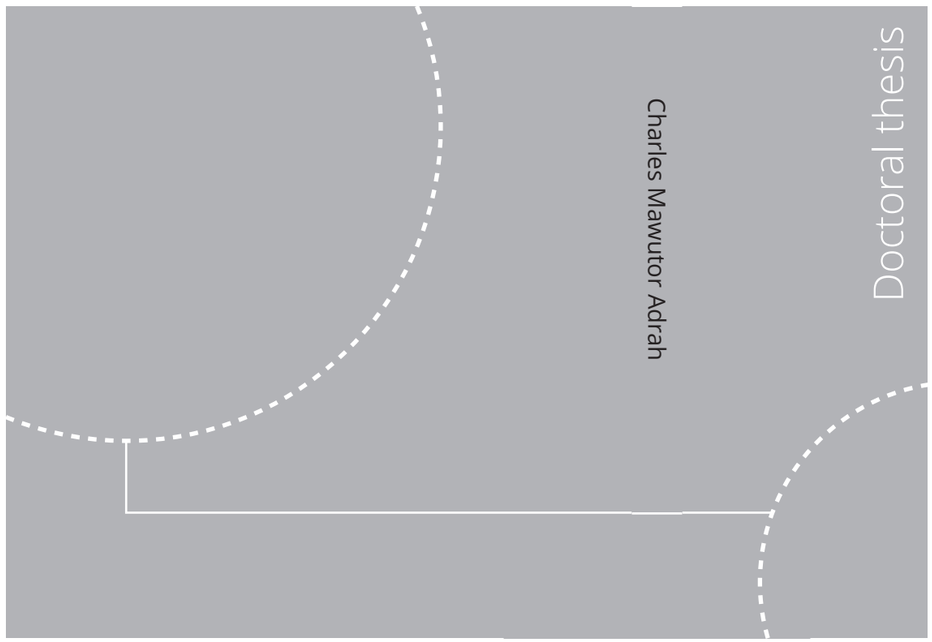
ISBN 978-82-326-4850-4 (printed ver.)
ISBN 978-82-326-4851-1 (electronic ver.)
ISSN 1503-8181




Doctoral theses at NTNU, 2020:251

Charles Mawutor Adrah

# Communication Networks for Protection Systems in Smart Transmission Grids

NTNU
Norwegian University of
Science and Technology

Doctoral theses at NTNU, 2020:251

**NTNU**
Norwegian University of
Science and Technology
Thesis for the degree of
Philosophiae Doctor
Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

NTNU
Norwegian University of
Science and Technology

Charles Mawutor Adrah

# Communication Networks for Protection Systems in Smart Transmission Grids

Thesis for the degree of Philosophiae Doctor

Trondheim, September 2020

Norwegian University of Science and Technology
Faculty of Information Technology
and Electrical Engineering
Department of Information Security and
Communication Technology

NTNU
Norwegian University of
Science and Technology

**NTNU**
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology



ISBN 978-82-326-4850-4 (printed ver.)
ISBN 978-82-326-4851-1 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2020:251

PRINTED IN NORWAY
NO - 1598

NORDIC SWAN ECOLABEL
Printed matter
2041 0731

Printed by Skipnes Kommunikasjon AS

# Abstract

The advances in Smart electric Transmission Grids (STG) have led to new developments in wide-area protection, control and state estimation applications. Protection systems in utility grids are particularly crucial in safeguarding personnel and equipment from damage. A robust, scalable and real-time Information and Communication Technology (ICT) network will be needed to support the operations in the STG. Within a substation, IEC 61850 standard provides protection and automation functions based on high-speed Ethernet Local Area Network (LAN). Guidelines have been provided to extend IEC 61850 beyond the substation to support Wide-Area Monitoring Protection and Control (WAMPAC) applications in STG. This will eventually replace the traditional IEEE c37.118 used for WAMPAC applications, which is limited by low data rates and slow responses for fast protection applications.

The ICT network plays an essential role in the delivery of timely information to the interconnected elements (i.e., substations and control center) in the STG. Therefore, the main objective set out in this thesis is to examine the role ICT networks play when protection systems are deployed in the STG. Specifically, the thesis investigates the interactions between protection applications and the ICT infrastructure, the ICT network approaches for routing IEC 61850 into wide-area, and the management of data traffic of protection applications in Ethernet networks to ensure predictable network services of delay, jitter, and packet loss.

The starting point of this thesis investigates the effects of interaction between protection algorithms and the ICT architectures. The approach taken to address this is to use tools to develop a framework that can capture the effects of ICT properties such as delays, jitter, and packet losses, and hence the impact on protection algorithms can be studied. The work developed a method based on a novel co-simulation framework to assess the reliability of protection algorithms taking into account ICT impairments. The results show that by using tools with real-time properties, protection applications can be modeled and the influence of ICT parameters investigated. Additionally, the method enables to achieve hardware-in-the-loop validation by connecting real-life protection devices to the test-set up. The co-simulation platform plays a significant role in the development and validation of protection schemes before actual deployment for the future smart transmission grids. As such, it is possible to identify challenges in the early stages of protection scheme testing before actual deployment in the grid.

The second topic addressed in the thesis is the support of ICT network architectures in routing IEC 61850 traffic in the STG. The work was done by evaluating ICT architectures based on the IEEE 802 family of standards. Two architectures identified and investigated were the application of Virtual LAN and IP multicast in wide-area networks. A VLAN-based communication architecture to route IEC 61850 traffic in wide-area between two substations was demonstrated, and the performance of a phasor estimation application was analyzed. Also, a method to construct network topologies from the power grid topology, meeting real-time con-

straints of IP multicast architectures, was proposed and analyzed. Additionally, a novel network design algorithm to meet real-time delay constraints of IP multicast networks was proposed. The network design algorithm finds additional links to be added to an existing topology such that the latency incurred on the multicast traffic are reduced. The findings show the feasibility of routing IEC 61850 protection traffic with these ICT architectures. The performance of the protection traffic needs to be analyzed carefully. The VLAN architecture for routing IEC 61850 traffic into wide-area can be suitable but should be at best restricted to the private utility ICT networks. IP multicast provides a scalable and dynamic network architecture for routing IEC 61850 traffic. However, its performance in meeting real-time constraints is influenced by the underlying ICT infrastructure and hence should be carefully considered in the design stage. The network design algorithm will aid a faster deployment of multicast architectures as the ICT infrastructure can quickly be redesigned to meet real-time constraints.

The third topic addressed is the determination of predictable network performance for tele-protection traffic in Ethernet networks. Ethernet was originally designed for best-effort services. Recently, there have been efforts to define Time Sensitive Networking (TSN) services that provide methods in scheduling, traffic shaping, reservation, redundancy, and synchronization to offer bounded network services. Specifically, this work investigates scheduling mechanisms of providing guaranteed QoS services (delay, jitter, and packet loss) for the tele-protection traffic running in a network with other STG traffic types such as management, video and file transfer. The thesis proposes a scheduling mechanism for the transport of tele-protection traffic in Ethernet networks to achieve fixed low delay, minimum jitter, and zero packet loss. As such, tele-protection traffic is offered a circuit-service class of hard QoS, while the other traffic in the network is offered of packet-service class with lower QoS. The results show that tele-protection traffic will require TSN mechanisms to guarantee predictable QoS when deployed in ICT networks. Since the results of unpredictable QoS consequently affect the protection schemes' reliability and protection breakdown.

# Preface

This dissertation is submitted in partial fulfillment of the requirements for the degree of Philosophiae Doctor (Ph.D.) at Norwegian University of Science and Technology (NTNU). The presented work was carried out at the Department of Information Security and Communication Technology (IIK) in the period from February 2016 - March 2020.

The work was supervised by Professor Poul E. Heegaard (NTNU) and Professor Øivind Kure at the University of Oslo (UiO), with Associate Professor David Palma (NTNU) as my co-supervisor. The work has been part of the ProSmart project, funded by the Norwegian Research council and collaboration with several industry partners.

## Acknowledgements

I would like to thank my supervisors Poul E. Heegaard and Øivind Kure for their guidance, support, and encouragement throughout my Ph.D. studies. I am also grateful to my co-supervisor, David Palma for providing invaluable insights towards my research work. I owe a special thanks to Adjunct Professor Steinar Bjørnstad (NTNU) for his collaboration, support and friendship.

I have been fortunate to be a part of the ProSmart project at NTNU which enabled me to collaborate and learn from colleagues in the Department of Electric Power Engineering at NTNU and Michigan Technical University (MTU), as well as industry partners. I am grateful for all the many useful discussions. I wish to also express my gratitude to my fellow Ph.D. colleagues and staff at the Department of Information Security and Communication Technology at NTNU.

Finally, my deepest appreciation goes to my parents and siblings for their unconditional love and support. Many thanks also to my friends Ben, Ray, Senam, Semere, and Yark for your encouragement. Last but not least, Sena, I appreciate all your support. To my son, Rune, I love you.

# Contents

# List of Tables

# List of Figures

# Acronyms

**ARP** Address Resolution Protocol

**CORE** Common Open Research Emulator

**CoS** Class of Service

**CRC** Cyclic Redundancy Check

**CSMA/CD** Carrier Sense Multiple Access with Collision Detection

**DetNet** Deterministic Networking

**ECN** Explicit Congestion Notification

**EoMPLS** Ethernet over MPLS

**FSQ** Fusion scheduling and queuing

**GOOSE** Generic Object Oriented Substation Event

**GPS** Global Positioning System

**GST** Guaranteed Service Transport

**HIL** Hardware-in-the-loop

**HMI** Human Machine Interface

**HOL** Head-Of-Line

**HSR** High Availability Seamless Redundancy

**I/O** Input/Output

**ICT** Information and Communication Technology

**IEC** International Electrotechnical Commission

**IED** Intelligent Electronic Device

**IEEE** Institute of Electrical and Electronics Engineers

**IETF** Internet Engieering Task Force

**IGMPv3** Internet Group Management Protocol version 3

**IHON** Integrated Hybrid Optical Networks

**IP** Internet Protocol

**ISM** Industrial, Scientific and Medical

**KDC** Key Distribution Center

**L2TP** Layer 2 Tunnelling Protocol

**LAN** Local Area Network

**MAC** Medium Access Control

**MMS** Manufacturing Message Specification

**MPLS** Multi Protocol Label Switching

**MTU** Maximum Transmission Unit

**MU** Merging Unit

**NDN** Named Data Networking

**ns-3** Network Simulator 3

**NTCF** Non-Time Critical Frame

**OPNET** Optimized Network Engineering Tools

**OSI** Open System Interconnect

**PDC** Phasor Data Concentrator

**PDH** Plesiochronous Digital Hierarchy

**PDV** Packet Delay Variation

**PIM-SSM** Protocol Independent Multicast-Source Specific Multicast

**PLC** Power Line Communication

**PMU** Phasor Measurement Unit

**PRP** Parallel Redundancy Protocol

**QoS** Quality of Service

**R-GOOSE** Routable GOOSE

**R-SV** Routable Sample Value

**RFC** Request for Comments

**ROMSC** Reduction Over Minimum Set Cover

**RTDS** Real Time Digital Simulator

**SAS** Substation Automation System

**SCADA** Supervisory Control and Data Acquisition

**SDH** Synchronous Digital Hierarchy

**SDN** Software-Defined Networking

**SM** Statistically Multiplexed

**SONET** Synchronous Optical Networking

**SPQ** Strict Priority scheduling and Queuing

**SS** Substation

**STG** Smart Transmission Grids

**SV** Sample Values

**TCF** Time Critical Frame

**TCP** Transport Control Protocol

**TR** Technical Report

**TSN** Time Sensitive Networking

**UDP** User Datagram Protocol

**VLAN** Virtual LAN

**WAMPAC** Wide-Area Measurement-based monitoring, Protection And Control

**WAN** Wide Area Network

# Part I

# Summary of the Thesis

# Chapter 1

# Introduction

The next-generation electric power system referred to as the Smart-Grid has the potential to change the power system sector dramatically. It incorporates advanced Information and Communication Technology (ICT) and pervasive computing to improve the control and management of electricity between suppliers, distributors, and consumers. Smart-Grid provides monitoring, protecting, and optimizing functions automatically to the operation of the interconnected elements covering generation, transmission, distribution, and to the consumers [YQST13].

The transmission element is the backbone used to deliver electricity from points of generation to the distribution. Smart Transmission Grids (STG) are expected to integrate modern features and functions, as well as to enable technologies into its major components of smart control centers, smart transmission networks, and smart substations [LQS+10].

In STG, power system protection or protective relaying is an essential operation. It acts as the brain which ensures the correct disconnection of faulty components in the power network. Protective relaying ensures that the life of personnel is protected, damage to equipment is minimized, and power system stability is maintained. Earlier technologies for relay protection were based on traditional hardwired analog and binary circuits between the primary substation equipment (i.e., electro-mechanical and numerical relays) and instrument transformers. However, there exists now modern generation digital relays called Intelligent Electronic Device (IED), which can communicate in real-time with a supporting communication network.

An international standard known as International Electrotechnical Commission (IEC) 61850 standard for substation automation has defined communication protocols for IEDs in utility substations [IEC13]. A substation is composed of IEDs, together with devices called Merging Units (MU), de-

ployed on an Ethernet-based Local Area Network (LAN). The LAN) is split into a process bus and station bus. The process bus involves communication between instrument transformers, MUs, and circuit breaker IEDs. The station bus involves communication between protection IEDs and towards the control room. The major benefits of the digitalized substation are reduced complexity of hardwired connections, reduced operating costs as well as the ability to implement new capabilities based on the advanced services and features of IEC 61850 [Mac06, IEC13].

The IEC 61850 standard enables protective relaying to be achieved inside the substation using two message types called Generic Object Oriented Substation Event (GOOSE) and Sample Values (SV). GOOSE messages communicate any type of information data (e.g., status or values) between IEDs while SV messages communicate digitized instantaneous values of current and voltages to the IEDs. Both GOOSE and SV messages are embedded into Ethernet data packets and implemented on a publisher-subscriber mechanism on multicast. IEC 61850 sets delay requirements for protective relaying within a substation between 3 to 4 msec.

The many advantages brought by IEC 61850 digitalized substations are expected to be utilized by the new protection systems between two substations as well as in wide-area monitoring, protection and control operations in the STG. IEC 61850 has proposed technical reports in 2010 to address communication between substations [IEC10b]. Also in 2012, a new technical report has defined mechanisms to use IEC 61850 to transmit synchrophasor information according to IEEE C37.118 [IEC12]. Therefore, the design and performance of the ICT architecture in the STG become crucial. This is because there is a risk to the protection system reliability being compromised if there is a failure in understanding the behavior of the IEDs and MUs operations, as well as of the supporting ICT infrastructure. However, the ICT architecture may be challenged by imperfect network conditions such as network delays, jitter, and packet losses, which therein affect the functions of the grid operations.

The network delays are influenced by different components such as the propagation, transmission, processing and queuing delays. The availability of high capacity media like fiber optic and advanced router capabilities tend to make propagation, transmission, and processing delays negligible. However, queuing delay, which is primarily caused by large volumes of network traffic, is the most affected.

An open issue is whether protection systems should have a physically separated ICT infrastructure or utilize a common infrastructure. Clearly, a separate infrastructure could offer advantages in terms of predictable per-

formance and reliability but at almost non-realizable investment costs. It would be beneficial from an economic sense to use the common ICT infrastructure for the different applications with some quality of service differentiation. Hence, this raises the question of investigating how the protection systems would be affected by the ICT infrastructure deployed in STG.

## 1.1 Motivation

In the smart transmission grid, protection systems are based on the IEC 61850 standard for substation automation. When deployed within a substation having a single Ethernet LAN, performance metrics such as delay, packet loss, and jitter are nearly constant with no variation between different source and destination IEDs and MUs. There is now a road map to extend the functions and features of IEC 61850 beyond a single substation. This will enable the entire STG to be operated with one seamless standardization.

The operations and applications deployed in an STG are effectively called Wide-Area Measurement-based monitoring, Protection And Control (WAMPAC). Thus, building a robust communication architecture that focuses on communication latency, cybersecurity threats, redundancy, and interoperability will need to be addressed [AAB+06]. In a wide-area setting, the communication network requirements will be heterogeneous for different STG applications, varying in both space and time. This is because different STG applications have different network requirements in terms of data payloads, sampling rates, latency, and reliability [KPR14]. Hence, there is a challenge in how the ICT system and architecture solutions will support grid applications.

