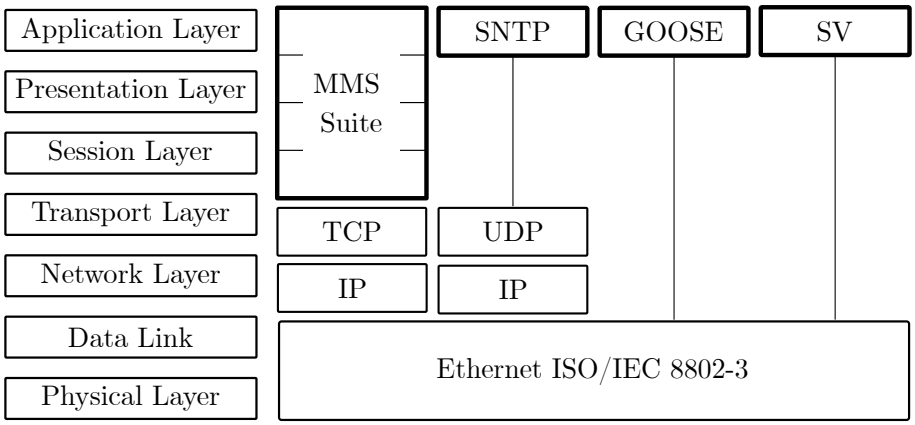



**Figure 2.3:** OSI mapping of IEC 61850 protocols

As presented in Table 2.2, the part IEC 61850-8-1 of the standard describes the mapping of the abstract services and data objects to the Manufacturing Message Specification (MMS) protocol that is defined in ISO/IEC 9506-1 and ISO/IEC 9506-2. The MMS protocol is used for the transmission of Real-Time (RT) data as well as the supervision and control information between the different components of the electrical substation. The details of the protocol stack of the IEC 61850 are provided in Figure 2.3.

The MMS protocol is an application-profile protocol implemented over TCP/IP and based on the OSI model. It is fully specified in ISO 9506 standard [56]. MMS messages are based on a client/server scheme and they are used for transmission of services (control, data access, file access, etc.) and reporting.

For the time synchronization of the entire system, the SNTP protocol is used. The 2 modes of operation client/server and publisher/subscriber are supported by the SNTP protocol. Moreover, different timestamps are used in SNTP to represent time values.

Requirements for time synchronization are specified in Part 5 of the IEC 61850 standard (refer to Table 2.2). The SNTP protocol is widely used in the implementation of IEC 61850 based electrical substations as it meets the requirements specified in Part 5 of the standard (refer to Table 2.2) as well as its simplicity.

While the functioning of the MMS protocol is based on the client/server mode that runs over TCP/IP, GOOSE and SV protocols follow the publisher/subscriber mechanism over high speed switched Ethernet. In the client/server operation mode, clients can access data made available by server or receive event-driven reports over TCP/IP. The connection is first opened by a client and several clients may communicate with the same server. However, in the publisher/subscriber mechanism, multicast messages are sent by a publisher to all subscribers without previous knowledge of which of the subscribers will receive the messages. And according to

the identification number of each message, subscribers may subscribe to specific messages they want to receive.

GOOSE and SV protocols have strict time requirements and use multicast and non-routable messages over the automation substation LAN. SV messages are used for the transmission of analog measurements. GOOSE protocol configuration is detailed in the part IEC 61850-8-1 of the Table 2.2 whereas details about the SV protocol can be found in the part IEC 61850-9.

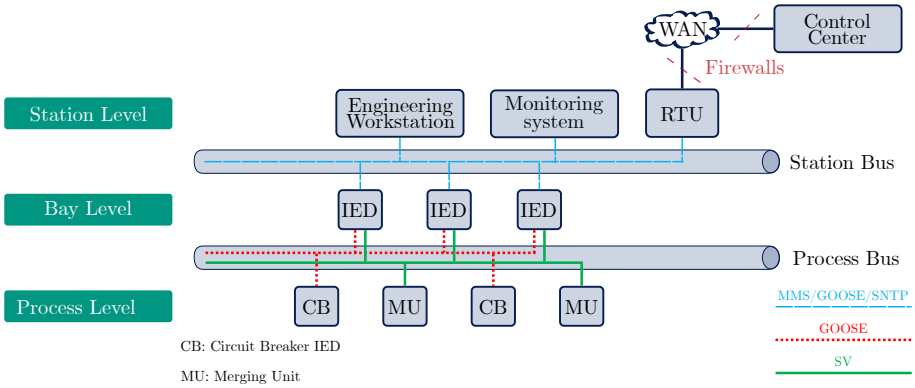
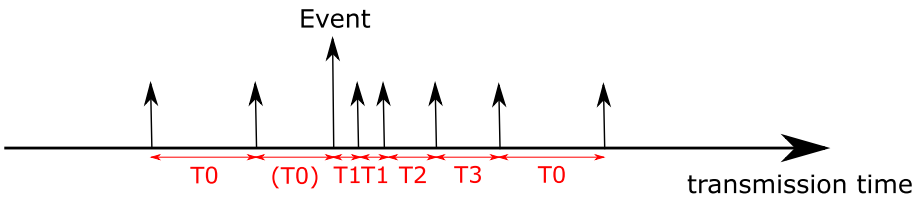



**Figure 2.4:** The different bays and protocols within an IEC 61850 substation [27] [a]

[a] This figure is based on one of our previous works that was published in [27]

The data object model defined in the IEC 61850 standard is mapped to different protocols. The GOOSE protocol [54] is a multicast publisher/subscriber data transfer method mapped directly over Ethernet. GOOSE messages are exchanged between process and bay levels as well as between IEDs in the bay level as shown in Figure 2.4.

The main function of GOOSE messages is to provide a fast way to exchange data between IEDs within the substation LAN. As already briefly described, the GOOSE protocol is event-based which implies that the publisher periodically, with a period of $T_0$, sends messages. But when an event happens, a burst of messages with new data is sent as depicted in Figure 2.5. The retransmission periods $T_1, T_2$ and $T_3$, following a GOOSE event are much shorter than the one for stable conditions $T_0$.




T0: retransmission in stable conditions
(T0): retransmission in stable conditions possibly shortened by an event
T1: shortest retransmission after an event
T2, T3: retransmission time until achieving the stable condition

**Figure 2.5:** The transmission mechanism of the GOOSE protocol [53]

A specific message transfer mechanism, depicted in Figure 2.5, is used to ensure the reliability of GOOSE messages without the conventional acknowledgment procedure. When an event occurs, a GOOSE message is generated and repeated first at high frequency, then at a slower one until reaching a predefined frequency in stable conditions.

Even though security is not the core of the IEC 61850 standard, there are some mechanisms to comply with the strict RT requirements. A first approach consists in mapping GOOSE messages directly to the link-layer to reduce processing time. Another mechanism to ensure efficient processing and transmission is to select a high priority tag to avoid slowing down the transmission of GOOSE packets.

The GOOSE message frame has a datagram complying with ISO/IEC 8802.3 and shown in Figure 2.6. More details can be found in IEC 61850-8.1 [54]. Within the frame structure, there is a 2-Byte field called "Additional Security" that is reserved for digital signature according to the recommendations in IEC 62351 [52]. However, no further details are provided in IEC 61850-8.1.

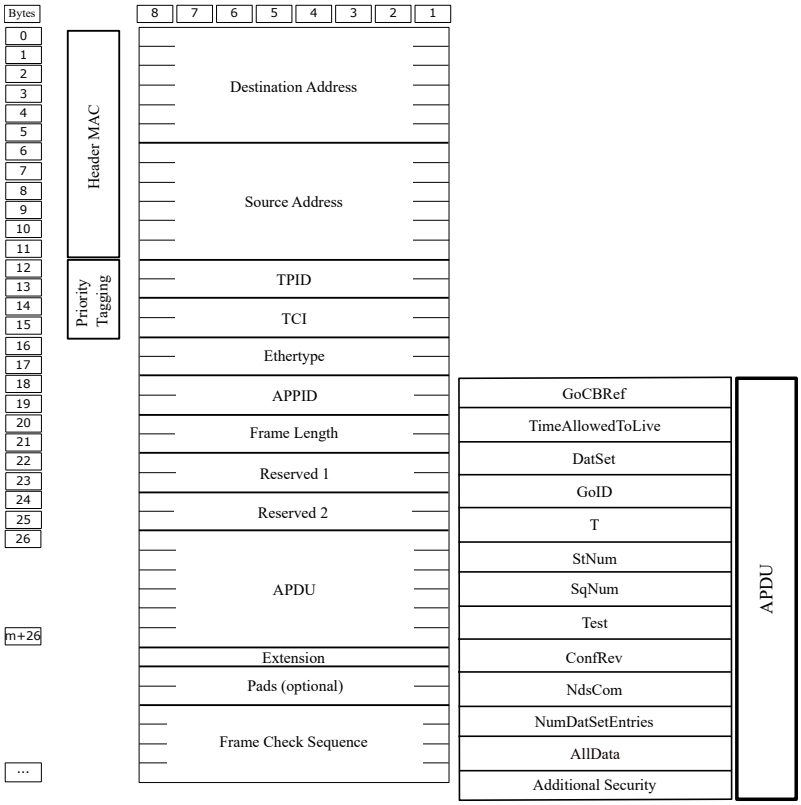



**Figure 2.6:** Description of the GOOSE frame [54]

## 2.3 Shortcomings of Security Recommendations in IEC 62351

Over the last few years, the IEC 61850 standard has been gaining an increasing acceptance in different power facilities worldwide. Thus, complete support and portfolio for IEC 61850 is already proposed by different recognized energy automation manu-

facturers such as Siemens, Hitachi ABB, etc. Integration of the recommendations suggested in IEC 61850 offers several assets for the electrical substations. However, the IEC 61850 standard was not conceived with security being a primary goal. The previous statement has been shown throughout the different attack scenarios crafted to target IEC 61850 substations and presented in the literature [61],[47], [97].

To overcome those limitations and others present in power systems, the IEC 62351 standard, developed by the Technical Committee 57 within the Working Group 15 (TC57 WG15) was first issued back in 2007. It introduces recommendations to guarantee the information security of power systems using, for instance, authentication mechanisms. The standard is split into eleven parts concerned with the end-to-end security of the communication in power systems. Security measures for the electrical substations based on IEC 61850 are proposed in Part 6 of the IEC 62351 standard.

As little to no focus on the threats affecting the network communication security of electrical substations was considered, the part 6 of IEC 62351 [52] was thereafter introduced in order to extend IEC 61850 with security measures. Further details about the the security recommendations are discussed in the next section.

The analysis of the security recommendations suggested in the IEC 62351 [52] standard shows few to no measures suitable for the security of the substation communication and mainly for the GOOSE protocol [29]. The main security shortcomings will be reviewed in Section 2.3.2.

### 2.3.1 Main Security Recommendations in IEC 62351

Different security recommendations were suggested for the different communication protocols used in IEC 61850 substations. Figure 2.7 represents a simplified mapping of the IEC 61850 protocols with the corresponding security measures suggested in

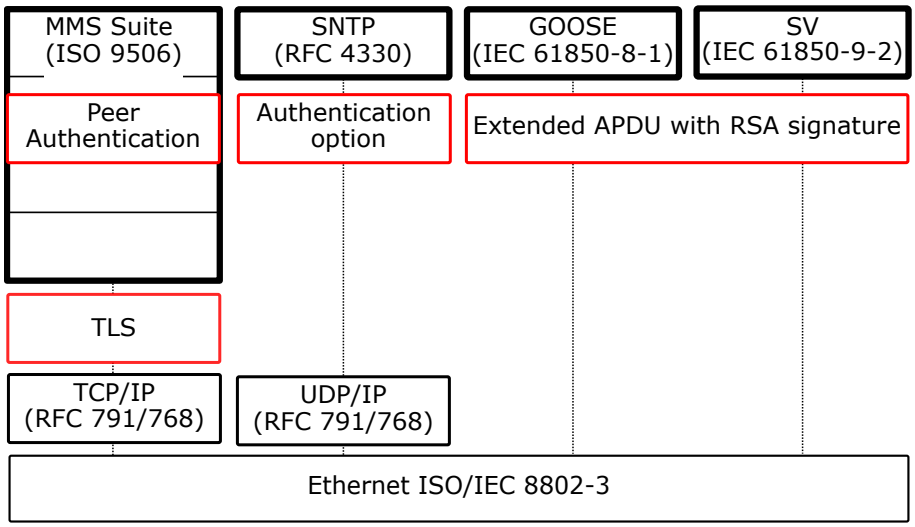



**Figure 2.7:** Mapping of IEC 61850 protocols with corresponding security measures suggested in IEC 62351

IEC 62351. Use of TLS and peer-authentication for MMS protocol was suggested. Authentication option for SNTP as well as for GOOSE and SV protocols was recommended.

In the following, there will be mainly a focus on security recommendations for the process network communication and particularly for the GOOSE protocol. Security measures for GOOSE and SV messages were described in IEC 62351-6 [52].

One of the security measures is focused on the use of the fields Reserved 1 for the number of the extension octets and Reserved 2 for a 16-bit cyclic redundancy check (CRC), as depicted in Figure 2.6.

Another security recommendation, suggested in the IEC 62351-6 standard [52], is the authentication of the GOOSE messages with a digital signature. In fact, extension of the Application Protocol Data Unit (APDU) with an RSA-based signature with Appendix-Probabilistic Signature Scheme (RSASSA-PSS) is proposed as authentication scheme. It is, however, worth noticing that the RSA signature explicitly excludes the Ethernet header and might introduce additional latency. Adding a digital signature to GOOSE communication guarantees the authentication and integrity of the messages. Additionally, IEC 62351-6 introduces an extension in the SCL files to allow the use of different certificates for GOOSE messages.

Defense against replay attacks is also suggested as an additional security measure. The proposed algorithm is based on a check of the freshness of the messages. It is in fact based on comparing the messages' timestamps with a clock skew. According to the IEC 62351-6 standard [52], a skew value of 2 minutes shall not be exceeded.

Although authentication of the GOOSE communication is recommended, encryption shall however be avoided. Indeed, for hard RT applications such as for GOOSE messages with 3 ms response time, no encryption scheme is suggested as stated in the standard that "for applications [...] requiring 3 ms response times, multicast configurations and low CPU overhead, encryption is not recommended." [52].

### 2.3.2 Security Flaws in IEC 62351

While the measures suggested in IEC 62351-6 standard enhance undeniably the overall security of electrical substations, there is still room for improvement. Integration of security measures for peer-to-peer communications might lead to an undesirable latency [47].

As previously mentioned, encryption of GOOSE messages is not recommended [52] which increases risk of DoS attacks stemming from GOOSE poisoning attacks. Thus, the security of GOOSE messages is limited to adding a digital signature to their APDU. More research is however needed, to better analyze the performance of the authentication mechanisms based on digital signatures recommended for SV and GOOSE communications.

In fact, strict RT requirements for specific communication messages cannot be respected as tested by [44]. This is particularly relevant when considering GOOSE messages of type 1A that should have a maximum of 3 ms response time as specified in IEC 61850 [55]. Therefore, one of the current challenges is to reconcile the needs for security and low latency [47] in electrical substations.

Works presented in the literarture ([29, 31, 44]) have been carried out with respect to testing the authenticity and integrity of GOOSE messages according to IEC 62351-6. It was shown that the HMAC scheme has a better computational time than the originally recommended RSASSA-PSS [29]. Thus, adjustment of the IEC 62351-6 considering the authentication scheme of GOOSE messages shall be considered in the next edition of the standard.

As mentioned earlier in this work about the conformance of IEC 61850 standard, it is worth noting that also for IEC 62351-6, that there is no certification tests available besides some industrial specific ones. Thus, most energy providers do not yet consider practical implementation of security measures due to the remaining ambiguity. The acceptance of security recommendations proposed in IEC 62351 largely depends on its impact on interoperability, performance, and manageability [44].

## 2.4 Security Assessment through a Risk Analysis of a Transmission Substation T1-1

To describe the exposure of IEC 61850 substations to attacks, a systematic approach to explain the different weak points is chosen. In our approach, we are interested in a qualitative assessment of the security risks in a transmission substation based on IEC 61850 of type T1-1.

Understanding how vulnerabilities in the network of electrical substations can be combined by attackers to perpetrate an intrusion, is important to develop efficient and adapted defense mechanisms. In fact, it can be identified how compromising one resource in the substation may increase risk of compromising another one. Simulation of the attacks scenarios of the different adversaries to evaluate further the novel IDS will be discussed further in Chapter 6.

Getting an insight on the system security is possible using cyber-attack modeling techniques. To unveil the vulnerabilities and in a further step present detection and mitigation tools, different cyber-attack modeling techniques were used such as attack graphs, diamond model, kill chain model [40]. To describe the different steps of an attack, kill chain models can be used. For cyber-intrusions, the kill chain model consists of seven steps namely reconnaissance, weaponization, delivery, exploitation, installation, command and control and finally actions on objectives.

Attack graphs help establish relationships between the different components to allow the reconstruction of possible attacks and their consequences.

Cyber-intrusion analysis using diamond model [10] focuses mainly on the event namely intrusion instead of the different steps as it is the case in the already mentioned approaches. There are four basic elements used to build a diamond diagram which are the adversary, the victim, the capability and the infrastructure. The dependencies between the different components are underlying in the structure of the diagram. However, the interconnections between the elements cannot be detailed. Thus, the model is not as flexible as other approaches and it cannot be easily extended.

The attack execution graphs are tree-based diagrams that represent the different paths in which an attack can be perpetrated [66]. An overview of all perspectives of possible adversary attacks can thus be considered. The main components in Attack Execution Graphs (AEGs) are the attack steps. However, there is also a description of attack skills, system knowledge, system access and finally the goals of the adversary. Considering the different advantages offered by AEG, our security assessment of the electrical transmission substation would be implemented using AEG.

### 2.4.1 Risk Analysis of the Station Network

The first case study considered in this work, is a simplified T1-1 transmission substation which contains one incoming line, one bus-bar and 2 outgoing lines.

The simplified Single Line Diagram (SLD) of the transmission substation T1-1 with the Intelligent Electronic Devices (IEDs) used for the different bays is depicted in Figure 2.8. The substation contains four bays that can be grouped into three main ones which are the transformer bay composed of $D01$ and and two feeders bays ($E01$ and $E03$). A Merging Unit (MU) has the function of a physical interface between the primary equipment in the switchgear and the protective devices as it digitizes the current and voltage measurements and sends it in the form of SV packets to the protection & control IEDs.

The transformer bay contains two MUs namely $MU_{D01}$ and $MU_{E02}$ as well as one P&C IEDs namely $IED_{D01}$. Each of the feeder bays contain one $MU_{E01}$and $MU_{E03}$ together with one P&C $IED_{E01}$ and $IED_{E03}$.

The communication between the station level and the bay level is established using MMS messages. A MITM attack could be launched via spoofing the ARP packets exchanged at the station network and MMS packets transmitted between the station Intelligent Electronic Device (IED) $IED_{D01}$ and the P&C IEDs are then intercepted. Further steps might result in gaining access to the process network to perpetrate different attacks. The previously mentioned attacks are mainly targeting the integrity of the data. However, another type of attacks against the availability of the data can

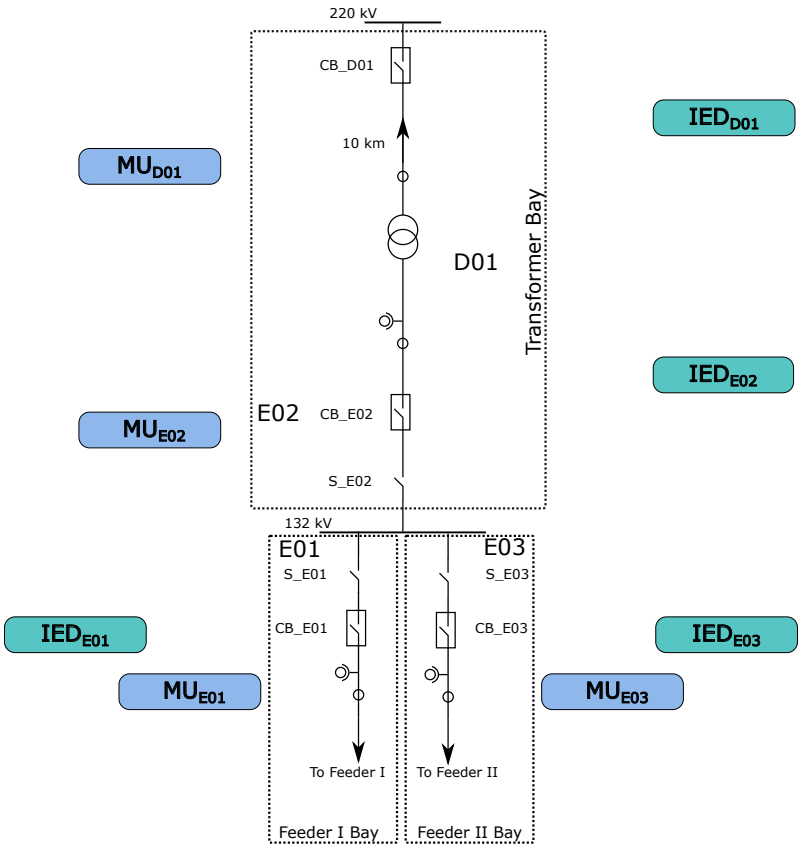



**Figure 2.8:** The Single Line Diagram (SLD) of the T1-1 substations with the used IEDs (depicted in green) and merging units (MUs) (depicted in blue)

occur in the substation level namely DoS attacks. An intruder might over-flood the communication by sending a huge number of network packets which will result in a disturbance of all communication-based functions. After gaining access through the substation LAN, it is supposed that the ultimate goal of an attacker would be directly related to the underlying physical process in the substation. Thus, attacks against the different bays in the T1-1 substation, presented in Section 6.2, are detailed in the following.

### 2.4.2 Risk Analysis of the Feeders I and II Bays

The transformer bay as described in Section 6.2.1 is composed of the two zones $D01$ and $E02$. The transformer bay is of a particular importance in the T1-1 substation as it is the origin of the power flow. Thus, the present Section 2.4.2 is dedicated to the study of the cyber-attacks modeling for this part of the T1-1 substation.

When considering a normal operating state of the substation, at least one of the two breakers $CB_{E03}$ or $CB_{E01}$ in the feeder I bay and feeder II bay respectively should be closed. A Man-In-The-Middle (MITM) attack between the station level and $IED_{E01}$ or $IED_{E03}$ would result in loss of power in feeder I or feeder II. Tripping only $CB_{E03}$ or $CB_{E01}$ is critical considering the structure of the T1-1 transmission substation. Tripping both previously mentioned CBs would however have more

serious consequences. Even though the interlocking function (F2) in $IED_{E01}$ an $IED_{E03}$ should prevent tripping both corresponding CBs, a false GOOSE message injected in the communication between $IED_{E01}$ and $IED_{E03}$ or from $IED_{E02}$ to $IED_{E01}$ and $IED_{E03}$ could disturb the normal operation state of the substation.

To study the CPS of the T1-1 electrical substations based on IEC 61850, hypothetical attack scenarios are proposed in Figure 2.9. Attack Execution Graphs (AEGs) are used to analyze the different details of some cyber-attacks examples such as the skills and the knowledge required by the intruder to reach his or her goal. The focus of the analysis is the transformer bay. According to IEC 61850-5, there are different states of operation namely normal, abnormal and post-fault state of operations. In the presented security assessment method, there will be a focus on the normal and the emergency states of operation.

### Normal state of operation

In normal state of operation, supervision and control tasks are carried out. A normal state of operation of the T1-1 substation is first considered. The study is only focused on undesirable events caused by malicious actions.

$D01$ zone is a critical part in the T1-1 substation as it is the entry point of the power flow. In the simple case considered, the threats are grouped into two main goals that are learning useful information concerning the electrical substation and the second one is to trip or close a Circuit Breaker (CB) ($CB_{D01}$). In fact, tripping $CB_{D01}$ would lead to the loss of power in the whole substation. It is supposed that access to the electrical substation network can be gained through the control center, the corporate network or the neighboring substation through the Wide Area Network (WAN) after compromising any firewalls as well as from a remote access (e.g. VPN, dial-up). The first goal of the intruder which is to gain an insight on the process can be reached by spoofing the communication packets exchanged between the station level and the different Intelligent Electronic Devices (IEDs). Fake GOOSE messages to trip the Circuit Breaker (CB) can be published after modification of the captured messages or directly generated from masqueraded IEDs replicating the GOOSE messages sent by $IED_{D01}$ or $IED_{E02}$. Another way to reach the goal of tripping the CB is to compromise the $MU_{E02}$ and to generate fake SV messages. Receiving corrupted measurements, $IED_{D01}$ and $IED_{E02}$ generates genuine GOOSE that triggers the overvoltage or overcurrent protection functions (F7) and (F8) respectively or the transformer differential protection (F6). The mentioned actions results in tripping $CB_{D01}$ to avoid damage to the substation. A more detailled overview about the different functions is given in Section 6.2.1.

### Emergency state of operation

When a fault occurs, an emergency state is established and protection actions such as alarms, trip and events are activated. In the transformer bay, such a state leads to sending messages from $IED_{D01}$ or $IED_{E02}$ to genuinely trip $CB_{D01}$. In that case an MMS message is sent from the concerned IED to the station level to report the tripping actions. If an intruder who gained access to the station network would whether temper with the transmitted MMS packet or even drop it, components of the station level such as the local or remote supervision center or the Human-Machine Interface (HMI) will not be aware of the real state of the breaker $CB_{D01}$. As a consequence, all related functions such as state estimation and control operations will be invalid. This will lead to the propagation of the fault in the whole substation and even to neighboring ones which may cause a power outage. In an emergency state requiring the isolation of a fault, the function (F4) is triggered and $CB_{E02}$ is supposed to trip. However, a fake GOOSE message from $IED_{E01}$ or $IED_{E03}$ might reveal a normal state of operation which will lead also to a fault propagation.

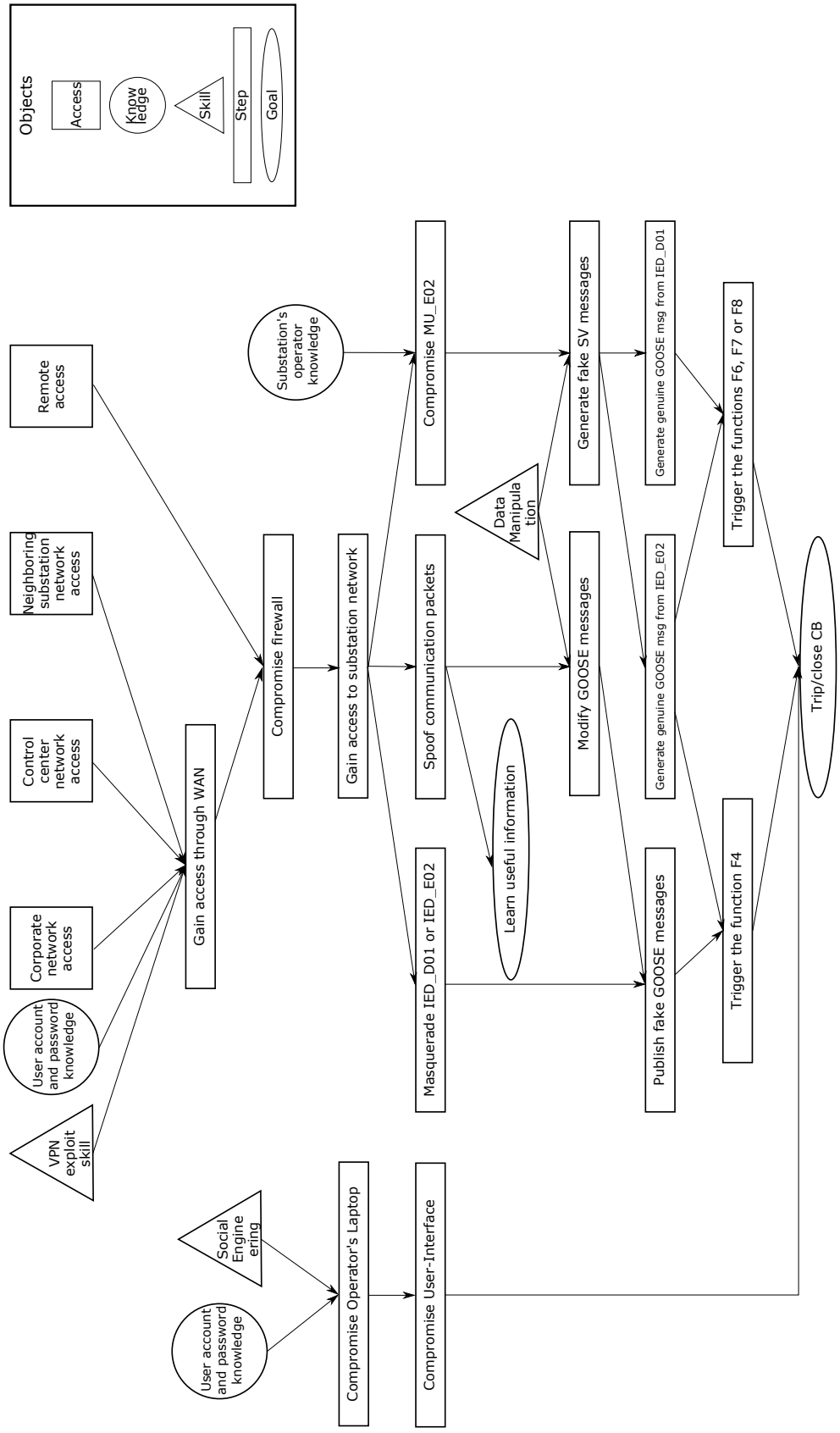



**Figure 2.9:** The Attack Execution Graph (AEG) in the transformer bay of the T1-1 substation

# CHAPTER 3

## Analysis and Long-Range Memory Modeling of the IEC 61850 Network Traffic

## List of Symbols

| Notation | Description |
|---|---|
| $a_i$ | An element of the $\mathbf{A}$ matrix |
| $\mathbf{A}$ | The state transition matrix $\in \mathbb{R}^{n \times n}$ |
| $B$ | Backshift operator |
| $\mathbf{C}$ | The measurement matrix $\in \mathbb{R}^{g \times n}$ |
| $d$ | The difference coefficient |
| D | A selection term for the measurement equation |
| $e[k]$ | Value of the sequence $\{e[k]\}$ at discrete-time $k$ |
| $H$ | Hurst parameter |
| $\mathbf{K}$ | The Kalman filter gain |
| $l$ | Delay order of the back-shift operator |
| $L$ | Length of non-overlaping intervals composing a time-series |
| $m$ | The level of aggregation |
| $N$ | Size of a time-series |
| $p$ | The order of the autoregressive polynomial |
| $q$ | The order of moving the average polynomial |

| Notation | Description |
|---|---|
| $\mathbf{Q}$ | A $n \times n$ covariance matrix of the states or process noise |
| $S_i$ | The standard deviation of a subset x calculated over the interval $[i,u]$ |
| $W_{i,u}$ | The partial sum of a subset x calculated over the interval $[i,u]$ |
| $x$ | A stochastic time-series |
| $x^{(m)}$ | The aggregated sequence by $m$ of $x$ |
| $\boldsymbol{\alpha}[k]$ | The state vector at sample $k$ |
| $\Gamma(.)$ | The gamma (generalized factorial) function |
| $\boldsymbol{\eta}[k]$ | A state disturbance vector $\in \mathbb{R}^{g\times 1}$ |
| $\boldsymbol{\varepsilon}$ | Model residuals |
| $\Theta(B)$ | Moving average (MA) polynomial operator of an ARFIMA model |
| $\boldsymbol{\Theta}$ | The parameter vector |
| $\boldsymbol{\mu}$ | The conditional mean of the state vector |
| $\boldsymbol{\sigma}$ | The conditional variance of the state vector |
| $\sigma_e^2$ | Variance of a white Gaussian noise process |
| $\phi(B)$ | Autoregressive (AR) polynomial operator of an ARFIMA model |
| $\psi_j$ | Parameters of the MA part of the ARFIMA model for $j = 1,...,m$ |

The present chapter provides an analysis of the characteristics of the network traffic in IEC 61850 substations. Findings from the analysis of the network traffic in the dataset in the considered case study presented in [7] show the presence of short and long range dependencies. Those findings agree with works presented in the literature [103], [100], [32] and [42]. However, the few works that have dealt with the

analysis of the communication in IEC 61850 substations do not propose an adequate mathematical modeling of the data. Indeed, this is one of the contributions introduced in the present work. We design in the present chapter an SS-AR approximation of an ARFIMA model that fits the statistical characteristics of the network traffic. Adequacy of the chosen model is shown using the case study presented in Section 6.3. Justification of the model choice as well as discussion of the modeling procedure is presented in Section 3.4. Additionally to the main contribution of this chapter, theoretical background necessary for the understanding of the previously mentioned contributions is also introduced.