The scope of issues addressed in this thesis is illustrated in Figure 1.1. The focus is on the transmission network of the power grid. Digital substations will be deployed in future transmission grids. These digital substations are Ethernet-based and, for WAMPAC applications, will be interconnected with optical fibers. Existing and new protection schemes will be one of the critical applications in the power system domain that the digitalized substations and ICT infrastructure should support. The thesis aims to address the effects in the interactions between protection applications and the ICT infrastructure, the ICT networks that enable routing of the data traffic of protection applications between two substations or among multiple substations, and the management of data traffic of protection applications in Ethernet networks to ensure a predictable quality of service.

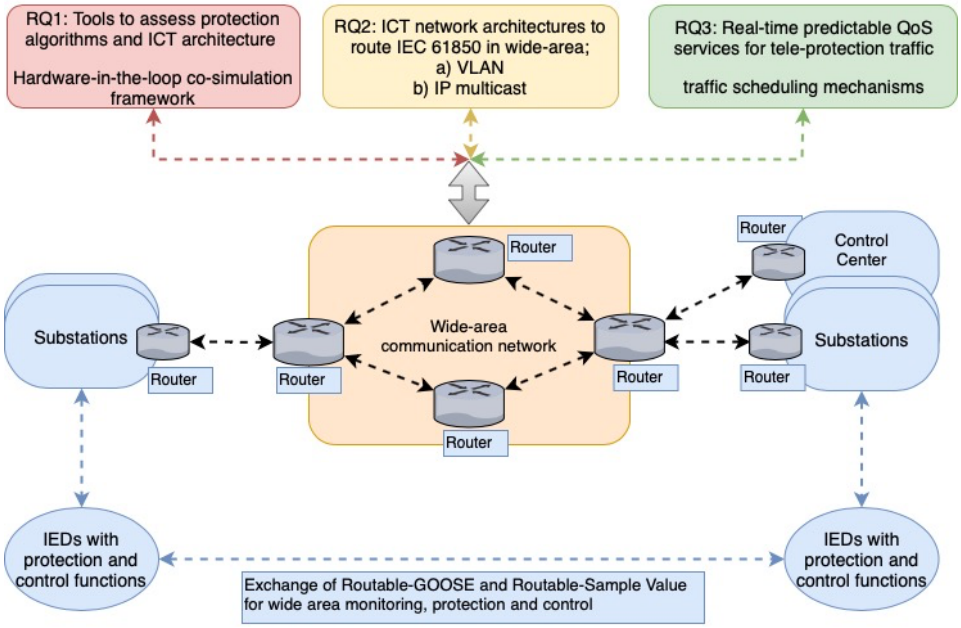



**Figure 1.1:** Overview of the role of communication networks in wide-area monitoring, protection and control in a smart transmission grid.

There is a need to investigate the interaction between protection algorithms and ICT infrastructure in the smart transmission grid. Understanding the impact ICT systems will have on the protection algorithms is crucial for how new protection schemes and algorithms will be designed.

Co-simulation is one technique that has been adopted to capture the power system and ICT dynamics in the smart grid. Embedded real-time tools able to model power systems behavior have become essential for operators. For example, these tools allow us to simulate and assess protection schemes conditions, and behavior.

Similarly, there is the need to utilize tools to simulate or emulate the real-time ICT system conditions to account for the smart grid behavior fully. For power protection applications, it is vital to test the real-time behavior of the protection algorithms installed in the relays or IEDs before actual deployment in the field.

The first motivation for this work is to utilize tools to develop a co-simulation framework involving the power and ICT systems. The aim is on modeling ICT system impairments that can affect the protection systems' reliability. The co-simulation framework is needed to analyze protection

algorithms, judge the impact of adding new algorithms, and in testing and validating new protection schemes.

Deploying protection systems and other applications in the STG will entail accompanying communication architectures. The ICT architecture should, for example, ensure the successful delivery of protection messages across the substations cooperating in a protection scheme within the real-time constraints acceptable to maintain the protection reliability. A transmission grid usually spans a few thousands of kilometers. For example, the total length of the transmission grid in Norway is about 11 000 km [aE]. Hence, the ICT architecture that connects the substations and the control center is through a Wide Area Network.

We assume an ICT architecture based on IETF and IEEE standards, which are typically used in the Internet or business network domains. These support a broad range of physical medium such as the optical fiber. In the case of STG, the underlying ICT architecture is expected to be based on the IEEE 802 family of standards. These are either deployed on top of a separate physical network or along the electrical power lines. The STG will most certainly be based on a standard architecture with Open System Interconnect (OSI) Layer 2 (Data Link) and Layer 3 (Internet Protocol) IP protocols. However, the high requirements in terms of latency for protection applications will require investigations to see suitability for deployment. The second motivation for this work is to investigate how ICT network architectures will support routing IEC 61850 traffic in WAMPAC.

Ethernet was originally designed for best-effort services. Without resource allocation, scheduling, and preemption, real-time services cannot be supported. Since IEC 61850 is based on Ethernet, deploying protection systems as part of the WAMPAC applications, in general, brings the challenge of achieving hard Quality of Service (QoS) for data traffic of protection applications.

The data traffic of protection applications, (also called tele-protection traffic), is critical traffic that should meet stringent latency requirements between 0.1 msec - 1 sec, minimum jitter and packet losses. For protection schemes, there is a challenge to guarantee that the lower limits of latency are not exceeded. Besides, the protection schemes that may need coordination from two or several substations could have their tele-protection traffic experiencing asymmetrical latencies. Asymmetrical latencies result from variable queuing delays incurred on alternative paths taken by the network traffic from the different substations (see chapter 2 for details). The consequences of unbounded delays, jitter, and packet losses could lead to the breakdown of an entire protection scheme.

There is a new kind of service gaining attention within Ethernet called the time-sensitive network (TSN) service [Fin18]. TSN offers time synchronization, priority, scheduling, preemption, slotted access, and resource reservation mechanisms. These mechanisms can be selectively used or combined to provide different degrees of real-time predictable network performance guarantees. Recently, IEEE has put together a task force to standardize TSN services called Time Sensitive Networking standards. The IEC 61850 standard has recommended the use of IEEE 802.1p priority scheduling as a mechanism to guaranteeing TSN services for intra-substation and WAMPAC applications. As such, there is a need to investigate mechanisms that provide predictable QoS services. The third motivation for this work focuses on investigating and evaluating methods to provide absolute QoS guarantees for protection traffic deployed in Ethernet.

In summary, the work in this thesis is motivated by the developments and challenges identified with IEC 61850, and the broader application of IEC 61850 in future STG protection systems and other applications. Consequently, the design and performance of the ICT networks deployed in the STG need to be carefully evaluated. Otherwise, the reliability of the protection systems may be affected, which can result in unmitigated consequences in the transmission grid.

## 1.2 Research Questions

The objective of this thesis is to study the role ICT networks have on protection systems deployed in the STG. This means understanding the challenges of ICT networks and services, in providing sufficient QoS for the new real-time protection systems based on IEC 61850, that will scale beyond the substation, i.e., WAMPAC applications.

The following research questions have been identified:

**RQ1** Which tools can be used to investigate the interaction between protection algorithms and ICT architectures?

**RQ2** How can existing ICT architectures and technologies be used for routing IEC 61850 into the wide-area network, meeting the real-time constraints of protection applications?

**RQ3** How can real-time QoS be guaranteed for protection traffic deployed in Ethernet networks?

**Table 1.1:** Studies performed based on the research questions and the resulting research papers.

| | Research Questions | Papers |
|---|---|---|
| RQ1 | Which tools can be used to investigate the interaction between protection algorithms and ICT architectures? | A, B |
| RQ2 | How can existing ICT architectures and technologies be used for routing IEC 61850 into the wide-area network, meeting the real-time constraints of protection applications? | C, D, E |
| RQ3 | How can real-time QoS be guaranteed for protection traffic deployed in Smart Transmission Grid Ethernet networks? | F, G |

## 1.3 Research Method

The research methodology adopted in this thesis follows the Design Science Research Methodology (DSRM) [PTRC08]. Design science involves a rigorous process to design artifacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate audiences [HMPR04]. DSRM results in a process model made up of six activities in a nominal sequence, shown here in Figure 1.2.

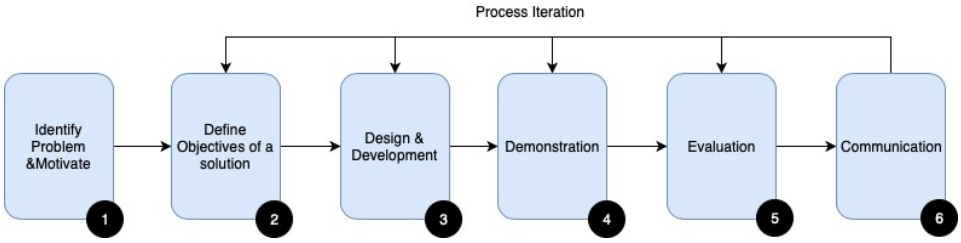



**Figure 1.2:** Process model of Design Science Research Methodology [PTRC08].

Having defined the overall objective of the thesis as the study of the impact ICT networks play on protection applications deployed in the Smart Transmission Grid, background research, and literature reviews were conducted to understand and identify problems within the research scope. Subsequently, the sub-objectives of the thesis were formulated. This led to three research questions being identified as enumerated in Section 1.2. Based on

these research questions, different activities in the design science methodology were employed to answer the research questions and hence satisfy the overall objective of the thesis. The resulting papers from the studies are summarized in Table 1.1.

A problem-centered approach was adopted to answer *RQ1*. The identified challenge was the need to study the interaction between protection applications and the effects of ICT network impairments. The motivation was that QoS properties of delay, jitter, and packet loss would influence protection application testing.

The defined objective was to develop a modeling framework with tools that can integrate power system models and communication models as a solution to test protection system reliability. The framework should use the new protocols in IEC 61850 substation automation, i.e., GOOSE and SV in modeling the protection applications. A significant challenge in the design and development process was to identify the pros and cons of tools that can enable this integration.

The artifact created was a test-bed that supports real-time modeling of the power systems and the supporting communication network, otherwise called co-simulation. The test-bed could be combined with real-life devices in the grid such as IEDs and MUs, thus forming what is called Hardware-in-the-loop (HIL) co-simulation, to test new protection schemes and algorithms.

The developed HIL co-simulation test-bed demonstrated the capability of combining a real-time simulator with a communication emulator, which was used to study the impact of ICT on protection applications. Case-based simulations studies were used to demonstrate the test-bed framework. The studies evaluated new protection schemes and investigated how they adapted to ICT network imperfections. From this, the protection reliability could be assessed. The modeling framework and the results from the case-studies were communicated through two publications (Papers A and B).

An objective-centered approach was used to answer *RQ2*. The objective was to investigate how established ICT architectures can be used to route IEC 61850 GOOSE/SV traffic into wide-area. The deployment of IEC 61850 substations are based on Ethernet. Hence, there was a need to investigate existing ICT architectures and technologies that can enable the delivery of protection systems traffic within the real-time constraints. In the design stage, two technologies, i.e., VLAN and IP multicast, were analyzed.

Firstly, using VLAN technology, a co-simulation method was developed to tunnel Sample Values across the WAN involving two substations. The method was demonstrated on the HIL co-simulation test-bed introduced

from RQ1. A case-base study was developed to analyze the performance of SV in state estimation in the grid. The results were presented in Paper C.

Secondly, IP multicast could potentially simplify the configuration of the IEDs involved in a protection scheme. The multicast topology will impact the delay incurred on the tele-protection traffic. Hence, there was a focus on a structural analysis of the multicast distribution trees. A method of designing a communication network topology from a STG was shown. The topology is designed to find the most cost-effective multicast trees, which consequently improve the real-time delivery of tele-protection traffic. Furthermore, a heuristic network design algorithm was developed, which could augment an ICT network topology via new link additions to meet real-time delivery of the protection traffic. The well-known IEEE-39 bus power grid network was used as a case-based study for the structural analysis. The algorithm was developed, and multicast groups evaluated using simulation. The results were communicated through publications in Papers D and E.

A problem-centered approach was used to answer *RQ3*. The challenge identified was how real-time QoS guarantees for the tele-protection traffic deployed in Ethernet networks could be supported. This was motivated by the fact that the tele-protection traffic needs to meet stringent requirements on latency, jitter, packet loss as well as synchronization. The artifact developed was the applicability of a scheduling mechanism called *Fusion* (FSQ), which is a contribution to TSN service, in transporting tele-protection traffic in Ethernet networks. A case-based scenario of a two-substation power network involved in a protection scheme was used. Analytical modeling was used to determine the worse-case delay values in the network when applying FSQ scheduling. The results were presented in Paper F.

Subsequently, a Fusion scheduling implementation, together with a case-based ICT network model of a power network, was developed in ns-3. The performance of FSQ, as compared to Strict Priority scheduling and Queuing, was investigated. The validation involved numerous stress testing of case-based scenarios of protection traffic combined with best-effort traffic. The results were presented in Paper G.

## 1.4 Thesis Structure

The thesis is structured in two parts. Part I contains five chapters. Chapter 2 presents a brief background knowledge of the thesis scope. Chapter 3 describes related work from literature studies, which gives input to the re-

search study and the thesis work carried out. The research contributions which answer the research questions are presented in Chapter 4. Chapter 5 presents the thesis concluding remarks and future research recommendations.

Part II includes all papers that present the contributions of this thesis. Also, the abstracts of the supplementary papers not included in the thesis are presented.

# Chapter 2

# Background

This chapter presents the underlying background information relevant to the thesis. Section 2.1 introduces the fundamental concepts in Smart Grid and how power system protection is affected within the smart grid context. Section 2.2 introduces IEC 61850 substation automation standardization and presents efforts towards its deployment in wide-area transmission operations. Section 2.3 presents the functional communication requirements, technologies, and architectures trends that have been deployed in transmission grids wide-area monitoring, protection, and control applications. Section 2.4 presents a summary of the evolution of Ethernet technology towards providing real-time services.

## 2.1 Smart Grid and the role of power system protection

Electric power has historically been generated and distributed in a hierarchical order consisting of three subsystems: generation, transmission, and distribution. In its basic operation, the power plants generate electricity, which is then stepped up to high voltages in the transmission systems for long-distance transmission in the grid. At the distribution substation, the high voltage electricity is stepped down to medium and low voltage, which are then delivered to end-users or consumers. Although the fundamental flow of electric power in the power grid has remained unchanged, there has been an evolution of the subsystems over time. This evolution has led to varying levels of automation added to the grid infrastructure, thereby making the electric grid "smart". Automation is achieved by using integrated communication networks and advanced devices. This integrated communications network covers the whole electric power grid, from generation to

distribution, as shown in Figure 2.1.

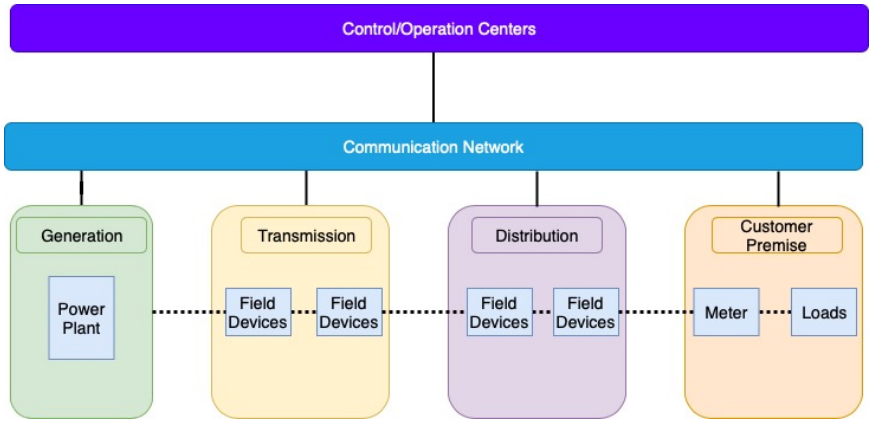



**Figure 2.1:** Smart Grid components.

In this thesis, the focus is on Smart Grid at transmission-level, also called Smart Transmission Grid. The transmission grid is the backbone that connects electricity from points of generation to the end consumers, hence its revolution needs to address varying challenges. One of the relevant features required in an STG is digitalization [LQS+10].

Digitalization is the fundamental feature needed to realize other smart features. The smart transmission grid will employ a unique, digital platform for fast and reliable sensing, measurement, communication, computation, control, protection, visualization, and maintenance of the entire transmission system. An adaptive communication network is required to achieve the smart features and characteristics in the STG. Such a communication network will allow open and standardized communication protocols to operate as real-time control based on fast and accurate information exchange in different platforms to improve system resilience.

In power systems, an essential operation is known as power systems protection or protective relaying. Protection refers to the part of the power system which operates to ensure the correct disconnection of faulty items to minimize the outages as much as possible. A basic flow of components in protection operations is shown in Figure 2.2.

Protective relaying has criteria such as selectivity, reliability, and speed. The purpose of these criteria is to make the related protection functions able to quickly isolate only the components under faults while leaving as much of the network as possible still in stable operation [And99].

In smart transmission grids, protection schemes require the exchange

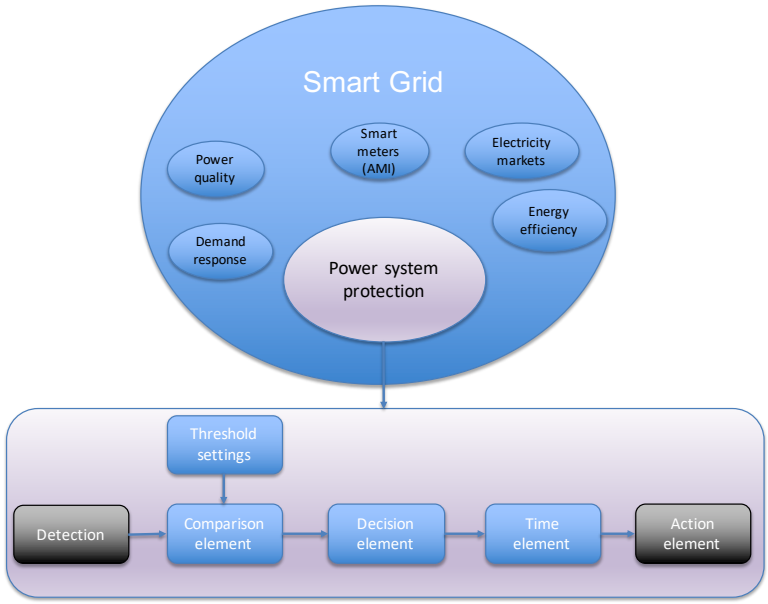



**Figure 2.2:** Protective relaying in Smart Grid.

of information between the transmission line terminals over a communication network or channel to provide fast fault clearing of the protected line. Presented next are examples of protection schemes that are deployed between substations [MFA09, IEC10b].

- Directional comparison, permissive tripping and blocking schemes; These schemes typically involve detecting a forward fault in an overreaching zone and sending a permissive signal or blocking signals to a remote end. These schemes usually require data signals of the size of a minimum of 1 bit up to 7 bits. The requirements for the propagation delay should be less than 5 msec.

- Current Differential Scheme: This involves relays measuring and exchanging current data of a protected line over the communications channel. It is the most sensitive to delay variations and asymmetry in the communication channel. It requires data to be synchronized between the substations to an accuracy of 0.1 msec, and for high-fault current sensitivity to an accuracy of 0.01 msec is required. Also, for fast tripping actions, the propagation delay should be small, 5 msec for extra high voltages to 10 msec for high voltages.

## 2.2 IEC 61850 in Smart Transmission Grid

### 2.2.1 IEC 61850 Overview

The smart transmission substation should have functions and capabilities including smart sensing and time-stamped measurements, high-speed LAN communication, autonomous control, adaptive protection, data management, and visualization, as well as monitoring and alarm [LQS+10]. The IEC 61850 standard [IEC10a, T.S05] is designed to offer high-speed Ethernet-based peer-to-peer communications for substation protection and automation. Some of its goals are to offer multi-vendor interoperability, reduce hardwired connections, and provide structured data modeling for the ease of interpretation [Mac06]. Figure 2.3 shows a digital substation with an overview of the logical allocation of functions and interfaces.

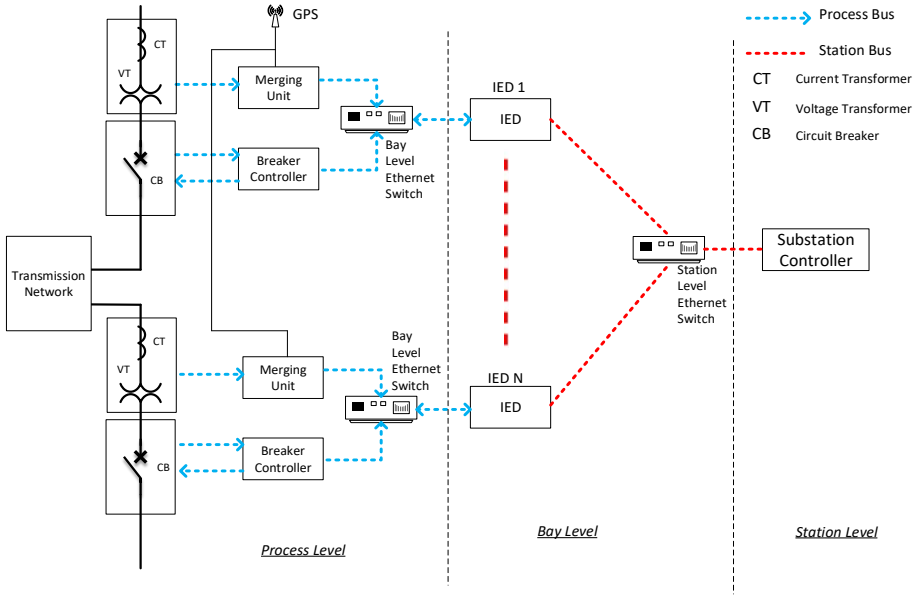



**Figure 2.3:** A digital substation architecture.

A typical Substation Automation System (SAS) is structured in three levels: station level, bay level, and process level. The process level gathers information from instrument transformer outputs, Merging Units (MU), and status information from breakers, which are connected to the primary power system components. The bay level includes auxiliary equipment, such

as protection and control IEDs, that receive information from the process level communicated over a LAN. The station-level, which is usually located in the control room, will include a Human Machine Interface (HMI) that provides an overview across the whole substation, and it is used for the local monitoring and engineering of the substation. In addition, there can be remote terminal units for interfacing with a Supervisory Control and Data Acquisition (SCADA) system and GPS receiver, which provides time synchronization for the correct time tagging of the events in the substation.

The SAS architecture is further classified into two logical communication buses that may share the same communication medium and infrastructure: process bus and station bus. The process level devices, together with bay level devices, form the process bus used for sharing measurements inside the substation. The bay level and station level devices form the station bus. The station bus provides high-level communication among the IEDs at the bay level and towards the control room. This communication enables substation protection, control, monitoring, and logging functions.

Both the station and process buses carry different types of traffic and therefore have different performance requirements. In scenarios where physical separation is not possible between the two buses, the logical separation should be ensured such that there is segregation of traffic to maintain the required performance and not overload the network [VRSG18]. This can be done using multicast filtering or Virtual LANs to segregate between the process bus and station bus traffic.

The IEC 61850 standard comprises of data models that are mapped over the protocol layers of the International Standards Open System Interconnect communication system model. This ensures the evolution of the substation communication model to the evolution of communication technology. There are three types of data models commonly used in the SAS; Manufacturing Message Specification (MMS), GOOSE, and SV.

- MMS defines a set of standard information exchanges between client-server type applications and includes general operational information for supervising and controlling the substation. MMS services are mostly confirmed services that send and receive an acknowledgment from the server or client. Hence, they are mapped on Transport Control Protocol (TCP)/IP frames. GOOSE and SV are the most important for substation protection services and applications and are mapped directly onto Ethernet data frames [AT06, ATG12].

- GOOSE messages are unidirectional and event-driven broadcasting messages. The GOOSE message exchanges are based on a multicast

publisher-subscriber mechanism. Messages are published by IEDs over the network that can be subscribed to by other IEDs in the process and station buses in the same network. The multicasting nature of GOOSE communication enables simultaneous delivery of the same message information to multiple IEDs in its peer group. GOOSE utilizes multicast with a built-in reliability mechanism. The reliability mechanism depends on fast and reliable re-transmission of arbitrary data sets from the publisher to the multiple subscribed peers. The re-transmission mechanism helps with managing the event-driven message transmission since the publisher does not wait for acknowledgments. Hence, GOOSE takes a pessimistic approach by assuming subscribers did not receive and re-transmit quickly no matter what. GOOSE messages are mapped directly on the link layer as Ethernet data packets to reduce overheard and support the time-critical protection applications.

- SV messages are configurable time-driven data-sets also transmitted with a multicast communication mechanism from one publisher to multiple subscribers. Its data-sets include 3-phase voltage and current measurements produced from the Merging Unit. The MU is an interface unit that accepts multiple analog current transformers or voltage transformers, generates and formats the SV messages for the 3-phase voltage and current measurements, and publishes the messages on the substation LAN. SV can be published at a sampling frequency varying from 80-256 samples/cycle for the power systems with 50 Hz or 60 Hz fundamental frequency. Unlike GOOSE, SV does not have a re-transmission cycle because, for a cycle, it has a different set of measurement information from the process level MU. Similar to GOOSE, SV measurement data is also mapped onto the link layer to support the time-critical protection functions in the substation.

### 2.2.2 IEC 61850 into Smart Transmission Grid applications

Prior to the IEC 61850 standardization, WAMPAC applications in transmission grids have relied on a synchronized measurement technology based on standardized IEEE c37.118 [IEE11] Phasor Measurement Units (PMUs). IEEE C37.118 PMU based WAMPAC applications have been researched and presented in literature, and in addition have seen active deployment in utility grids [TEM+05, TKC09, TVD+11, PT17]. These applications are deployed for monitoring, protection, and control as they can capture the entire system state [AAB+06, Pri06].

PMUs provide synchrophasor information such as voltage and current phasor, as well as frequency information, synchronized with high precision to a standard time reference provided by the Global Positioning System (GPS). Their operation is based on numerical measurement algorithms, which must be both computationally efficient and suitable for real-time applications, in particular for dynamic-response-type applications [TVD+11].

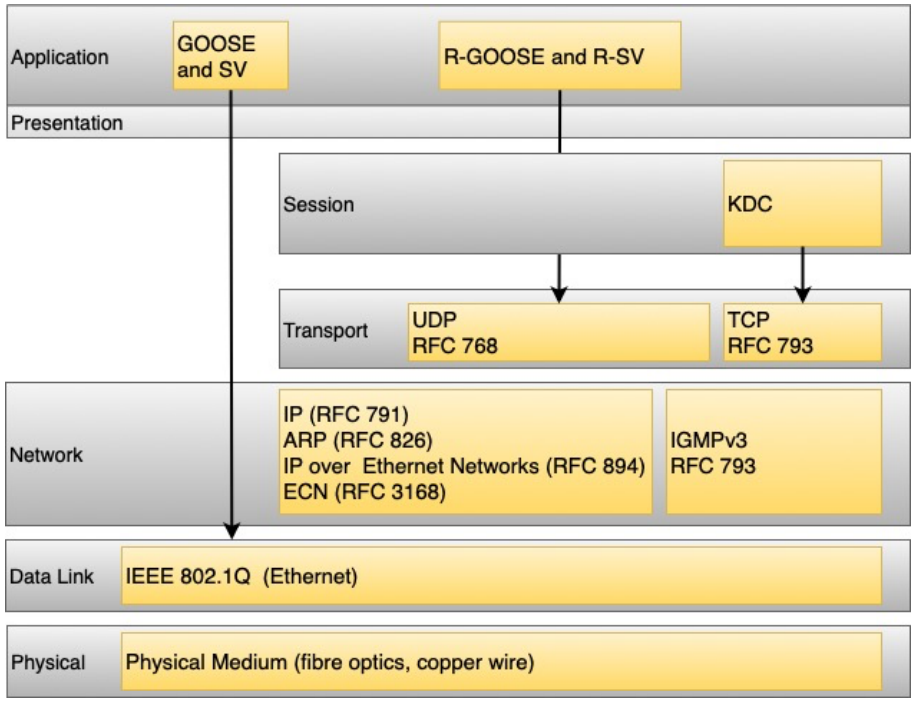



**Figure 2.4:** Communication stack from IEC TR 61850-90-5 [IEC12].

GOOSE and SV were initially designed for operation within the substation LAN. However, the benefits that they provide have encouraged the need to define new standards to incorporate them into WAMPAC applications. IEC technical reports (TR) in part 90 series offer guidelines on how to establish inter-substation communications between LANs, as well as use IEC 61850 to transmit synchrophasor information in accordance with IEEE c37.118.

The IEC TR 61850-90-5:2012 [IEC12] specifies how GOOSE and SV can be extended from LAN to WAN. The standard suggests tunneling and multicast over IP networks as mechanisms to achieve this. The terms Routable GOOSE (R-GOOSE) and Routable Sample Value (R-SV) have been introduced in some literature [Apo17, KCJ17] to differentiate between GOOSE

and SV application within the substation and outside the substation. Therefore R-GOOSE and R-SV messages refer to the application of GOOSE and SV beyond a substation LAN, which will usually be routed over layer-3 routers with UDP/IP headers. Figure 2.4 shows the mapping of different substation data traffic to the communication services provided, in addition to the application profiles and transport profiles defined for the standard specified in IEC/TR 61850-90-5.

## 2.3 Communication architectures, requirements, and technology trends in WAMPAC

### 2.3.1 Communication architectures for WAMPAC

In order to meet the stringent latency requirements of WAMPAC applications, the communication and power infrastructures have to collaborate strongly. The formats presently available to send PMU data for WAMPAC applications are:

- IEC 61850 SV
- IEEE c37.118–2005
- and IEC 61850–90-5 R-SV

SVs are mapped directly on Ethernet and typically remain within the confines of the LAN. The use of Ethernet framing without IP constricts the scope for the transfer of data geographically. SVs can be implemented across a WAN without requiring a Layer 3 header. This is achieved utilizing Ethernet VLAN framed messages. C37.118–2005 and R-SV specify the use of IP protocol transport, either using unicast or IP multicast, respectively, within the standards documentation [MTD12].

Traditionally, PMU measurement messages have been transmitted using IP/UDP unicast to pre-defined receivers which are typically PDCs or Super-PDCs (i.e., integrated PDC functionality and service applications within a single unit). Usually, a PDC receives C37.118 PMU data from one or several PMUs and aggregates them into a combined output stream before delivering it to the control center.

In literature, this approach of delivering PMU measurements to the control center is referred to as a centralized architecture [HBB05, Bos10,

BCZ+13]. It is a logical connection, where the substations are interconnected to the control center through a physical network that can have a meshed structure similar to the transmission grid. A centralized architecture is simple but has scalability challenges with applications that require high-speed control actions [WYB15]. Besides, without fault-tolerant mechanisms, the control center becomes a single point of failure for the WAMPAC system.

In some large transmission networks, PDCs can output their data stream to another PDC or Super-PDCs, which is known as PDC stacking. PDC stacking occurs due to the high amount of measurements collected in the numerous substations that are too many to centralize in a control center. In such scenarios, the PMU messages can traverse several interconnected PDCs before eventually arriving at the control center.

Along the paths from PMUs to the control center, intermediate sections (i.e., substations) can take some local actions based on the evaluation of their PMU measurements and comparison to other measurements received from other parts of the utility network. This type of architecture is referred to in the literature as a decentralized architecture [HBB05, Bos10, WYB15]. A decentralized architecture has nodes with logical functions acting as PDCs or middle-wares, which are added between the substations and the control center. These PDCs or middle-wares are placed closer to the substations in their geographic areas. They initiate local control and decision actions and forward only some measurements to the control center.

The requirements for having a decentralized with distributed data architecture in future WAMPAC applications have led to proposals of utilizing an IP Multicast subscription-based model for the transport of PMU measurement data packets [MTD12]. This new network architecture moves PDCs or middle-ware from the network path and allows them to be placed where they are most necessary and useful. The network routing elements are responsible for handling the subscription requests from potential PMU data receivers as well as the actual optimal path computation, optimization, and rerouting in the case of failures.

PDCs remain out of the network path and at the edge of the network. This allows specialized data forwarding elements such as IP routers to more efficiently forward PMU signaling data to consumers with improved performance, reliability, usability, and scalability. The use of IP multicast and R-GOOSE / R-SV is recommended for the future WAMPAC applications since this eliminates the need for PDC stacking. This architecture will also have a significant impact on how the network performs, reduce the complexity of management of the network, and help it to scale as the consumption

of PMU data in the network grows.