Integration of recommendations suggested in the IEC 61850 standard allows the use of IT technologies including standardized protocols, a systematic object-oriented structure for the configuration of the Substation Automation System (SAS). The support of Ethernet-based communication as well as the possibility of remote control actions is also offered within the IEC 61850 norm.

Typical IEC 61850 substation models have a hierarchical structure with three different levels, being the station, bay and process layers. The station level includes engineering workstations, Human-Machine Interfaces (HMIs) and gateways to the Energy Management System (EMS) and SCADA systems. The bay and process level network is an Ethernet network. More details about the architecture of IEC 61850 including basic concepts and object data model are presented in Section 2.2.

The particular structure of the electrical substation and the use of different protocols throughout the Substation Communication Network (SCN) results in an increased challenge for the understanding of the network communication patterns. In the present Chapter, different characteristics of the process network traffic is described and analyzed. Based on this, mathematical modeling of the network traffic in IEC 61850 substation is introduced. The required theoretical background is described in Section 3.2 and Section 3.3. Validation and further discussion of the modeling procedure by help of a use case is presented in Section 3.4.

## 3.1 Characteristics of the Network Traffic

Different types of messages are exchanged within the substation and can be divided from a data flow perspective into three types namely, cyclic, stochastic and burst data flows [109]. Cyclic data flows are time-driven data commonly used for transmitting power measurements from field devices within the process layer.

Sampled Values (SV) messages generated from MUs and transmitted to Protection and Control (P&C) IEDs in the bay level, result in cyclic data flows. This communication is used to transmit time-critical information and large amounts of data.

In case of a fault, protection actions need to be taken through, for instance, a status change of one or multiple CBs. In a similar situation, GOOSE messages change from a cyclic mode to a burst mode to transmit timely information about control and protection actions.

Therefore, the network traffic in IEC 61850 electrical substations has unique features as it includes large multicast traffic that is periodic in general but which also includes bursty sequences. Such characteristics can be challenging to analyze using conventional models. In the following subsections, an analysis of the network traffic in IEC 61850 electrical substations is presented.

A set of relevant characteristics is established based on [33]. Floyd and Paxson introduce a method to "search for invariants" to tackle the difficulties in modeling Internet traffic [33]. The term invariant is used to refer to a behavior that was empirically proven to hold in a very wide range of environments. In the present work, three invariants that are the most relevant to characterize the process traffic are considered.

### 3.1.1 Diurnal Patterns

The variation of activity, for instance depending on specific times, is one of the properties that can be observed in the network traffic. This variation does not only depend on human activity but can also result from specific network protocols, for instance, some used in the industrial field [33] or from automated operations. Indeed, correlation with the network activity is not always human-initiated. Inspection of the number of active connections, packets per second and bytes per second and other network telemetry measures might reveal diurnal patterns in the network activity. Thus, the analysis of diurnal patterns can be conducted on different network metrics. A relatively large dataset, of at least of one week or several days in the case of electrical substations, shall be available to deduce the presence of diurnal patterns.

### 3.1.2 Distributional Considerations of the Data

Several works ([109], [103], [42] and [100]) characterize the data flow in electrical substations using several models depending on the type of the messages. Depending on the type of the transmitted information, seven categories of messages are introduced in IEC 61850 [51], namely fast message, medium speed message,low speed message, raw data message, file transfer function, time synchronization message, and access control command . The classification of the messages is mainly based on the type of information broadcasted through the substation including information such as the protection commands or the measurement values from physical devices. Fast or medium speed messages have different features from, for instance, file transfer function or access control command messages. However, from the perspective of

a data flow characteristics in the time domain, they can be split in three different categories namely, cyclic, stochastic and burst data [109]. For instance, in [109], a Pareto distribution for analysis of burst data flow was suggested, whereas in [100], a Weibull distribution was adopted instead. Indeed, Ustun et al. [100] claim that a Weibull distribution fits better the increasing retransmission scheme of bursty GOOSE messages. Network traffic in general Internet can be represented by heavy-tail distributions such as Ethernet bursts and FTP activity [101].

In the previously mentioned works [100, 101, 109], the distributions in general internet traffic or only specific message types in substations are considered. Modeling the network traffic in IEC 61850 substations is a challenging task due to the various operation modes including normal and burst data flows in the case of faults. Studies focusing on describing the network traffic ([32], [103] and [42]) show that the network traffic in electrical substations exhibits short-range and long-range dependencies. Some research works ([32], [103] and [42]) have been developed to model the substation communication network. Considerations of the self-similarity of the network traffic in IEC 61850 was already investigated in only few of the previously mentioned works [42, 103] and similar conclusions were shown in Section 3.1.3 with data presented in our case studies. In the next Section 3.1.3, the possible presence of self-similarity features in the process traffic of IEC 61850 electrical substations will be studied.

### 3.1.3 Self-Similarity

The self-similarity can be seen, in practice, by the presence of extended periods where the traffic is larger than the sample mean at different time scales, for instance for the number of bytes per second. The degree of self-similarity in the network traffic is commonly determined by using the Hurst parameter [49].

These periods of "spikes" in the traffic are referred to as "burstiness" [65]. Let $\{x[k]\}$, $k = 0,...,N-1$ be a time-series of size $N$. If the time series $x$ is self-similar, the following holds [3]

$$x[k] \overset{d}{=} m^{1-H} x^{(m)}[k] \text{ for all } m \in \mathbb{N} \tag{3.1}$$

where $\overset{d}{=}$ is an equality in the sense of finite dimensional distribution, $H$ is the Hurst parameter and $x^{(m)}$ is the aggregated sequence by $m$ of $\mathbf{x}$:

$$x^{(m)}[k] = 1/m \sum_{k=(j-1)m+1}^{jm} x[k],\ j = 1,2,3\ldots \tag{3.2}$$

Several tests have been commonly used in the literature ([33, 65]) to show self-similarity of the data. Two of the most known visual methods to show self-similarity are the $R/S$ analysis and the variance-time plot [73].

For the next description of both tests, let $x[k]$ be the throughput at time $k$ with $N$ being the size of the time series.

### Variance time plots

The first test to verify the self-similarity of a time- series is the variance-time plot. The presence of self-similarity can be checked by observing the variance function of $x^{(m)}[k]$ defined in (3.2) versus the aggregation level $m$.

The variance $\sigma^2$ of the aggregated process defined in (3.2) is calculated as follows:

$$\sigma^2 = S^2(\mathbf{x}^{(m)}) = \frac{1}{(N/m)} \sum_{k=1}^{N/m} \left(x^{(m)}[k] - \bar{x}^{(m)}\right)^2 \tag{3.3}$$

The variance plot shown in Figure 3.1, is defined by plotting the variance of the aggregated process $x^{(m)}[k]$, versus different aggregation levels in log-log scale.

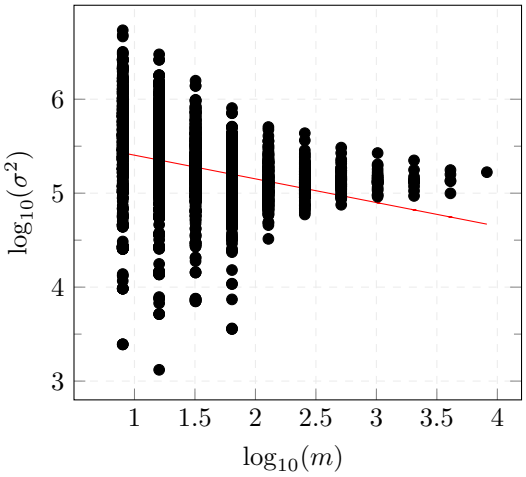



**Figure 3.1:** Variance time diagram

The Hurst parameter $H$ can be obtained from the previous plot with a line fitted to the curve, representing $\beta$ using least-squares with the relation $H = 1 + \beta/2$ which gives a value of $\hat{H} = 0.87$.

### Rescaled adjusted range (R/S)

The $R/S$ method is based on first dividing the time-series into non-overlapping intervals of length $L$. The partial sum for each of the intervals is then calculated. Let $\hat{\mu}$ or $\bar{x}$ be the sample mean of the time series $x$ with starting point $k_i$ and size $L$,

$$\hat{\mu}[k_i,\, L] = \bar{x}[k_i,L] = \frac{1}{L} \sum_{k=k_i}^{k_i+L} x[k] \tag{3.4}$$

and $\hat{\sigma}[k_i,\, L]$ be the sample standard deviation of a the time series $x$ with starting point $k_i$ and end point $k_{n_i} = k_i + L$

$$S[k_i,\, L] = \hat{\sigma}_i = \left( \frac{1}{L} \sum_{k=k_i}^{L-1} \left( x[k] - \bar{x}[k_i,\, L] \right)^2 \right)^{1/2} \tag{3.5}$$

The partial sum $W_{i,u}$ is defined as follows:

$$W[k_i,\, L,\, u] = \sum_{k=k_i}^{k_i+u} \left( x[k] - \bar{x}[k_i,\, L] \right) \tag{3.6}$$

where $u$ a running index of $k$ within the interval $[0,\, L]$.

The *rescaled adjusted range (R/S)* statistics is defined as the quotient of the difference between the maximum and the minimum of the partial sum and the standard deviation of the considered time series and is calculated as follows [71]:

$$R/S[k_i,\, L] = 1/S[k_i,\, L] \left[ \max_{0 \le u \le L} W[k_i,\, L,\, u] - \min_{0 \le u \le L} W[k_i,\, L,\, u] \right] \tag{3.7}$$

Figure 3.2 represents the $\log_{10}(R/S)$ versus $\log_{10}(L)$ for the considered dataset. The slope of the regression with the least-squares method of $\log_{10}(R/S)$ versus $\log_{10}(L)$ represents the estimate of the Hurst parameter $\hat{H}$ which is equal to 0.58 for the dataset described in Section 6.2.1.

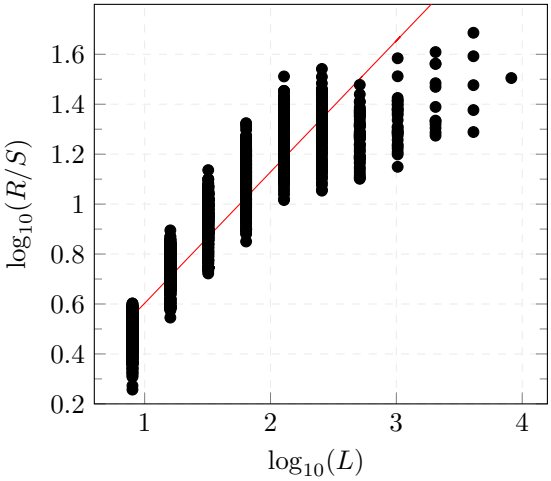



**Figure 3.2:** RS diagram

According to both tests, results show that the estimate of the Hurst parameter $\hat{H}$ of the considered dataset lies between 0.5 and 1 which indicates the self-similarity of the considered process. The time series representing the GOOSE network traffic in electrical substation has a statistical Long-Range Dependency (LRD) between the current value and values in different times of the series. One of the most used

models to describe long-memory characteristics is the Auto-Regressive Fractionally Integrated Moving Average (ARFIMA) model [9].

## 3.2 Mathematical ARFIMA Modeling of the Traffic in IEC 61850 Substations

After discussing the unique features of the IEC 61850 process network traffic, we select an Auto-Regressive Fractionally Integrated Moving Average (ARFIMA) model to describe the GOOSE network traffic. In the following, explanations of concepts necessary to describe a suitable model for the process network traffic as well as an adapted Anomaly Detection (AD) for DoS attacks in GOOSE communication is presented.

### 3.2.1 ARFIMA Model

Considering the particular characteristics of the IEC 61850 GOOSE traffic presented in Section 3.1, an ARFIMA model is, thus, suitable to describe the substation communication network. Signals containing spikes that exhibit properties of self-similarity and LRD cannot be processed by conventional time series models such as AR or ARMA.

An ARFIMA model consists of an Auto-Regressive (AR) part, a Moving Average (MA) filter, and an integration term (I) which is employed for differencing the raw measurements selected for modeling the IEC 61850 GOOSE traffic. (ARFIMA model is also referred to as Fractional ARIMA (FARIMA) model in some references [103] and [42]).

The ARFIMA model is a generalization of the integer order models being the autoregressive integral moving average (ARIMA) and autoregressive moving average (ARMA) model – two of the most known filters of these models.

The use of fractional difference operator rather than an integer one as in ARIMA models, was suggested by Hosking et al. [46] in the context of hydrology in order to represent the LRD.

An ARFIMA process is expressed as following:

$$\phi(B)(1-B)^d x[k] = \theta(B)e[k],\ e[k] \sim \mathcal{N}(0,\sigma_e^2) \tag{3.8}$$

where $x[k]$ is the GOOSE traffic in the SCN, $\phi(B) = 1 - \phi_1 B - \phi_2 B^2 - ... - \phi_p B^p$ is the autoregressive average polynomial and $\theta(B) = 1 + \theta_1 B + \theta_2 B^2 + ... + \theta_q B^q$ is the moving average polynomial. Thereby, $p$ is the auto-regressive order, $q$ is the moving average order and $d$ is the level of differencing. The term $e[k]$ is a sequence of independent and identically distributed (i.i.d) random variables, representing noise (error in data), i.e., white noise with variance $\sigma_e^2$.

$(1-B)^l$ is called the difference operator with $l$ being the delay order of the back-shift operator and $B$ being the backshift operator and defined by

$$B^l x[k] = x[k-l] \tag{3.9}$$

Contrarily to the ARMA or ARIMA model that can only represent the short-range dependency, the ARFIMA model can capture the LRD as the parameter $d$ is no longer restricted to integer values [46]. Accordingly, the difference operator can be expressed using a binomial expansion of the real number $d$ with the Gamma function:

$$(1-B)^d = \sum_{k=0}^{\infty} \binom{d}{k} (-B)^k \tag{3.10a}$$

$$= \sum_{k=0}^{\infty} \frac{\Gamma(d+1)}{\Gamma(k+1)\Gamma(d+1-k)} (-B)^k \tag{3.10b}$$

where $\Gamma(.)$ represents the gamma (generalized factorial) function that is defined as:

$$\Gamma(x) = \int_0^{\infty} e^{-t} t^{x-1} dt \tag{3.11}$$

Indeed, after computing the Hurst parameter $H$ and concluding the value of $d$ such as $d = H - 0.5$ [46].

In the following, general approaches for the parameter estimation and the model prediction will be discussed.

### 3.2.2 General Model Predictor

In a *good* model, the prediction errors shall be small [35] which indicates that the model can describe well the data. The general prediction model is expressed as a function of past data and parameters as:

$$\hat{x}[k] = f(x[k-1], \hat{\boldsymbol{\Theta}}) \tag{3.12}$$

where $\hat{x}[k]$ depends on measurement of $\mathbf{x}$ up to $k-1$ and $\hat{\boldsymbol{\Theta}}$, the estimated parameter vector. The prediction errors are thus expressed as follows:

$$\varepsilon[k] = x[k] - \hat{x}[k] \tag{3.13}$$

where $\varepsilon[k]$ is the model residual at time $k$.

Estimation methods attempt to compute the parameter vector $\boldsymbol{\Theta}$ that minimizes a cost function based on $\varepsilon[k]$ in (3.13).

The ARFIMA model was described in Section 3.2.1. According to Haslett and Raftery [43] an approximate one-step ARFIMA predictor of $x[k]$ is given by

$$\hat{x}[k] = \phi(B)\boldsymbol{\theta}^{-1}(B)\sum_{j=1}^{k-1}\Phi_{kj}x[k-j] \tag{3.14}$$

with

$$\Phi_{kj} = -\binom{k}{j}\frac{\Gamma(j-d)\Gamma(k-d-j+1)}{\Gamma(-d)\Gamma(k-d+1)}, \text{ for } j = 1,...,K \tag{3.15}$$

where $\Gamma(.)$ represents the gamma (generalized factorial) function that is defined in (3.11).

The prediction errors $\varepsilon[k]$ can be derived by replacing (3.14) in (3.13). Then, by maximizing (3.16), an estimation of the parameter vector $\boldsymbol{\theta}$ is obtained.

### 3.2.3 Maximum Likelihood Estimation

The Maximum Likelihood Estimator (MLE) is one of the most popular approaches to obtain a practical estimator that has an optimal performance when large enough data records are used [58]. The MLE is defined as the value of $\boldsymbol{\Theta}$ that maximizes the likelihood function $p(x;\boldsymbol{\Theta})$. The MLE is asymptotically efficient for large data records which defines the nature of the approximation obtained using the estimator.

The parameter vector can be estimated by maximizing the likelihood function [96]:

$$p(x;\boldsymbol{\Theta}) = \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}[\det \Lambda]}\exp\left[-\frac{1}{2}\sum_{k=0}^{N-1}\varepsilon[k]^T\Lambda^{-1}\varepsilon[k]\right] \tag{3.16}$$

where $\Lambda$ is the covariance matrix of the noise, $\boldsymbol{\Theta}$ represents the model parameters and $\sigma^2$ is the noise variance. In (3.16), $N$ represents the size of the estimation dataset.

As a first example, the computation of the MLE of a parameter vector of a signal consisting in a signal embedded in White Gaussian Noise (WGN) is considered.

#### Explanatory example: signal embedded in WGN

Let us consider the data

$$x[k] = A + e[k],\ k = 0,1,...,N-1 \tag{3.17}$$

where $A$ is a constant and $e[k]$ is WGN with variance $\sigma^2$. The vector parameter $\boldsymbol{\Theta} = [A\ \sigma^2]^T$ is to be estimated. The Probability Density Function (PDF) is defined as follows

$$p(\mathbf{x};\boldsymbol{\Theta}) = \frac{1}{(2\pi\sigma^2)^{\frac{N}{2}}} \exp\left[-\frac{1}{2\sigma^2}\sum_{k=0}^{N-1}(x[k]-A)^2\right] \tag{3.18}$$

Taking the first derivatives of Equation (3.18) yields

$$\frac{\partial \ln p(\mathbf{x};\boldsymbol{\Theta})}{\partial A} = \frac{1}{\sigma^2}\sum_{k=0}^{N-1}(x[k]-A) \tag{3.19a}$$

$$\frac{\partial \ln p(\mathbf{x};\boldsymbol{\Theta})}{\partial \sigma^2} = -\frac{N}{2\sigma^2} + \frac{1}{\sigma^4}\sum_{k=0}^{N-1}(x[k]-A)^2 \tag{3.19b}$$

When solving for $A$ from Equation (3.19a), the following equality holds:

$$\hat{A} = \bar{x} = \frac{1}{N}\sum_{k=0}^{N-1}x[k] \tag{3.20}$$

When solving for $A$ from Equation (3.19b) and using Equation (3.20):

$$\hat{\sigma}^2 = \frac{1}{N}\sum_{k=0}^{N-1}(x[k]-\bar{x})^2 \tag{3.21}$$

The MLE is obtained as follows:

$$\hat{\boldsymbol{\Theta}} = \begin{bmatrix} \bar{x} \\ \frac{1}{N}\sum_{k=0}^{N-1}(x[k]-\bar{x})^2 \end{bmatrix} \tag{3.22}$$

The MLE will be further applied for parameter estimation as part the proposed AD method. In the following, the model used for the description of the substation network traffic is presented.

The MLE of an ARFIMA model can be estimated numerically. For the computations of the ARFIMA MLE, approximations have been developed such as [43] and [34]. An overview of different likelihood-based methods for estimation of long-memory time series models was presented in [16]. Since the statistical hypothesis testing considered in this work depends on the MLE of the ARFIMA model, a numerical approximation will be used.

## 3.3 State Space Modeling

Using state space methods for long-memory fractional integration modeling has been presented in several works ([15, 37, 85]). In the pioneer research of [15], the modeling of an LRD process is developed in which a univariate Auto-Regressive Fractionally Integrated Moving Average (ARFIMA) model was considered. The work in [37] evaluated the truncation lag $m$ of the state space representation for ARFIMA models and validated it in different case studies including structural breaks and missing values.

### 3.3.1 State Space Representation of ARFIMA

Contrarily to standard ARIMA models, there are no finite-dimensional state space representations of ARFIMA models with long-memory parameter $d$ as demonstrated by Chan and Palma in [15].

For the sake of generality, a multivariate case of the time series $\mathbf{x}[k]$ is considered in the present Section 3.3. The general representation of a state space model includes two equations. The first equation, namely the transition equation, defines the evolution of the state vector $\boldsymbol{\alpha}[k]$ and is described by the (3.23):

$$\boldsymbol{\alpha}[k+1] = \mathbf{A}\boldsymbol{\alpha}[k] + \mathbf{H}\boldsymbol{\eta}[k],\ \boldsymbol{\eta}[k] \sim \mathcal{N}(0,\mathbf{Q}) \tag{3.23}$$

where $\mathbf{A} \in \mathbb{R}^{n\times n}$ is the state transition matrix and $\mathbf{H} \in \mathbb{R}^{n\times g}$ is a selection matrix. $\boldsymbol{\eta}[k]$ is a disturbance term with zero mean and covariance matrix $\mathbf{Q}$. The initial state $\alpha[0]$ is assumed to be Gaussian with known mean $\boldsymbol{\mu}_0$ and variance $\boldsymbol{\Sigma}_0$.

The second one, namely the measurement equation, describes the relation between the time series $\mathbf{x} \in \mathbb{R}$ and the state vector $\boldsymbol{\alpha}[k]$ and is defined as follows (see [37]):

$$x[k] = \mathbf{C}\boldsymbol{\alpha}[k] + \mathrm{D}e[k],\ e[k] \sim \mathcal{N}(0,\sigma_{\mathbf{e}}^2) \tag{3.24}$$

where $\mathbf{C} \in \mathbb{R}^{1\times n}$ is the output matrix and $\boldsymbol{\alpha}[k] \in \mathbb{R}^n$ is the state vector. $\mathrm{D} \in \mathbb{R}$ is a selection term.

According to [15], the previously presented state space system can be written in two different ways, namely, $AR(\infty)$ and $MA(\infty)$ for long-memory models. Choosing a large enough truncation lag $m$ allows the evaluation of an approximation of the likelihood function. Thus, $AR(m)$ and $MA(m)$ models can be presented in state space form and the states can be estimated using Kalman Filter (KF) recursions [37]. The multivariate representation of AR and MA are called VAR and VMA,

respectively [50]. For sake of simplicity, the univariate case is considered and the $SS\text{-}AR$ or $AR(m)$ approximation can be presented as follows:

$$\mathrm{D} = 0, \tag{3.25a}$$

$$\mathbf{C} = (1,0,...,0), \tag{3.25b}$$

$$\mathbf{A} = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{3.25c}$$

$$\mathbf{H} = (1\ 0 \cdots 0)^T \tag{3.25d}$$

where the parameters $a_i$ for $j = 1,...,m$ are computed according to [37]. Thus, expressing an ARFIMA $(p,d,q)$ model using a truncated infinite AR expansion yields

$$x[k] = \sum_{j=1}^{m} a_j x[k-j] + e[k] \tag{3.26}$$

A second way to write the state space of a long-memory model is using an $MA(m)$ approximation defined as follows:

$$\mathbf{C} = (1,0,...,0) \tag{3.27a}$$

$$\mathrm{D} = 0, \tag{3.27b}$$

$$\mathbf{A} = \begin{bmatrix} 0 & I_m \\ 0 & 0 \end{bmatrix}, \tag{3.27c}$$

$$\mathbf{H} = (1\ \psi_1\ \psi_2 \cdots \psi_m)^T \tag{3.27d}$$

with $\psi_j$ being the parameters computed according to [46]. Thus, the resulting ARFIMA $(p,d,q)$ model using a truncated infinite MA expansion is expressed as follows:

$$x[k] = \sum_{j=0}^{m} \psi_j e[k] \tag{3.28}$$

Parametric approaches for calculating the maximum likelihood estimation of stationary generalized long-memory models are generally computationally demanding. A Bayesian sampling algorithm for a bivariate process including one stationary long-memory component was proposed in [48]. To compute the maximum likelihood

estimator, the authors in [75] propose a sampling schema for stationary generalized long-memory models with one or more latent ARFIMA components. They showed the increasing numerical computation when more than two latent long-memory factors are present. In the following paragraphs, an SS-AR model to approximate the ARFIMA model is considered.

### 3.3.2 Estimation of State Space Models

In order to have consistent estimates of state-space models for long-range fractionally integrated systems, subspace methods were shown to be *good* candidates [6]. Subspace methods offers several attractive features. Their concept can be described as a model reduction applied to an initial high-order vector autoregression estimate. Their conceptual simplicity allows an easy handling of problems of missing values or demeaning and de-trending [6]. The efficiency of their numerical implementation is also, a considerable asset. However, the representation introduced in (3.25) requires alternative estimation methods due to the special form of the state space matrices. The expectation maximization (EM) algorithm has be shown to be a robust tool for parameter estimation of models as in (3.25).

The conditional mean $\boldsymbol{\mu}$ and variance $\boldsymbol{\Sigma}$ of the state vector are defined as follows:

$$\boldsymbol{\alpha}[k|k-1] = E(\boldsymbol{\alpha}[k]|x[k-1]) = \boldsymbol{\mu}, \tag{3.29a}$$

$$\mathbf{P}[k|k-1] = Var(\boldsymbol{\alpha}[k]|x[k-1]) = \boldsymbol{\Sigma} \tag{3.29b}$$

An iterative maximum likelihood estimator of the parameters of the state space model is derived from the following log-likelihood [23]:

$$\begin{aligned} \log L = &-\frac{1}{2}\log|\boldsymbol{\Sigma}| - \frac{1}{2}(\boldsymbol{\alpha}-\boldsymbol{\mu})^{\mathrm{T}}\boldsymbol{\Sigma}^{-1}(\boldsymbol{\alpha}-\boldsymbol{\mu}) \\ &- \frac{N}{2}\log|\mathbf{Q}| - \frac{1}{2}\sum_{k=1}^{N}(\boldsymbol{\alpha}[k]-\mathbf{A}\boldsymbol{\alpha}[k-1])^{\mathrm{T}}\mathbf{Q}^{-1}(\boldsymbol{\alpha}[k]-\mathbf{A}\boldsymbol{\alpha}[k-1]) \\ &- \frac{N}{2}\log|\mathbf{R}| - \frac{1}{2}\sum_{k=1}^{N}(\mathbf{x}[k]-\mathbf{C}\boldsymbol{\alpha}[k])^{\mathrm{T}}\mathbf{R}^{-1}(\mathbf{x}[k]-\mathbf{C}\boldsymbol{\alpha}[k]) \end{aligned} \tag{3.30}$$

where R is the variance of the sequence defined by $x[k]-\mathbf{C}\boldsymbol{\alpha}[k]$. Only the estimated log likelihood is accessible since some hidden states are unknown and the observations $x[0],\ldots,x[N-1]$ are accessible.

$$
\begin{aligned}
G(\Theta) =& E(\log L|x[1],\ldots,x[N]|) \\
=& -\frac{1}{2}\log|\boldsymbol{\Sigma}| - \frac{1}{2}\operatorname{Tr}\left[\boldsymbol{\Sigma}^{-1}(\mathbf{P}[0|N] + (\boldsymbol{\alpha}[0|N] - \boldsymbol{\mu})(\boldsymbol{\alpha}[0|N] - \boldsymbol{\mu})^{\mathrm{T}})\right] \\
& - \frac{N}{2}\log|\mathbf{Q}| - \frac{1}{2}\operatorname{Tr}\left[\mathbf{Q}^{-1}(\mathbf{F} - \mathbf{E}\mathbf{A}^{\mathrm{T}} - \mathbf{A}\mathbf{E}^{\mathrm{T}} + \mathbf{A}\mathrm{D}\mathbf{A}^{\mathrm{T}})\right] - \frac{N}{2}\log|\mathbf{R}| \\
& - \frac{1}{2}\operatorname{Tr}\left[\mathbf{R}^{-1}\sum_{k=1}^{N}(x[k] - \mathbf{C}\boldsymbol{\alpha}[k|N])(x[k] - \mathbf{C}\boldsymbol{\alpha}[k|N])^{\mathrm{T}}\mathbf{C}\mathbf{P}[k|N]\mathbf{C}^{\mathrm{T}}\right]
\end{aligned} \tag{3.31}
$$

The maximization of $G(\Theta)$ is obtained by setting its derivative to zero following those updating rules:

$$\mathbf{A}^{r+1} = \mathbf{E}\mathrm{D}^{-1} \tag{3.32a}$$

$$\mathbf{Q}^{r+1} = \frac{1}{N}(\mathbf{F} - \mathbf{E}\mathrm{D}^{-1}\mathbf{E}^{\mathrm{T}}) \tag{3.32b}$$

$$\mathbf{R}^{r+1} = \frac{1}{N}\sum_{k=1}^{N}\left((x[k] - \mathbf{C}\boldsymbol{\alpha}[k|N])(x[k] - \mathbf{C}\boldsymbol{\alpha}[k|N])^{\mathrm{T}} + \mathbf{C}\mathbf{P}[k|N]\mathbf{C}^{\mathrm{T}}\right) \tag{3.32c}$$

where,

$$\mathrm{D} = \sum_{k=1}^{N}(\mathbf{P}[k-1|N] + \boldsymbol{\alpha}[k-1|N]\boldsymbol{\alpha}^{\mathrm{T}}[k-1|N]) \tag{3.33a}$$

$$\mathbf{E} = \sum_{k=1}^{N}(\mathbf{P}[k|N] + \boldsymbol{\alpha}[k|N]\boldsymbol{\alpha}^{\mathrm{T}}[k-1|N]) \tag{3.33b}$$

$$\mathbf{F} = \sum_{k=1}^{N}(\mathbf{P}[k|N] + \boldsymbol{\alpha}[k|N]\boldsymbol{\alpha}^{\mathrm{T}}[k|N]) \tag{3.33c}$$

The quantities required in (3.33) are computed using the Kalman smoother as in (3.38). At each iteration, the rules in (3.32) are computed using (3.33).