### 2.3.2 Communication requirements for WAMPAC

Table 2.1 gives an overview of the latency requirements for some of the WAMPAC applications. One of the disadvantages of IEEE C37.118 PMU is the low sampling rates of the measurements, i.e., between 30 to 60 samples per cycle. On the other hand, the introduction IEC 61850 having PMU functionality will enable higher sampling rates of between 80 to 256 samples per cycle. Hence, transient based wide-area protection applications can be achieved [KB11, IEC12].

**Table 2.1:** Overview of latency requirements for WAMPAC operations [KB12].

| Main Application | Types | Latency Requirements |
|---|---|---|
| Protection | Small Signal Stability, Transient Angle Stability, Short Circuit Faults, Unit Protection - Line, Transformer, Generator, Busbar | 0.1 msec - 1 sec |
| Stability and Control | Long-Term Voltage Stability, Cascading Outages, SVC/STATCOM Control | 1 msec - 1 sec |
| Monitoring | SCADA/EMS/DMS, Economic Load Dispatch/ Optimal Power Flow/ Operation Algorithms | 10 sec - 100 sec |

WAMPAC applications will be deployed in a wide area spanning several distances and have high requirements on latency ranging from 0.1 msec to 100 sec. For these applications to be realized, a fast communication infrastructure that can handle a vast amount of data exchange and can provide near real-time data delivery will be required. Latency and bandwidth are critical issues for such communication infrastructures to be used.

### 2.3.3 Communication technologies for WAMPAC

Communications-based transmission line wide area protection schemes have been in service for well over half a century. The most popular communication technologies used are power line communication (PLC), microwave, and fiber optics.

PLC enabled the transmission of data and electricity simultaneously over existing power lines as an alternative to constructing dedicated communic-

ations infrastructure. Utility-owned microwave links have also been used in transmission grids as a cost-effective and reliable communications solution for wide-area protection systems [AAB+06, GL06].

Optical fiber-based networks are seen as the long term solution for the evolving needs of the future STG [AKV10]. Optical fiber offers high bandwidth capacity, reliable, and noise-resistant communication. It is easier for the utilities to install optical fibers as they have the right of way on their transmission networks using existing transmission poles and underground conduits. Hence, the cost of installing optical fiber cables for the STG will be inexpensive for a utility company [MFA09]. In addition, the digital substation is expected to replace the copper wires with fiber-optics with both the station and process buses having fiber-connectivity. Optical fiber has dielectric properties that give immunity to electromagnetic interference and hence provides significant advantages over copper-based communication systems.

## 2.4 Evolution of Ethernet towards industrial applications

The IEEE Std 802.3 Ethernet standard was first published in 1985, specifying a half-duplex Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Medium Access Control (MAC) protocol operating at 10 Mbps data rate. It was operational on a coaxial cable medium and supported a bus topology between the attached end stations [LDD+13]. Since then, Ethernet has evolved to support new media types such as twisted-pair and fiber optic. Development support for Ethernet data rates also increased throughout the period to 100 Mbps Fast Ethernet, and most recently, Gigabit Ethernet adding operation up to 40 Gbps and 100 Gbps.

Initially, the conventional Ethernet had passive devices called hubs that repeated whatever was received from their input port to all output ports. This created collisions in the network with unbounded delays. Conventional Ethernet was later replaced by switched Ethernet, where each station communicates with a switch that could identify destination ports and relay traffic to them only. This led to a significant reduction in network delays since collisions are only possible if station and switch attempt to communicate with each other at the same time [LL02]. Furthermore, a full-duplex mode was introduced in modern Ethernet where the station and switch can simultaneously send and receive. Hence, when using a switch, there are no collisions. Even that, Ethernet delivers a class of service called *best-effort*, where there is no guarantee that the data is delivered or that delivery meets

any QoS. IEEE 802.3 has defined a standardized frame, which is a unit of data that is ready to be sent on the network medium. The Ethernet frame contains the MAC address of the destination and source devices, along with the data received from upper OSI layers, and the cyclic redundancy check (CRC), which is a mathematical computation that helps detect errors.

### 2.4.1 Guaranteeing real-time services in Ethernet

The IEEE 802.3 family of standards has been extended into new markets and to address new application fields in industrial settings. Examples of such industrial application fields include such as augmented reality, remote motion control, autonomous driving, audio, and video production, electrical transmission substation automation, and tele-protection. However, for the industrial application traffic, they are unable to use best-effort services due to the requirements to guarantee QoS in terms of bounds for end-to-end latency, variation in latency, and packet loss. These requirements are defined as a new class of service in Ethernet called *time-sensitive network* service [Fin18]. This service class offers network services such as bandwidth limitation and reservation, buffering, preemption, and scheduling resources for the exclusive use of time-sensitive applications. It aims to provide services that guarantee packet transport with bounded latency, low packet delay variation, and low packet loss [FBG18].

Time Sensitive Networking standards have recently been amended under the IEEE 802.1 standards to offer network services to time-sensitive applications. The standards are formalized with several manufactures having incorporated them into their products. TSN standards can be grouped into three categories, namely:

- scheduling and traffic shaping
- path control and reservation and redundancy
- time synchronization

Even though each of the categories can operate self sufficiently, it is when only all three are used in a concerted way that a complete deterministic real-time solution is achieved. By reserving resources for critical traffic, and applying various queuing and shaping techniques, TSN achieves zero congestion loss for critical data traffic. This also allows TSN to guarantee a worst-case end-to-end latency for critical data. TSN mechanisms also provide ultra-reliability for data traffic via a data packet level reliability

mechanism as well as protection against bandwidth violation, malfunctioning, malicious attacks, etc. Besides, TSN includes reliable time synchronization, a profile of IEEE 1588, which provides the basis for many other TSN functions. Table 2.2 shows some of the TSN enhancements published under the IEEE 802.1 Working Group.

**Table 2.2:** IEEE TSN Standards

| **Categories** | **IEEE Standard** | **Scope** |
|---|---|---|
| Scheduling and traffic shaping | 802.1Q,<br>802.1Qbu,<br>802.1Qbv,<br>802.1Qcr,<br>802.1Qav | Strict priority scheduler,<br>Frame-preemption,<br>Time aware shaper,<br>Asynchronous traffic shaper,<br>Credit-based scheduler |
| Path control and reservation, and redundancy | 802.1Qca<br><br><br>802.1cb | Shortest path control and reservation<br><br>Frame replication and elimination |
| Time synchronization | 802.1as | PTP profile for clock synchronization |

Concerning scheduling and traffic shaping, two IEEE TSN mechanisms that extend the data plane functionality of bridges to guarantee very low latency and jitter values are IEEE 802.1Qbu frame preemption and IEEE 802.1Qbv enhancements for scheduled traffic [SMM18]. Both queuing mechanisms can be used to control packet transmission at each output port to achieve the bounded QoS.

In the IEEE 802.1Qbu [IEE16a] preemption queuing mechanism, the transmission of a Non-Time Critical Frame (NTCF) can be interrupted by one or more express or Time Critical Frames (TCFs), and then the interrupted NTCF can continue transmission. The system resumes processing the next NTCF after the TCF is processed if there is no more TCF in the queue. With this mechanism, TCFs are processed in a minimum wait equivalent to the Maximum Transmission Unit (MTU) in the network upon arrival. Hence, they experience a smaller delay and jitter as possible under system generating capacity at light load [JLC13].

The IEEE 802.1Qbv [IEE16b] Enhancements for Scheduled Traffic adds new capabilities of time-based gates to the output of the eight priority queues, which were initially defined in IEEE 802.1p and merged into 802.1Q. The

time-based gates are controlled by a rotating schedule called the gate control list which permits or deny the queues to present data for transmission selection. A timed gate can be in an open or closed state at a given time. When the gate opens, frames from the respective queue are forwarded for transmission in first-in-first-out order. If two gates are opened at the same time, a priority selection mechanism enforces that the higher priority frame is selected for transmission delaying the other lower priority traffic. IEEE 802.1Qbv requires an appropriate synchronization mechanism.

In order to support Layer 3 connectivity, there is an IETF Deterministic Networking (DetNet) working group established to focus on deterministic data paths. Their work will operate over Layer 2 bridges, Layer 3 routers, and MPLS label switches where the deterministic paths can provide bounds on latency, packet loss, jitter, and high reliability [FTVF18]. IETF DetNet working group collaborates with IEEE 802.1 TSN task group, which is responsible for Layer 2 operations, to define a common architecture for both Layer 2 and Layer 3. The key goal of the IETF DetNet work is to utilize the common themes of congestion control and traffic scheduling to offer bounded latency to time-sensitive applications with these requirements.

### 2.4.2 TSN services in smart transmission grid

There have been proposals of how IEEE TSN standards could be used in the STG and the use-case applications that can be supported [SGF+19]. IEC 61850 standards have recommended IEEE 802.1Q priority scheduling and IEEE 802.1as PTP time synchronization. IEC 61850 standard has adopted ISO/IEC 62439-3 Parallel Redundancy Protocol (PRP) and High Availability Seamless Redundancy (HSR) to offer redundancy solutions in substation automation.

The operation of IEEE 802.1cb is similar to PRP / HSR, where messages are replicated in parallel disjoint paths in the network. However, interoperability between IEEE 802.1cb and PRP/HSR remains a challenge to be addressed if there could be an adoption of IEEE 802.1cb in substation automation. Two STG use-case applications where TSN could be used are within the substation where mission-critical protection functions such as tripping, interlocking, or sending permissive or blocking signals in the station and process buses. Also, tele-protection between remote substations will require TSN services where reliable and predictable low end-to-end latency is required.

# Chapter 3

# Related Work

In the included papers for this thesis, there is a section discussing related works for the research objectives defined. In this chapter, the main approaches and related work on the research questions (RQ1, RQ2, and RQ3) posited in the thesis are reviewed in sections 3.1, 3.2, and 3.3. It is shown how the thesis and its contributions relate to other works in literature.

## 3.1 Tools used to investigate the interaction between protection algorithms and ICT architecture

The defined objective is to utilize tools that enable assessing relay protection schemes and algorithms, taking into account the influence of ICT. Hence, there is a need to analyze the power system and ICT networks in a joint and integrated approach. Among the many integrated simulation approaches, this thesis focuses on real-time Hardware-in-the-loop (HIL) co-simulation. The real-time enables protection algorithms to be rapidly deployed and tested with real field devices such as the IEDs and MUs.

The use of co-simulation to simulate the mutual influences of ICT and power systems, and therefore the behavior of intelligent power systems have become significant [PvdML+17, LAH11]. Developing a comprehensive simulation by constructing a new simulator that supports the simulation of both power system dynamics and communication network events is time-consuming and expensive [LFS+14]. Co-simulation enables the evaluation of the smart transmission grid using separate dedicated power and ICT simulators to model each subsystem.

The integration of the co-simulation tools brings its sets of challenges,

since the power system simulators are usually time-driven, while communication network simulators are event-driven. This makes the time scales or synchronization and how data is exchanged between the combined power and ICT tools the critical challenges in selecting the type of co-simulation platform to use for a smart grid use case.

Weilin et al. [LFS+14] explain that the decision about the type of co-simulation platform to select is influenced by whether time-domain power system simulation is required and if there is a need for real-time simulation, which is necessary in case of testing real hardware. For example, when studying applications that involve loose real-time guarantees and long time scales, such as advanced metering infrastructure reading, it would be possible to choose the interfacing and synchronization methods for co-simulation platforms that do not have strong coupling for real-time guarantees.

However, when studying applications that involve strict real-time guarantees and short time scales, such as PMU-based monitoring and protection applications, it would require real-time co-simulation techniques based on powerful real-time simulators. Real-time simulations compute the model time as fast as a wall clock to achieve real-time simulation. Hence combining the power system and communication system will give that advantage in terms of synchronization of the systems since both the power and communication network models are running at the same rate as a wall clock [GHM+13].

**Table 3.1:** Real-time simulators used for modelling power systems [PvdML+17].

| **Real-time Simulator** | **Communication Protocols** | **Software Supported** | **Interfacing and I/O** |
|---|---|---|---|
| RTDS from RTDS Technologies Inc. | IEC 61850, TCP/IP, IEEE C37.118 PMU, DNP3 | RSCAD | Optical fiber, Gigabit Ethernet, analog and digital I/O |
| eMegasim from OPAL-RT Technologies Inc. | IEC 61850, IEEE C37.118, DNP3 | Simulink, C/C++, MATLAB | Gigabit Ethernet, FPGA-based analog and digital I/O |
| HYPERSIM from OPAL-RT Technologies Inc. | IEC 61850 | Hypersim Software Suite | Gigabit Ethernet, Standard PCIe interface |
| Typhoon HIL from Typhoon HIL Inc. | IEEE 184C, Ethernet RJ45 | Typhoon Software Suite | FPGA-based analog and digital I/Os |

Real-time simulations can be made in offline mode or HIL mode. In offline mode, the entire model of the system under analysis is simulated on a dedicated platform with some simulation software that can ensure the fulfill-

ment of real-time constraints. In HIL mode, part of the model is replaced by physical components such as IEDs or MUs. HIL simulation has been used in the power system field for relay testing in protection applications, and it has been used in the design, study, and testing of relay coordination and for distance relay protection [MKW+92, PvdML+17].

Real-time co-simulation also serves as a platform to study the mutual impact of coupling power systems and ICT infrastructure in an intelligent power system framework. Hence, a real-time simulation platform allows multiple users to be connected to the real-time simulator concurrently to perform collaborative simulation, for which distributed control and HIL operation can be easily realized [GHM+13, PvdML+17]. Table 3.1 shows the different real-time simulators used for power engineering applications in terms of the interfacing methods used, the type of hardware used, and the communication protocols supported. The main advantage of these real-time simulators is that they have libraries with application-specific models that are accepted by the industry.

The ICT simulators to be used should have real-time properties to support the co-simulation. They should be able to run in real-world clock time such that real devices and other network equipment can be connected to interact with it. As such, this provides the fidelity of running live applications. In Table 3.2 a selection of works based on real-time co-simulation frameworks in smart grids is presented.

**Table 3.2:** A selection of some works on real-time co-simulation.

| **Author Reference** | **Real-time Simulator** | **Communication Simulator** |
|---|---|---|
| [VBLS15] | RTDS | ns-3 [HRFR06] |
| [CBPGK14] | RTDS | OPNET |
| [VSH16] | RTDS | CORE[ADHK08] |
| [BCZ+13] | OPAL-RT | OPNET |
| [GHM+13] | OPAL-RT | OPNET |

The works done by the authors in [VBLS15], [CBPGK14] and [VSH16] used Real Time Digital Simulator (RTDS) as the real-time simulator, while using Network Simulator 3 (ns-3), Optimized Network Engineering Tools (OPNET) and Common Open Research Emulator (CORE) respectively to simulate or emulate the communication systems. For these works, the co-simulation test-beds were applied in wide-area monitoring and control applications such as voltage stability monitoring algorithms, studying the impact of cyber attacks on system transient stability, and the impact of cyber events on micro-grids.

ns-3 is a discrete-event network simulator which does not readily support real-time simulations. It is challenging to synchronize with the real-world clock, real-time simulators, and ns-3. Usually, there needs to be a coordinator that is responsible for exchanging information between the simulators. CORE is a tool used for emulating networks on one or more machines and can support real-time connections to physical systems. However, it also requires a TCP/IP interface, implemented in Python, to connect the two modeling tools (i.e., RTDS and CORE).

In [BCZ+13] and [GHM+13], a co-simulation platform using OPAL-RT as the real-time simulator and OPNET to simulate the communication system, were developed to study wide-area monitoring and control system analysis and development. The platforms enabled to assess the impact of supporting ICT systems on PMU-based applications.

OPAL-RT supports software-based synchronized PMU (SoftPMU) designed and developed to be run in the OPAL-RT simulator. SoftPMU is a virtualized device that packs the raw measurement data according to C37.118.2-2011 standard and sends them to communication networks emulator over TCP or UDP. OPNET supports a real-time simulation gateway called system-in-the-loop, which makes it possible to connect the simulation model to live network hardware and provides the ability to exchange packets with the OPAL-RT via an Ethernet link while the simulation is running in real-time.

Even though OPNET can operate in real-time mode, it requires complex modeling. Besides, there are limitations in modifying ready-made models, hence not very scalable. Also, there is limited flexibility to vary ICT network parameters at run time. The OPNET tool is also expensive, which limits the tool's extensive usage. The framework implemented by the authors in [BCZ+13] is shown in Figure 3.1. The components in the co-simulation test-bed platform show the corresponding data in the power system model from OPAL-RT being sent to the external computer running OPNET through physical Ethernet links.