#### Convergence properties of the Expectation Maximization (EM) algorithm

In the following, an introductory example to analyze the convergence properties of the Expectation Maximization (EM) algorithm is considered.

Consider an example of an ARFIMA(1,d,1) model which is approximated using a state space (SS-AR) model whose parameters are estimated with the EM algorithm. A total of 25 experiments is performed on the ARFIMA model.

The log-likelihood function is maximized in the estimation algorithm and the results are shown in Figure 3.3 for each experiment.

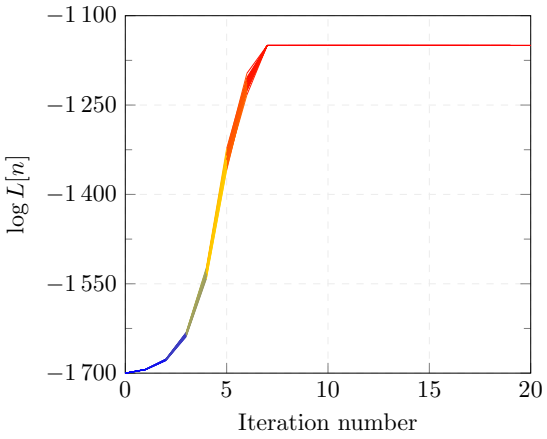



**Figure 3.3:** Maximization of the log-likelihood function

The EM algorithm can guarantee for the present case study convergence of the log-likelihood function after relatively few iterations. The estimated value of the model parameters is presented in the following.

$$\mathrm{D} = 0, \tag{3.34a}$$

$$\mathbf{C} = (1 \quad 0 \quad \dots \quad 0), \tag{3.34b}$$

$$\mathbf{A} = \begin{pmatrix} 0.33 & 0.21 & 0.24 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \tag{3.34c}$$

$$\mathrm{R} = 1.02, \tag{3.34d}$$

$$\mathbf{Q} = \begin{pmatrix} 0.47 & 0 & 0 \\ 0 & 1.73 & \\ 0 & 0 & 0.16 \end{pmatrix} \tag{3.34e}$$

$$\mathbf{H} = (1 \quad 0 \quad 0)^T \tag{3.34f}$$

In the discussion Section 3.4, the parameters of the **A** matrix are further analyzed and discussed.

### 3.3.3 Kalman Filter (KF)

The problem of finding an optimal solution of the state estimation for a discrete-time stochastic linear dynamic system can be solved using the Kalman filter [24, 37]. The KF [24] is used to build the one-step-ahead predictor of $\mathbf{x}[k]$ as it produces the minimum mean square estimator of the state space vector and the mean square error matrix under the assumption of White Gaussian Noise (WGN). The likelihood can be

evaluated according to the prediction error decomposition due to the independence of the one-step-ahead prediction errors [37].

The input to the KF algorithm are the observations and the system matrices and it returns the innovations or the one-step-ahead prediction errors $\boldsymbol{\nu}[k]$ with the variance R, the one-step-ahead predictor of the states as well as their conditional covariance matrix.

The recursive expressions for $k = 1,...,T$ of KF equations is the following:

$$\boldsymbol{\alpha}[k+1|k] = \mathbf{A}\boldsymbol{\alpha}[k|k-1] + \mathbf{K}[k]\boldsymbol{\nu}[k] \tag{3.35a}$$

$$\mathbf{P}[k+1|k] = \mathbf{A}\mathbf{P}[k|k-1](\mathbf{A} - \mathbf{K}[k]\mathbf{C})^{\mathrm{T}} + \mathbf{H}\mathbf{Q}\mathbf{H}^{\mathrm{T}} \tag{3.35b}$$

The innovation process $\boldsymbol{\nu}$ and the Kalman filter gain $\mathbf{K}$ are defined as follows:

$$\text{The innovation process:} \qquad \nu[k] = x[k] - \mathbf{C}\boldsymbol{\alpha}[k|k-1] \tag{3.36}$$

$$\text{The Kalman gain: } \mathbf{K}[k] = \mathbf{A}\mathbf{P}[k|k-1]\mathbf{C}^{\mathrm{T}}(\mathbf{C}\mathbf{P}[k|k-1]\mathbf{C}^{\mathrm{T}} + \mathrm{R}\mathbf{D}\mathbf{D}^{\mathrm{T}})^{-1} \tag{3.37}$$

where $\mathbf{Q} \in \mathbb{R}^{n \times n}$ is the covariance matrix of the states or process noise and $\mathrm{R} \in \mathbb{R}$ is the variance of the measurement or signal noise. The estimation of $\boldsymbol{\alpha}[k+1]$ given $x[k], x[k-1]...$ is expressed by $\mathbf{P}[k+1]$

The Kalman smoother is proposed for state estimation based on the values of the signal $x[k]$. The equations for the Kalman smoother are expressed as following for $k = n, n-1, \ldots, 1$:

$$\mathbf{J}[k-1] = \mathbf{P}[k-1|k-1]\mathbf{A}^{\mathrm{T}}(\mathbf{P}[k|k-1])^{-1} \tag{3.38a}$$

$$\boldsymbol{\alpha}[k-1|n] = \boldsymbol{\alpha}[k-1|k-1] + \mathbf{J}[k-1](\boldsymbol{\alpha}[k|n] - \mathbf{A}\boldsymbol{\alpha}[k-1|k-1]) \tag{3.38b}$$

$$\mathbf{P}[k-1|n] = \mathbf{P}[k-1|k-1] + \mathbf{J}[k-1](\mathbf{P}[k|n] - \mathbf{P}[k|k-1])\mathbf{J}[k-1]^{\mathrm{T}} \tag{3.38c}$$

The initial values for the smoother are the final estimates of the filter.

### 3.3.4 Multi-step ahead Predictor for State Space Models

Depending on the the length of the data and at the step-ahead number of the estimator, several predictors can be defined [36]. The vector of one step-ahead predictor $\boldsymbol{\alpha}[k+1]$ or Kalman filter estimators is defined based on (3.24) and (3.23).

The state vector at $k+j$ can be written as follows [36]:

$$\boldsymbol{\alpha}[k+j] = \mathbf{A}^{j-1}\boldsymbol{\alpha}[k+1] + \boldsymbol{w}[k] \tag{3.39a}$$

$$w[k] = \mathbf{A}^{j-1}\mathbf{H}\boldsymbol{\eta}[k] + \mathbf{A}^{j-2}\mathbf{H}\boldsymbol{\eta}[k+1] + \cdots + \mathbf{H}\boldsymbol{\eta}[k+j-1] \tag{3.39b}$$

The general expression of the j-step ahead forecast with $j > 1$ of the state vector $\hat{\boldsymbol{\alpha}}[k+j|k]$ is expressed from the conditional expectation of (3.39)

$$\hat{\boldsymbol{\alpha}}[k+j|k] = \mathbf{A}^{j-1}\hat{\boldsymbol{\alpha}}[k+1|k] \tag{3.40}$$

The error of the forecast of the state vector can be calculated as follows:

$$\boldsymbol{\alpha}[k+j] - \hat{\boldsymbol{\alpha}}[k+j|k] = \boldsymbol{\alpha}[k+j] - \mathbf{A}^{j}\hat{\boldsymbol{\alpha}}[k|k] \tag{3.41}$$

The previously introduced equation (3.40) can be used to describe the $j$-step ahead forecasts of the observation vector $x[k+j]$.

$$\hat{\mathbf{x}}[k+j|k] = \mathbf{C}\mathbf{A}^{j}\hat{\boldsymbol{\alpha}}[k|k] \tag{3.42}$$

The error of the forecast calculated in (3.42) is:

$$\mathbf{x}[k+j] - \hat{\mathbf{x}}[k+j|k] = \mathbf{x}[k+j] - \mathbf{C}\mathbf{A}^{j}\hat{\boldsymbol{\alpha}}[k|k] \tag{3.43}$$

## 3.4 Modeling Process Network Traffic using SS-AR

Considering the different characteristics of the network traffic analyzed in the previous sections, an Auto-Regressive Fractionally Integrated Moving Average (ARFIMA) model can be used to describe the Long-Range Dependency (LRD) in network communication of IEC 61850 substations [25]. Review of the theoretical and mathematical features of an ARFIMA model shows that using a state space representation of an ARFIMA model is adapted and offers several advantages as explained in Section 3.3.

For the modeling of the network traffic, a state space AR (SS-AR) model is selected to describe the communication. The state space modeling of long-range dependent data, that was first considered as an ARFIMA model, is achieved through a state-space representation reported in [15].

In the present section, modeling of the network traffic in an IEC 61850 substation using an SS-AR model is performed. The modeling process explained in the previous section (Section 3.3) is applied to the second use case described in Section 6.3.1.

Results of the obtained model are discussed and validation of the modeling accuracy is achieved using well-established criteria.

Given the model order $n$, the parameter vector $\boldsymbol{\Theta}$ that includes $\mathbf{A}$,$\mathbf{Q}$ and R is estimated from the univariate signal $\mathbf{x}_{\text{est}}$.

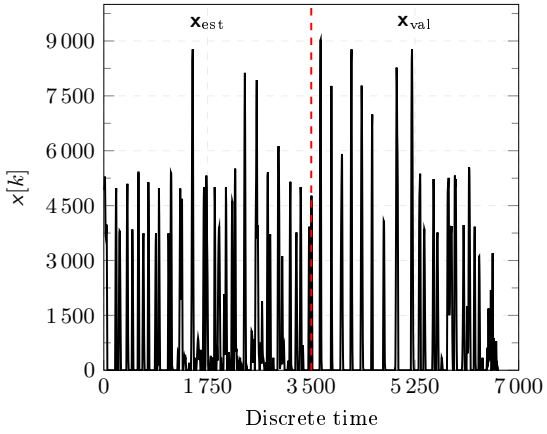



**Figure 3.4:** Estimation and validation datasets

The datasets $\mathbf{x}_{\text{est}}$ and $\mathbf{x}_{\text{val}}$, shown in Figure 3.4 are derived from the network traffic presented in the 66/11kV testbed [7].

The model predictions are computed using a validation dataset $\mathbf{x}_{\text{val}}$. The obtained values are compared with the signal measurements for model validation. The validation of the model through this last step is necessary to evaluate its accuracy. If after the validation step the model is accepted, it can be further used for prediction and detection. Otherwise, the estimation step shall be repeated changing user-defined parameters until satisfactory results about the estimated model are obtained.

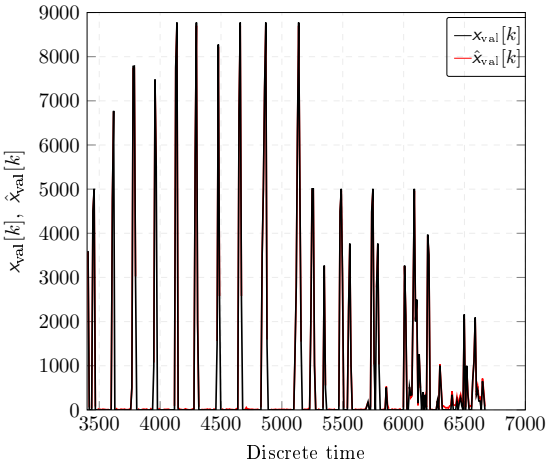



**Figure 3.5:** Substation network traffic used for estimation (depicted in black) and SS-AR model prediction (depicted in red)

The previously described modeling procedure is applied to one of the use cases presented in Section 6.3.1. It represents 10 mins of network traffic in bytes per second (bps) of an IEC 61850 substation.

As an example, the estimated parameters for the normal use case without variable load is presented. The definition of the parameters of the state space-AR model are introduced in (3.24), (3.44) and (3.23).

The estimated parameters for the SS-AR model of order $n = 10$ that is obtained empirically, are the following:

$$\mathbf{D} = 0, \tag{3.44a}$$

$$\mathbf{C} = (1 \quad 0 \quad \dots \quad 0), \tag{3.44b}$$

$$\mathbf{A} = \begin{pmatrix} -0.45 & -0.01 & 0.005 & -0.01 & 0.017 & -0.005 & -0.002 & 0.015 & 0.007 & -0.008 \\ 1 & 0 & 0 & & & \cdots & & 0 & 0 & 0 \\ 0 & 1 & 0 & & & \cdots & & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & & \ddots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & & & \cdots & & 0 & 1 & 0 \end{pmatrix}, \tag{3.44c}$$

$$\mathrm{R} = 0.3464, \tag{3.44d}$$

$$\mathbf{Q} = \mathrm{diag}(0.49,\ 1.13,\ 1.48,\ 1.82,\ 0.91,\ 0.60,\ 0.16,\ 0.60,\ 0.77,\ 0.63), \tag{3.44e}$$

$$\mathrm{H} = (1 \quad 0 \quad \dots \quad 0)^{\mathrm{T}} \tag{3.44f}$$

**Evaluation of the modeling of the substation traffic**

The model is evaluated using the validation dataset $x_{\mathrm{val}}$ presented in Figure 3.4. Figure 3.5 shows the real and the estimated signals, $x_{\mathrm{val}}[k]$ and $\hat{x}_{\mathrm{val}}[k]$ respectively. The output of the SS-AR model for the validation GOOSE traffic, $\hat{x}_{\mathrm{val}}[k]$, in red, and the dataset used for comparison $x_{\mathrm{val}}[k]$, in black, are shown in Figure 3.5.

To further assess the model performance, the goodness-of-fit is used as evaluation criterion which is defined as follows:

$$\mathrm{fit} = (1 - \mathrm{NRMSE}\,(x_{\mathrm{val}}[k], \hat{x}_{\mathrm{val}}[k])) \cdot 100\,\% \tag{3.45}$$

where a perfect fit is 100 %. Thereby the Normalized Root Mean Square Error (NRMSE) is defined by:

$$\mathrm{NRMSE} = \sqrt{\frac{\sum_{k=1}^{N} \left(x_{\mathrm{val}}[k] - \hat{x}_{\mathrm{val}}[k]\right)^2}{\sum_{k=1}^{N} \left(x_{\mathrm{val}}[k] - \bar{x}_{\mathrm{val}}[k]\right)^2}} \tag{3.46}$$

where $\bar{x}_{\mathrm{val}}[k] = \frac{1}{N} \sum_{k=1}^{N} x_{\mathrm{val}}[k]$ is the sample mean of the validation dataset, $x_{\mathrm{val}}[k]$ is the measured substation network traffic at discrete time $k$ and $\hat{x}_{\mathrm{val}}[k]$ is the model

prediction. The fit of the data to the state space AR approximation of an ARFIMA model as expressed in (3.45) yields 73.65 % which indicates that the chosen model can describe well the time series.

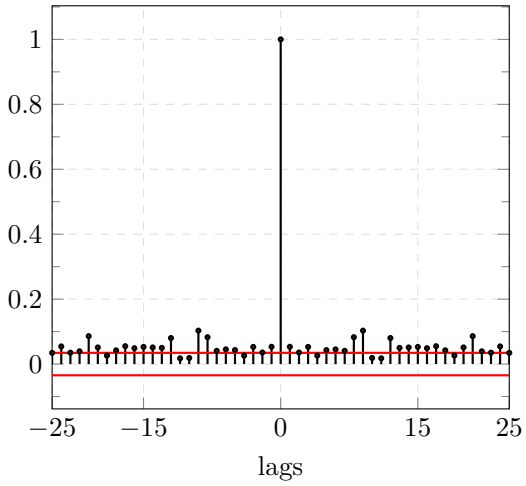



**Figure 3.6:** Auto-correlation of state-space model residuals

In addition to the model fit, an analysis of the residuals confirms the adequacy of the chosen model. The residuals obtained in the validation step are computed using the predictor of the model with the parameters of the SS-AR model and the validation dataset $\hat{\mathbf{x}}_{\text{val}}$.

The Auto-Correlation Function (ACF) of the residuals are computed and shown in Figure 3.6. The ACF of $\varepsilon[k]$ (see (3.13)) falls into the confidence level which indicates that the residuals can be considered as WGN and confirms that the model describes the GOOSE traffic data satisfactorily.

## 3.5 Discussion

In the present chapter, an analysis of the network traffic for the modeling the communication in electrical substations is investigated. A mathematical ARFIMA was first introduced to describe the Long-Range Dependency (LRD) of the traffic. A more general representation based on state space (SS) modeling is thereafter adopted to approximate the ARFIMA model.

Estimation and convergence properties of the SS-AR model regarding the log-likelihood function are discussed. The model parameters of the example considered in Section 3.3.2 are reported. In the following, the parameters of the $\mathbf{A}$ are analyzed.

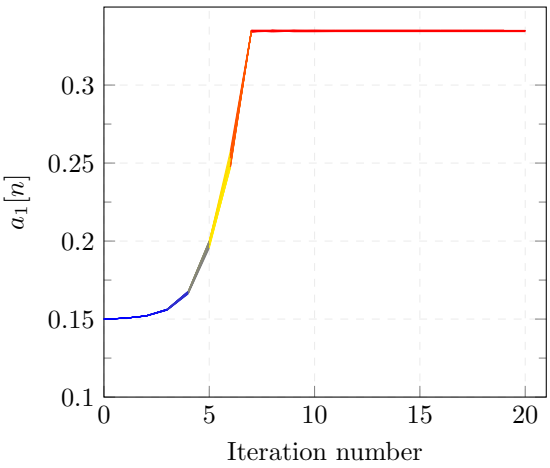



**Figure 3.7:** Convergence of the first element $a_1[n]$ of the **A** matrix in the SS-AR model

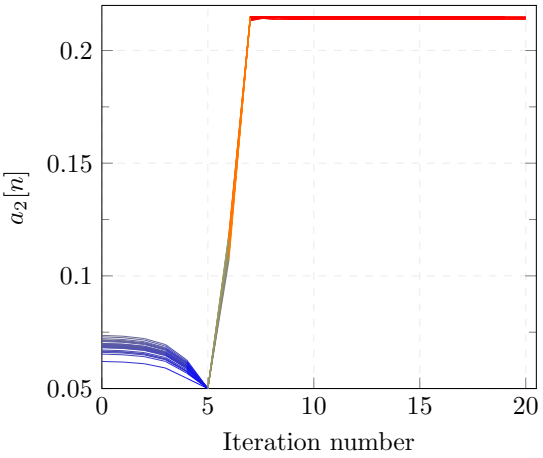



**Figure 3.8:** Convergence of the second element $a_2[n]$ of the matrix **A** matrix in the SS-AR model

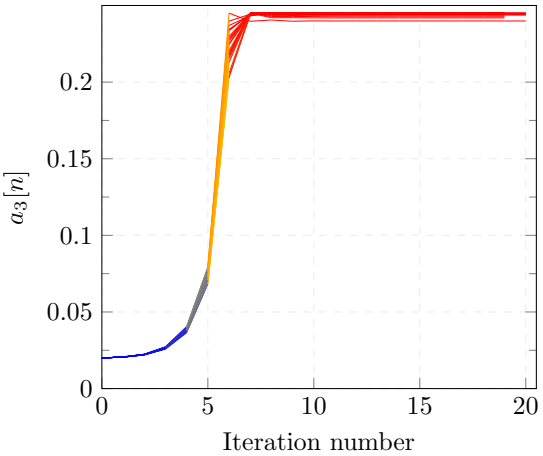



**Figure 3.9:** Convergence of the third element $a_3[n]$ of the **A** matrix in the SS-AR model

The different values of the estimated parameters $a_i$ of the matrix **A** of the obtained SS-AR are shown respectively in Figure 3.7, Figure 3.8 and Figure 3.9. The parameter

converge after some iterations for the same experiment. However, the parameter $a_2[k]$ ranges over a larger span of values in the first iterations in comparison with the other parameters. The cost function in the expectation-maximization (EM) algorithm is minimized for different combination of the parameters depicted in Figure 3.7 and Figure 3.9. The convergence properties are similar to Figure 3.3. The expectation-maximization algorithm can be adjusted by fixing the value of some parameters and computing the remaining ones. Knowledge about the signal under analysis is, thus required since the initial values of the parameters should be assigned based on the experience of the user.

# CHAPTER 4

## An Extension of the Detection Problem to IEC 61850 Network Traffic

## List of Symbols

| Notation | Description |
|---|---|
| $\mathbf{A}$ | The state transition matrix $\in \mathbb{R}^{n \times n}$ |
| $\mathbf{C}$ | The measurement matrix $\in \mathbb{R}^{g \times n}$ |
| D | A selection term for the measurement equation |
| $g$ | The CUSUM decision function |
| $\mathbf{H}$ | A selection matrix for the state equation |
| $\mathbf{Q}$ | A $n \times n$ covariance matrix of the states or process noise |
| $s[k]$ | Log-likelihood ratio increment |
| $x$ | A stochastic time-series |
| $\beta$ | The signature of additive change on the estimates |
| $\gamma$ | The threshold for the statistical detector |
| $\Gamma_x$ | Gain matrix for $\Upsilon_x$ |
| $\delta$ | The signature of additive change on the states |
| $\boldsymbol{\eta}[k]$ | A state disturbance vector $\in \mathbb{R}^{g \times 1}$ |
| $\boldsymbol{\varepsilon}$ | Model residuals |
| $\boldsymbol{\Theta}$ | The parameter vector |

| Notation | Description |
|---|---|
| $\Xi_\alpha$ | Gain matrix for $\Upsilon_\alpha$ |
| $\rho$ | The signature of additive change on the innovations |
| $\sigma_k$ | Variance matrix of the innovations |
| $\Upsilon_\alpha$ | Term to represent additive change in the states |
| $\Upsilon_x$ | Term to represent additive change in the observations |

Chapter 4 is mainly focused on formulating our detection problem as a statistical hypothesis testing for anomaly detection. Hence, introduction and extension of well-known techniques for our specific detection problem are presented. Setting the foundations of the detection problem is necessary to formulate the attack detection in IEC 61850 network traffic as a statistical hypothesis testing.

In fact, basics and extensions of well-known techniques for statistical anomaly detection are investigated in Section 4.1.1 and Section 4.1.2. After establishing the foundations for the basic statistical anomaly detection problem, the adaption of detectors to the state space model introduced in Section 3 as a well-suited model to describe the network traffic in IEC 61850 substations are described.

It is considered that anomalies affecting the communication traffic can be referred to as changes from the normal behavior. In order to better specify the considered attacks, different types of changes, namely additive and non-additive changes [5] are introduced in Section 4.2. According to the type of change, the adaption of the detectors used in our anomaly detection problem is presented. Discussion of the particular case of modeling the DoS attacks is presented in Section 4.4 using state space modeling adopted for IEC 61850 network traffic and the adequate formulation of the type of change.

## 4.1 Introduction to the Detection Problem

### 4.1.1 Statistical Hypothesis Testing

The network traffic in electrical substations based on IEC 61850 exhibits long-range dependency which can be described using models that account for those properties such as the state space representation of an ARFIMA model introduced in Chapter 3.

The problem of detecting attacks in the communication network traffic can be formulated as a change point detection problem which can be stated using statistical hypothesis related to the state of the system. The task to be addressed, is to decide between acceptance or rejection of anomaly that are formulated using two competing hypotheses. The hypothesis $\mathcal{H}_0$, referred to as the *null hypothesis*, indicates absence of anomaly. Furthermore, the hypothesis $\mathcal{H}_1$ indicates presence of an anomaly. In the most general situation, noise parameters such as variance or covariance matrix are also assumed to be unknown and need to be computed within the detection problem. This case is referred to as composite hypothesis testing [58].

To address the previously introduced problem, detectors are tools used to decide between two competing hypothesis. To better explain the detection problem, an example of a well-know detector, namely the Generalized Likelihood Ratio Test (GLRT) detector will be adopted. The GLRT detector [72] decides for $\mathcal{H}_1$ if

$$L_G(x) = \frac{p(\mathbf{x}; \boldsymbol{\Theta}_1, \mathcal{H}_1)}{p(\mathbf{x}; \boldsymbol{\Theta}_0, \mathcal{H}_0)} > \gamma \tag{4.1}$$

The numerator and denominator in (4.1) represent the Probability Density Function (PDF) under the hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, expressed by $p(\mathbf{x}; \boldsymbol{\Theta}_0, \mathcal{H}_0)$ and $p(\mathbf{x}; \boldsymbol{\Theta}_1, \mathcal{H}_1)$, respectively. $\gamma$ is the threshold that should be chosen as a trade-off between the Detection Rate (DR) and False Alarms (FAs). The term $\boldsymbol{\Theta}$ contains the different model parameters.

Since the occurrence time of an anomaly is assumed to be unknown, the network traffic measurements $x[k]$ should be analyzed sequentially for the computation of (4.1). The problem as stated in (4.1) is solved by computing the PDF under each hypothesis using different data windows. Some detectors such as the cumulative sum (CUSUM) test [83] can be formulated recursively depending of the type of change analyzed [5]. This will be further investigated in the next Section 4.1.2.

### 4.1.2 Introduction of Detectors

A commonly encountered problem in detection tasks is to locate an unknown abrupt change in a system. To formally state this problem, decision rules are defined in the form of statistical hypothesis testing as introduced in Section 4.1.1. Detectors commonly used to distinguish between the two competing hypothesis are based on likelihood ratio statistics. The cumulative sum (CUSUM) test proposed by [83] is a very well- known detection test based on the probability density functions of the system in the case of independent and identically distributed (i.i.d) random variables. The CUSUM is the optimal solution to the detection problem that, given a fixed false alarm rate, yields the smallest mean time delay [5, 83].

The CUSUM algorithm, first presented in [83], is used as a convenient detector for the problem presented in (4.1). The CUSUM decides for $\mathcal{H}_1$ if

$$g[k] > \gamma \tag{4.2}$$

The $\gamma$ is a user-defined threshold and $g[k]$ is the decision function that is defined depending on the analyzed case as follows:

$$\begin{aligned} g[k] &= (g[k-1] + s[k])^+ \\ \text{where } (g[k-1] + s[k])^+ &= \sup(0,\, g[k-1] + s[k]) \end{aligned} \tag{4.3}$$

The decision function is initialized as following $g[k] = 0$ and reset each time the condition (4.2) holds.

The log-likelihood ratio increment $s[k]$ is expressed in (4.4) according to [5]:

$$\begin{aligned} s[k] &= \frac{1}{2} \ln \frac{\hat{\sigma}_0^2}{\hat{\sigma}_1^2} + \frac{(\varepsilon_0[k])^2}{2\hat{\sigma}_0^2} - \frac{(\varepsilon_1[k])^2}{2\hat{\sigma}_1^2} \\ \text{with } \varepsilon_i[k] &= x_i[k] - \hat{x}_i[k],\ i = 0{,}1 \end{aligned} \tag{4.4}$$

$\varepsilon_i[k]$ and $\hat{\sigma}_i^2$ are the residuals and sample variance at time $k$ for the $i$-th hypothesis. The model output $\hat{x}_i[k]$ is computed using (3.14). In our case and most of the practical cases, the model parameters are unknown prior to the experiment, Maximum Likelihood Estimator (MLE) estimates of the model are used instead.

It is worth noting that the developed algorithm is able to detect multiple anomalies at unknown change times and assuming unknown noise parameters. This is particularly relevant in attacks such as double strike DDOS attacks that exhibits two consecutive pulses in the traffic intensity.

## 4.2 Types of Changes

To distinguish between the different types of changes, change point models can be adopted. There are two main approaches when determining when the change can occur namely Bayesian or non-Bayesian. Following the Bayesian approach, a change point is considered to be a random variable where a prior distribution of the change is assumed. Whereas for the non-Bayesian approach, the change point is not necessarily assumed to be a random number. For example, the minimax is a non-Bayesian approach for which Lorden formulated an optimization problem presented in [72].

Changes can be classified into two different categories namely additive and non-additive changes. The different characteristics of each type of change will be introduced in the present section. In Figure 4.1 and Figure 4.2, the qualitative difference between an additive and a non-additive change point is depicted.

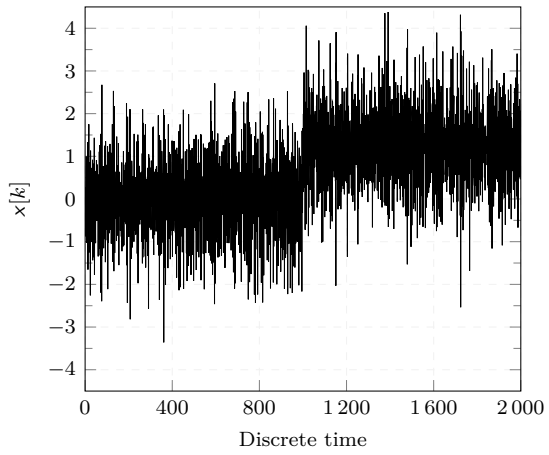



**Figure 4.1:** Additive change in the mean of a WGN process

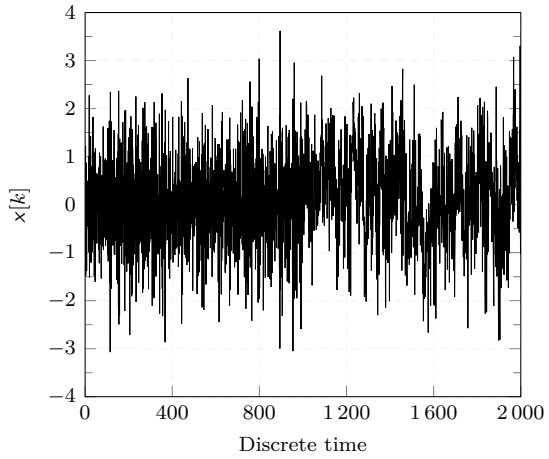



**Figure 4.2:** Non-additive change in the model of a WGN process

On one hand, an additive change in a signal is related, for instance, only to a change in the mean value of the signal and is represented for a step by a jump as shown in Figure 4.1. On the other hand, a non-additive change can be intuitively associated to a change, for instance, in the variance as depicted in Figure 4.2.

An example of change in the mean value of the sequence of observations is represented in Figure 4.1. The process depicted in Figure 4.1 is zero-mean White Gaussian Noise (WGN) before the change at $k = 1000$ and from that instant, the mean changes to $\mu = 1.5$ and the Probability Density Function (PDF) remains unchanged. In this case, the system dynamics remain the same.

Non-additive changes are also referred to, in the literature, as spectral changes. In fact, they are more general as they can represent changes in the variance, in the spectral characteristics and in the system dynamics. Non additive changes, including changes in the variance and spectral changes, act in a non-linear way with respect to the observations $x[k]$, as reported [5].

An example of non-additive change is depicted in Figure 4.2 where the variance of the WGN is $\sigma^2 = 1$ before the change and $\sigma^2 = 1.5$ after the change.

Different detectors should be derived for each type of non-aditive change. In fact, non-additive changes introduce additional complexity in the detection process as the log-likelihood ratio shall be modified.

For ease of understanding, additive and non-additive changes are only considered separately. However, it is important to notice that the two types of changes can occur simultaneously and particular considerations shall be taken into account in this case.

### 4.2.1 Modeling of Changes in State Space Models

In the present section, additive changes in the state or observation equation of a linear time invariant system of a state space model are presented.

This type of changes result, for instance, in changes in the mean of the time-series $\mathbf{x}$. Additive changes are modeled as follows:

$$x[k] = \mathbf{C}\boldsymbol{\alpha}[k] + \mathrm{D}e[k] + \Gamma_x \Upsilon_x[k,k_0],\ e[k] \sim \mathcal{N}(0,\sigma_e^2) \tag{4.5a}$$

$$\boldsymbol{\alpha}[k+1] = \mathbf{A}\boldsymbol{\alpha}[k] + \mathbf{H}\boldsymbol{\eta}[k] + \Xi_\alpha \Upsilon_\alpha[k,k_0],\ \boldsymbol{\eta}[k] \sim \mathcal{N}(0,\mathbf{Q}) \tag{4.5b}$$

The term $\mathbf{A} \in \mathbb{R}^{n\times n}$ is the state transition matrix, $\mathbf{H} \in \mathbb{R}^{n\times g}$ is a selection matrix and $\boldsymbol{\eta}[k]$ is a $g \times 1$ disturbance vector. $\mathbf{Q}$ is a $g \times g$ covariance matrix of $\boldsymbol{\eta}[k]$ . $\Xi_\alpha$ is a matrix of dimensions $n \times \tilde{n}$ and $\Upsilon_\alpha(k,k_0)$ is the *the dynamic profile* of one of the assumed changes of dimensions $\tilde{n} \times 1$.

Thereby, $\mathbf{C} \in \mathbb{R}^{1\times n}$ is the measurement matrix and $\boldsymbol{\alpha}[k] \in \mathbb{R}^{n\times 1}$ is the state vector. $\mathrm{D} \in \mathbb{R}$ is a selection scalar and $\xi[k] \in \mathbb{R}$ is the measurement error. R is the variance of $\xi[k]$. $\Gamma_x$ is a vector of dimensions $1 \times r$ and $\Upsilon_x(k,k_0)$ of dimensions $r \times 1$, represents the *the dynamic profile* of the change in the states.

The form of the matrices $\Upsilon_x(k,k_0)$ and $\Upsilon_\alpha(k,k_0)$ depends on the type of change being studied. The change time $k_0$ is assumed to be unknown i.e. $\Upsilon(k,k_0) = 0$ for $k < k_0$.

Additive changes are represented by different dynamic profiles observed in $\Upsilon_x$ and $\Upsilon_\alpha$.

Consequently, an additive change at $k = k_0$, in form of a step signal, can be expressed as follows:

$$\Upsilon(k,k_0) = \begin{cases} 0 \text{ if } k < k_0 \\ 1 \text{ if } k \geq k_0 \end{cases} \tag{4.6}$$

It should be noted that other types of additive changes can be considered by using appropriate functions for $\Upsilon_x$ and $\Upsilon_\alpha$.

Non-additive changes include change in the variance and spectral changes. The changes in the variance result in a change in the covariance matrix $\mathbf{Q}$ and in the variance R. The other class of non-additive changes that affect the dynamics of the system are referred to as spectral changes and can be modeled by changes in the transition matrix $\mathbf{A}$ as follows [5]:

$$\mathbf{A} = \begin{cases} \mathbf{A}_0 \text{ if } k < t_0 \\ \mathbf{A}_1 \text{ if } k \geq t_0 \end{cases} \tag{4.7}$$

To simplify the mathematical formulation and connection to the considered case studies in the present work, there will be mainly focus on additive changes in the following sections.

### 4.2.2 Estimation of State Space Models including Changes

For the detection of additive changes, an important fact to consider is that the effect of such changes is reflected as a change in the mean on the residuals or innovations [5].

The detectability depends on the actual change on the innovations. In fact, if the change consists of a dynamic profile, the definition of the detectability is less obvious than when the change is a step [5]. Since the detection presented in Section 4.1.2, is based on the log likelihood it is essential to consider the innovations. Thus, the investigation of the additive changes on the states and the observations is necessary.

For the detection of additive changes, Kalman Filter (KF) is used to express the transformation from observations to innovations. The model of change can be reflected in a specific profile of the innovations. In fact, it was demonstrated in [5] that a step change in the signal results in a change with a dynamic profile in the innovation. Additive changes introduce additional terms in the KF equations presented in Section 3.3.2. The estimation of the model state with the additive change using the KF is stated in the present section. The effect of the change $(\Gamma_x \Upsilon_x, \Xi_\alpha \Upsilon_\alpha)$ on the state, the state estimate and the innovation is defined as follows [5]:

$$\boldsymbol{\alpha}[k] = \boldsymbol{\alpha}[k] + \delta[k,k_0] \tag{4.8a}$$

$$\hat{\boldsymbol{\alpha}}[k|k] = \hat{\boldsymbol{\alpha}}_0[k|k] + \beta[k,k_0] \tag{4.8b}$$

$$\boldsymbol{\nu}[k] = \boldsymbol{\nu}_0[k] + \rho[k,k_0] \tag{4.8c}$$

The index 0 in (4.8) refers to the unchanged state and estimate (3.24) and (3.23). The terms $\delta$, $\beta$ and $\rho$ are functions representing the signature of additive change on

the states, the estimates and the innovations. The previously mentioned functions are computed recursively as follows

$$\delta[k,k_0] = \mathbf{A}\delta[k-1,k_0] + \Gamma_x\Upsilon_x[k-1,k_0] \tag{4.9a}$$

$$\begin{aligned}\beta[k,k_0] &= (\mathbf{I}-\mathbf{K}[k]\mathbf{C})\mathbf{A}\beta[k-1,k_0] + \mathbf{K}[k](\mathbf{C}\delta[k,k_0] + \Xi_\alpha\Upsilon_\alpha[k,k_0]) \\ &= \mathbf{A}\beta[k-1,k_0] + \mathbf{K}[k]\rho[k,k_0]\end{aligned} \tag{4.9b}$$

$$\rho[k,k_0] = \mathbf{C}(\delta[k,k_0] - \mathbf{A}\beta[k-1,k_0]) + \Xi_\alpha\Upsilon_\alpha[k,k_0] \tag{4.9c}$$

with the initial conditions

$$\delta[k_0,k_0] = 0 \tag{4.10a}$$

$$\beta[k_0-1,k_0] = 0 \tag{4.10b}$$

The detailed derivation of the recursive equations and explicit formulas for the dynamic profile of the signature of the change on the innovation is explained in [5].

## 4.3 Detectors for State Space Models

The detection problem is unchanged under the transformation from the observations to the innovations [98]. Indeed, the effect of additive changes is observed in the model innovation i.e. residuals. The innovations have different distributions before and after a change. The innovations $\boldsymbol{\nu}[k]$ resulting from the application of the KF has the following distribution:

$$p(\boldsymbol{\nu}[k];\boldsymbol{\Theta}) = \begin{cases} \mathcal{N}(0,\sigma_k) \text{ if no change occurs} \\ \mathcal{N}(\rho[k,k_0],\sigma_k) \text{ after change} \end{cases} \tag{4.11}$$

with $\sigma_k$ is the covariance matrix of the innovations and $\rho$ is the signature of additive change on the innovation when considering the KF reaching the steady-state, and is defined in the following:

$$\begin{aligned}\rho[k,k_0] = &\sum_{i=0}^{k-k_0-1} \left(C\bar{A}^i\Gamma_x\Upsilon_x[k-i-1,k_0]\right) \\ &- \sum_{i=0}^{k-k_0-1} \left(C\bar{A}^iA\Xi_\alpha\Upsilon_\alpha[k-i-1,k_0]\right) \\ &+ \Xi_\alpha\Upsilon_\alpha[k,k_0]\end{aligned} \tag{4.12}$$

The statistical detection problem of additive changes with unknown parameter vector is presented as following:

$$\begin{aligned} k_{alarm} &= \min\{k : g[k] \geq \gamma\} \\ with\ g[k] &= \max_{1\leq j\leq k} \frac{k-j+1}{2} (\{\nu\}_{k=1}^{j})^{\mathrm{T}} \sigma_k^{-1} \{\nu\}_{k=1}^{j} \end{aligned} \tag{4.13}$$

For detection of non-additive changes (changes in variance and spectrum), the generalized likelihood ratio (GLR) statistics were proposed in [5].

The innovations of the models before and after the change are necessary for the detection of non-additive changes contrarily to the detection of additive changes where only the innovation of the model before the change is required.

For demonstration purposes, let us consider the following the state-space model [90].

$$\boldsymbol{\alpha}[k+1] = 0.9\boldsymbol{\alpha}[k] + \boldsymbol{\eta}[k] + \Xi_\alpha \Upsilon_\alpha[k,k_0] \tag{4.14a}$$

$$x[k] = \frac{1}{2}\boldsymbol{\alpha}[k] + e[k] + \Gamma_x \Upsilon_x[k,k_0] \tag{4.14b}$$

with,

$$\begin{pmatrix} \eta[k] \\ \xi[k] \end{pmatrix} \sim \mathcal{N}\left( \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0.1 & 0 \\ 0 & 0.1 \end{pmatrix} \right) \tag{4.14c}$$

with the following definitions

$$\Xi_\alpha = \Gamma_x = b \tag{4.15a}$$

$$\Upsilon_\alpha[k,k_0] = \Upsilon_x[k,k_0] = \begin{cases} 0 \text{ if } k < k_0 \\ 1 \text{ if } k \geq k_0 \end{cases} \tag{4.15b}$$

where $b$ is a scalar to indicate the magnitude of the change.

In Figure 4.3, the detection of an additive change in a white Gaussian noise using the CUSUM test is depicted. The decision function $g[k]$ and the log-likelihood ratio increment $s[k]$ are defined as in (4.3). The change was injected at $k = 500$ and detected at $k_{alarm} = 508$ as depicted in the bottom subfigure in Figure 4.3.

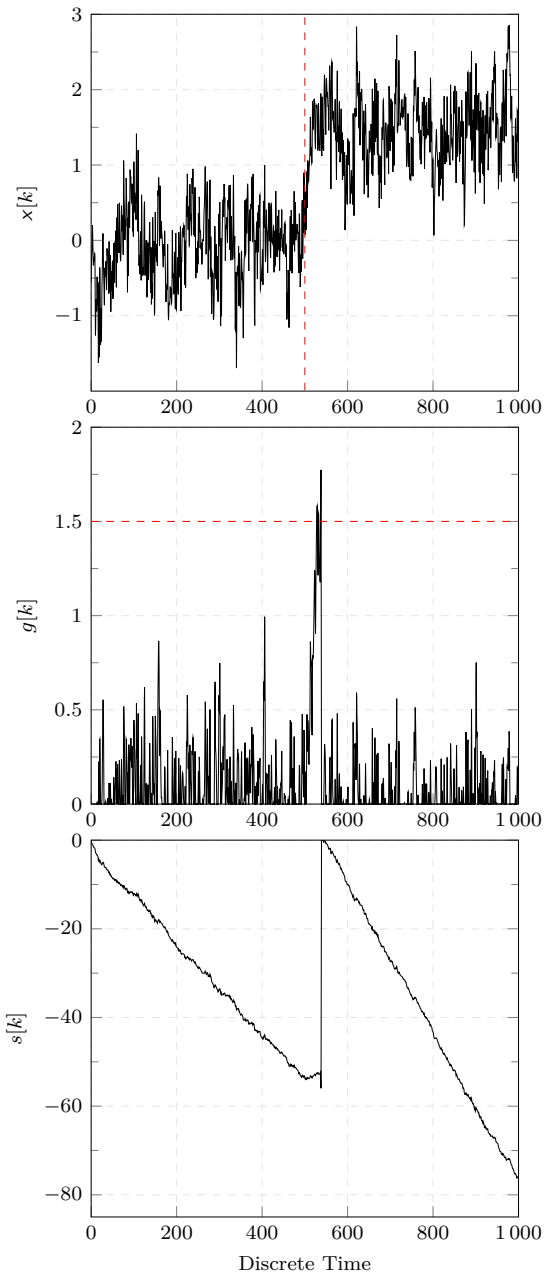



**Figure 4.3:** CUSUM detection of an additive change in WGN

## 4.4 Discussion

In the present chapter, basic concepts related to the detection problem are defined. The developed anomaly detection problem is formulated as a statistical hypothesis test with an adapted detector. In fact, change point detection algorithms using statistical tests have been gaining increasing interest within the research community since raising concerns regarding Cyber-Physical Security (CPS) of critical and industrial infrastructures.

As explained previously in Section 4.3, the CUSUM test was chosen, for the particular case of the off-line detection, as a suitable detector for the considered changes in the network traffic. In fact, the CUSUM statistical test, one of the

most widely used approaches, offer several advantages. Besides representing the optimal solution in case of i.i.d variables, see [79] for the minimax criterion developed by Lorden [72], it has a good tradeoff between the detection performance and the detection delay. Contrarily to other approaches such as neural networks, detectors based on sequential test account explicitly for the time.

Introduction of different changes in the network traffic is analyzed and modeled as state space representation. Thus, the detection problem is extended according to the type of changes being additive and non-additive. In the present work, detection of DoS attacks resulting for a GOOSE poisoning are the main focus. Indeed, the different types of DoS were shown to result in spikes in the packets flows [22]. Thus, they can be considered as additive changes i.e.changes in the mean within the network traffic time-series.

# CHAPTER 5

## EDA4GNeT: Early Detection of Attacks for GOOSE Network Traffic

## List of Symbols

| Notation | Description |
|---|---|
| $\mathbf{A}$ | The state transition matrix $\in \mathbb{R}^{n \times n}$ |
| $\mathbf{C}$ | The measurement matrix $\in \mathbb{R}^{g \times n}$ |
| $\mathbf{Q}$ | A $n \times n$ covariance matrix of the states or process noise |
| R | The variance of the measurement or signal noise |
| $S[k]$ | The novel score function |
| $x$ | A stochastic time-series |
| $\gamma$ | The threshold for the statistical detector |
| $\varepsilon$ | Model residuals |
| $\boldsymbol{\Theta}$ | The parameter vector |

In the previous Chapter 4, the detection of attacks in electrical substations has been formulated as a change point detection using statistical hypothesis testing. However despite the different statistical advances, within the community, those statistical approaches have not been translated into convenient algorithms for adoption in operational cyber-physical systems [20]. The Smart Grid security in particular requires specific analysis of the network traffic in order to propose a suitable Intrusion

Detection System (IDS). In the present chapter, we first present the requirements and properties of a suitable detection method against availability attacks.

The mathematical modeling presented in Section 3.2 and Section 3.3 that accounts for the specific features of IEC 61850 substations is used as basis for our novel detection method EDA4GNeT. A detailed overview of the algorithm including the different steps as well as the novel score function is provided in Section 5.2. The different design parameters of EDA4GNeT are introduced and discussed and suggestions on optimal choice for the parameters are given.

## 5.1 General Properties

Traditionally, the network traffic in industrial control systems generally and in energy systems particularly is assumed to be at steady-state. However, the network traffic in ICS or energy systems might exhibit time-varying characteristics due, for instance, to change of the operating conditions of the physical system or the grid [3].

One of the main advantages of the developed detection method is the adaptability to the dynamics of the systems since the different traffic fluctuations are taken into account as part of the normal operation. Despite fluctuations in the traffic, the test statistics designed within the EDA4GNeT method remains within the normal range when no attacks are injected. Adapting to changes of the network traffic reduces considerably the rate of false alarms and thus improves the overall performance of the developed novel detection method.

Besides the adaptability to normal network fluctuations in IEC 61850 substations, another important feature that was included in the novel detection method is a recursive implementation property. In fact, the capability of recursive computations in the anomaly detection approach developed in the present work is suitable for model adaption in a real-time application similar to the case of GOOSE messages. In the developed EDA4GNeT approach, re-building the whole model from scratch at each collected network traffic sample is not necessary. This avoids the increasing computational complexity and memory problems due to appending a new collected sample to the training set at each iteration. The calculation of the predictions of the state-space AR model developed in the present work is recursive *i.e.* the prediction at the current sample is estimated using only previous samples which avoids the previously mentioned limitations.

Together with the former presented features, EDA4GNeT is designed with the detection time as a central requirement. In fact, performance metrics for detectors include the delay for detection which refers to the time difference when an alarm occurs w.r.t. the instant an anomaly actually happens. In EDA4GNeT, early detection of GOOSE attacks in the substation network is possible since it incorporates a robust forecasting algorithm. Early detection of attacks helps preventing loss of energy and

revenues due to possible physical consequences of attacks such as fatigue damage or resonance attacks [28].

## 5.2 Developed Detection Method

In the present section, an overview of the algorithm developed in EDA4GNeT is explained. Details about the different steps as well as the parameters used for the modeling, prediction and detection are presented.

### 5.2.1 Overview of the Algorithm

The collected network traffic is first analyzed thoroughly to better understand its characteristics in electrical substations. Relevant invariants of the communication network presented in [33] were studied in order to model the network traffic $\mathbf{x}_{\text{est}}$. Long-Range Dependency (LRD) characteristics of the network were showed which helps choose an appropriate model. The description of the network traffic characteristics can be reviewed in Section 3. In the modeling procedure depicted in Figure 5.1, a state-space AR model is selected to describe the communication. The state space (SS) modeling of long-range dependent data that was first considered as an Auto-Regressive Fractionally Integrated Moving Average (ARFIMA) model is made possible thanks to the approximation using an SS model introduced in [15] and explained in Section 3.3. The parameter vector of the considered model $\hat{\boldsymbol{\Theta}}$ is estimated using the sequence $\mathbf{x}_{\text{est}}$. The Expectation Maximization (EM) algorithm is used to estimate $\hat{\boldsymbol{\Theta}}$ which contains the parameters of the state-space model ($\mathbf{A}$, $\mathbf{Q}$, R) as defined in (3.24), (3.23) and (3.44). The estimation algorithm is adapted to consider the specific description of the AR approximation of an ARFIMA model i.e. the structure of the $\mathbf{A}$ and $\mathbf{C}$ as defined in (3.44). The values obtained from the estimation algorithm are used for initialization in the Kalman Filter (KF). Use of KF is suitable to efficiently fit the dynamics of the network traffic in IEC 61850 substations. Appropriate initialization values for the KF help guarantee a good detection performance of ED4GNeT. The Expectation Maximization (EM) algorithm is suitable as it allows fast convergence and a good performance is achieved after few iterations [23].

To estimate states on linear dynamic systems represented as state space models, KF are used. The KF is well-adapted for the estimation of the system state by minimizing the mean squared error. In fact, KF provides optimal estimates in the case of linear models with additive White Gaussian Noise (WGN). The statistics of the noise are estimated within the Expectation Maximization (EM) algorithm. However, in most practical cases, the statistics of the noises are generally unknown and hence also non-Gaussian. The covariance matrix $\mathbf{Q}$ and the variance R are, thus, one of the tuning parameters that can be adjusted to reach the required performance.

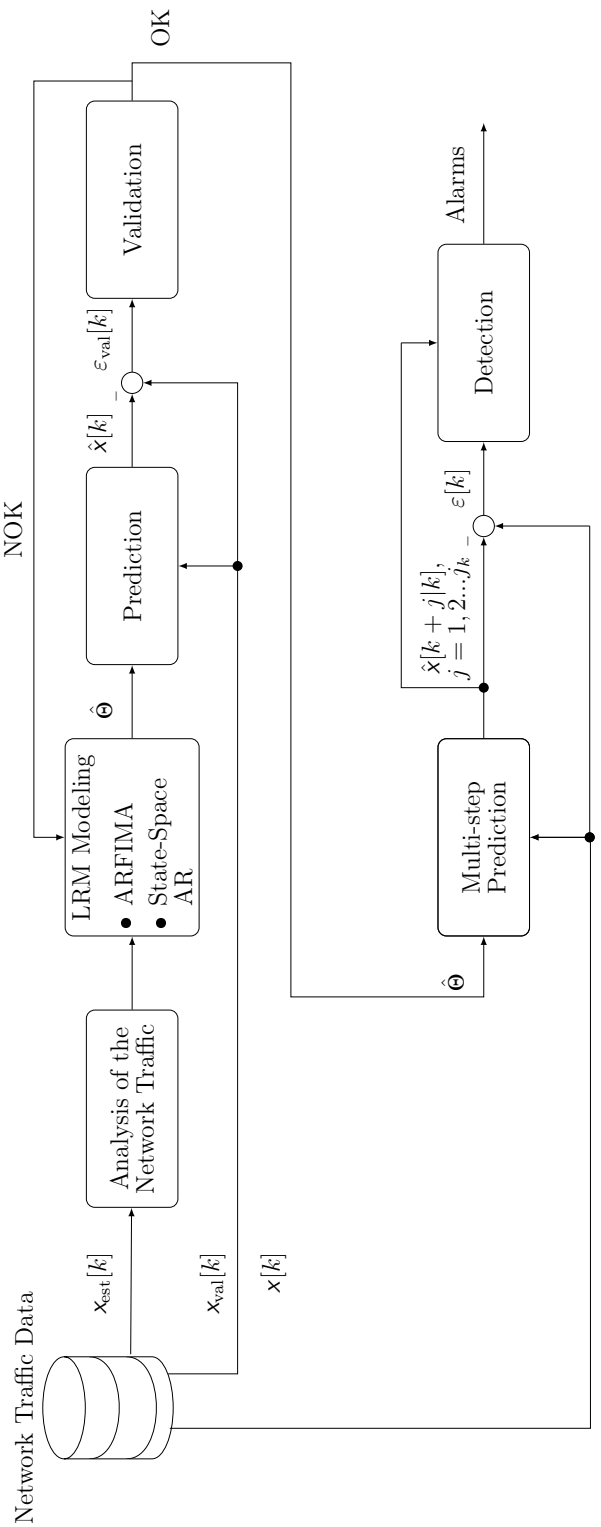



**Figure 5.1:** Block diagram of the EDA4GNeT method

The parameter vector $\hat{\boldsymbol{\Theta}}$ is further used to compute the predictions that are denoted by $\hat{\mathbf{x}}_{\text{off}}$. The performed computations are explained in (3.35), (3.36) and (3.37).

Two criteria can be used for validation namely, the prediction computed with the model and residuals analysis. Firstly, the prediction is compared with the real signal and a measure such as the NRMSE can be used to define the quality of the model. The distribution of the residuals $\varepsilon_{\text{off}}[k]$ resulting from the difference between the real signal $\mathbf{x}_{\text{val}}$ and the predicted one $\hat{\mathbf{x}}_{\text{off}}$ is also evaluated to determine the performance of the modeling procedure.

Depending on the accuracy of the model, the estimation step using the EM algorithm with adjusted user-defined parameters, shall be repeated until satisfactory results are obtained. Whenever the validation yields an acceptable model, the parameter vector can be further used for recursive computations using the KF. Once a model is validated and accepted, the parameter $\hat{\boldsymbol{\Theta}}_0$ is used for further computations.

In Figure 5.1, the "multi-step prediction" block takes as input $\hat{\boldsymbol{\Theta}}_0$ and computes the equations (3.35), (3.36) and (3.37). The prediction $\hat{x}[k+j|k]$ is computed using the output of the former block $\hat{\boldsymbol{\Theta}}_K$. The value $j$ with $j = 1,2,\ldots,j_k$ refers to the $j$ step-ahead prediction. In fact, when $j = 1$, $\hat{\mathbf{x}}$ represents the commonly known one-step ahead predictor.

An anomaly can be observed in the measurement or in the transition equations (cf (4.5)). Presence of an anomaly will affect the states and, consequently, it will be observed also in the residuals. For $j = 1$, the EDA4GNeT method is based on the CUSUM detection test that receives as input the residuals $\varepsilon_{\text{on}}[k]$ resulting from the difference between the signals $x[k]$ and $\hat{x}[k|k-1]$.

For early detection, $j$ is chosen as $j > 1$ and the detector for EDA4GNeT is based on a novel score function instead of the residuals as described in Section 5.2.2. The input to the score function is the $j$-step ahead prediction.

### 5.2.2 New Score Function

We investigate the detection procedure within the developed ED4GNeT method. Our detection problem can be formulated as an early change point detection where the anomalies can occur at unknown times and would result in changes in the statistical properties of the network traffic. The novel detection procedure shall allow an early detection of network attacks while respecting an acceptable False Alarm (FA) rate.

Two competing hypotheses are described in Section 4.1.1. To decide for the null or the alternative hypothesis, the CUSUM test is a known change point detection procedure with interesting optimal properties [5, 83]. However, for the early detection of anomalies in the substation network traffic, a change point detection procedure

based on the residuals such as the basic CUSUM test can not be used as the values of the measurements at sample $k + j$ are not available.

Instead, a new score function is introduced to detect the changes based on [98]. The concept proposed by Tartakovsky et al. in [98] is extended in the present work for an early parametric approach.

A further extension of the score function is used in our detection method. In the following, the test statistic $g[k]$ is described

$$\begin{aligned} k_{alarm} &= \min\{k : g[k] \geq \gamma\} \\ with\ g[k] &= \max(0,\ g[k-1] + S[k]) \end{aligned} \tag{5.1}$$

A novel score function $S[k]$ is based on the predictions of $\hat{x}[k + j|k]$. The term $\hat{y}$ corresponds to a scaled and centered values so that $S[k]$ fits applications with different amplitudes.

$$\begin{aligned} &S(\hat{y}[k + j|k]) = a_1\hat{y}[k + j|k] + a_2\hat{y}^2[k + j|k] - a_0 \\ &\text{where } \hat{y}[k|k + j] = \frac{\hat{x}[k|k + j] - \bar{x}}{\sigma_{\mathbf{x}}} \end{aligned} \tag{5.2}$$

The score function is represented in a linear-quadratic form with $a_0, a_1$ and $a_2$ being positive design parameters that accounts for changes in the mean and in the variance whenever an anomaly occurs.

### 5.2.3 Early Detection

Known methods for early detection can be ineffective due to the high false alarm rates and their lateness of detection.

One of the many advantages of an early detection system is to considerably reduce operational costs by avoiding loss of availability of the network in IEC 61850 substations resulting of a disturbance of the electric grid or even outages in same cases.

The developed method allows, in one hand an early detection of anomalies in the IEC 61850 network traffic and in the other hand a false alarm rate that is comparable to the standard anomaly detection implemented for comparison. Analysis and further results are listed in Section 6.3.3.

In fact, few approaches allow an online implementation with a low computational load and a short time for the model calibration [82]. Techniques using ARIMA models, for instance, are widely spread. However, they have shown to require a considerable time for model estimation [95]. As alternative methods, techniques based on machine learning algorithms, such as support vector machines can be applied in real time with the main disadvantage that they require high quality datasets [82].

Early detection using EDA4GNeT is based on the novel score function presented in Section 5.2.2 and computed with the j-step ahead prediction. The equations of the KF are extended to compute $\hat{x}[k+j|k]$. The one-step ahead prediction of the state is used in (3.42) for computation of the j-step ahead. Then, the model prediction is computed as in the right side of (3.36) based on the estimation of the state described previously.

In the simplest case of $j = 1$, the method reduces to the one-step ahead prediction. This particular case is further analyzed in Section 6.2. The larger $j$ is, the higher FA rate is since the quality of the prediction degrades when $j$ is large. This statement will be further discussed in Section 6.4.

The developed approach is possible because the novel score function is based on model prediction that are obtained as in (3.42) and not on the residuals that are defined for the one-step ahead predictor.

## 5.3 Design Parameters

General guidelines about the choice of the design parameters of EDA4GNeT is provided in the present section. More details about the general concepts can be, however found in [5, 98]. On one hand, for the modeling and forecasting of the network traffic in IEC 61850 substations, two main design parameters are required, being the order of the state space model and the number of step ahead for the forecasting. On the other hand, two additional design parameters need to be set for the detection which are the parameters of the novel score function and the detection threshold $\gamma$.

For the mathematical modeling of the network traffic, choosing a suitable state space model order helps in obtaining accurate results for the further detection of anomalies. The order $n$ and initial values for the Expectation Maximization (EM) algorithm are initially set. The order of the model $n$ is adjusted according to the simulation results. It is however, worth mentioning that the model order $n$ can be also determined based on the Akaike Information Criteria (AIC) and the Bayesian Information Criteria (BIC). Independent use of any of them can result in overfit and underfit modeling problem. Thus, a combined use of both criteria is proposed in [17] as an appropriate approach to define the model order based on the data. This procedure is repeated iteratively until acceptable results are obtained. In case knowledge about the process is available, this information might help choose the model order. A tradeoff between the model complexity and preservation of generality shall be, however, kept in account. Once an acceptable model is computed then its parameters are used for computations in the Kalman Filter (KF).

Acceptable model parameters allow validation of the model for use in the multi-step prediction as explained in Section 5.2.1 and depicted in Figure 5.1. The proposed

approach allows forecasting the network traffic for more than one-step ahead. This is particularly relevant as it can be efficiently implementable online to guarantee an early detection of attacks against the network traffic.

The forecasting for j-step ahead depends mainly on the one-step ahead prediction of the estimated state and on the value of the $\mathbf{A}$ estimated in the modeling stage. The performance of the early detection is linked to the results of the forecasting. The one-step ahead predictor can be generalized by shifting the terms of the state vector as explained in [96].

The value of the parameters for the score function are set according to the type of anomaly addressed. In some works [98], it is assumed that attacks such as TCP SYN result only in changes in the mean or in changes in the variance that is significantly smaller than a change in the mean. This results thus in setting the coefficient $a_2$ to zero.

Last but not least, one of the most common design parameters in anomaly detection methods is the detection threshold. Choice of threshold $\gamma$ in the developed detection test (5.2) might be challenging as it is tightly associated to the number of false alarms and to the detection of anomalies. The detection threshold shall be set so as to obtain the desired level of false alarm rate. Generally, selection of the threshold can be done using Monte-Carlo simulations sampling-based methods for stochastic optimization problems [98].

## 5.4 Discussion

Description of the traffic using a state space model allows representation of multivariate signals that can be evaluated for anomaly detection. Analysis of multivariate signals will yield adaption of the detection test since the forecasting consists of multiple signals. In fact, the detection test is based on the quality of the forecasting that are used in the computation of the novel score function.

The number of step-ahead for computation of forecasting needs to be set. In fact, the earliness of detection is associated with the number of steps ahead. However, it is worth noticing that setting a high value of the number of steps ahead would affect the false alarms rate.

Indeed, to show the effect of the number of selected step ahead on the forecasting, let us recall the introductory example introduced in Section 3.3.2. The forecasting of $x[k]$, shown in gray, with different number of steps ahead, is depicted in Figure 5.2.

The accuracy of the j-step ahead predictions $\hat{x}[k+j|k]$ degrades with an increasing value of $j$. Indeed, the $\hat{x}[k+5|k]$ is the closest to the real time series whereas $\hat{x}[k+20|k]$ follows the general trend of $x[k]$ however with a quite large deviation as shown in Figure 5.2.

More details about the previously mentioned tradeoff is analyzed in Section 6.3.

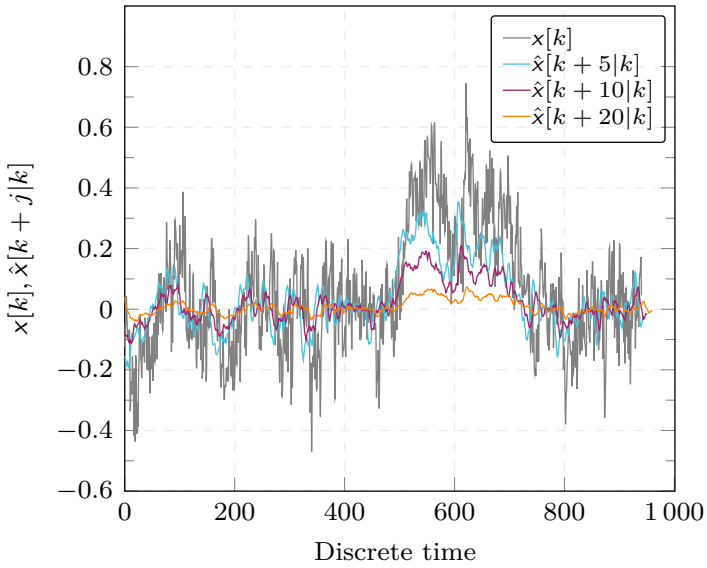



**Figure 5.2:** Forecasting with different number of steps ahead

The score function in EDA4GNeT is able to retrieve changes other that in the mean i.e. the non-additive changes for e.g. change in the variance. In fact, the parameters associated to the quadratic terms can account for non-additive changes. For additive changes, the parameter associated to the linear term in the score function defined in Section 5.2.2 is used to detect changes in the mean.