The communication requirements for these power system applications reviewed with the test-beds mentioned above were slow responding. Protection algorithms and relay protection schemes were not tested on these real-time co-simulation platforms. Also, IEC61850 GOOSE and SV were not exploited with these test-beds, primarily because they are not routable and not implemented in the client-server architecture.

In assessing the interaction between protection applications and the ICT architecture, there is a need to design a framework capable of incorporating the physical protection devices such as IEDs and MUs within the control

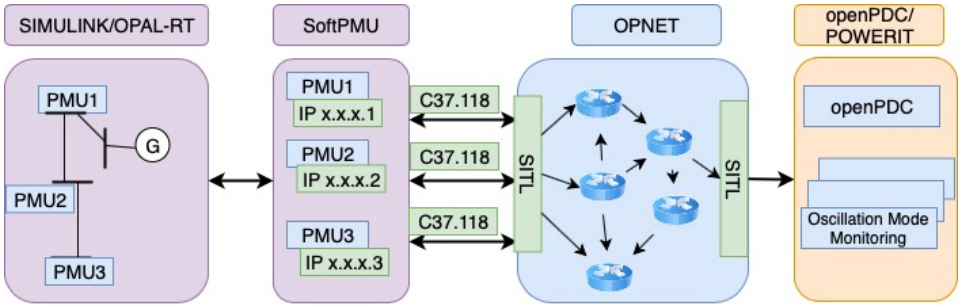



**Figure 3.1:** An OPAL-RT and OPNET test-bed [BCZ+13]

loop of real-time co-simulation platforms. This framework should focus on the new IEC 61850 protocols GOOSE and SV for protection system applications. Hence the supporting communication modeling tool should have the flexibility to experiment with these new protocols. Also, the goal of the communication modeling tool should support modeling the associated communication architecture and properties for the transmission grid in both inter-substation protection scenarios and wide-area grid operations. The tool should also support running real applications and be connected in real-time to physical networks.

## 3.2 ICT architectures and technologies for routing IEC 61850 R-GOOSE/R-SV into wide-area network

The benefits of Ethernet-based transmission digital substation LANs have been well documented in the literature. However, what is less known are the methods and devices necessary for interconnecting the individual substation LANs into a reliable and secure utility-wide network capable of satisfying different needs presented by SCADA, engineering/maintenance access and Wide-Area Measurement-based monitoring, Protection And Control applications [SJB02, SM06]. Two networking methods that have been suggested in the literature for interconnecting substations Local Area Networks and routing R-GOOSE/R-SV are Virtual LAN and Internet Protocol.

### 3.2.1 Interconnecting substation LANs using Virtual Local Area Networking

Virtual Local Area Networking and Class of Service (CoS) are essential technologies for segregating and prioritizing Ethernet traffic as networks

grow in size, complexity, and traffic diversity. A VLAN is a subnetwork that can group collections of devices on a separate Ethernet network that shares physical cabling and equipment infrastructure with other VLANs. VLANs create multiple logical LANs that selectively include various specific paths or parts of the full local and wide area networking arrangement [WHU12].

Each VLAN on a network has a separate broadcast domain, meaning that Ethernet frames from one VLAN will not be transmitted onto another VLAN. The IEEE 802.1Q [IEE18] standard defines a 4-byte extension to the Ethernet frame header that allows traffic from one VLAN to be distinguished from anotherVLAN as shown in Figure 3.2. The VLAN Identifier (VID) is a 12-bit field that allows 4094 different VLANs to exist on a single LAN. Also there includes a Priority flag (PCP) for quality of service differentiation.

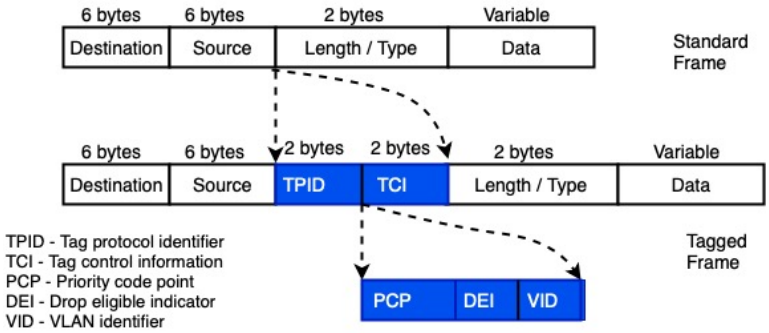



**Figure 3.2:** A tagged Ethernet frame structure [IEE18]

VLANs can be port-based or tag-based. A port-based VLAN assigns a specific port or group of ports to belong to a VLAN. When using tag-based VLANs, a tag called a VLAN identifier is sent as part of the message. This tag allows the message to move across multiple Ethernet switches whose ports are part of the same tagged VLAN. Tagged VLANs and priority flag are used within IEC61850 GOOSE and SV messaging. Depending on the Ethernet switches used, up to 32 VLANs can be defined per Ethernet network [WA11].

There have been extensions to IEEE 802.1Q, known as VLAN stacking or QinQ. VLAN stacking enables multiple VLAN tags to be inserted into a single frame. This gives capabilities in managing metro Ethernet network topologies. IEEE 802.1ad [IEE06] VLAN stacking limits to two tags where a 4-byte tag is added to the original VLAN tag. Internet service providers can identify and segregate traffic from different customers using this outer VLAN tag. Hence all traffic from one customer, which could have multiple inner VLAN tags, is placed into a single outer VLAN tag to simplify management

across the network.

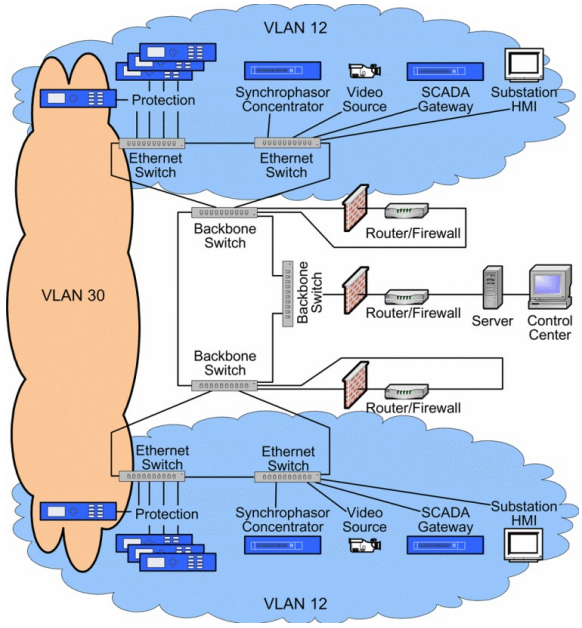



**Figure 3.3:** A VLAN segregated network showing VLAN 30 for inter-substation communication [SM06]

Using VLAN to connect multiple substations in utility-owned communication networks has been proposed in [SM06]. The VLAN architecture shown here in Figure 3.3 will enable segregating traffic within each substation and between the two substations by preventing GOOSE and SV multicast traffic created inside the substation from flooding the rest of the network. Although there have been proposals on applying such methods in the literature, there has been little attention to evaluating the performance of IEC 61850 GOOSE/SV. One of the challenges is that devices and testbed opportunities have been limited. Hence, it will be useful to design a VLAN framework for evaluating the performance of IEC 61850 GOOSE/SV between two or multiple substations. With such a framework, it will be possible to study the effects of related ICT properties such as latency, jitter, and background traffic have on the WAMPAC applications.

### 3.2.2 Interconnecting substation LANs using IP

IP unicast, which has been used to transport C37.118–PMU data in wide-area, is faced with the challenge that the data is transmitted only once from

the PMU source and has only one destination (i.e., PDC). To be able to send to multiple destinations or substation LANs, the PMU has to be transmitted multiple times from the source, which can cause both link capacity challenges as well as increased processing at the PMU source.

IEC 61850 GOOSE/SV can also utilize layer 2 transport technology solutions to interconnect over the WAN. This was demonstrated in [WHU12] where the performance of GOOSE was investigated under different traffic conditions over a WAN link using Layer 2 Tunnelling Protocol (L2TP) and Ethernet over MPLS (EoMPLS) transport mechanisms. L2TP requires encapsulating Ethernet data packets with UDP datagram while EoMPLS encapsulates Ethernet protocol data units inside MPLS packets and forwards the packets using label stacking.

However, both EoMPLS and L2TP are point-to-point tunneling solutions. They can connect a substation to a control center, but not connect two substations and a control center over the same tunnel. Hence, even though these techniques enable transporting GOOSE messages between substations connected by a WAN link, they cannot support the distributed sharing of the GOOSE message among several substations. In order to share the GOOSE message with several substations, separate tunnels will need to be established between all the substations interested in receiving the GOOSE message. This brings similar challenges as with IP unicast in terms of scalability. Hence, the methods of IP unicast and layer 2 transport technology solutions bring challenges that can impact delay, jitter, scalability, and availability when connecting several LANs that share GOOSE/SV or C37.118–PMU or R-GOOSE/R-SV data.

IP multicast has been proposed as a solution to connect multiple LANs in the grid to disseminate R-GOOSE/R-SV data, which supports underlying WAMPAC applications [MTD12, See13]. PMU is recognized as a classical multicast streaming source. It sends a continuous stream of measurement data to several subscribers. Hence, it is a logical step to consider IP multicast as the proper network architecture to implement this communication pattern. The utilization of IP multicast supports efficient bandwidth utilization and minimizes packet replication as the PMU does not have to replicate traffic or manage subscribers.

Figure 3.4 shows an IP multicast architecture proposed in [See13] to send R-SV data over the WAN. The components include IED and MU devices that publish and subscribe to the R-SV data. Also, there are routers placed in at the edge of the substations and inside the WAN. The architecture uses a variant of IP multicast called Protocol Independent Multicast-Source Specific Multicast (PIM-SSM) to provide an optimal delivery path for low

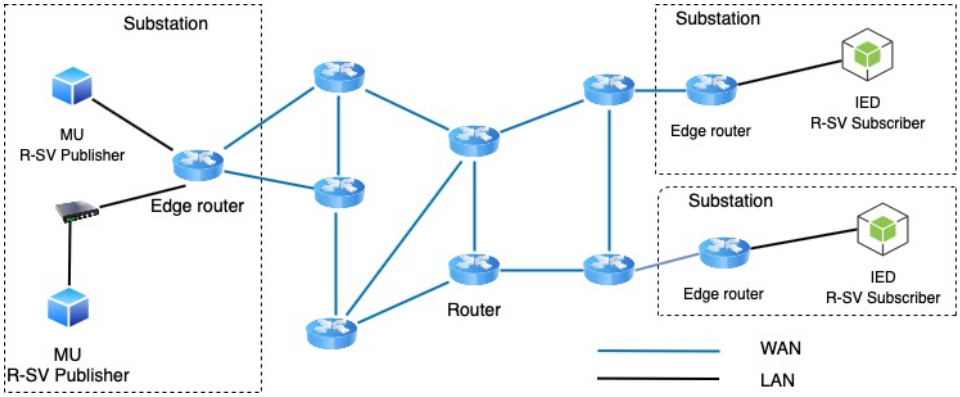



**Figure 3.4:** A generalized network architecture using IP-multicast to send R-SV data over a wide area network [See13].

latency traffic.

The routers at the edge of each substation are the first nodes acting as a source in the multicast tree. The subscriber IEDs interested in receiving R-SV data from a particular substation use signaling to join the source node tree and then receive R-SV data. The received R-SV data is forwarded onto the LAN, which is typically a substation bus, to which the receiving IEDs are attached.

A publishing IED is not burdened with replication and management of traffic or subscriber lists, which allows efficient utilization of computation and communication resources. Furthermore, from an architectural perspective, the network will replicate packets at optimal points, which can lead to scalability and efficient network utilization. In conclusion, IP multicast will be the architecture that provides the network transport for R-GOOSE/R-SV in WAMPAC applications utilizing standardized, existing, and deployed technologies to accomplish this.

In deploying IP multicast architecture for (WAMPAC) applications that have strict requirements on QoS such as latency, there are challenges as to how the communication network should be designed for such multicast deployments in the smart transmission grid. The studies reviewed in the literature have only proposed IP multicast as an architecture possible for wide-area applications in the grid without any evaluations or considerations for the underlying topology design. Furthermore, methods of constructing communication network structures, designing, and evaluating the performance of IP multicast on network topologies for utility grids has received little focus. It will be useful to study how these communication architectures can

be designed to achieve low latency by building efficient network structures from the power grid topologies. Here, the goal will be to construct network architectures that satisfy the QoS requirements and constraints such as low latency.

## 3.3 How can real-time QoS be guaranteed for protection traffic deployed in Smart Transmission Grid Ethernet network?

Most transmission utility grids have previously relied on legacy circuit-switched services such as PDH or SDH/SONET for their tele-protection communications applications between substations. With the standardization efforts of IEC 61850, many utilities have investigated and implemented communication supported by Ethernet for tele-protection signaling between substations because of the high-speed performance, flexibility, and maintainability it promises [SEM13, FYM+14].

One recommendation to lower delays and achieve real-time services on tele-protection data in Ethernet networks is over-provisioning [IEC10b]. With over-provisioning, the communication network has significantly more physical link bandwidth and buffer space than is required by the time-critical data. This approach is not cost-efficient and leads to a waste of network resources. IEEE 802.1Q [80211] prioritization has been the current and significant recommendation to achieve low delays for the tele-protection traffic. This standard allows priorities, queue mappings, and queue service disciplines to be managed to best support the users' goals. Prioritization assigns the highest priority in the network, to the tele-protection traffic (i.e., TCF) to minimize the impact of non-time critical traffic.

The authors in [RL14, Nok16, RMW+18, BBD+18, FHR18] have proposed and evaluated the use of IEEE 802.1p QoS prioritization to test protection schemes in Ethernet networks. These were deployed with either Ethernet Layer 2 or IP/MPLS technologies. The tests mainly measured the protection traffic times as well as evaluating the protection performance. Usually, it is expected that the tele-protection traffic packets experience minimum latency in the network. The results have shown Ethernet packet-switched networks for tele-protection promises the same advances in reliability and reduced costs. However, some main challenges that have been encountered when using Ethernet to provide tele-protection services are:

- latency and jitter; High latency in the network affects tripping signals and can result in miscoordination between the protection relays.

Current differential line protection schemes are particularly sensitive to jitter or PDV, in addition to asymmetrical latency or the fluctuating difference in latencies in the opposite direction for two substations involved the protection channel data exchange [BBD+18, SWFR12].

- Synchronization; Protection schemes such as current differential protection systems require time synchronization to accuracy of 0.1 msec and even less than 0.01 msec in some cases [IEC10b], in that current phasors measured at each terminal are synchronized or time-stamped. This is essential so that each protection relay can properly compare local and remote phasor measurements. GPS and IEEE 1588 PTP [IEE17] are mechanisms to enable synchronization in such systems.

Jitter occurs in Ethernet networks due to variable queuing latency mainly caused by Head-of-line (HOL) blocking [Nok16, BBD+18]. HOL occurs when a high-priority packet is delayed due to a low-priority packet being already transmitted on the same egress port. The random latency incurred varies depending on the sizes of the low-priority packets transmitted and the link speed capacity. Some network switches overcome HOL using virtual output queuing [GL02] technique where separate queues are maintained for each possible output location, rather than keeping all traffic in a single queue. However, the throughput performance is dependent on the scheduling and traffic shaping mechanisms used. Hence, the higher priority packets will still need to wait until the low-priority packet is processed for transmission, assuming IEEE 802.1p scheduling was used. Therefore, fixed latency cannot be guaranteed for the time-critical protection traffic.

Even though the newly standardized TSN IEEE 802.1Qbu and IEEE 802.1Qbv are suitable to provide time-sensitive services, they do not result in fixed latency in the network. With IEEE 802.1Qbu, TCFs are processed in a minimum wait equivalent to the MTU in the network upon arrival. Some PDV might be experienced on high priority packets because preemption is only performed if at least 60 bytes of the preempt-able frame has been transmitted, and at least 64 bytes (including the frame CRC) remain to be transmitted. Adding the Ethernet mandatory inter-frame gap, preamble and delimiter, this results in a worst-case of 1240 bit (155 bytes) of delay, and a best-case of zero delays. With IEEE 802.1Qbv, the switching mechanism is achieved through individual on/off transmission gates associated with each traffic class queue with a list of defined gate operations that control each gate. The sequence of gate operations provides a repeating cycle of gate state changes. However, the duration and start of the time-slots may vary,

hence, some PDV might occur.

The widely popular IEEE 802.1p, and the TSN standards IEEE 802.1Qbu and IEEE 802.1Qbv, even though are mechanisms for enabling time-sensitive services, are not able to offer fixed latency and ultra-low PDV for tele-protection traffic in some cases. This is because primarily, the QoS prioritization techniques employed to manage high priority traffic will still be affected by lower priority packets at some point in the network. Hence, an alternate approach is investigated that can be employed to guarantee real-time deterministic latency for tele-protection applications deployed in shared Ethernet.

In guaranteeing real-time QoS for tele-protection traffic in Ethernet networks, there is a need to investigate scheduling mechanisms that can enable TSN services of fixed latency, ultra-low jitter, and zero packet losses. From the reviewed works in literature, recommendations to reduce delay in tele-protection over Ethernet layer 2 or layer 3 or MPLS has been based on IEEE 802.1p prioritization techniques. Hence, the goal is to investigate an alternative scheduling discipline that enables fixed latency in the delivery of protection traffic in the smart transmission grid.

# Chapter 4

# Contributions

The contributions of the thesis can be divided into three main categories:

1. **A novel co-simulation framework for analyzing protection algorithms**
2. **ICT architectures for routing R-GOOSE/R-SV in WAMPAC applications**
    - A communication framework based on VLAN to evaluate SV performance in wide-area
    - A new algorithm for building network topologies to meet real-time constraints in the delivery of IP multicast
3. **An approach of achieving hard QoS properties of minimum delays, packet losses and PDV for the transport of protection traffic.**

These three categories are aimed to provide answers to the research questions defined in Section 1.2. The research results are contained in 10 scientific publications. Table 4.1 outlines the list of 7 publications (Papers A-G), included as contributions for this thesis work. Table 4.2 lists 3 supplementary publications (Paper H-G), not included in the thesis. The order of presentation of the research publications are not chronological, but rather in relation to the research questions to give a natural flow in the exposition of the thesis.

Figure 4.1 gives an overview of the included papers, their connection to the research questions listed in Section 1.2, as well as how the papers relate to one another.

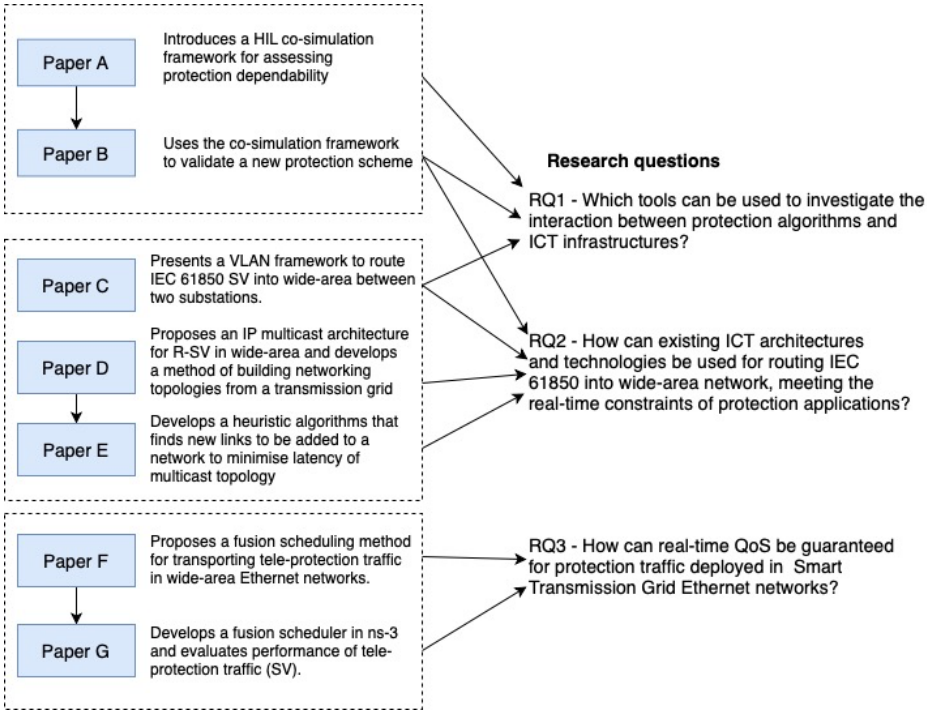



**Figure 4.1:** Overview of the papers included in the thesis as grouped based on the research questions. The relations between the papers are also shown

Firstly, a HIL co-simulation framework is proposed to be used to test and assess protection algorithms (Paper A [AKLH17]). The framework enables the effects of dynamics in QoS for the ICT network on protection reliability to be analyzed. The co-simulation framework is used in Paper B [PAHK19], where the effects of ICT impairments are modeled, and the protection reliability of a protection scheme is analyzed.

Secondly, a VLAN framework to route IEC 61850 SV between two substations (Paper C [AKY+18]) is presented. The co-simulation framework is extended to implement this framework. The framework enables us to characterize the performance with a use case WAMPAC application (state estimation) where the influence of transmission delays and background traffic could be measured. The results indicate that some delays caused by the background traffic on the system seem to have impacted the state estimation output. These impacts may be severe when a vast network with background traffic from sources besides IEC 61850 is being considered. Paper D [AJK+19] proposes an IP multicast architecture to route R-SV in a wide-area transmission grid. The use case assumed is a decentralized

**Table 4.1:** List of publications included in the thesis

| Paper | Title. Author List. Conference/Journal |
|---|---|
| A | **Communication Network Modeling for Real-Time HIL Power System Protection Test Bench**<br>C. M. Adrah, Z. Liu, Ø. Kure, and H. Kr. Høidalen<br>IEEE PES PowerAfrica, Accra, Ghana, 27–30 June 2017, pp. 1–6 |
| B | **Experimental validation of a new impedance based protection for networks with distributed generation using co-simulation test platform**<br>K. Pandakov, C. M. Adrah, H. Kr. Høidalen, and Ø. Kure,<br>in IEEE Transactions on Power Delivery, doi: 10.1109/TPWRD.2019.2935834 |
| C | **A Methodology to Implement and Investigate Performance of Sampled Values for Wide-Area Protection**<br>C. M. Adrah, Ø. Kure, J. R. A. K. Yellajosula, S. Paudyal, and B. Mork,<br>2018 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC) Kuala Lumpur, 2018, pp. 84-90. |
| D | **An IP Multicast Framework for Routable Sample Value Communication in Transmission Grids**<br>C. M. Adrah, J. R. A. K. Yellajosula, Ø. Kure, D Palma, and P. E. Heegaard<br>Journal of Communications vol 14 (9) (2019) 765–772. |
| E | **A Network Design Algorithm for Multicast Communication Architectures in Smart Transmission Grids**<br>C. M. Adrah, D Palma, Ø. Kure, and P E Heegaard<br>in Electric Power Systems Research Journal, doi: 10.1016/j.epsr.2020.106484 |
| F | **Fusion Networking for IEC 61850 Inter Substation Communication: Use Case Applications**<br>C. M. Adrah, S. Bjørnstad, and Ø. Kure<br>Journal of Communications vol 12 (9) (2017) 510-517. |
| G | **Achieving Guaranteed Performance for Protection Traffic in Smart Grids Wide-Area Networks**,<br>C. M. Adrah, A. K. Kamath, S. Bjørnstad, and M. P. Tahiliani<br>2019 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 42-47. |

WAMPAC application where multiple groups of substations in the grid act as sources/receivers and publish/subscribe to R-SV measurements. Here, the impact of underlying network topology on such a WAMPAC application is investigated. A method of building network topologies from the transmission grid is developed to improve the performance of multicast delivery. However, the multicast groups for a given networking topology could be limited by constraints on latency. To address this problem, Paper E proposes a heuristic network design algorithm that can effectively rewire the underlying network topology to meet the real-time requirements.

Thirdly, a scheduling mechanism is proposed to enable TSN services of fixed latency and jitter for tele-protection traffic (Paper F [ABK17b]). The scheduling mechanism, Fusion, is a concept developed in Integrated Hybrid Optical Networks. The proposed method does not reflect in the IEEE TSN standardization. However, the mechanism contributes to achieving

bounded deterministic delay and jitter for time-sensitive applications. Paper G [AKBT19] further develops the FSQ in ns-3, which demonstrates the proposed deterministic delay and jitter behavior. A case-study of a wide-area communication network to transport tele-protection traffic between substations is modeled, and analysis of the scheduling mechanism was investigated.

## 4.1 Summary of Results Contributing to the Thesis

In this section, a summary of the papers included in Part II of the thesis is presented. The contributions of the papers are discussed with respect to the relevant related works.

### Paper A: Communication Network Modeling for Real-Time HIL Power System Protection Test Bench

- C. M. Adrah, Z. Liu, Ø. Kure, H.Kr. Høidalen
  IEEE PES PowerAfrica, Accra, Ghana, 27–30 June 2017, pp. 1–6

Paper A presents the design and implementation of a network emulator. The network emulator is a component integrated with a real-time simulator to form a co-simulation environment. The network emulator is used together with OPAL-RT real-time simulator to build up the test bench for testing of power system protection applications. The co-simulation platform also enables us to achieve hardware-in-the-loop real-time testing of protection algorithms and applications. The authors in [GHM+13, BCZ+13] used both OPAL-RT combined with OPNET for their co-simulation. With OPNET, there are challenges of cumbersome initial set up and the need to ensure that it runs synchronously with OPAL-RT. Besides, there is limited flexibility in using IEC 61850 GOOSE and SV protocols within OPNET. The network emulator has real-time properties that enable real network packets (GOOSE and SV) from OPAL-RT to be introduced into the emulation environment. The ICT network properties can then be emulated and the resulting packets emitted from the emulation back into the OPAL-RT or field devices such as IEDs and MUs.

The network emulator is developed using *click router* [KMC+01], which is a software framework for building flexible and configurable routers. Click Router has a flexible, open, and modular architecture enabling us to compose new features and extend existing features for experimentation. Also,

click router supports real-time traffic; hence it efficiently combines with OPAL-RT simulator to form a real-time co-simulation platform. The key functionalities of the co-simulation framework with the network emulator identified were; to emulate the communication properties (delay, jitter, and packet loss) of ICT topology for inter substation protection applications. Also, to model and vary new network properties and communication services that can affect protection system applications. The technical design choices and limits of the network emulator for real-time performance are discussed. A limitation identified is that, for the network emulator, which is a software-based system running on standard Linux, interrupts in the operating system will create delays and jitter affecting the delay granularities that can be realized. However, through experimentation, we recorded high confidence in the delay granularities, which can be applicable for WAMPAC applications involving several substations.

The development of the framework has contributed to insight into the impacts of communication network impairments on power grid protection. Also, the complex dependencies between the power and the ICT systems can be taken into account during the development and testing of these protection applications with this method.

### Paper B: Experimental validation of a new impedance-based protection for networks with distributed generation using co-simulation test platform

- K. Pandakov, C. M. Adrah, H. K. Høidalen, Ø. Kure, IEEE Transactions on Power Delivery, doi: 10.1109/TPWRD.2019.2935834

The co-simulation framework introduced in Paper A was used to achieve the objectives in Paper B. The objective of Paper B was the experimental verification of a relay protection scheme utilizing the co-simulation framework. The first part of the paper proposes a new protection scheme developed by the first author K. Pandakov for medium voltage networks with distributed generation based on impedance measurements with compensation of remote in-feed currents and high fault resistances.

The second part of the paper studies the performance of the protection scheme in laboratory conditions using the co-simulation platform of OPAL-RT and click-router based communication emulator. The aim was to study the impact of communication network impairments on overall protection dependability. As such, it was possible to create controlled communication network parameters for protection testing that are close to real-life environments. Communication network impairments that were emulated were jitter

and burst packet drops (packet losses). The results obtained showed that communication network imperfections such as jitter and data loss deteriorate the protection scheme dependability. Also, the impact of background traffic (i.e., when other data occupy the channel bandwidth) in the network was tested. The results lead to an increase in communication latency and packet losses with similar consequences for protection scheme dependability. The contribution of using the co-simulation framework, including the techniques of emulating network imperfections, enabled bench-marking of protection algorithms and the protection dependability.

### Paper C: A Methodology to Implement and Investigate Performance of Sample Values for Wide-Area Protection

- C. M. Adrah, Ø. Kure, J. R. A. K. Yellajosula, S. Paudyal, B. Mork 2018 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC), Kuala Lumpur, 2018, pp. 84-90.

In Paper C, a communication framework is presented to route Sample Value measurements between two substations on different Ethernet networks based on VLAN-id's. The communication framework is achieved by extending the co-simulation framework in Paper A with L2 and L3 network devices as well as emulate network traffic conditions with the communication network emulator.

Although using VLAN has been proposed in [SM06] to connect multiple substations in power grid utility-owned communication networks, there is not a lot of research effort in how WAMPAC applications will perform with such an architecture. The work in this paper is based on the VLAN architecture using the co-simulation framework. The framework enables us to investigate the performance of Sample Value data (in a phasor estimation application) in a wide-area network with the influence of delays caused by transmission, background traffic, the physical distance between the substations and unintentional delays due to communication devices. With the testbed, the impacts of communication variability could be tested and measured. Consequently, the measured network variability could be used on delay correction and time-stamp alignment during the phasor estimation, which is a WAMPAC use case application. The challenges that have been identified with VLAN-based wide-area architecture include the complexity with engineering efforts to design such a framework for extensive substation networks. The engineering complexity can lead to misconfigurations, difficulty in different utility operators in coordinating which VLAN-ids to designated for wide-area use, as well as the difficulty of routing R-SV to several destination

substations. The proposed VLAN framework shows that there is a need to analyze in detail to understand and mitigate the influence of background traffic in the phasor estimation application.

### Paper D: An IP Multicast Framework for Routable Sample Value Communication in Transmission Grids

- C. M. Adrah, J. R. A. K. Yellajosula, Ø. Kure, D Palma, P. E. Heegaard, Journal of Communications vol 14 (9) (2019) 765–772.

In paper D, we conducted a study on how PIM-SSM, an IP multicast routing protocol enables R-SV transmission in decentralized wide-area applications and construct network topologies to support the formation of multicast groups for an IEEE 39-bus transmission system. The paper discusses the differences between wide-area centralized and decentralized operations, and how using IP multicast as a communication architecture will assist the dissemination of R-SV for WAMPAC applications. We first show how PIM-SSM can be realized in a transmission grid communication network, and present a qualitative analysis of effects on multicast when link failures occur.

We follow the network structure proposed in [YHP+12], where substations in the same regional area of the power grid are connected to a backbone ring. Hence the communication infrastructure proposed is based on groups of a ring supported by a mesh core network. We identify two criteria that enable building such a communication infrastructure from the power grid, with the aim to improve the performance of multicast delivery. These are the nodes in different rings that are connected to the core mesh and the number of rings that can be formed based on the existing number of substations in the transmission grid. To determine the nodes to connect to the core mesh, we find the Betweenness Centrality [Fre77] for all nodes in the transmission grid and, as a generic rule, connect the nodes with the highest Betweenness Centrality to the core mesh. Forming rings was done with a general consideration of the proximity of nodes to form regional areas We then present a quantitative study to evaluate the performance of PIM-SSM, on the designed communication network topologies where the focus is on analyzing different topology structures that can support multicast groups to achieve a reduction in the shortest path lengths. In our case study evaluated, we observe that selecting the right topology resulted in 4 times reduction in shortest path lengths and 3 times lower delays. The paper's contributions show that communication technology will play a critical role in the efficient delivery of R-SV data in a multicast framework and that improvements

in the networking infrastructure design lead to better performance of the multicast delivery.

### Paper E: A Network Design Algorithm for Multicast Communication Architectures in Smart Transmission Grids

- C. M. Adrah, D. Palma, Ø. Kure, P. E. Heegaard, in Electric Power Systems Research Journal, doi: 10.1016/j.epsr.2020.106484

Paper E extends our work in Paper D in network infrastructure design that leads to better performance of the multicast delivery. We propose a heuristic algorithm for communication network design to meet real-time constraints of WAMPAC applications.