# CHAPTER 6

## Case Studies

## List of Symbols

| Notation | Description |
|---|---|
| $\boldsymbol{B}$ | base rate representing the probability that there is an intrusion in the observed data set |
| $C$ | The ratio of the cost of an IDS failing to detect an intrusion and its cost when it generates a false alarm |
| $C_{exp}$ | The expected cost metric |
| $C_{ID}$ | The intrusion detection capability metric |
| $g$ | The CUSUM decision function |
| $k$ | Discrete time index |
| $x$ | A stochastic time-series |
| $\gamma$ | The threshold for the statistical detector |
| $\sigma_e^2$ | Variance of a white Gaussian noise process |

To assess the performance of the developed method, relevant metrics grouped in three categories namely, basic and advanced metrics and Receiver Operating Characteristic (ROC) plots are introduced in the present chapter. ROC plots are a graphical illustration of the basic performance metrics that shows the connection between the true positive rate (sensitivity) in function of the false positive rate (specificity).

To test the effectiveness of EDA4GNeT method, two case studies, T1-1 and 66/11kV substations are introduced. Different adversary models are introduced to cover a large spectrum of attacks that might target the electrical substations. Those attacks result in various changes in the network traffic including the time and the amplitude of the changes.

The different experiments carried out in both use cases are presented. The obtained results are analyzed and evaluated using relevant criteria that are introduced and explained at the beginning of the present chapter. Detailed interpretation of the acquired results is presented in Section 6.2.3 and Section 6.3.3 as well an overall discussion including the most relevant conclusions is analyzed at the end of the chapter.

## 6.1 Performance Assessment

### 6.1.1 Basic Performance Metrics

A False Alarm (FA) indicates that $\mathcal{H}_1$ is selected by the detection method when $\mathcal{H}_0$ is true. FAs are also referred to as false positives (FPs). True positives (TPs) (i.e. a hit) refer to the case where the detector decides correctly for $\mathcal{H}_1$. A true negative (TN) (i.e. correct rejection) indicates that $\mathcal{H}_1$ is correctly rejected. A false negative (FN) (i.e. miss) occurs when $\mathcal{H}_0$ is selected even though the hypothesis $\mathcal{H}_1$ is true. The presented concepts are further used to define the performance assessment criteria.

The accuracy is one of the considered performance metrics and it refers to the frequency with which the anomaly detection test identifies properly the anomaly. However, considering only the accuracy might be misleading for the assessment of an anomaly detection method in case of a high imbalance between false positives and false negatives.

When the cost of FNs is high, the TPR also called DR or recall, might help give additional information about the model. The TNR, also called specificity, indicates the proportion of correctly classified non-anomalous samples w.r.t. the total number of samples of the dataset. The FPR represents the rate of FAs which is also referred to as type I errors in statistics. FNR or miss rate represents the proportion of type II error, i.e the hypothesis $\mathcal{H}_0$ is selected when $\mathcal{H}_1$ is true.

The computation of the basic performance metrics are presented in the following:

$$FPR = \frac{False\ positives}{False\ positives + True\ negatives} \tag{6.1a}$$

$$FNR = \frac{False\ negatives}{False\ negatives + True\ positives} \tag{6.1b}$$

$$DR = \frac{True\ positives}{True\ positives + False\ negatives} = 1 - FNR \tag{6.1c}$$

$$TNR = \frac{True\ negatives}{True\ negatives + False\ positives} = 1 - FPR \tag{6.1d}$$

The detection time is another performance indicator used to assess intrusion detection algorithms and describes the instant when an anomaly is detected. Subtracting the detection time from the real time of the attack gives an indication of the detection delay in the case of an offline detection and the earliness of detection in the case of an early detection. The previously introduced metrics can be combined with other criteria to deduce advanced performance measures introduced in Section 6.1.3 and that allow a simpler and straightforward comparison between the different anomaly detection methods.

### 6.1.2 ROC Plots

ROC curves depicts the probability of detection against the probability of false alarms and are used to quantify the detection performance. ROC curves gives an overview of the relation between the detection rate and FAs for different threshold. Without an accurate domain-knowledge of the system at different operation modes, it might be difficult to choose the best operation point which depends on a particular configuration.

The ROC plots can be, however, helpful for the comparison of the performance of different intrusion detection systems. It is worth noting that the comparison is only accurate when the curves of two IDSs do not cross which means that the IDS with the curve always above has a higher detection rate with a lower number of false alarms. In the other case, if the curves cross then the comparison might not be easy or relevant as no clear decision can be made

As an additional performance criteria, we consider the previously introduced metrics as well as additional advanced parameters, refereed to in the next sections as composite detection metrics.

### 6.1.3 Advanced Performance Metrics

To better compare the performance of the IDSs, the two composite detection metrics presented in [76] are used. The composite metrics give an overall overview of the detection performance and are computed using the basic performance criteria. Those

additional metrics do not however, replace the basics ones [38]. The expected cost metric $C_{exp}$ requires a user-defined parameter $C$ which is the ratio of the cost of an IDS failing to detect an intrusion and the cost when an IDS generates an alert when an intrusion has not occurred. The expected cost metric $C_{exp}$ is computed as follows:

$$C_{exp} = min(C \cdot FNR \cdot \boldsymbol{B}, TNR \cdot (1-\boldsymbol{B})) + min(C \cdot TPR \cdot \boldsymbol{B}, TPR \cdot (1-\boldsymbol{B})) \quad (6.2)$$

where $\boldsymbol{B}$ is the base rate i.e. the probability that there is an intrusion in the observed data set and in the following experiments it is assumed that $\boldsymbol{B} = 0.1$.

For our experiments, the cost of a FNR is considered to be much higher than the cost of FPR i.e. the value of $C$ is chosen to be equal to 10 following [76]. In fact, missing an anomaly within the communication of electrical substations might result in an increased risk on the physical system and thus affecting the stability of the electric grid.

To compare the performance of the different IDSs, the approach with the lowest $C_{exp}$ is considered to be the best [76]. $C_{exp}$ gives a practical way to relate the different basic metrics however it is a cost-based metric that depends on a subjective measure which is $C$. In fact, it might be challenging to define the cost of generating a false alarm versus the one of detecting an intrusion as this depends on several factors specific, for instance, to the size of the substation.

A second composite metric $C_{ID}$, first introduced in [38], provides a more objective evaluation of the performance of the considered IDSs. Thus, the $C_{ID}$ metric is more adequate to compare in an objective form the performance of intrusion detection systems. The intrusion detection capability $C_{ID}$ presents the ratio of the mutual information between the IDS input and output to the entropy of the input. For derivation details of this metric, the reader is referred to [38]. To compare IDSs, the maximum value of $C_{ID}$ obtained for each approach shall be compared between them.

## 6.2 Case Study: T1-1 Transmission Substation

### 6.2.1 Description of a Simplified T1-1 Substation

In order to meet the need to carry power for long distances while keeping or stepping up or down the voltage, several types of transmission substations exist based on their size. Small transmission substations may contain only one bus and few switches and Circuit Breakers (CBs) whereas large size transmission substations include several bus levels as well as huge number of components, thus a complex monitoring and control structure. A small transmission substation of T1-1 is chosen the first use case in the present work. Indeed, it is assumed that security investigation analyzed in the present contribution might be scaled to larger electrical substations.

The first case study considered in the present work, is a simplified T1-1 transmission substation. It mainly contains one incoming line, one bus-bar and 2 outgoing lines.

The simplified SLD of the transmission substation T1-1 is presented in Figure 2.8. It is composed of four bays grouped into three main ones which are the transformer bay composed of $D01$ and and two feeders bays ($E01$ and $E03$). The IEDs used for the different bays are represented in Figure 2.8. The transformer bay contains two MUs namely $MU_{D01}$ and $MU_{E02}$ that have the function of a conventional MU. There is also a P&C IEDs namely $IED_{D01}$ in the transformer bay. Each of the feeder bays contain one $MU_{E01}$and $MU_{E03}$ as well as one Protection and Control P&C $IED_{E01}$ and $IED_{E03}$.

The mapping to Logical Nodes (LNs) of the different IEDs and MUs used in the three bays is presented in Figure 6.1. LN that do not refer to any function such as LLN0, that contain generic information about the device and which is, thus, contained in all devices, are omitted in Figure 6.1 for simplification purposes. Considering the flexibility offered by the IEC 61850 standard, there are different configuration options of LNs. The choice is conditioned upon design issues and the expected features. The different LNs are clustered and structured in functions used to establish the associated protection and control scheme of the T1-1 substation. For instance, in the Feeder I, the interlocking function is composed from the CILO and CSWI nodes in the bay level of the substation. It needs however, the states of their related CBs and switches $CB_{E01}$ and $S_{E01}$ available trough the nodes XSWI and XCBR in the $MU_{E01}$ from the process level as shown in Figure 6.1. For the ease of reading, only the functions related to the bay level and used in our example are mentioned in Figure 6.1. Another example consists in the nodes PTOV, PIOC and ATCC, part of the $IED_{D01}$, that are used for the overcurrent and overvoltage functions. The distance protection function F4 in the two feeder bays E01 and E03 contains several LNs among which TCTR, TVTR and XCBR in the process level, PDIS in the bay level and ITMI, ITCI and IHMI in the station level. It shall be noticed that back-up functions such as RBRF, which is a breaker failure protection, are not considered in the analyzed mapping.

The previously described use case is implemented using the cost-efficient testbed described in [28]. The power system is used to simulate the physical model using Simscape toolbox. For the process level, merging units are simulated as virtual machines (VMs) and implemented in C using the libiec61850 library [110] to have an interface that merges sampled data of the measurements between electronic measurement transformers and protection and control IEDs. Virtual IEDs are used in the bay level. They are computing units implemented as hosts or VMs that are responsible for protection and control functions. The libiec61850 project offers to

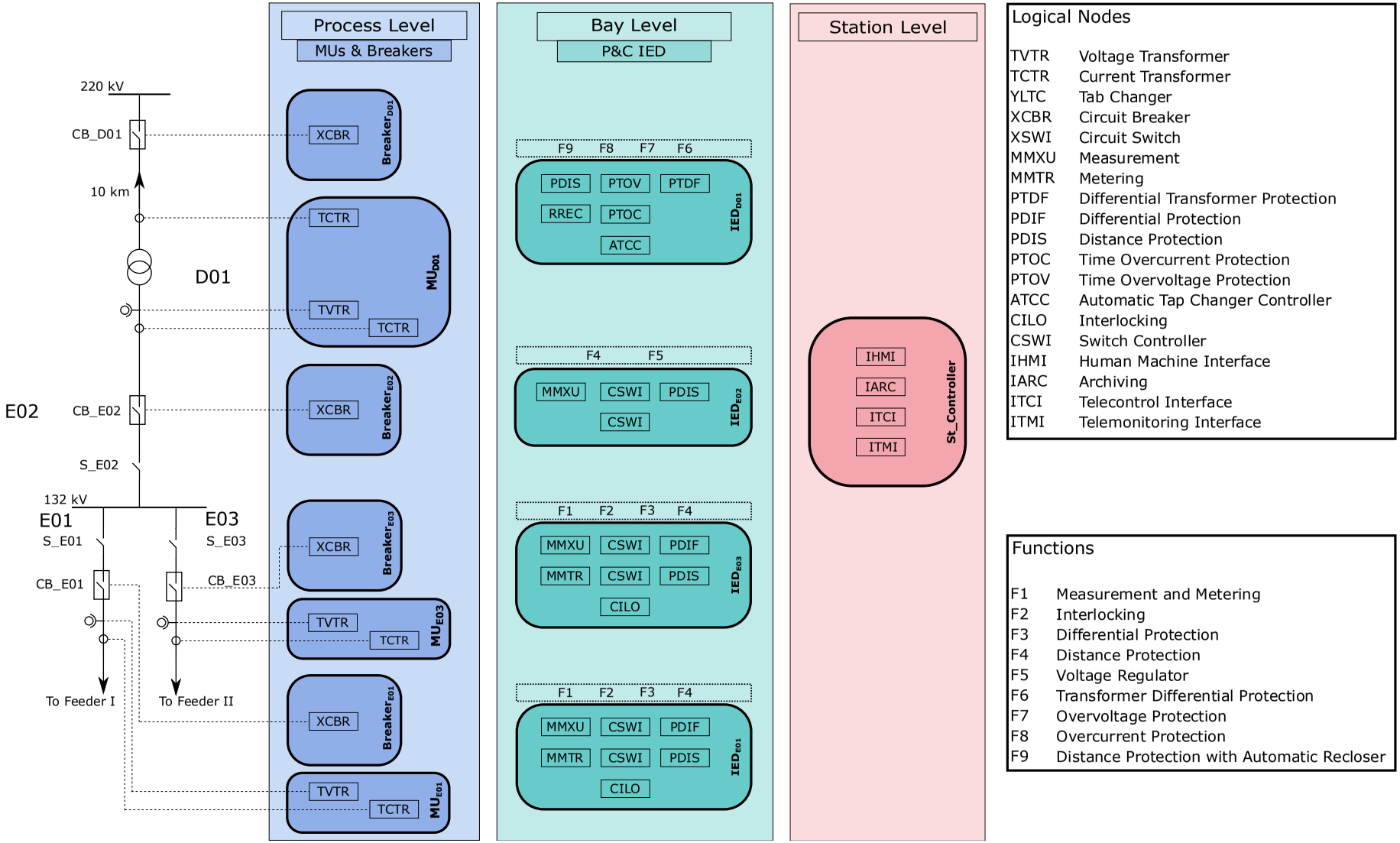



**Figure 6.1:** The Logical Nodes (LNs) used in each of the defined Intelligent Electronic Devices (IEDs)

convert IED Capability Description (ICD) files into C files creating a complete static data model of the server that is further compiled into the application.

For the simulation of the communication protocols between the different IEDs, the open-source library libiec61850 [110] is used. A server/client as well as a publisher/subscriber communication models from the available examples were modified to be adapted to our particular case. For the interfacing between the network communication and the power model, a basic synchronization schema was chosen. A predetermined communication time was fixed. This means that both processes simulating the network and the physical system are running separately and at predetermined time points with the execution being paused before exchanging data.

### 6.2.2 Description of the Threat Model

Loosing availability in critical infrastructures' networks can have a more severe impact than, for instance, in commercial systems. Thus, a denial of service attack resulting from a GOOSE poisoning attack in communication of the T1-1 substation is considered as the adversary model based on the risk analysis presented in Section 2.4. Different variants of this attack are considered in the literature. In fact, The GOOSE poisoning attack reported in [47] can result in a DoS. When an attacker injects a spoofed GOOSE packet with a very high status number (*StNum*), all the messages with a smaller *StNum* will be discarded according to the definition of the transmission mechanism of the GOOSE protocol described in the IEC 61850 standard [51]. Another variant is the high rate flooding attack that injects multiple GOOSE packets with incremental *StNum* that exceed the *StNum* of a legitimate packet. The last situation, called semantic attack, is based on monitoring the network traffic and spoofing the GOOSE packets with a higher rate of changing *StNum* than the normal one. As a result of the semantic attack, the subscribers would be prevented from processing legitimate packets. In [45], another variant of GOOSE DoS attack is demonstrated in [45] by causing an IED to loose functionality caused by the injection of a consequential number of GOOSE packets that is greater than the limit allowed for the packet transmission time.

Other situations that might lead to a GOOSE DoS attack are a non-matching between the actual length of the PDU in the GOOSE frame and its PDU which can occur when injecting a malformed PDU. Other conditions leading to a DoS attack are described in [1]. A DoS attack can also be perpetrated when a GOOSE frame is delayed until the expiration of the time allowed to live. A detailed description of the previously mentioned attack can be found in [64].

The adversary model consists in the simulation of a GOOSE DoS attack resulting from a poisoning attack as described in Figure 6.2. More details about the trans-

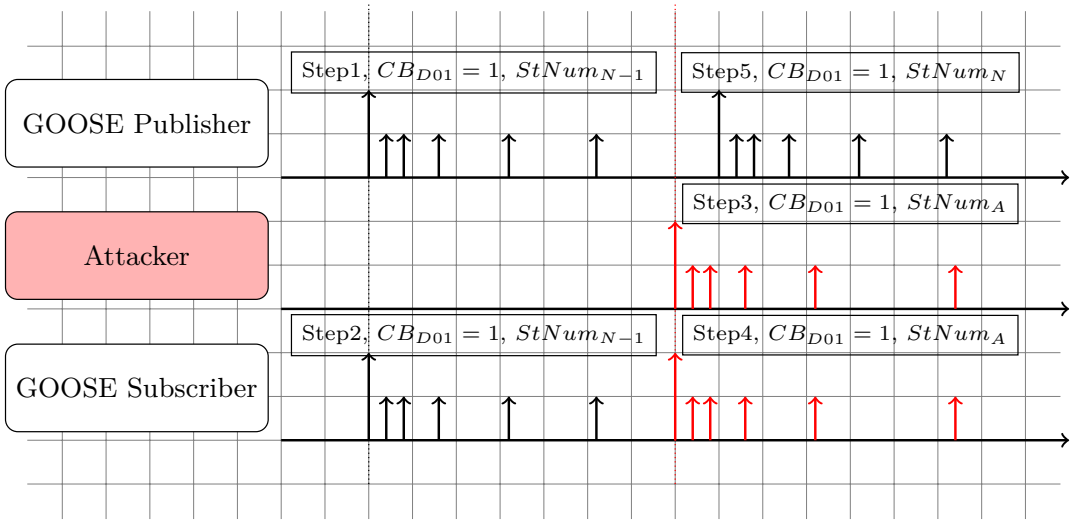



**Figure 6.2:** DoS attack resulting from a GOOSE poisoning attack

mission mechanism of the GOOSE protocol depicted in Figure 6.2, is explained in Figure 2.5.

The attack script is implemented in Python based on the work presented in [47] and a traffic attack replay tool such as Tcpreplay [99] was used. The first step consists in compromising the GOOSE communication by spoofing the transmitted messages. The attack model is based on compromising the GOOSE communication. By spoofing the transmitted messages, the attacker can masquerade a legitimate IED to inject maliciously crafted GOOSE messages. By masquerading a legitimate IED, maliciously crafted GOOSE messages with a high *StNum* would result in a DoS attack.

The injection of the maliciously crafted packet is possible when the attack flooding rate is higher that the legitimate transmission rate. When the attacker's sending advantage of packets with a higher StNum over the legitimate GOOSE publisher is reached, the poisoning attack can start. If it is assumed that the attacker in previous reconnaissance steps was able to monitor the network traffic thus he has an idea about the legitimate GOOSE frame rate. From a defender perspective, the worst case scenario would be an attacker that can launch a successful poisoning attack with a small flooding rate that would be hardly distinguished from the normal traffic. In the present work, this worst case scenario is assumed in order to demonstrate the capabilities of the EDA4GNET detection method. It is worth noting that further analysis of the success rate of poisoning attacks required to cause a DoS attack shall be conducted. However, the success of an attack in terms of malicious GOOSE flooding causing a DoS attack is out of the scope of the present work. Interested reader can, however find further details in [47, 97, 102].

### 6.2.3 Results and Discussion

To test the performance of EDA4GNeT and compare it to the closest works to ours in the literature, the results of several experiments are reported in the present section.

In [63] and [103], statistical anomaly detection methods against attacks in IEC 61850 substations, are proposed. The authors in [63], present a statistical detection based on a comparison of the residuals with a variance-based threshold while assuming a white Gaussian noise model for the network traffic in electrical substations. In contrast to [63], where the residuals are obtained from a signal embedded in WGN, a modified version with the residuals computed from the appropriate mathematical model developed in Section 3 are considered instead.

The approach presented in [103] is based on an anomaly score resulting from the comparison of the network traffic with a minimum and a maximum value extracted from real measurements. No details were provided in [103] for the choice of the user-defined parameters necessary for the anomaly detection score. Thus, empirically adapted values are chosen which would allow a high probability of attack detection for the considered use case. Both approaches are implemented for comparison with EDA4GNeT method.

The implementation of several experiments including a flooding attack at time $k = 500$ are generated following the threat model and the network traffic described previously in Section 6.2.1. WGN with sample variance derived from the estimated model is used for simulation.

The performance of the EDA4GNeT detection method is evaluated for several thresholds $\gamma$s.

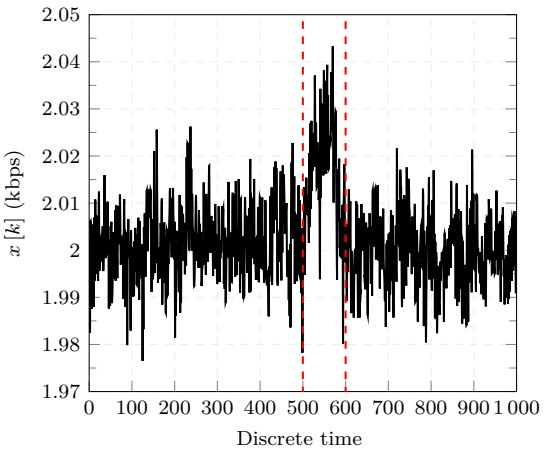



**Figure 6.3:** Example of simulated GOOSE network traffic with a DoS attack

The experiments are performed using a computer equipped with an Intel processor i7-2.00 GHz and 32GB RAM. A total number of 25 Monte-Carlo simulations are performed for each threshold and under different realizations of WGN for each experiment. A realization of one of the experiments is shown in Figure 6.3. The

generated network traffic, depicted in Figure 6.3, include a flooding attack that starts at $k = 500$ and ends at $k = 605$. The result of the detector based on the particular case of the score function in EDA4GNeT introduced in Section 5 for one of the experiments is shown in Figure 6.4.

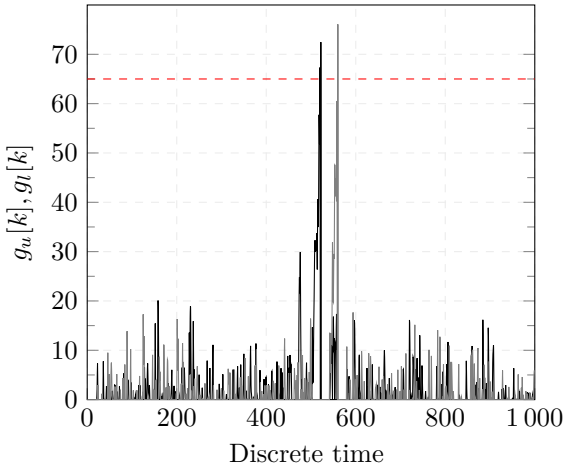



**Figure 6.4:** Results of the detection test

Before a change occurs, the values of the score functions oscillate within a certain range. The detectors $g_u[k]$ and $g_l[k]$ corresponds to the detection of the lower and the upper bound of the attack

$g_u[k]$ is computed according to (4.3) and $g_l[k]$ is computed similarly but the log-likelihood ratio is subtracted in the computation of $g[k]$. When a change occurs, the values of the detectors $g_u[k]$ and $g_l[k]$ change abruptly which indicates that the start and the end of the attack was successfully detected as shown in Figure 6.4. In case of the $g_u[k]$ and $g_l[k]$ detectors, as shown in Figure 6.4, no FAs were present and the threshold $\gamma$ (dashed red line) was only exceeded in the case of a change in the network traffic.

The test statistics $g_u[k]$ and $g_l[k]$ are reset in the EDA4GNeT detection approach after a change is detected. Further changes can be, thus, detected which makes our novel approach are able to detect several attacks.

Even though, in this first use case, we focused on the detection of one change, in the second use case of a 66/11kV electrical substation model, presented in Section 6.3.1, the detection of several changes was analyzed as depicted in Figure 6.8.

The performance of EDA4GNeT in comparison with the closest literature [63, 103] is further analyzed using Receiver Operating Characteristic (ROC) plots. In fact, as described in Section 6.1.2, ROC plots help inspect the tradeoff between FPR and FNR over a complete spectrum of operating conditions including the settings of the decision threshold $\gamma$. The ROC curve represents the relation between the probability of detection $P_D$ i.e. TPR and the probability of false alarm $P_{FA}$ i.e. FPR to help assess the performance of the detectors depending on the requirements of the

application. An algorithm is considered to be *good* if the ROC curve reaches rapidly the upper left-hand corner i.e. if the area under the curve is *large*. Under simple assumptions such as the analysis of a signal embedded in Gaussian noise, the ROC curve can be typically derived analytically. This is not the case in the present work as a more complex model is used which requires experimental computation of the ROC curve.

The detection results of EDA4GNeT, [103] and [63] are depicted in Figure 6.5. Considering that our threat model corresponds to the worst case scenario of a high rate flooding attack where the DoS attack results in a small and short fluctuation of the

The EDA4GNeT method has, however, the highest detection rate with lowest number of false alarms.

To further evaluate the performance of the EDA4GNeT method with one-step ahead detection, three scenarios for different signal-to-noise ratios (SNRs) are considered.

The SNR is defined by:

$$\mathrm{SNR} = 10 \log_{10} \frac{\sigma_x^2}{\sigma_e^2} \ \mathrm{dB} \tag{6.3}$$

where $\sigma_x^2$ and $\sigma_e^2$ are the variances of the signal $\mathbf{x}$ and noise $\mathbf{e}$, respectively. SNR values in network traffic of electrical substations oscillates typically between 13 dB and 38 dB [86]. To better evaluate the performance of the developed method, low values of SNR are considered to cover worst case scenarios The performance of EDA4GNeT degrades, overall, for lower SNR values ( i.e. a high noise content) is shown in Figure 6.6. This can be explained by high deviations of the estimates with respect to the true values when the noise variance increases.

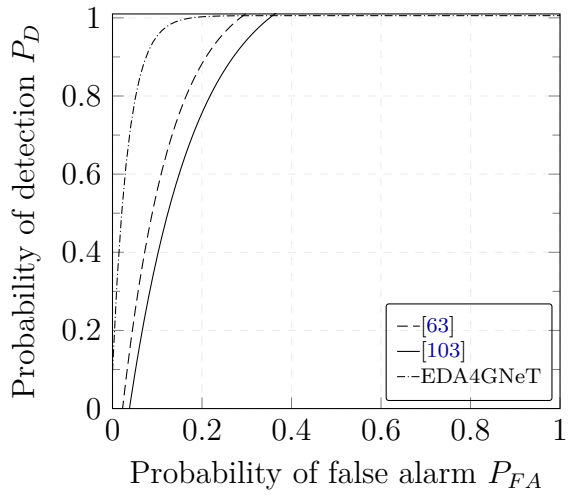



**Figure 6.5:** Comparison of the ROC curve of the different methods

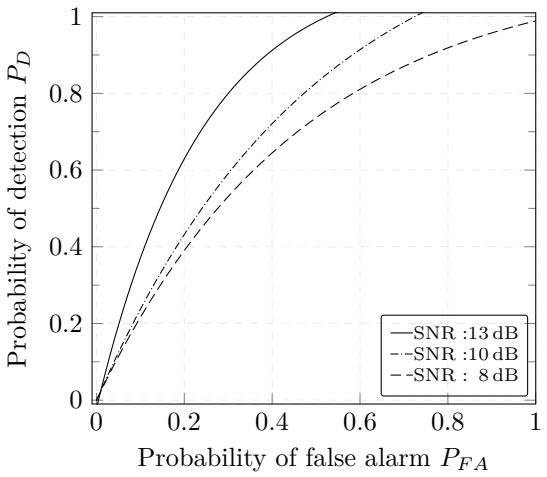



**Figure 6.6:** ROC curve of EDA4GNeT with different SNR

For small values of the threshold, the detection test has a good DR but also a high FPR. To alleviate the previously described situation, the threshold $\gamma$ should be adjusted in order to have few FAs, low FNR and an acceptable accuracy and DR.

In the following, a more detailed analysis of the detection performance of EDA4GNeT in comparison with the available approaches is presented. To that end, the basic and complex metrics, described in Section 6.1.1 and Section 6.1.3 are used to assess the performance of the different approaches.

**Table 6.2:** Comparison of the one-step ahead detection results with available methods

| Threshold | Basic | | | | | | Composite | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | FPR [%] | | | FNR [%] | | | $C_{exp}$ | | | $C_{ID}$ | | |
| | [63] | [103] | EDA4GNeT* | [63] | [103] | EDA4GNeT* | [63] | [103] | EDA4GNeT* | [63] | [103] | EDA4GNeT* |
| 0.1 | 5.2015 | 5.4982 | 4.1987 | 0.2124 | 0.8697 | 0.2004 | **0.1124** | 0.1978 | 0.1061 | 0.3748 | 0.1938 | 0.3287 |
| 0.2 | 5.7047 | 5.5014 | 4.0030 | 0.2124 | 0.9158 | 0.2124 | 0.1129 | 0.1898 | 0.0950 | 0.4769 | 0.2111 | 0.4196 |
| 0.3 | 4.1024 | 3.7037 | 3.1975 | 0.2305 | 1.0000 | 0.2204 | 0.1138 | 0.1807 | 0.0901 | 0.5318 | 0.2145 | **0.5896** |
| 0.4 | 3.1043 | 3.1990 | 2.5049 | 0.2305 | 1.1884 | 0.2204 | 0.1143 | 0.1704 | 0.0869 | **0.5346** | 0.2594 | 0.5361 |
| 0.5 | 2.6999 | 2.1042 | 1.7020 | 0.2305 | 1.3547 | 0.2305 | 0.1144 | 0.1593 | 0.0838 | 0.4836 | 0.2749 | 0.4515 |
| 0.6 | 1.2043 | 0.8030 | 0.6998 | 0.2345 | 1.7034 | 0.2505 | 0.1148 | 0.1522 | 0.0815 | 0.4318 | 0.3034 | 0.4205 |
| 0.7 | 0.3042 | 0.4034 | 0.1483 | 0.2605 | 1.9679 | 0.2425 | 0.1149 | 0.1451 | 0.0791 | 0.3898 | 0.3183 | 0.3499 |
| 0.8 | 0.2597 | 0.1004 | 0.1728 | 0.3307 | 2.6493 | 0.2345 | 0.1149 | 0.1398 | 0.0749 | 0.3696 | 0.3446 | 0.3548 |
| 0.9 | 0.2204 | 0.2042 | 0.2735 | 0.3647 | 3.4689 | 0.3527 | 0.1155 | 0.1342 | 0.0715 | 0.2802 | 0.3583 | 0.2594 |
| 1 | 0.2047 | 0.5993 | 0.2524 | 1.1122 | 4.5391 | 0.7014 | 0.1152 | **0.1276** | **0.0681** | 0.2871 | **0.3648** | 0.3016 |

* A special case of the EDA4GNeT method

Our AD statistical method is compared with the most relevant approaches available in the literature [63, 103], described at the beginning of this subsection, and the results are listed in Table 6.2.

Under similar operating conditions and using the same scenario, the average values of 50 Monte-Carlo simulations are presented in Table 6.2.

Table 6.2 shows the performance of the detection approaches for SNR = 10 dB. The first column in Table 6.2 represents normalized values of the thresholds for the different anomaly detection methods.

Initially, there will be a focus on the basic performance metrics presented in Section 6.1.1. For a better readability of the different results in Table 6.2, only the FPR and the FNR are included as the other basic detection criteria can be directly concluded from (6.1c) −(6.1b).

The EDA4GNeT approach has for each threshold the lowest FPR. For instance, its value is 1.7 % for a normalized threshold of 0.5. The FPR of the detection algorithm presented in [103] and [63] are, in general, higher than our method.

The EDA4GNeT method exhibits FNR values that are similar or lower than the two other detection approaches. For instance, for a normalized threshold equal to 0.5, the corresponding FNR has a value of 0.23 % thus a DR value of 99.77 %. The modified approach from [63] has a rather low FNR ranging between 0.21 % and 1.11 % whereas the FNR for the approach based on [103] has the largest range among the different normalized thresholds.

It is worth mentioning that for all three approaches, the FNR increases with a bigger values of normalized threshold as less changes i.e attacks can be detected.

In summary, our EDA4GNeT approach has overall the the lowest values of FPR and FNR when compared with the techniques developed in [63] and [103]. To further compare the different intrusion detection, combined assessment metrics are also included in Table 6.2.

$C_{exp}$ is the first composite criteria used to compare IDSs. The minimal value of $C_{exp}$ for each approach is shown in bold in the Table 6.2. Our EDA4GNeT anomaly detection method has the lowest expected cost, among all considered normalized thresholds, approximately equal to $C_{exp} = 0.07$ compared with the closest works to ours available in the literature. The cost-based metric $C_{exp}$ presents only a preliminary metric to compare the anomaly detection as it depends on the parameter $C$ which is a subjective measure. Indeed, we consider $C = 10$ which refers to the fact that the cost of not responding to an attack is 10 times higher than the cost of responding to a false alert.

The second composite criteria, proposed in [38] and used to compare the performance of intrusion detection methods is $C_{ID}$. The maximum value of $C_{ID}$ obtained for each approach shall be compared between them. According to [76], higher values

of the intrusion capability $C_{ID}$ represents a better performance of the corresponding IDS. The maximum value of $C_{ID}$ for each approach is depicted in bold in Table 6.2. The lowest value of $C_{ID}$ is computed with the approach proposed [103]. The value of $C_{ID}$ of EDA4GNeT method is around 5.9 which is the highest value among all the considered approaches. Those observations support the results concluded from the first composite metric $C_{exp}$. Under similar operating conditions, our novel EDA4GNeT anomaly detection approach is experimentally proven to perform better than the two closest works to ours ([103] and [63]) for the detection of DoS attacks resulting from GOOSE poisoning attack.

## 6.3 Case Study: 66/11kV Substation

### 6.3.1 Description of the Use Case

In the present section, a synthesized dataset generated by the Advanced Digital Sciences Center (ADSC) [7] is used. The testbed describes the operation of a 66/11kV electrical substation model including circuit breakers and IEDs depicted in Figure 6.7. A typical network architecture was adopted using the recommended protocols in IEC 61850 standard i.e. GOOSE and SV communication between CTs, VTs and IEDs via Ethernet VLAN and MMS protocol at the station level for the connection

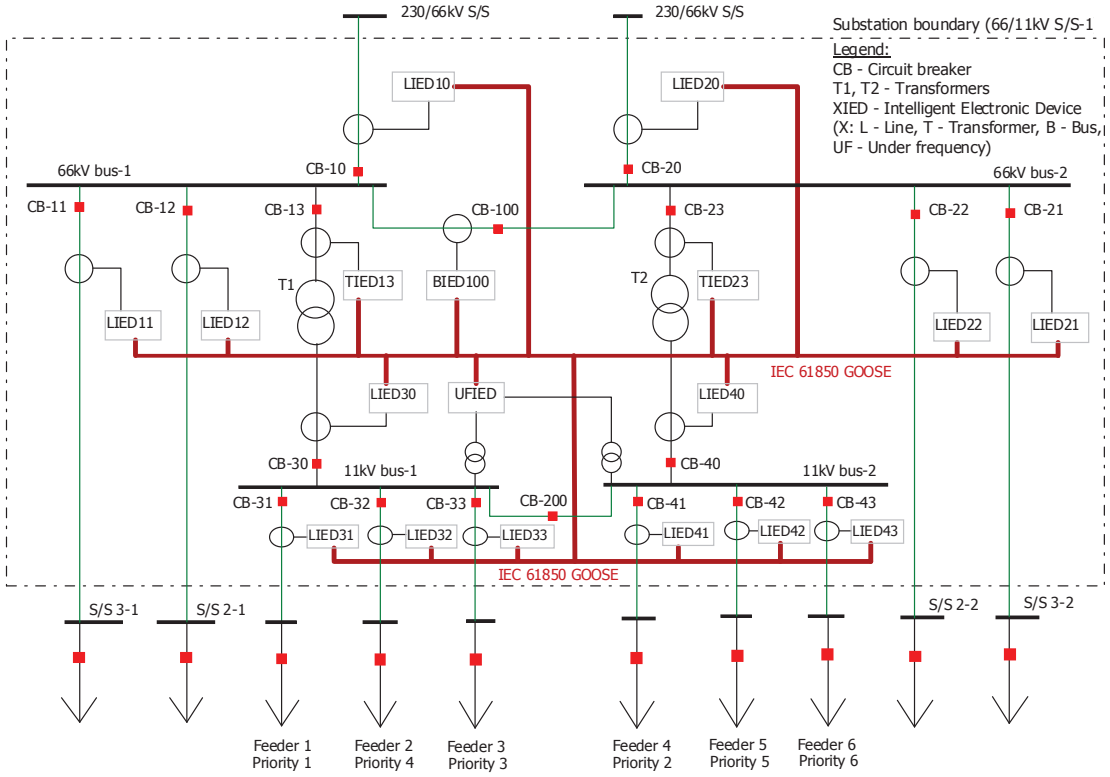



**Figure 6.7:** The single-line diagram of a 66/11kV substation [7]

between Human-Machine Interfaces (HMIs) and IEDs. All 18 simulated IEDs are within the same multicast group.

The normal operation in an electrical substation might also include disturbances such as a breaker failure or a busbar protection where specific GOOSE messages are sent to address such event changes.

### 6.3.2 Description of the Threat Model

Normal operation in the electrical substation might be hindered by disturbances or malicious actions. In the following, a description of the considered threat model is introduced. In modern electrical substations, HMIs are equipped with monitoring and control interfaces that are remotely accessible. Attackers are assumed to be able to compromise this entry point through for instance social engineering in order to connect to IEDs.

The simulated attack was generated synthetically using an attack-free network scenario, an attack script and a traffic attack replay tool such as Tcpreplay [99]. An automatic trace generator program is used to get an attack-induced trace by injecting malicious GOOSE packets. The attack model is based on compromising the GOOSE communication. By spoofing the transmitted messages, the attacker can masquerade a legitimate IED to inject maliciously crafted GOOSE messages. There are several ways to perpetrate a DoS attack. Impact of loosing availability in critical infrastructures' networks can be much more severe than, for instance, in commercial systems. In the considered case, the simulated DoS results from flooding the network with bogus frames. More details about the generation framework of the different attack and attack-free scenarios can be found in [7]. Among others, a DoS attack on the GOOSE communication was simulated and resulting network data is recorded.

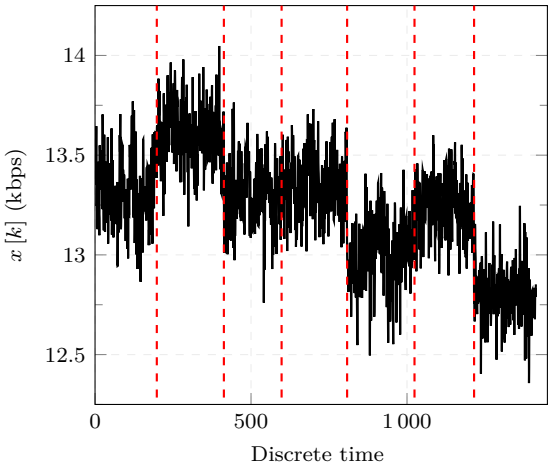



**Figure 6.8:** Simulated GOOSE network traffic with several changes

In order to thoroughly test our EDA4GNeT method, several experiments with different noise realizations are run. As an adversary model, a similar attack technique

as described in Section 6.2.2 where a high rate flooding attack results in a GOOSE DoS attack is used. In this second use case, a coumpound case study is considered where several attacks in the network traffic of an IEC 61850 substation are considered with different characteristics including the duration and the amplitude of the changes. The designed use case is depicted in Figure 6.8.

A normal GOOSE network traffic is simulated based on the modeling procedure described in Section 3.4. The first attack starts at $k = 198$ and lasts 215. The second simulated attack starts at $k = 413$ and ends at $k = 625$. The start of the attack can hardly be distinguished with the naked eye. The third and last attack starts at $k = 1024$ and finishes at $k = 1215$. It is worth noting that although the changes representing some of the attacks can be perceived in Figure 6.8, it is difficult to tell with the naked eye when it actually begins. It can be also remarked that a change in the dynamics of the system was introduced from the sample $k = 809$. In electrical substations, such changes can occur in case of modification in the physical system that require adaption of the operating conditions.

### 6.3.3 Results and Discussion

A similar hardware set-up as in Section 6.2.3 is used. A Monte-Carlo simulation of 100 experiments is run to test the performance the EDA4GNeT method.

To test the performance of EDA4GNeT, the detection rate and the false alarm rate considering a one-step ahead detection versus multi-step detection are compared. The ROC plot depicted in Figure 6.9 shows, as expected a better performance when considering only one-step ahead. It is however important to notice that the performance with multi-step ahead is still acceptable especially that this case would offer an early detection of the attacks in GOOSE network traffic.

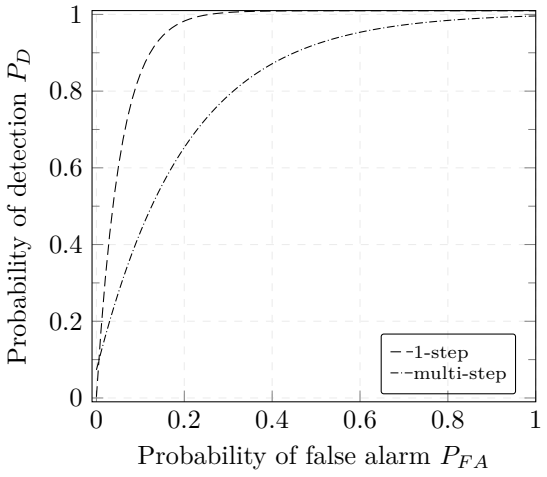



**Figure 6.9:** ROC curve of the one step versus the multi-step configuration of EDA4GNeT

**Table 6.3:** Comparison of detection results using EDA4GNeT

| Change | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 1 | – | −22.08 | 3.0772 | 3.2357 | 0.2013 | 0.3033 | 0.0938 | 0.1120 | **0.9880** | 0.4535 |
| 2 | – | −17.24 | 2.6179 | 3.0211 | 0.2501 | 0.3067 | 0.0915 | 0.1032 | 0.9665 | 0.5359 |
| 3 | – | −20.92 | 2.1123 | 2.8405 | 0.3499 | 0.3000 | 0.0891 | 0.0975 | 0.9409 | **0.8666** |
| 4 | – | −23.02 | 1.9458 | 2.6419 | 0.0401 | 0.1800 | 0.0849 | 0.0912 | 0.9320 | 0.5197 |
| 5 | – | −33.68 | 1.5386 | 2.5436 | 0.0667 | 0.1433 | 0.0815 | 0.0873 | 0.9274 | 0.6100 |
| 6 | – | −14.84 | 1.4764 | 2.3410 | 0.2014 | 0.1100 | **0.0781** | **0.0830** | 0.9770 | 0.3117 |

* Detection delay expressed in discrete time $k$

In the following, an average of the results of the different Monte-Carlo experiments is presented in Table 6.3. The optimal thresholds for the 1-step as well as for the multi-step ahead detection are used, respectively for computations for the values in Table 6.3. As explained at the beginning of the present section, in the multi-step case of EDA4GNeT, an early detection of attacks is possible in average 21 samples ahead. To the best of our knowledge, none of the currently available anomaly detection methods based on an accurate mathematical model is able to offer an early detection which accounts for the dynamics of the network traffic.

For all the changes, the average FPR values for the 1-step ahead detection are smaller than for the multi-step ahead. The FNR values range between 0.07 % and 0.35 % for the one-step ahead EDA4GNET. For most of the changes, the multi-step ahead case of EDA4GNeT has a higher FNR than for the one-step ahead case.

Those results of the basic metrics are consistent with the ones obtained from the composite metrics as for all the considered changes the cost metric $C_{exp}$ is smaller than the multi-step case. The lowest value of $C_{exp}$ is equal to around 0.078, whereas for the multi-step ahead it corresponds to around 0.083 as depicted in bold in Table 6.3. Whereas, the intrusion capability $C_{ID}$ of all the values of the changes in the second use case are bigger for the one-step case than the ones for the multi-step ahead case.

It is however important to highlight that despite the superior detection performance of the simplified case of EDA4GNeT with one-step ahead, the performance, in terms of basic and composite metrics, of the general case of EDA4GNeT with the multi-step ahead detection have acceptable results. This can be explained by the adequacy of the selected model for the description of the network traffic in IEC 61850 substations as well as the accuracy of our detector introduced in Section 5.2.2.

EDA4GNeT offers a remarkable advantage in comparison with the available approaches as it is able to detect in average the start of the attacks introduced in Section 6.3.2. The earliness of detection is expressed in samples and it represents the number of discrete time samples after which the anomaly is detected. Regardless of the amplitude and duration of the change, EDA4GNeT is able to detect them in average 20 samples in advance with an approximate detection rate of 97.3 %.

Even though, the detection statistics (i.e basic and composite metrics) remain better in the case on a step-ahead detection, the multi-step ahead detection offers a good compromise between the detection time and the detection statistics. It is worth mentioning that the one-step and multi-step ahead prediction can be computed simultaneously in EDA4GNeT. In fact, the multi-step ahead prediction allows an early detection of attacks whereas the one-step ahead can be used as a highly accurate detection system with an associated detection delay.

## 6.4 Discussion

For different case studies, authors in [106] report a detection rate of 100 %, however a hybrid approach using whitelisting and deep packet inspection (DPI) is adopted. This method requires additional data processing and computational complexity that can constraint its application in real scenarios. Similar detection results are reported in [11] with the use of critical state analysis that are based on a comprehensive description of the physical models of the considered power system. To achieve a good performance, IDSs based on ML approaches generally use supervised algorithms which require two different datasets for training of the detection algorithm. This is a considerable limitation as they increase the deployment and operational costs and a large amount of data sets are required for setting the algorithm. In the field of statistics, methods related to change point detection have been successfully applied in different research areas. However, literature research shows that use of these robust approaches for anomaly detection for smart grids, especially for IEC 61850 electrical substations has not been explored.

The proposed technique in the present chapter has a comparable detection rate as other approaches for detection of DoS attacks. But a major advantage of EDA4GNeT method is that it does not require to include DPI or to build a set of rules that need to be constantly maintained. Reliable detection rates are achieved using a novel method which combines robustness of change point detection adapted to the particular field of IEC 61850 substations. The performance of the developed novel detection method is evaluated and discussed under different scenarios in two case studies.

In the first case study, one DoS attack resulting from a GOOSE poisoning attack is considered which is a typical threat an IEC 61850 substation can be exposed to. The developed method shows a superior performance when compared to related approaches reported in the literature in terms an average a DR of 99.72% and FPR of 1.97%. Better detection performance confirms the advantageous properties of the ED4GNeT method. Basic performance criteria such as FPR and FNR are reported and its use for representation of ROC curves also shows the capabilities of the proposed method to successfully address the considered type of attacks.

Early detection is explored in a second case study under different forecasting conditions for prediction. The early detection feature aims at predicting as fast as possible attacks to avoid propagation of the consequences of an attack on the physical grid. The ED4GNeT method shows acceptable performance for different values of $j$-step ahead prediction. However, the forecasting degrades for large values which coincides with results reported in the literature for model prediction. The choice of suitable values, that are adjusted empirically for the score function and

forecasting allows early detection of attacks in IEC 61850 substations and represents a novel feature in ED4GNeT method when compared with available approaches.

# CHAPTER 7

# Conclusions and Outlook

## 7.1 Conclusions

Integration of Information and Communication Technology (ICT) in modern energy systems has considerably improved the interconnection between the different parts of the grid. Critical infrastructures are highly dependent on digital control, supervision and monitoring for a safe and optimal operation. Secure communication in Smart Grids (SGs) is a key component in ensuring a reliable and stable operation of power facilities. Besides the advantages offered by the use of ICT, additional threats might rise due to the modern communication structure of SGs, as for instance, the infamous Stuxnet worm back in 2010. According to to ICS-CERT, the energy sector was the number one target of incidents in 2014. Thus, modern infrastructures such as SGs are encountering increasing exposure to different cyber-attacks.

The interconnection between the different parts of the grid is carried out using specific network protocols. Those protocols particularly used in energy systems are not primarily designed with security in mind which exposed the whole power grid domain as an attractive target for attackers.

Developing defense techniques for authentication, integrity and real-time availability of the communication networks in SGs is part of the presented research work. One of the first steps is to review and analyze the different attacks against SGs that are summarized in a novel classification that gives an overall view of the state of cyber-physical security of power systems in Section 2. It is concluded from this first work that considering the new generation of energy systems, secure communication is a key component in ensuring a reliable and stable operation of electrical substations based on IEC 61850 standard.

In order to help improve the overall Cyber-Physical Security (CPS) of the SG, the present work tackles the challenge of enhancing the availability of the data in communication networks in electrical substations based on IEC 61850. Modeling of the network traffic in IEC 61850 substations in order to design an online method for early detection of attacks in GOOSE network traffic is established within this work.

Indeed, the Substation Communication Network (SCN) traffic is analyzed in order to gather necessary knowledge for the characterization of the GOOSE network traffic.

Based on the studied characteristics presented in Section 3.1, the mathematical modeling is discussed using a state space representation of an ARFIMA model of the network traffic. The primary goal of modeling the GOOSE network traffic is to design an efficient anomaly detection method for early detection of flooding attacks. However, modeling of the communication network can also support the research in forecasting the traffic with a high accuracy and in designing the GOOSE network architecture of electrical substations. The estimated model is evaluated on two use cases and described in Section 3.4.

Thereafter the obtained model is used for developing a novel Anomaly Detection (AD) based on statistical hypothesis testing. EDA4GNeT is an efficient anomaly detection that addresses limitations of available methods and achieves remarkable results in terms of detection rate and detection time. In fact, the recursive implementation adopted for EDA4GNet is suitable for online model adaption in a real-time application similar to the case of time-critical operations. The EDA4GNeT method consists in a robust statistical method to distinguish between the absence and the presence of an anomaly based on a novel detection test defined in Section 5.2.2. To validate the performance of EDA4GNeT, two use cases are adapted including the simulation of different attacks. The results reported in Chapter 6 show an improved performance when compared with the closest works to ours in the literature. The adopted state space representation used to approximate the ARFIMA model can describe well the network traffic as shown in Section 3.4.

In the case study of Section 6.2, basic and composite performance properties are considered for analysis. A DoS attack is simulated in the communication network which causes an increase in the traffic flow. The CUSUM test is adapted with the state space representation assumed for modeling. Computation of the test statistic $g[k]$ allows the detection of the change regardless of its duration or amplitude. Results obtained for the false positive and false negative rates show a better performance for EDA4GNeT which is confirmed with the ROC curves Figure 6.5. Values from $C_{exp}$ and $C_{ID}$ confirm the performance of the proposed method discussed previously.

The EDA4GNeT method is extended for early detection which can detect attacks within acceptable confidence levels. Early detection is performed using a novel score function based on the $j$-step ahead predictions (see Section 5.2). The equations of the Kalman filter are extended to compute the predictions required by the score function. The performance of the proposed approach is evaluated in a second case study and discussed in Section 6.3.1. Different values for steps ahead are used to analyze the capability of anomaly detection based on forecasting Section 5.4. The proposed novel

method is able to detect possible future attacks while keeping acceptable false alarm rates.

## 7.2 Outlook

The anomaly detection method developed in the present work offers a reliable solution to enhance the cybersecurity of IEC 61850 substations. This research direction is very promising as it can be extended in several directions that can be further explored.

**Use of multiple signals**

Use of a state space model to represent the network traffic in electrical substations facilitates extension to address multiple signals.

In order to detect other types of attacks, additional features of different protocols of the network traffic can be integrated in the same model instead of considering each feature separately as proposed in [2]. A total of 25 features of the network traffic are considered for experiments in [2] where they are modeled separately as ARFIMA models. Detection of the anomalies is based on the comparison of the parameters of normal behavior and parameters of the real network traffic of the different time series separately. However, challenges found in modeling of multivariate time series such as possible correlations and non-unique representation are not discussed.

Different features to analyze and detect anomalies in GOOSE network traffic is presented in [64]. A preprocessing step shall be carried out to select the most relevant features that can be further used in the state space model to represent the network traffic within the substation. The developed anomaly detection method can then be directly used on the obtained model to detect attacks resulting in deviation in the characteristics of the network traffic.

**Adaption of the score function**

The novel score function proposed for early detection can be adapted to consider different types of attacks. Moreover, other polynomials can be proposed based on the $j$-step ahead predictions obtained with the adapted Kalman filter. Choice of alternative score functions should be oriented based on the results related to true positives rate and false alarms. The goal of forecasting possible attacks can yield easy-trigger detectors with high false alarms. Indeed, the values parameters of alternative score function can also be adapted depending on the changing conditions of the network traffic.

**Extension to different case studies**

The EDA4GNeT method is implemented and tested on two simulation case studies presented in Section 6 that are based on systems typically found in real applications.

The network traffic as well as the physical grid are simulated using adequate software to replicate as close as possible the real conditions in an electrical substation. It would be however relevant to evaluate the developed AD method on data retrieved from a substation operating in real conditions. The main challenge we faced is the scarcity of real data from electrical substations which is due to several reasons. First, protocols recommended in IEC 61850 such as GOOSE and SV are not always adopted in legacy substations. Secondly, the network traffic is not always collected and even when it is the case, only the communication traffic at the higher level of the substation is monitored. The next limitation that is commonly found when designing IDS for energy systems or ICS in general, is the confidentiality of the data that can be rarely shared with the community for research purposes. Evaluation with data from real system can enrich the discussion on the performance of the proposed method and will yield to further improvements.

**Integration and extension to process knowledge**

Our work focuses on the network traffic in IEC 61850 substations. However, the EDA4GNeT can be extended to detect anomalies at the process level. Signals based on the process variables can be adopted in the EDA4GNeT method with a corresponding adjustment of the developed score function in order to detect physical attacks. For instance, resonance attacks are caused when an adversary induces repeatedly small variations until reaching the resonance. Another type of attacks that have results on similar effects such as DoS is surge attacks which damages the equipment by introducing malicious commands within the Process Control System (PCS) to exceed the boundaries of the process variables or result in a DoS alike state due to emergency shutdown. Provided that relevant process signals are chosen, the EDA4GNeT AD method can detect attacks at the process level such as the previously mentioned ones.

Coupling detection of attacks at the process and the communication level using EDA4GNeT would lead to the detection of a wider range of attacks. This would enable integration of physical process information to the detection system. Combining physical information to EDA4GNeT allows to leverage semantic content of the communication traffic i.e. of the inspected packets.

**Alarm correlation for help in decision-making process**

Alarms collected from the EDA4GNeT AD or other IDS techniques shall be further analyzed. These alarms can be retrieved from the network traffic, physical system or the logging software. Developing a method for an alert management and risk analysis system including an alert aggregator and corresponding manager might be relevant to help in decision-making process. In fact, a relevant further step of the research

introduced in the present work would be to design and implement a system for help in decision-making process through analysis and clustering of alarms including an evaluation of the alarms and possibly an automated response system through their post processing.

**Integration into a global SIEM architecture**

NSM provides system security awareness through the use of data objects to manage and monitor the information through the grid infrastructure. Recommendations for the development of the NSM platform are provided in IEC 62351-7 edition 2017. A well-defined use of the NSM data objects for the system security to mitigate possible cyber-attacks is however not directly addressed in IEC 62351. Integration of the EDA4GNeT anomaly detection method on top of the platform built following guidelines in IEC 62351-7 can be further pursued. In fact, the large amount of data collected through the NSM corresponds to information about the IEDs and their communication. It can be used to model the network traffic and detect anomalies using EDA4GNeT AD method. A promising research direction is to propose a global security information and event management (SIEM) including the IDS designed in this work and an appropriate NSM according to recommendations in IEC 62351-7. This will help centralize all the information sent to the SIEM in order to possibly carry out adequate response actions.

**Application to the KASTEL Security Lab Energy and to the Energy Lab 2.0**

Cyber-Physical Security (CPS) is a substantial concern in critical infrastructures. The interconnected structure of SGs increases considerably its exposure to cyber-attacks such as Man-in-the-Middle, data theft, False Data Injection and other manipulations. Such attacks can have severe consequences on the stability of the electric grid and might lead to blackouts. To defend against those threats, designing and developing effective countermeasures for the CPS for the transition to future energy systems is essential.

The KASTEL Security Lab Energy is a facility that is being built at the IAI institute within the KASTEL project as one of three planned labs: mobility, energy and production. Within the KASTEL Security Lab Energy, the cyber-security of smart grids in which power generators, storage, distribution and consumers are interconnected to ensure optimal operation, is investigated.

The comprehensive use of ICT offers many advantages such as effective integration of renewable energies and ability to respond to fluctuations of the demand and response. The interdependence of more networked devices might however lead to

additional threats. The research carried out in the present work, shows that secure communication is key for a reliable and stable operation of energy networks.

The KASTEL Security Lab Energy is composed of three subsystems with the first one mainly consisting of components from Siemens and will be referred to as the homogeneous Subsystem. A similar facility to the first Subsystem is present at the E-Lab 2.0. The second one represents a scale substation with components from different manufacturers and will be referred to as the heterogeneous Subsystem where IEC 61850 interoperability challenges will be investigated.

As mentioned above, the first subsystem is a small-scale SG with an energy supply part (wind turbine, battery and solar panels) and a transmission substation are implemented as Matlab/Simulink model. Siemens PLCs and IEDs are responsible for controlling the dynamic behavior of the different models and for taking corrective actions. An engineering and monitoring workstation is used to carry out supervisory actions. The Network Security Monitoring (NSM) station provides a continuous collection, attack detection and analysis of communication data.

As a high-level control system for cyber-security research for future energy systems, the KASTEL Security Lab Energy and the SecLabE at the Energy Lab 2.0 facilitate the implementation of attack scenarios and manipulation of hardware and software components. This enables the analysis of risks and possible malfunctions in the electric system caused by cyber-attacks. The KASTEL Security Lab Energy is used for development of efficient methods and algorithms for detection and prevention of cyber-attacks. This includes the development of supervision tools, the design of security features in protocols, software and systems as well as recovery strategies.

The contributions of the present work including mainly the investigation of the security standards for energy systems in IEC 62351 and the early detection method EDA4GNeT helped design our security Labs i.e. SecLab-E and KASTEL Security Lab Energy. In fact, the Subsystem 2 of the KASTEL Security Lab Energy has been designed based on knowledge explored within the present work. Essential questions about the interoperability of the components from different manufacturers, integration of specifications described in IEC 61850 as well as security recommendations proposed in IEC 62351-6 were established in the present work. Technical application and verification will be achieved through implementation of those questions within the Subsystem 1 and 2. To answer the first question of how far are the specifications in IEC 61850 are integrated in components from different manufacturers, different experiments and scenarios will be implemented. This will leverage one of the main challenges in integrating IEC 61850 in substations. Technical recommendations to facilitate the engineering and configuration process for the utilities will be tested and published.

The second main question that would be investigated within the homogeneous and heterogeneous Subsystems of the KASTEL Security Lab Energy, is to which extend can the security recommendations proposed in IEC 62351 be implemented in a small scale substation without affecting the normal operation and respecting the resources constraints. Work on the integration of the IEC 62351 standard is being carried out not only to address the security of communication protocols, as it is the case in the present work, but also to further work on network management, role-based access control as new research topics developed within the IAI and the KASTEL institutes or together with partners.

# A Description of the Cost-Efficient Software Testbed

## A.1 Communication Interface with IEC 61850 Logic in Matlab/Simulink

The main goal is to establish a communication based on link-layer protocols in IEC 61850 between a Matlab/Simulink simulation of an electrical substation and Intelligent Electronic Devices (IEDs). For the transmission of voltage and current measurements, Sampled Values (SV) messages shall be used whereas the transmission of the state of breakers and switches, is done using Generic Object Oriented Substation Event (GOOSE) messages. Additional details about the configuration of the communication according to the IEC 61850 standard are described in Section 2.2.

Some communication interfaces in protocols such as Modbus/TCP exist in Matlab/Simulink. However, no interface for publishing GOOSE and SV messages is available. Considering the increasing compliance of several substations with the IEC 61850 standard, it is particularly relevant and useful to develop a GOOSE/SV interface to integrate in Matlab/Simulink simulations. Such an interface or library is not directly available in Matlab as previously mentioned, which is one of the contributions of the present work.

The overall simulation consists of the following elements depicted in Figure A.1

- a substation - A simulation of a T1-1 substation in Matlab/Simulink is used. More details about the different measurements values retrieved from the simulation are described further in Section A.2.
- GOOSE/SV library - The open-source C library available in [110] is integrated in the developed interface to send the data from the Matlab/Simulink model as GOOSE and SV packets. Detailed explanation of the developed communication interface is given further in this section.
- GOOSE/SV interface - GOOSE/SV interface is created using C Caller blocks in Simulink. In the C Caller blocks, specific functions for GOOSE and SV packets are defined. Once the data is received, the control commands are transferred to the function call and then executed. The formed GOOSE and SV packets are sent out. Detailed steps about creation of the C Caller blocks is explained in the present section.

- Intelligent Electronic Device (IED) - The communication with an Intelligent Electronic Device (IED) is simulated on a virtual machine. The local host or loopback interface is used to view the transmitted GOOSE and SV messages on a network protocol analyzer software for instance in this case Wireshark.

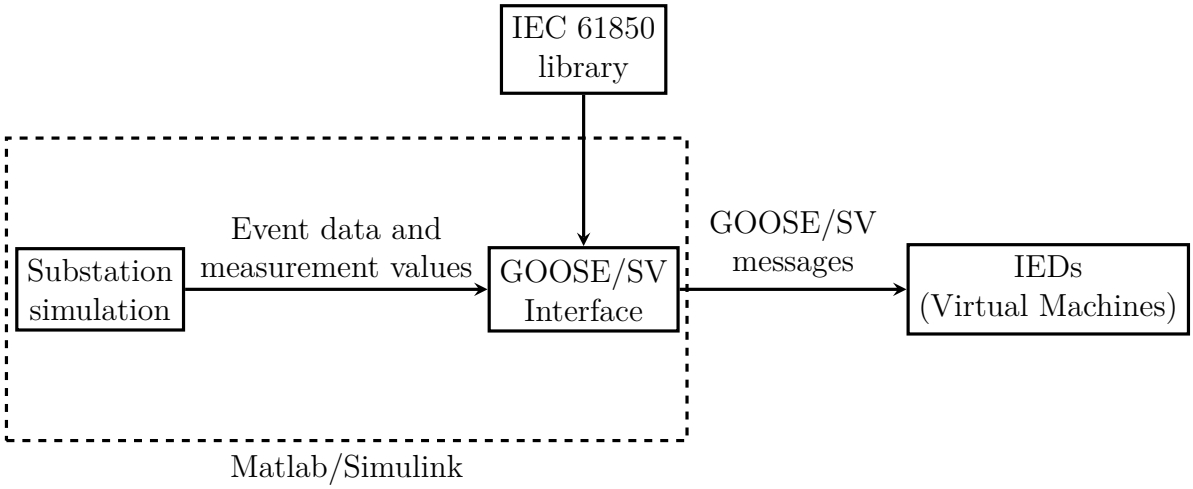



**Figure A.1:** Description of the communication setup

A representation of the different blocks constituting the developed communication interface is depicted in the following diagram Figure A.2 below.