The future smart transmission grids will rely on distributed applications that will benefit from the deployment of multicast technology for communication. Sharing of routable-sample values (R-SV) among the digital substations for wide-area protection and control will be needed. There have been proposals of using IP Source-Specific Multicast as an architecture to transport PMU data in wide-area monitoring and protection applications in [See13] and the challenge of designing utility grid networking topologies and its' impacts on achieving optimal delivery paths identified. This demand for the concurrent delivery of R-SV measurement data will put constraints on the underlying supporting networking infrastructure. In such a case, it must be ensured that the paths taken to route data traffic are within the bounds of delay to achieve the aims of the protection application. The problem of network topology augmentation through link additions is therefore addressed.

The algorithm called *reduction over minimum set cover* (ROMSC) finds additional new links to be added to an existing topology, and thereby change the underlying topology. As such, the latency of multicast traffic based on defined multicast groups can be limited. We compare the performance of the ROMSC and clustering algorithm used in [DZ10] to minimize the diameter of network topology with a defined multicast configuration. The results show that by adding a few new links to the network topology, the delay incurred by the multicast traffic from sources to destinations can be reduced. Our algorithm shows how the communication network topology can support WAMPAC applications based on latency constraints through topology augmentation.

### Paper F: Fusion Networking for IEC 61850 Inter Substation Communication: Use Case Applications

- C. M. Adrah, S. Bjørnstad, and Ø. Kure, Journal of Communications vol 12 (9) (2017) 510-517.

*Paper F* proposes the use of Fusion networking technology for transporting time-critical protection applications traffic in wide-area networks among utility substations, to attain deterministic or fixed low delay, zero packet loss, and ultra-low packet delay variation. IEC 61850 substation automation is deployed with Ethernet technology. Lowering latency on the protection traffic requires techniques such as priority scheduling and Class of Service (CoS) mechanisms recommended in IEEE 802.1Q. However, we contend that these techniques alone might not give an absolute QoS guarantee for tele-protection traffic having stringent requirements on latency as well as synchronization. The benefit of giving absolute QoS guarantee for tele-protection enables the communication link latency to by consistent and predictable. As such, the protection scheme's reliability is not compromised.

Fusion networking provides packet-based networks with the advantages of circuit-switched networks. The concept is built from Integrated Hybrid Optical Networks (IHON) [BHS06], which brings packet and circuit network domains together. IHON supports two classes of service. The first service class is called Guaranteed Service Transport (GST), offering a hard QoS guarantee of zero packet jitter, zero packet loss, and low deterministic delay. The second class is a packet service class called statistically multiplexed (SM) offering lower QoS guarantees. The requirements for inter substation communications are presented with a focus on the IEC 61850 protocols of Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SV) and their adaptability to the traffic classes of guaranteed service transport (GST) and statistically multiplexed (SM) in Fusion networking technology. GOOSE and SV for protection applications have transfer times of 10 msec. Use case applications are explained for communication between two substations and three substations. Each substation has an edge router/node running the scheduling mechanism based on Fusion networking. An analytical evaluation was made for a case study scenario of two substations, each with an edge node running Fusion scheduling and transporting protection traffic over a 100km distance. It was found that the delay experienced on the protection traffic was 556.6 us, which was significantly lower than the acceptable transfer time of a maximum of 10 msec.

In conclusion, the analysis shows that using a Fusion scheduling mechanism for the transport of time-critical tele-protection traffic across substa-

tions in the utility grid, is a feasible solution to guarantee hard QoS of low deterministic delay and ultra-low PDV.

### Paper G: Achieving Guaranteed Performance for Protection Traffic in Smart Grid Wide-Area Networks

- C. M. Adrah, A. K. Kamath, S. Bjørnstad, and M. P. Tahiliani, 2019 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 42-47.

*Paper G* extends the proposal in Paper E, where it is explored through a performance simulation study the suitability of applying Fusion scheduling and queuing (FSQ) as a time-sensitive network (TSN) service mechanism. TSN services are a class of services defined in Ethernet to offer bounded latency and zero congestion loss, and other benefits for time-critical traffic in best-effort Ethernet networks. With FSQ, it can offer fixed latency and ultra-low PDV in smart grid tele-protection applications. In addition, a zero packet loss can be achieved with the necessary traffic engineering methods applied. The Fusion scheduler is developed in ns-3 [HRFR06].

The authors in [FHR18] used Strict Priority Queuing and scheduling (SPQ), which has been the foremost existing TSN service scheduling technique, in proposing a deterministic transport method for tele-protection traffic. The approach only gives a guarantee for the worse case PDV for each network egress port. A qualitative discussion on two approaches of IEEE TSN scheduling mechanisms and how they differ from our proposed alternative FSQ was done. While IEEE 802.1Qbu [IEE16a] uses a preemption mechanism to enable the minimum delay on time-critical frames, there might be PDV experienced on high priority packets due to limitations on the preempt-able frames. In the case of IEEE 802.1Qbv [IEE16b], which allows the transmission to be switched on and off on a timed basis for the different traffic classes. PDV occurs due to the variations in the duration and start of the time-slots. With FSQ, we ensure fixed latency and zero PDV on high priority packets by eliminating the influence of lower priority traffic on the high priority traffic.

We demonstrate FSQ performance in tele-protection for power system networks and compare it with SPQ, which is recommended for real-time industrial applications. A ring communication network topology is modeled for a 4-bus power grid, and the performance of protection traffic is measured between two chosen units in the grid. The protection traffic was also effectively modeled, and the QoS metrics of delay, packet delivery ratio, and

packet delay variation were used in this evaluation. The results show that by applying FSQ, we can guarantee a fixed delay, zero PDV, and packet loss through the network. Furthermore, it is shown that through proper network dimensioning, lower priority traffic can additionally be added with delays within acceptable limits.

## 4.2 Summary of contributions and answers to research questions

*Paper A* and *Paper B* answer RQ1. Paper A presents a co-simulation framework that can be used to assess relay protection algorithms in the smart grid context. Paper B uses the co-simulation framework introduced in Paper A to test and study the impact of network impairments on a new impedance-based protection scheme.

*Paper C, Paper D, and Paper E* answer RQ2. Paper C presents a VLAN framework to route IEC 61850 SV in wide-area between two substations. The performance of SV for a phasor estimation use case is analyzed with respect to network traffic delays and the influence of background traffic. Paper D presents an IP multicast architecture and a method of building networking topologies based on the transmission power grid topology. Paper E presents a heuristic algorithm to find additional links that can change the underlying topology, and reduce latency on multicast traffic based on defined multicast groups. This shows how the communication network topology can support WAMPAC based on latency constraints through topology augmentation.

*Paper F* and *Paper G* answer RQ3. Paper F highlights the requirements of tele-protection traffic applications and describes the mechanism that provides deterministic delay, minimum jitter, and zero packet loss in a shared Ethernet network. Paper G presents a simulation case study in ns-3. The performance of FSQ is compared with SPQ to evaluate IEC 61850 Sample Value traffic.

The results obtained throughout the research work provides insight to utility operators about the critical role of ICT network architectures and systems on protection system operations and WAMPAC applications in general.

**Table 4.2:** List of supplementary publications

| Paper | Title. Author List. Conference/Journal |
|---|---|
| H [PAL+18] | **Hardware-in-the-loop testing of impedance protection with compensation of fault impedance and DG infeed current**,<br>K. Pandakov, C. M. Adrah, Z. Liu, H. Kr. Høidalen, and Ø. Kure,<br>The Journal of Engineering, vol. 2018, no. 15, pp. 1018-1022, 10 2018. |
| I [ABK17a] | **Fusion Networking for IEC 61850 Inter Substation Communication**<br>C. M. Adrah, S. Bjørnstad, and Ø. Kure<br>2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC), Singapore, 2017, pp. 152-156. |
| J [AAH19] | **A Method for Performability Study on Wide Area Communication Architectures for Smart Grid**<br>T. Amare, C. M. Adrah, and B. E. Helvik<br>2019 IEEE International Conference on Smart Grid (icSmartGrid) |

# Chapter 5

# Concluding Remarks and Future Work

## 5.1 Concluding Remarks

This thesis has sought to present a perspective on the challenges communication performance and system architectures present to the digital protection systems deployed in wide-area smart transmission grids. The communication infrastructure supporting STG will be very crucial and expected to handle future real-time information exchange. The ICT infrastructure will support time-synchronized measurements which will be available in all STG substations at much higher rates. Protection systems that have very stringent QoS performance requirements will significantly benefit from the supporting ICT infrastructure.

With the increasing complexity in the power grid, testing of protection systems becomes very important. In a 2015 North America Electric Reliability Corporation [Cor15] (NERC) misoperations report, the highest causes of misoperation were incorrect settings, logic, and design errors. Also, communication failures resulted in the third-highest cause, which shows the relevance of the ICT system is a vital part. The behavior of the ICT network has the potential to influence the relay settings, design, and logic. Therefore, the ICT network interaction will need to be considered in design protection test methods. The growing deployment of communication-based schemes will only increase the need for co-simulation tools and HIL approaches in protection testing and validations. These tools and techniques will become indispensable tools for validating the behavior of protection applications. This thesis has developed a real-time HIL co-simulation framework using

OPAL-RT and click modular router tools to assess the interaction between protection algorithms and the ICT infrastructure.

Furthermore, the supporting ICT infrastructure is expected to be high performance, reliable, scalable, and secure for deployment and operation. Communication delays are one of the critical performance metrics in STG applications. Hence, the ICT infrastructure needs careful planning in order to meet the set performance requirements. The support for IP based networks, specifically multicast, will be seen as essential to manage STG networks. It provides a scalable and dynamic network architecture where the network is responsible for the transport utilizing standardized and existing technologies to achieve this. General-purpose networks with core networks can support real-time of most applications, the network should be flexible to maintain direct link connections between substations that cannot satisfy latency, and in some cases best link placements. Eventually, it is expected as a future trend, convergence, and support of STG applications for teleprotection and wide-area monitoring systems on the same general purpose networks. To this end, the thesis has proposed a network design algorithm that finds the best links to be added to an existing ICT topology such that the latency incurred on the multicast traffic is reduced.

Finally, the acceptance of TSN and adoption into IEEE and IETF DetNet standards is expected to generate much interest in smart transmission grid operations. This thesis has investigated a mechanism that provides deterministic delay, jitter, and packet loss requirements for the protection applications running over a shared Ethernet network. Protection applications especially will benefit from these mechanisms since they are mission-critical, time-sensitive data that must be delivered within strict bounds of latency and reliability. As the suite of TSN features is improved and adopted, it is expected to provide solutions of deterministic, time-sensitive, and reliable communications that co-exists with best-effort traffic. The network infrastructure could then be simplified, where instead of relying on multiple ICT infrastructures to handle different types of traffic such as teleprotection traffic, everything can be carried over Ethernet. A challenge is to develop confidence and understanding in these new technologies that have the potential to reduce costs for utility grid operations.

## 5.2 Future work

This thesis has given a contribution to the role communication networks will play towards protection systems in smart transmission grids. The field

remains challenging with the need for the actual realization of some of the research prospects. Besides, emerging new communication systems and technologies will have to be considered as the STG matures.

The co-simulation framework presented in this thesis can be extended with ns-3, which is interface-able with real-time systems [MZM14]. As such, the works in Papers F and G, proposing and implementation fusion scheduling to enable TSN services for tele-protection, can be deployed in larger network topologies together with the real-time platform.

The next technological and networking developments such as Named Data Networking (NDN) and Software-Defined Networking (SDN) are expected to be incorporated in STG communication networks.

- NDN and data-centric approaches to networking [JST+09, XVS+14] have been proposed as a future internet architecture because the Internet is increasingly used for information dissemination, rather than for pair-wise communication between end hosts. NDN proposes the replacement of IP's endpoint-to-endpoint communication model with one centered around named objects. NDN has the potential to be deployed for STG WAMPAC applications.

- SDN is an innovation in computer networking that builds intelligence into an ICT network through software control. An SDN-based network can make high-level decisions that impact detailed network functionality, optimizing the network's performance in a manner not easily possible with traditional network management techniques [CHHK13]. Deploying SDN in the STG will bring benefits that can address the challenges of network management, security, and resilience. Hence, a good research direction is to focus on transmission grids use of R-GOOSE and R-SV in wide-area protection applications and how SDN and the traffic patterns of WAMPAC applications can improve data management in the network.

# Bibliography


[80211] IEEE 802.1Q. 802.1Q-2011 - IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks, 2011.

[AAB+06] M. G. Adamiak, A. P. Apostolov, M. M. Begovic, C. F. Henville, K. E. Martin, G. L. Michel, A. G. Phadke, and J. S. Thorp. Wide area protection - Technology and infrastructures. *IEEE Transactions on Power Delivery*, 21(2):601–609, apr 2006.

[AAH19] T. Amare, C. M. Adrah, and B. E. Helvik. A method for performability study on wide area communication architectures for smart grid. In *2019 7th International Conference on Smart Grid (icSmartGrid)*, pages 64–73, Dec 2019.

[ABK17a] C. M. Adrah, S. Bjørnstad, and Ø. Kure. Fusion networking technology for iec 61850 inter substation communication. In *2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, pages 152–156, July 2017.

[ABK17b] Charles M. Adrah, Steinar Bjørnstad, and Øivind Kure. Fusion networking for IEC 61850 inter substation communication: Use case applications. *Journal of Communications*, 12(9):510–517, 2017.

[ADHK08] Jeff Ahrenholz, Claudiu Danilov, Thomas R. Henderson, and Jae H. Kim. CORE: A real-time network emulator. In *MILCOM 2008 - 2008 IEEE Military Communications Conference*, pages 1–7. IEEE, nov 2008.

[aE] Norwegian Ministry of Petroleum and Energy. The electricity grid - Energifakta Norge.

[AJK+19] Charles M. Adrah, Jaya R. Jaya, Øivind Kure, David Palma, and Poul E. Heegaard. An IP multicast framework for routable sample value communication in transmission grids. *Journal of Communications*, 14(9):765–772, 2019.

[AKBT19] Charles M. Adrah, Aditya K. Kamath, Steinar Bjornstad, and Mohit P. Tahiliani. Achieving Guaranteed Performance for Protection Traffic in Smart Grid Wide-Area Networks. In *Proceedings of 2019 the 7th International Conference on Smart Energy Grid Engineering, SEGE 2019*, pages 42–47. IEEE, aug 2019.

[AKLH17] C.M. Adrah, O. Kure, Z. Liu, and H.K. Hoidalen. Communication network modeling for real-time HIL power system protection test bench. In *Proceedings - 2017 IEEE PES-IAS PowerAfrica Conference: Harnessing Energy, Information and Communications Technology (ICT) for Affordable Electrification of Africa, PowerAfrica 2017*, 2017.

[AKV10] Amit Aggarwal, Swathi Kunta, and Pramode K. Verma. A proposed communications infrastructure for the smart grid. In *Innovative Smart Grid Technologies Conference, ISGT 2010*, pages 1–5. IEEE, jan 2010.

[AKY+18] Charles M. Adrah, Oivind Kure, Jaya R.A.K. Yellajosula, Sumit Paudyal, and Bruce Mork. A Methodology to Implement and Investigate Performance of Sampled Values for Wide-Area Protection. In *2nd International Conference on Smart Grid and Smart Cities, ICSGSC 2018*, pages 84–90. IEEE, aug 2018.

[And99] P. M. (Paul M.) Anderson. *Power system protection*. A John Wiley & Sons, Inc., New Jersey, 1999.

[Apo17] Alexander Apostolov. R-GOOSE: what it is and its application in distribution automation. *CIRED - Open Access Proceedings Journal*, 2017(1):1438–1441, oct 2017.

[AT06] A. Apostolov and D. Tholomier. Impact of IEC 61850 on power system protection. In *2006 IEEE PES Power Systems*

*Conference and Exposition, PSCE 2006 - Proceedings*, pages 1053–1058. IEEE, 2006.

[ATG12] Ikbal Ali, Mini S. Thomas, and Sunil Gupta. Methodology & tools for performance evaluation of IEC 61850 GOOSE based protection schemes. In *2012 IEEE 5th Power India Conference, PICONF 2012*, pages 1–6. IEEE, dec 2012.

[BBD+18] Steven M. Blair, Campbell D. Booth, Bram De Valck, Dominique Verhulst, and Kin-Yee Wong. Modeling and Analysis of Asymmetrical Latency in Packet-Based Networks for Current Differential Protection Application. *IEEE Transactions on Power Delivery*, 33(3):1185–1193, jun 2018.