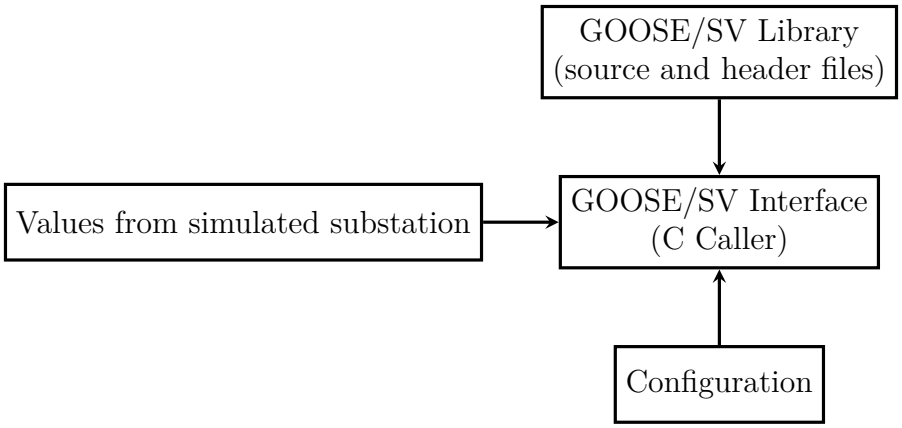



**Figure A.2:** Schematic representation of the communication interface

The open-source IEC61850 library [110] is used for the GOOSE and SV communication and compiled into a new library in Matlab/Simulink.

The C Caller function makes it possible to integrate new or existing C code into Simulink models. To create custom blocks in Simulink models, the C Caller block allows to call external C functions specified in external source code and libraries.

To integrate the libiec61850 library into the Simulink model, the following steps are required:

1. The **Configuration Parameters** should be first specified in the Simulink tool strip

2. The **Simulation Target** shall be selected
3. To enable code parsing by the C Caller block, it must be ensured that the **Import custom code** box is selected. The directories and file paths can be absolute or relative file paths to model directories or current working directory.
4. The **Header file** is selected including the declaration of the C file called directly in the Simulink model
5. The **Source file** with the adequate path shall be selected.
6. When the requested function through the C Caller is encountered during the simulation, the control is transferred to the function call and the C program will be executed. The Eclipse C compiler is used for compiling and executing the piece of software.
7. The next step is to configure the **model parameters**. It is worth noting that the configuration parameters like the Solver selection and step size shall match with the ones from the substation model.

## A.2 The Matlab-Simulink Model

The goal of the communication interface developed in the present work, is to simulate the communication behavior between the circuit breakers, merging units and a substation model.

In fact, measurements values shall be sent periodically using the sampled values protocol from the Matlab/Simulink model to the simulated intelligent electronic device. The previously described behavior is implemented in a C Caller block to simulate a SV publisher. A simulated GOOSE subscriber using also a C caller function continuously runs to listen to the status of the circuit breakers and update control commands accordingly.

The developed communication interface is integrated into the T1-1 simulated substation described in Section 6.2.1.

The substation consists of a 100 MVA, 220 kV three phase source connected, in external mode to a three phase circuit breaker as depicted in Figure A.3. When in external switching time mode, a Simulink logical signal is used to control the breaker operation. The three phase current and voltage are measured and refereed V-D01 and I-D01, respectively. The block 10km represents a three phase transmission line. The model consists of one set of RL series elements connected between input and output terminals and two sets of shunt capacitance lumped at both ends of the line. The three phase current and voltage are measured at the transformer bay and referred to as V-E01 and I-E01, respectively. A three phase circuit breaker in external switching time mode is connected between the transformer and the bus line.

The 3 phase PLL blocks are used to measure the frequency at both parts of the substation i.e. at D01 and E02 and named $Freq_{D01}$ and Freq_E02, respectively. All the measured frequencies, voltages and currents are given as input to the C Caller blocks to transmit the information as GOOSE and SV packets. The substation delivers to two loads of 90 MW. Two circuit breakers in internal switching mode and the three phase voltage and current measurement circuits are connected between the buse and loads. Three phase voltage and current delivered to the first load are referred to VI-E01 whereas the ones delivered to the second load are referred VI-E03.

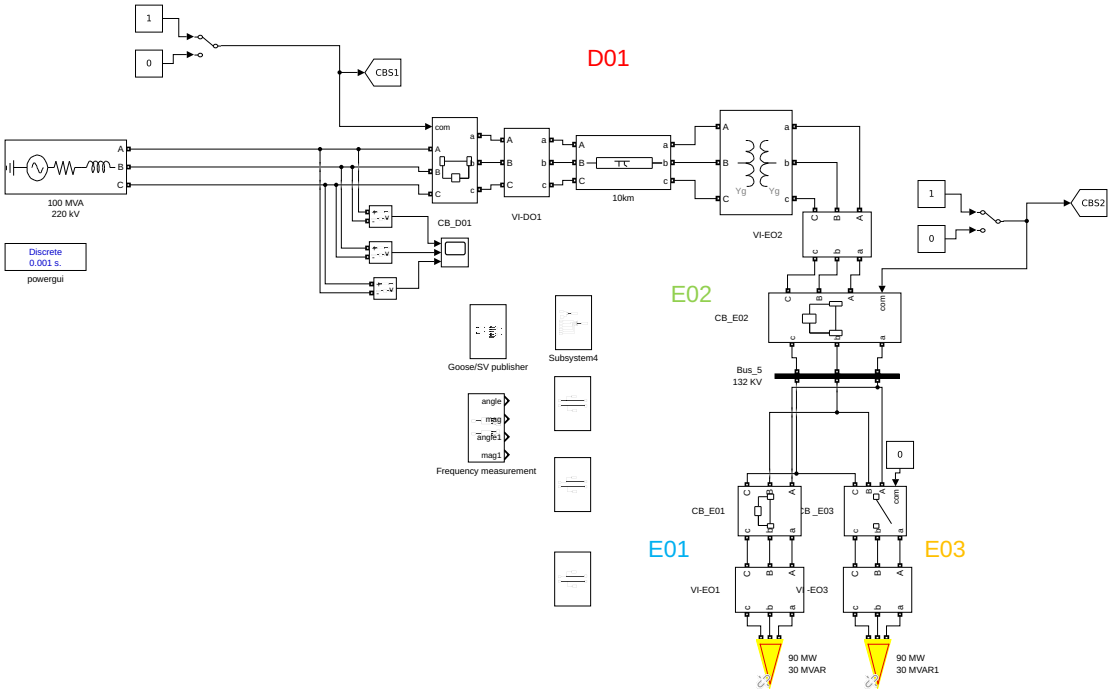



**Figure A.3:** Substation simulation in Simulink

GOOSE and SV C Caller interface blocks are implemented as subsystem in the substation simulation as shown in Figure A.3. The subsystem after adding GOOSE calls for all the circuit breaker status and SV calls for all the three phase current and voltage values will look as in the figure below Figure A.4:

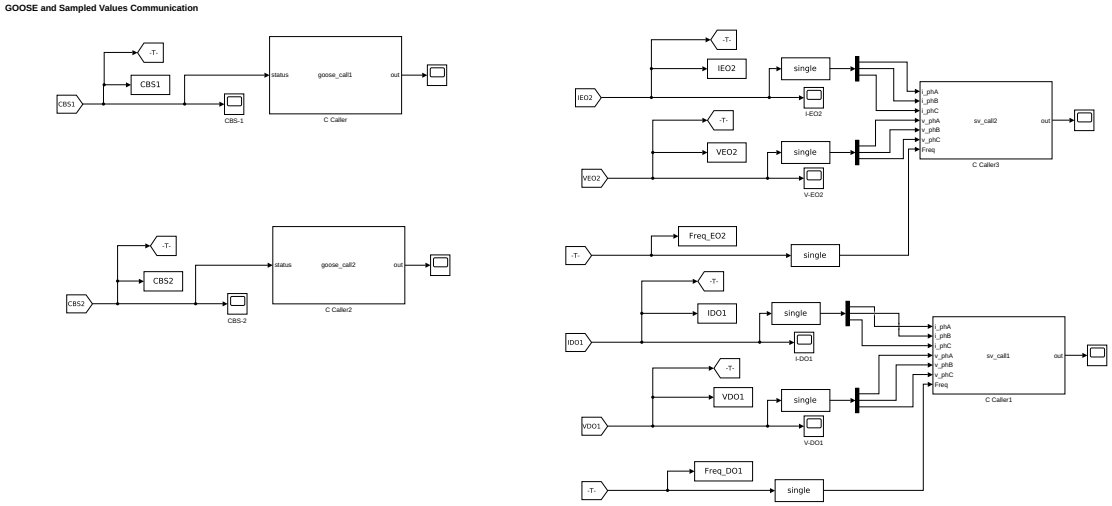



**Figure A.4:** GOOSE and SV communication subsystem

To test the interface, the GOOSE and SV messages are transmitted to a simulated IED on a virtual machine.

For testing the GOOSE/SV interface in the Simulink simulation, Wireshark is used. Figure A.5 and Figure A.6 represent an example of the captured packets.

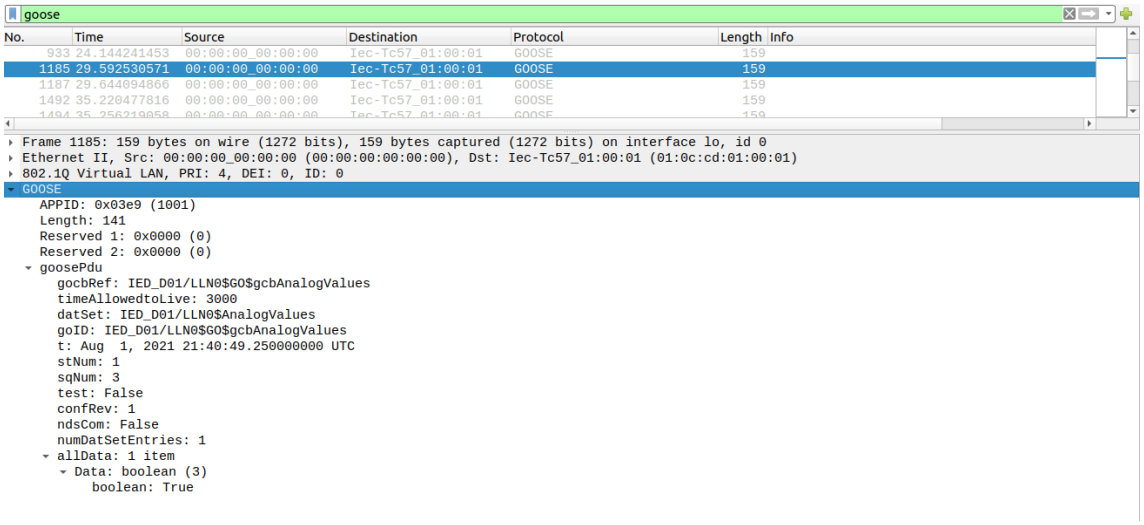



**Figure A.5:** GOOSE message on Wireshark

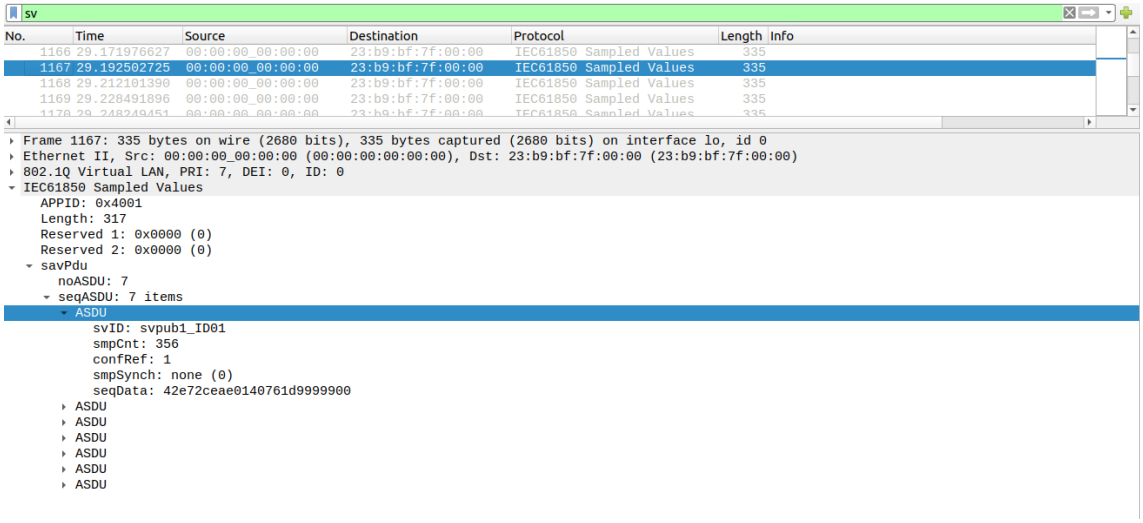



**Figure A.6:** SV message on Wireshark

The circuit breaker status and the measurement data is also sent to Matlab workspace from where it can be stored into .xls or csv file which can be used later if needed. This is mainly done for data storage and may be used for analysis of data at later stage.

## A.3 The GNS3 network model

### A.3.1 The GNS3 Network Model and Available Hardware Resources

The network topology of the whole network is depicted in Figure A.7.

The network simulation tool, GNS3, is used to model the communication between the different virtual machines simulating Intelligent Electronic Devices (IEDs).

The host PC used for most of the testing is equipped with an AMD Ryzen 5 2600 CPU with 6 cores and 12 threads and 16 GB RAM. The virtual machines are generally set up according the following configuration. In fact, the attacker machine has access to all cores at 100% performance and 1300 MB RAM, all other VMs are restricted to use 1 CPU core with a 40% execution cap. It is worth mentioning that below this value, the IEDs were not able to satisfy the desired time constraints. In the following subsections, a description of the behaviour of the main virtual machines is given, under normal circumstances.

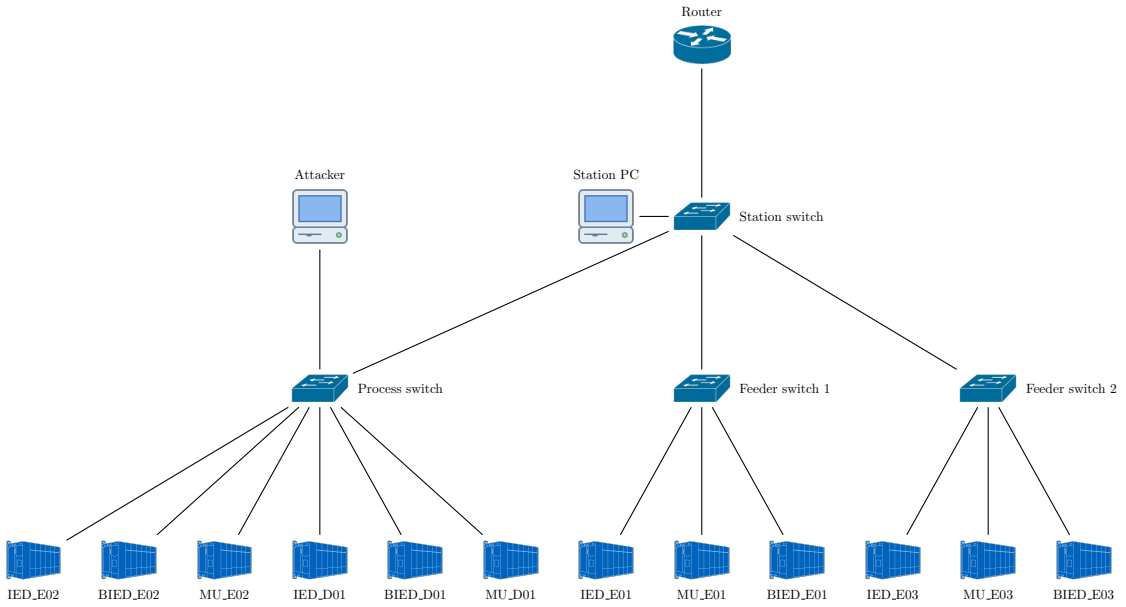



**Figure A.7:** GNS3 network topology

### IED-D01

The server IED listens to the Sampled Values (SV) messages sent by MU_D01 and analyzes them according to the configured protection and control functions. A simplified operation of a server IED is implemented. Indeed, if any of the measurements transmitted from SV messages is above a certain threshold, a circuit breaker must be activated indicating a possible fault. According to this, a boolean attribute value on the server is set which triggers a burst GOOSE. In normal operation, IED_D01 resends the same unchanged packet. When a fault occurs, a burst of GOOSE messages is triggered. In this case, the fault packets are retransmitted with increasing time delays of $[minTime * 2^n], n = 1,2,\ldots$ for 1000 ms. One second after the fault, the GOOSE communication returns to the normal 1000 ms repetition process.

These changes in the server attribute values are also sent to the Station PC in form of MMS reports. The MMS connection between IED_D01 and Station PC is TLS encrypted as recommended in [52].

### B-IED-D01

The circuit breaker IED listens to the GOOSE transmission from IED_D01, and when the respective boolean attribute value is set to true, the device interrupts the flow of current. Then, as a confirmation message, a burst of GOOSE messages with the new circuit breaker state is sent back to IED_D01. For demonstration purposes,

the timestamp in the prefix of the incoming GOOSE packet with the command from IED_D01 is included in the dataset of the outgoing GOOSE. This means that a change in timestamp of the incoming GOOSE message triggers a burst GOOSE for B_IED_D01, however, it does not change the desired behaviour since the prefix timestamp change occurs as a consequence of a change in the dataset. The same GOOSE timing rules apply as for IED_D01.

#### Station PC

The Station PC serves the purpose of a Human-Machine Interface as it provides monitoring and controlling possibilities. As mentioned above, the server IED reports the anomalies to the Station PC.

### A.3.2 Logging

The data transmitted between the different simulated components of the substation are recorded in log files. The logs produced by each simulated device is presented in the following.

- MU_D01 writes out the content of all sent SV messages.
- IED_D01 prints all incoming SV and GOOSE packets reaching the receiver module. In fact, if they are considered to be valid, the same packets are printed when reaching the listener module. Once the Time-allowed-To-Live (TTL) timespan has been exceeded, the internal counters of the receiver module are reset, assuming the connection is lost. So the next incoming GOOSE packet can be evaluated as valid irrespectively of their stNum and sqNum.
- B_IED_D01 prints the same information as IED_D01. However, it is worth mentioning that the simulated B_IED_D01 wt does not subsrcibe to any SV messages contrarily to IED_D01.
- The station PC prints out the received MMS reports (there was an error while recording so these logs are missing at the moment).

```
No.     Time           Source                Destination           Protocol Length Info
   1185 29.592530571   00:00:00_00:00:00     Iec-Tc57_01:00:01     GOOSE    159
Frame 1185: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface lo, id 0
    Interface id: 0 (lo)
        Interface name: lo
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  1, 2021 23:40:49.250532789 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1627854049.250532789 seconds
    [Time delta from previous captured frame: 0.020457659 seconds]
    [Time delta from previous displayed frame: 5.448289118 seconds]
    [Time since reference or first frame: 29.592530571 seconds]
    Frame Number: 1185
    Frame Length: 159 bytes (1272 bits)
    Capture Length: 159 bytes (1272 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:vlan:ethertype:goose]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: Iec-Tc57_01:00:01 (01:0c:cd:01:00:01)
    Destination: Iec-Tc57_01:00:01 (01:0c:cd:01:00:01)
        Address: Iec-Tc57_01:00:01 (01:0c:cd:01:00:01)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 4, DEI: 0, ID: 0
    100. .... .... .... = Priority: Video, < 100ms latency and jitter (4)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 0000 = ID: 0
    Type: IEC 61850/GOOSE (0x88b8)
GOOSE
    APPID: 0x03e9 (1001)
    Length: 141
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
    goosePdu
        gocbRef: IED_D01/LLN0$GO$gcbAnalogValues
        timeAllowedtoLive: 3000
        datSet: IED_D01/LLN0$AnalogValues
        goID: IED_D01/LLN0$GO$gcbAnalogValues
        t: Aug  1, 2021 21:40:49.250000000 UTC
        stNum: 1
        sqNum: 3
        test: False
        confRev: 1
        ndsCom: False
        numDatSetEntries: 1
        allData: 1 item
            Data: boolean (3)
                boolean: True
```

**Figure A.8:** Log of a GOOSE message

```
No.     Time           Source                Destination           Protocol Length Info
   1167 29.192502725   00:00:00_00:00:00     23:b9:bf:7f:00:00     IEC61850 Sampled Values 335
Frame 1167: 335 bytes on wire (2680 bits), 335 bytes captured (2680 bits) on interface lo, id 0
    Interface id: 0 (lo)
        Interface name: lo
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug  1, 2021 23:40:48.850504943 CEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1627854048.850504943 seconds
    [Time delta from previous captured frame: 0.020526098 seconds]
    [Time delta from previous displayed frame: 0.020526098 seconds]
    [Time since reference or first frame: 29.192502725 seconds]
    Frame Number: 1167
    Frame Length: 335 bytes (2680 bits)
    Capture Length: 335 bytes (2680 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:vlan:ethertype:sv]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 23:b9:bf:7f:00:00 (23:b9:bf:7f:00:00)
    Destination: 23:b9:bf:7f:00:00 (23:b9:bf:7f:00:00)
        Address: 23:b9:bf:7f:00:00 (23:b9:bf:7f:00:00)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory
default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00_00:00:00 (00:00:00:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 0
    111. .... .... .... = Priority: Network Control (7)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 0000 = ID: 0
    Type: IEC 61850/SV (Sampled Value Transmission (0x88ba)
IEC61850 Sampled Values
    APPID: 0x4001
    Length: 317
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
    savPdu
        noASDU: 7
        seqASDU: 7 items
            ASDU
                svID: svpub1_ID01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: 42e72ceae0140761d9999900
            ASDU
                svID: svpub2_ID01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: c2c93153e0140761d9999900
            ASDU
                svID: svpub3_ID01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: c17016c0e0140761d9999900
            ASDU
                svID: svpub4_VD01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: 488b9e86e0140761d9999900
            ASDU
                svID: svpub5_VD01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: c79ae428e0140761d9999900
            ASDU
                svID: svpub6_VD01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: c849caf7e0140761d9999900
            ASDU
                svID: svpub _Freq_D01
                smpCnt: 356
                confRef: 1
                smpSynch: none (0)
                seqData: 42c80000e0140761d9999900
```

**Figure A.9:** Log of a SV message

# B Analysis of Parameters Convergence of SS-AR Model

An SS-AR model of order $n = 10$ was used for modeling the network traffic of the substation introduced in Chapter 3. The choice of $n = 10$ is based on a trade-off between model complexity and description of the corresponding time series. Different experiments were performed using the estimated model to generate simulation data. An SS-AR model was computed for each experiment and the parameters are shown in Figure B.2 and Figure B.1. The initialization values were kept constant for all the experiments. After approximately 25 iterations, the parameters converge to the final values.

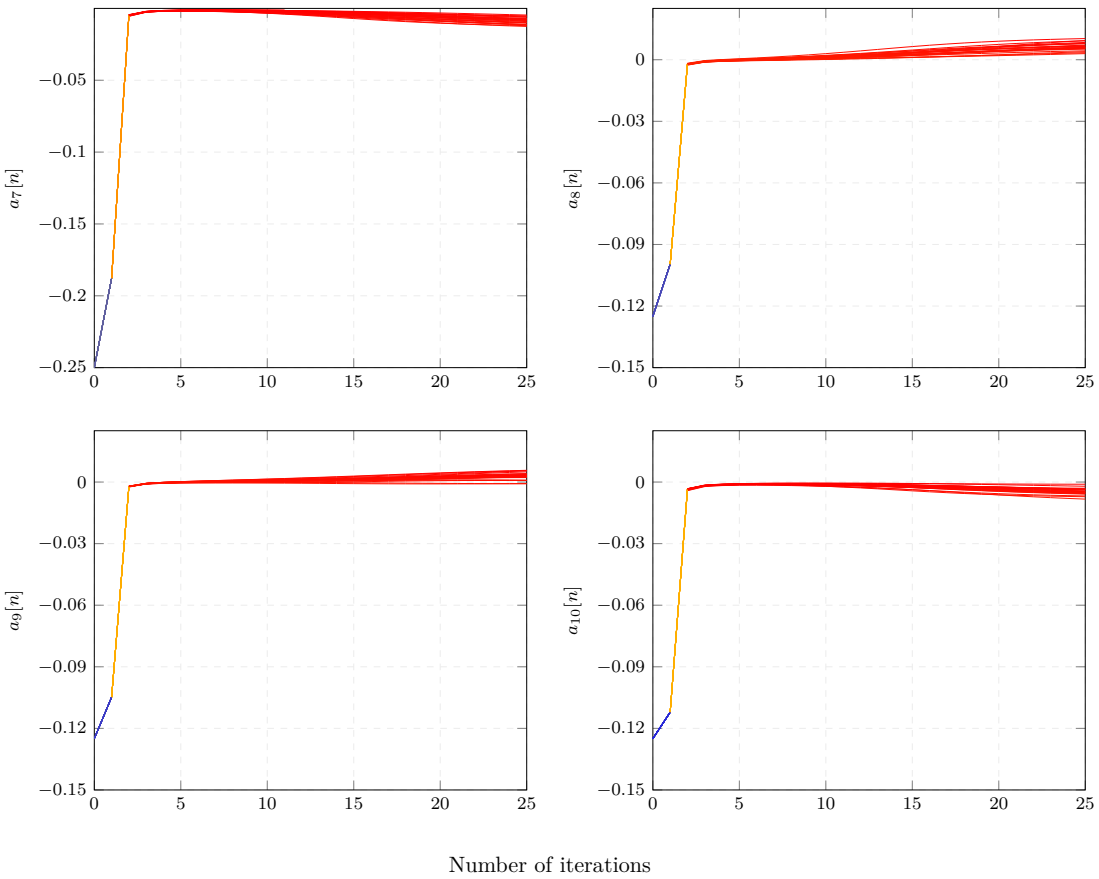



**Figure B.1:** Convergence of $a_7$ to $a_{10}$

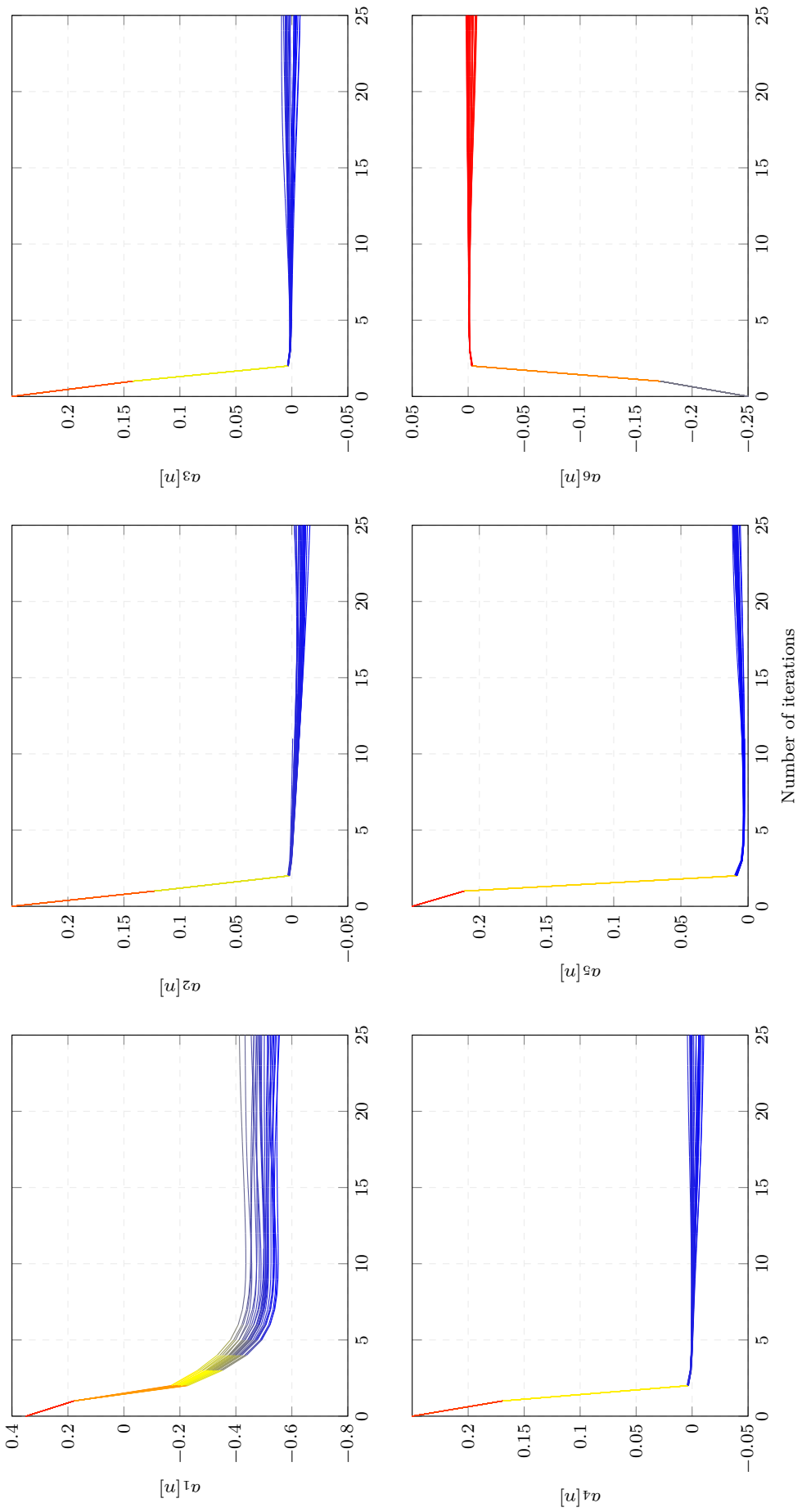



**Figure B.2:** Convergence of $a_1$ to $a_6$

# C Details of the Detection Results in the Second Use Case

In the present appendix, detailed results related to the case study of Section 6.3 summarized in Table 6.3 are presented. Tables Table C.1 to Table C.6 corresponds to the detection of the changes for different thresholds reported in the aforementioned case study. The detection performance including the detection time are described. The smallest values among the different thresholds of the expected cost $C_{exp}$ of EDA4GNeT are depicted in bold. The maximum values of the intrusion capability $C_{ID}$ of the different threshold values of each change in the second use case are shown in bold.

**Table C.1:** Comparison of detection results of first change using EDA4GNeT

| Threshold | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 0.1 | – | −22.80 | 3.2730 | 3.8417 | 0.1245 | 0.1185 | 0.0962 | 0.1001 | 0.9002 | 0.5488 |
| 0.2 | – | −22.72 | 2.5375 | 3.7980 | 0.2303 | 0.1260 | 0.0996 | 0.1190 | 1.0139 | 0.5154 |
| 0.3 | – | −21.69 | 1.2511 | 1.7688 | 0.1554 | 0.1304 | 0.1694 | 0.1020 | 1.0040 | 0.9131 |
| 0.4 | – | −22.69 | 5.5811 | 3.0741 | 0.1233 | 0.1370 | **0.0174** | 0.1090 | 1.0048 | 0.8198 |
| 0.5 | – | −22.78 | 3.6245 | 2.4879 | 0.0333 | 0.1493 | 0.0758 | 0.1112 | 0.9628 | 0.5286 |
| 0.6 | – | −20.19 | 2.7281 | 3.0663 | 0.3067 | 0.1549 | 0.0717 | 0.1100 | 0.9701 | 0.3284 |
| 0.7 | – | −22.44 | 3.8151 | 3.5628 | 0.1395 | 0.1592 | 0.0906 | 0.1500 | 0.9101 | 0.4912 |
| 0.8 | – | −21.86 | 3.4238 | 3.0522 | 0.1307 | 0.1999 | 0.0912 | **0.1000** | 1.0017 | **0.9896** |
| 0.9 | – | −22.53 | 3.6641 | 3.4166 | 0.2430 | 0.2613 | 0.1090 | 0.1020 | 0.9017 | 0.7999 |
| 1 | – | −21.11 | 0.3643 | 3.3020 | 0.2731 | 0.3073 | 0.1097 | 0.1100 | **1.2057** | 0.5985 |

* Detection delay expressed in discrete time $k$

**Table C.2:** Comparison of detection results of second change using EDA4GNeT

| Threshold | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 0.1 | – | −16.96 | 3.1320 | 3.1778 | 0.0912 | 0.3056 | 0.0962 | 0.1032 | 0.9599 | 0.5189 |
| 0.2 | – | −17.82 | 3.4391 | 2.8778 | 0.2333 | 0.2545 | 0.0965 | 0.0932 | 0.9685 | 0.5249 |
| 0.3 | – | −17.22 | 2.4742 | 2.9778 | 0.2617 | 0.2139 | 0.0964 | 0.0914 | 0.9688 | 0.5613 |
| 0.4 | – | −17.08 | 1.4417 | 3.1356 | 0.2060 | 0.3220 | 0.0992 | 0.1036 | 0.9601 | 0.5488 |
| 0.5 | – | −17.63 | 1.7340 | 3.2104 | 0.2333 | 0.2460 | 0.0951 | **0.0890** | 0.9635 | 0.5125 |
| 0.6 | – | −17.06 | 1.4723 | 2.2889 | 0.2024 | 0.1138 | **0.0801** | 0.1034 | 0.9516 | **0.5849** |
| 0.7 | – | −17.32 | 4.0056 | 3.1067 | 0.2307 | 0.3217 | 0.0899 | 0.1033 | **0.9798** | 0.5497 |
| 0.8 | – | −17.01 | 3.5346 | 3.1556 | 0.2058 | 0.3085 | 0.0890 | 0.1133 | 0.9682 | 0.5281 |
| 0.9 | – | −17.00 | 2.0442 | 3.4219 | 0.2800 | 0.2397 | 0.0809 | 0.1133 | 0.9698 | 0.5024 |
| 1 | – | −17.31 | 2.0794 | 2.1122 | 0.1890 | 0.3260 | 0.0894 | 0.1095 | 0.9676 | 0.5201 |

* Detection delay expressed in discrete time $k$

**Table C.3:** Comparison of detection results of third change using EDA4GNeT

| Threshold | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 0.1 | – | −21.40 | 2.0692 | 3.0713 | −0.4015 | 0.4017 | 0.0990 | 0.0904 | 0.9152 | 0.8642 |
| 0.2 | – | −19.99 | 2.1903 | 2.0713 | −0.3148 | 0.4074 | 0.0938 | **0.0903** | 0.9462 | **0.9484** |
| 0.3 | – | −20.84 | 2.1081 | 2.0851 | −0.4143 | 0.4072 | 0.0886 | 0.0920 | **0.9472** | 0.9187 |
| 0.4 | – | −20.08 | 1.7895 | 2.0752 | −0.3130 | 0.4274 | **0.0712** | 0.1001 | 0.9418 | 0.8944 |
| 0.5 | – | −21.00 | 2.5214 | 3.0733 | −0.3350 | 0.4127 | 0.0864 | 0.1001 | 0.9418 | 0.8102 |
| 0.6 | – | −20.96 | 1.9709 | 3.0752 | −0.3120 | 0.4017 | 0.0808 | 0.1001 | 0.9418 | 0.8630 |
| 0.7 | – | −21.94 | 2.2801 | 3.0733 | −0.3911 | 0.4274 | 0.0904 | 0.1001 | 0.9409 | 0.8315 |
| 0.8 | – | −21.00 | 1.6651 | 3.1792 | −0.2105 | 0.4173 | 0.0952 | 0.1000 | 0.9418 | 0.8157 |
| 0.9 | – | −20.95 | 2.3883 | 2.8851 | −0.3290 | 0.3122 | 0.0935 | 0.1002 | 0.9418 | 0.8128 |
| 1 | – | −20.94 | 1.9745 | 2.9752 | −0.3520 | 0.3148 | 0.0903 | 0.1002 | 0.9418 | 0.8951 |

* Detection delay expressed in discrete time $k$

**Table C.4:** Comparison of detection results of fourth change using EDA4GNeT

| Threshold | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 0.1 | – | −24.57 | 0.9245 | 2.5144 | 0.0402 | 0.0992 | **0.0803** | 0.0912 | 0.9348 | **0.6152** |
| 0.2 | – | −21.28 | 1.4050 | 2.6144 | 0.0400 | 0.1980 | 0.0830 | 0.0902 | 0.9266 | 0.5014 |
| 0.3 | – | −23.66 | 1.3285 | 2.7881 | 0.0401 | 0.1877 | 0.0839 | 0.0911 | 0.9250 | 0.5110 |
| 0.4 | – | −19.29 | 1.3765 | 2.8124 | 0.0401 | 0.1791 | 0.0848 | 0.0901 | **0.9398** | 0.5106 |
| 0.5 | – | −22.84 | 2.3085 | 2.9122 | 0.0400 | 0.1800 | 0.0854 | 0.0902 | 0.9352 | 0.5020 |
| 0.6 | – | −23.06 | 2.5382 | 2.9148 | 0.0401 | 0.1809 | 0.0836 | 0.0902 | 0.9347 | 0.5117 |
| 0.7 | – | −23.04 | 2.5775 | 2.1179 | 0.0403 | 0.1799 | 0.0844 | **0.0879** | 0.9324 | 0.5097 |
| 0.8 | – | −26.92 | 2.3902 | 2.1589 | 0.0401 | 0.1838 | 0.0841 | 0.0919 | 0.9335 | 0.5193 |
| 0.9 | – | −22.19 | 2.2164 | 2.5151 | 0.0401 | 0.1000 | 0.0850 | 0.0934 | 0.9313 | 0.5074 |
| 1 | – | −23.36 | 2.3711 | 2.8167 | 0.0401 | 0.1820 | 0.0855 | 0.0947 | 0.9224 | 0.5002 |

* Detection delay expressed in discrete time $k$

**Table C.5:** Comparison of detection results of fifth change using EDA4GNeT

| Threshold | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 0.1 | – | −33.69 | 1.5206 | 2.5117 | 0.0669 | 0.1390 | 0.0806 | 0.0871 | 0.9292 | **0.6154** |
| 0.2 | – | −33.96 | 1.5605 | 2.5417 | 0.0667 | 0.1391 | 0.0817 | 0.0911 | 0.9229 | 0.6094 |
| 0.3 | – | −29.05 | 1.5104 | 2.5518 | 0.0663 | 0.1390 | 0.0810 | 0.0891 | 0.9292 | 0.6103 |
| 0.4 | – | −35.53 | 1.5003 | 2.5071 | 0.0663 | 0.1390 | 0.0821 | 0.0810 | 0.9225 | 0.6012 |
| 0.5 | – | −34.00 | 1.5004 | 2.5317 | 0.0663 | 0.1390 | 0.0829 | 0.0881 | **0.9478** | 0.6081 |
| 0.6 | – | −34.97 | 1.5004 | 2.5317 | 0.0669 | 0.1390 | 0.0830 | 0.0910 | 0.9225 | 0.6125 |
| 0.7 | – | −34.00 | 1.5904 | 2.5217 | 0.0673 | 0.1391 | 0.0829 | 0.0880 | 0.9252 | 0.6106 |
| 0.8 | – | −33.91 | 1.5104 | 2.5267 | 0.0670 | 0.1390 | 0.0804 | 0.0870 | 0.9295 | 0.6105 |
| 0.9 | – | −33.82 | 1.5518 | 2.5492 | 0.0669 | 0.1390 | **0.0802** | 0.0872 | 0.9225 | 0.6101 |
| 1 | – | −33.87 | 1.5793 | 2.5417 | 0.0670 | 0.1390 | 0.0806 | **0.0840** | 0.9224 | 0.6102 |

* Detection delay expressed in discrete time $k$

**Table C.6:** Comparison of detection results of sixth change using EDA4GNeT

| Threshold | Earliness of Detection* | | Basic | | | | Composite | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | FPR [%] | | FNR [%] | | $C_{exp}$ | | $C_{ID}$ | |
| | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step | 1-step | multi-step |
| 0.1 | – | −14.88 | 1.5288 | 2.3510 | 0.1645 | 0.0912 | 0.0944 | 0.0930 | 0.9837 | 0.4613 |
| 0.2 | – | −14.02 | 1.5090 | 2.3610 | 0.1144 | 0.0935 | 0.0719 | **0.0650** | 0.9372 | **0.5746** |
| 0.3 | – | −14.83 | 1.9858 | 2.3491 | 0.0347 | 0.1147 | 0.0820 | 0.0801 | 0.9937 | 0.2724 |
| 0.4 | – | −16.00 | 1.9517 | 2.3401 | 0.1936 | 0.0978 | 0.0764 | 0.0804 | **1.3708** | 0.2560 |
| 0.5 | – | −18.98 | 0.8422 | 2.3110 | 0.2217 | 0.1680 | 0.0626 | 0.0903 | 1.0037 | 0.0866 |
| 0.6 | – | −10.58 | 0.8358 | 2.3310 | 0.1667 | 0.1178 | 0.0847 | 0.1003 | 0.8469 | 0.2506 |
| 0.7 | – | −14.24 | 1.2989 | 2.3510 | 0.0399 | 0.0888 | 0.0848 | 0.1101 | 0.8987 | 0.2925 |
| 0.8 | – | −13.25 | 1.7929 | 2.3310 | 0.3940 | 0.0985 | 0.0992 | 0.1001 | 0.9798 | 0.1229 |
| 0.9 | – | −17.17 | 1.6989 | 2.3410 | 0.2917 | 0.1348 | **0.0617** | 0.0103 | 0.8474 | 0.4160 |
| 1 | – | −14.44 | 1.3192 | 2.3428 | 0.3925 | 0.0948 | 0.0624 | 0.1011 | 0.9072 | 0.3811 |

* Detection delay expressed in discrete time $k$

# Bibliography


[1] A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, R. Hadjidj, M. Debbabi, and A. Youssef: 'Security monitoring of IEC 61850 substations using IEC 62351-7 network and system management'. *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2019: pp. 1–7.

[2] T. Andrysiak, L. Saganowski, M. Choras, and R. Kozik: 'Network traffic prediction and anomaly detection based on ARFIMA model'. *International Joint Conference SOCO14-CISIS14-ICEUTE14*. Springer. 2014: pp. 545–554.

[3] R. R. R. Barbosa: *Anomaly detection in SCADA systems: a network based approach*. 2014.

[4] M. Basseville: 'Detecting changes in signals and systems a survey'. *Automatica* (1988), vol. 24(3): pp. 309–326.

[5] M. Basseville, I. V. Nikiforov, et al.: *Detection of abrupt changes: theory and application*. Vol. 104. prentice Hall Englewood Cliffs, 1993.

[6] D. Bauer: 'Using Subspace Methods to Model Long-Memory Processes'. *International Conference on Time Series and Forecasting*. Springer. 2018: pp. 171–185.

[7] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen: 'A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation'. *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2019: pp. 1–7.

[8] A. Bohara, J. Ros-Giralt, G. Elbez, A. Valdes, K. Nahrstedt, and W. H. Sanders: 'ED4GAP: Efficient Detection for GOOSE-Based Poisoning Attacks on IEC 61850 Substations'. *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2020: pp. 1–7.

[9] H. Boubaker: 'A generalized ARFIMA model with smooth transition fractional integration parameter'. *Journal of Time Series Econometrics* (2017), vol. 10(1).

[10] S. Caltagirone, A. Pendergast, and C. Betz: *The diamond model of intrusion analysis*. Tech. rep. Center For Cyber Intelligence Analysis and Threat Research Hanover Md, 2013.

[11] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta: 'A multidimensional critical state analysis for detecting intrusions in SCADA systems'. *IEEE Transactions on Industrial Informatics* (2011), vol. 7(2): pp. 179–186.

[12] F. Castano, S. Strzelczak, A. Villalonga, R. E. Haber, and J. Kossakowska: 'Sensor reliability in cyber-physical systems using internet-of-things data: A review and case study'. *Remote sensing* (2019), vol. 11(19): p. 2252.

[13] CEN-CENELEC-ETSI: 'Group: Smart grid reference architecture (November 2012)'. 2015.

[14] CENELEC: 'Smart Grid Coordination Group SGCGM490/Smart Grid Set of Standards'. (2014), vol.

[15] N. H. Chan and W. Palma: 'State space modeling of long-memory processes'. *Annals of Statistics* (1998), vol.: pp. 719–740.

[16] N. H. Chan and W. Palma: 'Estimation of long-memory time series models: A survey of different likelihood-based methods'. *Advances in Econometrics* (2006), vol. 20(2): pp. 89–121.

[17] C.-S. Chen, Y.-H. Lee, and H.-W. Hsu: 'Adaptive order selection for autoregressive models'. *Journal of Statistical Computation and Simulation* (2014), vol. 84(9): pp. 1963–1974.

[18] A. Cherepanov and R. Lipovsky: *Industroyer: Biggest threat to industrial control systems since Stuxnet*. 2017.

[19] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes: 'Using model-based intrusion detection for SCADA networks'. *Proceedings of the SCADA security scientific symposium*. Vol. 46. Citeseer. 2007: pp. 1–12.

[20] A. Coluccia and A. Fascista: 'An alternative procedure to cumulative sum for cyber-physical attack detection'. *Internet Technology Letters* (2018), vol. 1(3): e2.

[21] V. Coughlin, C. Rubio-Medrano, Z. Zhao, and G.-J. Ahn: 'EDSGuard: Enforcing Network Security Requirements for Energy Delivery Systems'. *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2018: pp. 1–6.

[22] S. Dietrich, N. Long, and D. Dittrich: 'Analyzing Distributed Denial of Service Tools: The Shaft Case.' *LISA*. 2000: pp. 329–339.

[23] V. Digalakis, J. R. Rohlicek, and M. Ostendorf: 'ML estimation of a stochastic linear system with the EM algorithm and its application to speech recognition'. *IEEE Transactions on speech and audio processing* (1993), vol. 1(4): pp. 431–442.

[24] J. Durbin and S. J. Koopman: *Time series analysis by state space methods*. Oxford university press, 2012.

[25] G. Elbez, H. B. Keller, A. Bohara, K. Nahrstedt, and V. Hagenmeyer: 'Detection of DoS Attacks Using ARFIMA Modeling of GOOSE Communication in IEC 61850 Substations'. *Energies* (2020), vol. 13(19): p. 5176.

[26] G. Elbez, H. B. Keller, and V. Hagenmeyer: *Novel Classification of Attacks against Smart Grids: Ensuring the Cyber-Physical Security of Modern Power Systems (Poster)*. 6. Jahrestagung KIT-Zentrum Energie, 2017.

[27] G. Elbez, H. B. Keller, and V. Hagenmeyer: 'A cost-efficient software testbed for cyber-physical security in iec 61850-based substations'. *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2018: pp. 1–6.

[28] G. Elbez, H. B. Keller, and V. Hagenmeyer: 'A new classification of attacks against the cyber-physical security of smart grids'. *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 2018: pp. 1–6.

[29] G. Elbez, H. B. Keller, and V. Hagenmeyer: 'Authentication of GOOSE messages under timing constraints in IEC 61850 substations'. *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*. 2019: pp. 137–143.

[30] ENISA: *EU Regulation 2019/881 of the European parliament and of the council (The European Union Agency for Cybersecurity)*. 2019.

[31] S. M. Farooq, S. S. Hussain, and T. S. Ustun: 'Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages'. *IEEE Access* (2019), vol. 7: pp. 32343–32351.

[32] R. Feizimirkhani, A. I. Bratcu, and Y. Besanger: 'Time-series Modelling of IEC 61850 GOOSE Communication Traffic between IEDs in smart grids-a parametric analysis'. *IFAC-PapersOnLine* (2018), vol. 51(28): pp. 444–449.

[33] S. Floyd and V. Paxson: 'Difficulties in simulating the Internet'. *IEEE/ACm Transactions on Networking* (2001), vol. 9(4): pp. 392–403.

[34] R. Fox and M. S. Taqqu: 'Large-sample properties of parameter estimates for strongly dependent stationary Gaussian time series'. *The Annals of Statistics* (1986), vol.: pp. 517–532.

[35] G. C. Goodwin, G. GC, and P. RL: 'Dynamic System Identification. Experiment Design And Data Analysis.' (1977), vol.

[36] J. G. de Gooijer and A. Klein: 'On the cumulated multi-step-ahead predictions of vector autoregressive moving average processes'. *International Journal of Forecasting* (1992), vol. 7(4): pp. 501–513.

[37] S. Grassi and P. S. De Magistris: 'When long memory meets the Kalman filter: A comparative study'. *Computational Statistics & Data Analysis* (2014), vol. 76: pp. 301–319.

[38] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skoric: 'Measuring intrusion detection capability: an information-theoretic approach'. *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*. 2006: pp. 90–101.

[39] V. Hagenmeyer, H. Kemal Cakmak, C. Dupmeier, T. Faulwasser, J. Isele, H. B. Keller, P. Kohlhepp, U. Kuhnapfel, U. Stucky, S. Waczowicz, et al.: 'Information and communication technology in energy lab 2.0: Smart energies system simulation and control center with an open-street-map-based power flow simulation example'. *Energy Technology* (2016), vol. 4(1): pp. 145–162.

[40] A. Hahn and M. Govindarasu: 'Cyber attack exposure evaluation framework for the smart grid'. *IEEE Transactions on Smart Grid* (2011), vol. 2(4): pp. 835–843.

[41] G. Hale: *Ukraine Attack: An Insiders Perspective*. 2017.

[42] W. Hao and Q. Yang: 'Data Traffic Characterization in Intelligent Electric Substations using FARIMA based Threshold Model'. *Energy Procedia* (2018), vol. 145: pp. 413–420.

[43] J. Haslett and A. E. Raftery: 'Space-time modelling with long-memory dependence: Assessing Ireland's wind power resource'. *Journal of the Royal Statistical Society: Series C (Applied Statistics)* (1989), vol. 38(1): pp. 1–21.

[44] F. Hohlbaum, M. Braendle, and F. Alvarez: 'Cyber Security Practical considerations for implementing IEC 62351'. *PAC World Conference*. 2010.

[45] J. Hong, C. C. Liu, and M. Govindarasu: 'Integrated Anomaly Detection for Cyber Security of the Substations'. *IEEE Transactions on Smart Grid* (July 2014), vol. 5(4): pp. 1643–1653.

[46] J. Hosking: 'Fractional Differencing Modeling in Hydrology'. *JAWRA Journal of the American Water Resources Association* (1985), vol. 21(4): pp. 677–682.

[47] J. Hoyos, M. Dehus, and T. X. Brown: 'Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure'. *Globecom Workshops (GC Wkshps), 2012 IEEE*. IEEE. 2012: pp. 1508–1513.

[48] N.-J. Hsu, B. K. Ray, and F. BREIDT: 'Bayesian estimation of common long-range dependent models'. *Proc. of Seventh Vilnius Conference on Probability Theory and Mathematical Statistics*. 1999: pp. 311–324.

[49] H. E. Hurst: 'Long-term storage capacity of reservoirs'. *Trans. Amer. Soc. Civil Eng.* (1951), vol. 116: pp. 770–799.

[50] R. J. Hyndman: 'CRAN task view: Time series analysis'. (2021), vol.

[51] IEC: *Communication networks and systems in substations - IEC 61850 Part 5: Communication requirements for functions and device models*. 2003.

[52] IEC: *International Electrotechnical Commission (IEC) 62351: Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 62351*. 2007.

[53] IEC: *International Electrotechnical Commission 61850-7-4:2010 Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes*. 2010.

[54] IEC: 'International Electrotechnical Commission Part 8-1: Specific communication service mapping (SCSM) Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3'. *International Standard IEC* (2011), vol. 61850.

[55] IEC: 'International Electrotechnical Commission 61850 Power Utility Automation'. *International Electrotechnical Commission: Geneva, Switzerland* (2016), vol.

[56] ISO: *International Organization for Standardization (ISO) 9506: Industrial automation systems - Manufacturing Message specification*. 2003.

[57] M. Kabir-Querrec, S. Mocanu, J.-M. Thiriet, and E. Savary: 'Power utility automation cybersecurity: IEC 61850 specification of an intrusion detection function'. *25th European Safety and Reliability Conference (ESREL 2015)*. CRC Press. 2015.

[58] S. M. Kay: *Fundamentals of statistical signal processing*. Prentice Hall PTR, 1993.

[59] H. B. Keller, O. Schneider, J. Matthes, and V. Hagenmeyer: 'Reliable, safe and secure software of connected future control systems-challenges and solutions'. *at - Automatisierungstechnik* (2016), vol. 64(12): pp. 930–947.

[60] E. D. Knapp and R. Samani: *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes, 2013.

[61] N. S. Kush, E. Ahmed, M. Branagan, and E. Foo: 'Poisoned GOOSE: Exploiting the GOOSE protocol'. *Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)[Conferences in Research and Practice in Information Technology, Volume 149]*. Australian Computer Society Inc. 2014: pp. 17–22.

[62] C. Kwon, W. Liu, and I. Hwang: 'Security analysis for cyber-physical systems against stealthy deception attacks'. *2013 American control conference*. IEEE. 2013: pp. 3344–3349.

[63] Y. Kwon, H. K. Kim, Y. H. Lim, and J. I. Lim: 'A behavior-based intrusion detection technique for smart grid infrastructure'. *2015 IEEE Eindhoven PowerTech*. IEEE. 2015: pp. 1–6.

[64] H. Lahza, K. Radke, and E. Foo: 'Applying domain-specific knowledge to construct features for detecting distributed denial-of-service attacks on the GOOSE and MMS protocols'. *International Journal of Critical Infrastructure Protection* (2018), vol. 20: pp. 48–67.

[65] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson: 'On the self-similar nature of Ethernet traffic (extended version)'. *IEEE/ACM Transactions on networking* (1994), vol. 2(1): pp. 1–15.

[66] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke: 'Model-based security metrics using adversary view security evaluation (advise)'. *2011 Eighth International Conference on Quantitative Evaluation of SysTems*. IEEE. 2011: pp. 191–200.

[67] H. Lin, A. Slagell, C. Di Martino, Z. Kalbarczyk, and R. K. Iyer: 'Adapting bro into scada: building a specification-based intrusion detection system for the dnp3 protocol'. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*. 2013: pp. 1–4.

[68] G. Liobikiene and M. Butkus: 'The European Union possibilities to achieve targets of Europe 2020 and Paris agreement climate policy'. *Renewable Energy* (2017), vol. 106: pp. 298–309.

[69] S. C. Litos: *The Smart Grid: An Introduction*. 2008.

[70] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen: 'Cyber security and privacy issues in smart grids'. *IEEE Communications Surveys & Tutorials* (2012), vol. 14(4): pp. 981–997.

[71] E. Lloyd and D. Warren: 'The historically adjusted range and the historically rescaled adjusted range'. *Stochastic Hydrology and Hydraulics* (1988), vol. 2(3): pp. 175–188.

[72] G. Lorden: 'Procedures for reacting to a change in distribution'. *The Annals of Mathematical Statistics* (1971), vol.: pp. 1897–1908.

[73] B. Mandelbrot: 'Statistical methodology for nonperiodic cycles: from the covariance to R/S analysis'. *Annals of Economic and Social Measurement, Volume 1, Number 3*. NBER, 1972: pp. 259–290.

[74] T. Maynard and N. Beecroft: 'Business Blackout: The Insurance Implications of a Cyber Attack On the US Power Grid'. *Lloydâ€™s of London. Accessed March* (2015), vol. 15: p. 2019.

[75] G. Mesters, S. J. Koopman, and M. Ooms: 'Monte Carlo Maximum Likelihood Estimation for Generalized Long-Memory Time Series Models'. (2011), vol.

[76] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne: 'Evaluating computer intrusion detection systems: A survey of common practices'. *ACM Computing Surveys (CSUR)* (2015), vol. 48(1): pp. 1–41.

[77] B. Miller and D. Rowe: 'A survey SCADA of and critical infrastructure incidents'. *Proceedings of the 1st Annual conference on Research in information technology*. 2012: pp. 51–56.

[78] T. Morris, R. Vaughn, and Y. Dandass: 'A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems'. *2012 45th Hawaii International Conference on System Sciences*. IEEE. 2012: pp. 2338–2345.

[79] G. V. Moustakides: 'Optimal stopping times for detecting changes in distributions'. *the Annals of Statistics* (1986), vol. 14(4): pp. 1379–1387.

[80] H. Nguyen, T. Pongthawornkamol, and K. Nahrstedt: 'Alibi framework for identifying reactive jamming nodes in wireless LAN'. *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*. IEEE. 2011: pp. 1–6.

[81] J. Nivethan and M. Papa: 'Dynamic rule generation for SCADA intrusion detection'. *2016 IEEE Symposium on Technologies for Homeland Security (HST)*. IEEE. 2016: pp. 1–5.

[82] L. L. Ojeda, A. Y. Kibangou, and C. C. De Wit: 'Adaptive Kalman filtering for multi-step ahead traffic flow prediction'. *2013 American Control Conference*. IEEE. 2013: pp. 4724–4729.

[83] E. S. Page: 'Continuous inspection schemes'. *Biometrika* (1954), vol. 41(1/2): pp. 100–115.

[84] A. Pal, A. R. Jolfaei, and K. Kant: *A Fast Prekeying Based Integrity Protection for Smart Grid Communications*. 2020.

[85] W. Palma: *Long-memory time series: theory and methods*. Vol. 662. John Wiley & Sons, 2007.

[86] P. P. Parikh, T. S. Sidhu, and A. Shami: 'A comprehensive investigation of wireless LAN for IEC 61850–based smart distribution substation applications'. *IEEE Transactions on Industrial Informatics* (2012), vol. 9(3): pp. 1466–1476.

[87] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan: 'An intrusion detection system for IEC61850 automated substations'. *IEEE Transactions on Power Delivery* (2010), vol. 25(4): pp. 2376–2383.

[88] W. Ren, T. Yardley, and K. Nahrstedt: 'EDMAND: Edge-Based Multi-Level Anomaly Detection for SCADA Networks'. *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE. 2018: pp. 1–7.

[89] RISI: *The Repository of Industrial Security Incidents*. 2015.

[90] T. Schoen: *An explanation of the expectation maximization algorithm*. 2009.

[91] E. Al-Shaer and M. A. Rahman: 'Security and resiliency analytics for smart grids'. *Advances in Information Security* (2016), vol.

[92] W. Shang, L. Li, M. Wan, and P. Zeng: 'Industrial communication intrusion detection algorithm based on improved one-class SVM'. *2015 World Congress on Industrial Control Systems Security (WCICSS)*. IEEE. 2015: pp. 21–25.

[93] W. Shang, P. Zeng, M. Wan, L. Li, and P. An: 'Intrusion detection algorithm based on OCSVM in industrial control system'. *Security and Communication Networks* (2016), vol. 9(10): pp. 1040–1049.

[94] J. Slowik: *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack*. 2019.

[95] B. L. Smith, B. M. Williams, and R. K. Oswald: 'Comparison of parametric and nonparametric models for traffic flow forecasting'. *Transportation Research Part C: Emerging Technologies* (2002), vol. 10(4): pp. 303–321.

[96] T. Soderstrom and P. Stoica: *System identification*. Prentice-Hall, Inc., 1988.

[97] M. Strobel, N. Wiedermann, and C. Eckert: 'Novel weaknesses in IEC 62351 protected smart grid control systems'. *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. 2016: pp. 266–270.

[98] A. Tartakovsky, I. Nikiforov, and M. Basseville: *Sequential analysis: Hypothesis testing and changepoint detection*. CRC Press, 2014.

[99] A. Turner: *Tcpreplay*. 2003.

[100] T. S. Ustun, M. A. Aftab, I. Ali, and S. S. Hussain: 'A Novel Scheme for Performance Evaluation of an IEC 61850-Based Active Distribution System Substation'. *IEEE Access* (2019), vol. 7: pp. 123893–123902.

[101] W. Willinger, M. S. Taqqu, R. Sherman, and D. V. Wilson: 'Self-similarity through high-variability: statistical analysis of Ethernet LAN traffic at the source level'. *IEEE/ACM Transactions on networking* (1997), vol. 5(1): pp. 71–86.

[102] J. G. Wright and S. D. Wolthusen: 'Stealthy Injection Attacks Against IEC61850's GOOSE Messaging Service'. *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE. 2018: pp. 1–6.

[103] Q. Yang, W. Hao, L. Ge, W. Ruan, and F. Chi: 'FARIMA model-based communication traffic anomaly detection in intelligent electric power substations'. *IET Cyber-Physical Systems: Theory & Applications* (2019), vol. 4(1): pp. 22–29.

[104] Y. Yang, K. McLaughlin, L. Gao, S. Sezer, Y. Yuan, and Y. Gong: 'Intrusion detection system for IEC 61850 based smart substations'. *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE. 2016: pp. 1–5.

[105] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer: 'Multidimensional intrusion detection system for IEC 61850-based SCADA networks'. *IEEE Transactions on Power Delivery* (2016), vol. 32(2): pp. 1068–1078.

[106] Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, and S. Sezer: 'Multidimensional intrusion detection system for IEC 61850-based SCADA networks'. *IEEE Transactions on Power Delivery* (2016), vol. 32(2): pp. 1068–1078.

[107] H. Yoo and T. Shon: 'Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture'. *Future generation computer systems* (2016), vol. 61: pp. 128–136.

[108] M. Zeller: 'Myth or reality-Does the aurora vulnerability pose a risk to my generator?' *2011 64th Annual Conference for Protective Relay Engineers*. IEEE. 2011: pp. 130–136.

[109] Z. Zhang, X. Huang, B. Keune, Y. Cao, and Y. Li: 'Modeling and simulation of data flow for vlan-based communication in substations'. *IEEE Systems Journal* (2015), vol. 11(4): pp. 2467–2478.

[110] M. Zillgith: *libIEC61850 open source library for IEC 61850*. 2016.