[BCZ+13] Davood Babazadeh, Moustafa Chenine, Kun Zhu, Lars Nordstrom, and Ahmad Al-Hammouri. A platform for wide area monitoring and control system ICT analysis and development. In *2013 IEEE Grenoble Conference PowerTech, POWERTECH 2013*, pages 1–7. IEEE, jun 2013.

[BHS06] S. Bjornstad, D. R. Hjelme, and N. Stol. A packet-switched hybrid optical network with service guarantees. *IEEE Journal on Selected Areas in Communications*, 24(8):107, Aug 2006.

[Bos10] Anjan Bose. Smart transmission grid applications and their supporting infrastructure. *IEEE Transactions on Smart Grid*, 1(1):11–19, jun 2010.

[CBPGK14] Bo Chen, Karen L. Butler-Purry, Ana Goulart, and Deepa Kundur. Implementing a real-time cyber-physical system test bed in RTDS and OPNET. In *2014 North American Power Symposium (NAPS)*, pages 1–6. IEEE, sep 2014.

[CHHK13] A. Cahn, J. Hoyos, M. Hulse, and E. Keller. Software-defined energy communication networks: From substation automation to future smart grids. In *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 558–563, Oct 2013.

[Cor15] North American Electric Reliability Corporation. Analysis of System Protection Misoperations. Technical Report December, North American Electric Reliability Corporation, 2015.

[DZ10] Erik D. Demaine and Morteza Zadimoghaddam. Minimizing the diameter of a network using shortcut edges. In Haim Kaplan, editor, *Algorithm Theory - SWAT 2010*, pages 420–431, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[FBG18] Janos Farkas, Lucia Lo Bello, and Craig Gunther. Time-Sensitive Networking Standards. *IEEE Communications Standards Magazine*, 2(2):20–21, jun 2018.

[FHR18] Kenneth Fodero, Christopher Huntley, and Paul Robertson. Deterministic communications for protection applications over packet-based wide-area networks. In *2018 71st Annual Conference for Protective Relay Engineers (CPRE)*, pages 1–6. IEEE, mar 2018.

[Fin18] Norman Finn. Introduction to Time-Sensitive Networking. *IEEE Communications Standards Magazine*, 2(2):22–28, jun 2018.

[Fre77] Linton C. Freeman. A set of measures of centrality based on betweenness. *Sociometry*, 40(1):35–41, 1977.

[FTVF18] N. Finn, P. Thubert, B. Varga, and J. Farkas. Deterministic Networking Architecture draft-ietf-detnet-architecture-13. Technical report, IETF, 2018.

[FYM+14] S. Fukushima, J. Yamada, T. Mori, F. Kawano, H. Okamura, S. Kohiga, and H. Yamakawa. Development of line current differential relay over native Ethernet. In *IET Conference Publications*, pages 5.1.1–5.1.1. Institution of Engineering and Technology, 2014.

[GHM+13] Feng Guo, Luis Herrera, Robert Murawski, Ernesto Inoa, Chih-Lun Wang, Philippe Beauchamp, Eylem Ekici, and Jin Wang. Comprehensive Real-Time Simulation of the Smart Grid. *IEEE Transactions on Industry Applications*, 49(2):899–908, mar 2013.

[GL02] Yiping Gong and Bin Liu. Performance evaluation of a parallel-poll virtual output queued switch with two priority levels. In *2002 International Conference on Communications, Circuits and Systems and West Sino Exposition, ICCCAS 2002 - Proceedings*, volume 1, pages 669–674. IEEE, 2002.

[GL06] V.C. Gungor and F.C. Lambert. A survey on communication networks for electric system automation. *Computer Networks*, 50(7):877–897, may 2006.

[HBB05] C.H. Hauser, D.E. Bakken, and A. Bose. A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid. *IEEE Power and Energy Magazine*, 3(2):47–55, mar 2005.

[HMPR04] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Q.*, 28(1):75–105, March 2004.

[HRFR06] Thomas R. Henderson, Sumit Roy, Sally Floyd, and George F. Riley. Ns-3 project goals. In *Proceeding from the 2006 Workshop on Ns-2: The IP Network Simulator*, WNS2 '06, New York, NY, USA, 2006. ACM.

[IEC10a] IEC. IEC standard for communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models. Technical report, IEC, 2010.

[IEC10b] IEC. IEC standard for communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations. Technical report, IEC, 2010.

[IEC12] IEC. IEC standard for communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasors information according to IEEE C37.118 IEC 61850-90-5 TR Ed 1.0. Technical report, IEC, 2012.

[IEC13] IEC. IEC standard for communication networks and systems for power utility automation - Part 1: Introduction and overview. Technical report, IEC, 2013.

[IEE06] IEEE. Ieee standard for local and metropolitan area networks—virtual bridged local area networks—amendment 4: Provider bridges. *IEEE Std 802.1ad-2005 (Amendment to IEEE Std 802.1Q-2005)*, pages 1–74, May 2006.

[IEE11] IEEE. C37.118.2-2011 IEEE Standard for Synchrophasor Data Transfer for Power Systems. Technical report, IEEE, 2011.

[IEE16a] IEEE Standards Association. IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks – Amendment 26: Frame Preemption. *IEEE Std 802.1Qbu-2016 (Amendment to IEEE Std 802.1Q-2014)*, pages 1 – 52, 2016.

[IEE16b] IEEE Standards Association. IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks - Amendment 25: Enhancements for Scheduled Traffic. *IEEE Std 802.1Qbv-2015 (Amendment to IEEE Std 802.1Q-2014 as amended by IEEE Std 802.1Qca-2015, IEEE Std 802.1Qcd-2015, and IEEE Std 802.1Q-2014/Cor 1-2015)*, page 57, 2016.

[IEE17] IEEE. IEEE Standard Profile for Use of IEEE 1588™ Precision Time Protocol in Power System Applications. *IEEE Std C37.238-2017 (Revision of IEEE Std C37.238-2011)*, 2017:1–67, 2017.

[IEE18] IEEE. IEEE Std 802.1Q-2018 : IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks. Technical report, IEEE, 2018.

[JLC13] Wen Kang Jia, Gen Hen Liu, and Yaw Chung Chen. Performance evaluation of IEEE 802.1Qbu: Experimental and simulation results. In *Proceedings - Conference on Local Computer Networks, LCN*, pages 659–662. IEEE, oct 2013.

[JST+09] Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies - CoNEXT '09*, page 1, New York, New York, USA, 2009. ACM Press.

[KB11] Prashant Kansal and Anjan Bose. Smart grid communication requirements for the high voltage power system. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–6. IEEE, jul 2011.

[KB12] Prashant Kansal and Anjan Bose. Bandwidth and Latency Requirements for Smart Transmission Grid Applications. *IEEE Transactions on Smart Grid*, 3(3):1344–1352, sep 2012.

[KCJ17] Mital Kanabar, Anca Cioraca, and Anthony Johnson. Wide Area Protection & Control using high-speed and secured Routable GOOSE Mechanism. In *69th Annual Conference for Protective Relay Engineers, CPRE 2016*, pages 1–6. IEEE, apr 2017.

[KMC+01] Eddie Kohler, Robert Morris, Benjie Chen, John Jannotti, and M. Kaashoek. The click modular router. *ACM Transactions on Computer Systems*, 18, 05 2001.

[KPR14] Murat Kuzlu, Manisa Pipattanasomporn, and Saifur Rahman. Communication network requirements for major smart grid applications in HAN, NAN and WAN, 2014.

[LAH11] Vincenzo Liberatore and Ahmad Al-Hammouri. Smart grid communication and co-simulation. In *IEEE 2011 EnergyTech, ENERGYTECH 2011*, pages 1–5. IEEE, may 2011.

[LDD+13] David Law, Dan Dove, John D'Ambrosia, Marek Hajduczenia, Mark Laubach, and Steve Carlson. Evolution of ethernet standards in the IEEE 802.3 working group. *IEEE Communications Magazine*, 51(8):88–96, aug 2013.

[LFS+14] Weilin Li, Mohsen Ferdowsi, Marija Stevic, Antonello Monti, and Ferdinanda Ponci. Cosimulation for smart grid communications. *IEEE Transactions on Industrial Informatics*, 10(4):2374–2384, nov 2014.

[LL02] Kyung Chang Lee and Suk Lee. Performance evaluation of switched Ethernet for real-time industrial communications. *Computer Standards and Interfaces*, 24(5):411–423, nov 2002.

[LQS+10] Fangxing Li, Wei Qiao, Hongbin Sun, Hui Wan, Jianhui Wang, Yan Xia, Zhao Xu, and Pei Zhang. Smart Transmission Grid: Vision and Framework. *IEEE Transactions on Smart Grid*, 1(2):168–177, sep 2010.

[Mac06] R. E. MacKiewicz. Overview of IEC 61850 and benefits. In *2006 IEEE PES Power Systems Conference and Exposition, PSCE 2006 - Proceedings*, pages 623–630. IEEE, 2006.

[MFA09] Roy Moxley, Ken Fodero, and Hector J. Altuve. Updated transmission line protection communications. In *2009 Power Systems Conference*, pages 1–8. IEEE, mar 2009.

[MKW+92] P.G. McLaren, R. Kuffel, R. Wierckx, J. Giesbrecht, and L. Arendt. A real time digital simulator for testing relays. *IEEE Transactions on Power Delivery*, 7(1):207–213, 1992.

[MTD12] Paul T. Myrda, Jeffrey Taft, and Paul Donner. Recommended approach to a NASPInet architecture. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, pages 2072–2081. IEEE, jan 2012.

[MZM14] T. Molloy, Zhenhui Yuan, and G. Muntean. Real time emulation of an lte network using ns-3. In *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, pages 251–257, June 2014.

[Nok16] Nokia. Mission-critical communications networks for power utilities Enabling reliable transport for teleprotection Application Note. Technical report, Nokia, 2016.

[PAHK19] Konstantin Pandakov, Charles Mawutor Adrah, Hans Kristian Hoidalen, and Oivind Kure. Experimental validation of a new impedance based protection for networks with distributed generation using co-simulation test platform. *IEEE Transactions on Power Delivery*, pages 1–1, 2019.

[PAL+18] K. Pandakov, C. M. Adrah, Z. Liu, H. K. Høidalen, and Ø. Kure. Hardware-in-the-loop testing of impedance protection with compensation of fault impedance and dg infeed current. *The Journal of Engineering*, 2018(15):1018–1022, 2018.

[Pri06] Elmo Price. Practical considerations for implementing wide area monitoring, protection and control. In *2006 59th Annual Conference for Protective Relay Engineers*, volume 2006, pages 36–47. IEEE, 2006.

[PT17] Arun G Phadke and James S Thorp. *Power Electronics and Power Systems Synchronized Phasor Measurements and Their Applications Second Edition*. Springer International Publishing AG, second edition, 2017.

[PTRC08] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3):45–77, dec 2008.

[PvdML+17] Peter Palensky, Arjen van der Meer, Claudio Lopez, Arun Joseph, and Kaikai Pan. Applied Cosimulation of Intelligent Power Systems: Implementing Hybrid Simulators for Complex Power Systems. *IEEE Industrial Electronics Magazine*, 11(2):6–21, jun 2017.

[RL14] Silvio Roesler and Ruben Lobo. Proving viability of line current differential over packet switched networks. In *2014 67th Annual Conference for Protective Relay Engineers, CPRE 2014*, pages 542–551. IEEE, mar 2014.

[RMW+18] Tariq Rahman, James Moralez, Solveig Ward, Eric A. Udren, Michael Bryson, and Kamal Garg. Teleprotection with MPLS ethernet communications - Development and testing of practical installations. In *71st Annual Conference for Protective Relay Engineers, CPRE 2018*, volume 2018-Janua, pages 1–18. IEEE, mar 2018.

[See13] M. Seewald. Building an architecture based on IP-Multicast for large phasor measurement unit (PMU) networks. In *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5. IEEE, feb 2013.

[SEM13] Rodolfo García Sierra, Carlos Medina Etayo, and Nelson Marin Mejia. Tele-protection implementation experience at power substations using metro ethernet networks. In *IET Conference Publications*, pages 0439–0439. Institution of Engineering and Technology, 2013.

[SGF+19] R. Salazar, T. Godfrey, N. Finn, C. Powell, B. Rolfe, and M. Seewald. Utility applications of time sensitive networking white paper. *Utility Applications of Time Sensitive Networking White Paper*, pages 1–19, Oct 2019.

[SJB02] Tor Skeie, Svein Johannessen, and Christoph Brunner. Ethernet in substation automation. *IEEE Control Systems*, 22(3):43–51, jun 2002.

[SM06] Veselin Skendzic and Roger Moore. Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet. In *2006 IEEE PES Power Systems Conference and Exposition*, pages 641–649. IEEE, 2006.

[SMM18] Csaba Simon, Markosz Maliosz, and Miklos Mate. Design Aspects of Low-Latency Services with Time-Sensitive Networking. *IEEE Communications Standards Magazine*, 2(2):48–54, jun 2018.

[SWFR12] Edmund O Schweitzer, David Whitehead, Ken Fodero, and Paul Robertson. Merging SONET and Ethernet Communications for Power System Applications. *SEL Journal of Reliable Power*, 3(2), 2012.

[TEM+05] C.W. Taylor, D.C. Erickson, K.E. Martin, R.E. Wilson, and V. Venkatasubramanian. WACS-Wide-Area Stability and Voltage Control System: R&D and Online Demonstration. *Proceedings of the IEEE*, 93(5):892–906, may 2005.

[TKC09] D. Tholomier, H Kang, and B Cvorovic. Phasor measurement units: Functionality and applications. In *2009 Power Systems Conference*, pages 1–12. IEEE, mar 2009.

[T.S05] Pradeep K. Gangadharan T.S. Sidhu. Control and automation of power system substation using IEC61850 communication. In *Proceedings of 2005 IEEE Conference on Control Applications, 2005. CCA 2005.*, pages 1331–1336. IEEE, 2005.

[TVD+11] Vladimir Terzija, Gustavo Valverde, Deyu Cai, Pawel Regulski, Vahid Madani, John Fitch, Srdjan Skok, Miroslav M Begovic, and Arun Phadke. Wide-Area Monitoring, Protection, and Control of Future Electric Power Networks. *Proceedings of the IEEE*, 99(1):80–93, jan 2011.

[VBLS15] Ceeman B. Vellaithurai, Saugata S. Biswas, Ren Liu, and Anurag Srivastava. Real time modeling and simulation of cyber-power system. *Power Systems*, 79:43–74, 2015.

[VRSG18] Harsh Vardhan, R Ramlachan, Wojciech Szela, and Edward Gdowik. Deploying digital substations: Experience with a digital substation pilot in North America. In *71st Annual Con-*

*ference for Protective Relay Engineers, CPRE 2018*, volume 2018-Janua, pages 1–9. IEEE, mar 2018.

[VSH16] Venkatesh Venkataramanan, Anurag Srivastava, and Adam Hahn. Real-time co-simulation testbed for microgrid cyber-physical analysis. In *2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, pages 1–6. IEEE, apr 2016.

[WA11] Craig Wester and Mark Adamiak. Practical applications of Ethernet in substations and industrial facilities. In *2011 64th Annual Conference for Protective Relay Engineers*, pages 67–78. IEEE, apr 2011.

[WHU12] Jun Wen, Craig Hammond, and Eric A. Udren. Wide-area Ethernet network configuration for system protection messaging. In *2012 65th Annual Conference for Protective Relay Engineers*, pages 52–72. IEEE, apr 2012.

[WYB15] Yannan Wang, Pradeep Yemula, and Anjan Bose. Decentralized Communication and Control Systems for Power System Operation. *IEEE Transactions on Smart Grid*, 6(2):885–893, mar 2015.

[XVS+14] George Xylomenos, Christopher N. Ververidis, Vasilios A. Siris, Nikos Fotiou, Christos Tsilopoulos, Xenofon Vasilakos, Konstantinos V. Katsaros, and George C. Polyzos. A Survey of information-centric networking research. *IEEE Communications Surveys and Tutorials*, 16(2):1024–1049, 2014.

[YHP+12] Yi Deng, Hua Lin, A. G. Phadke, S. Shukla, J. S. Thorp, and L. Mili. Communication network modeling and simulation for wide area measurement applications. In *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1–6, Jan 2012.

[YQST13] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges. *IEEE Communications Surveys & Tutorials*, 15(1):5–20, 2013.

# Part II

# Included Papers

# PAPER A

## Communication Network Modeling for Real-Time HIL Power System Protection Test Bench

C. M. Adrah, Z. Liu , Ø. Kure, H. Kr. Høidalen,

IEEE PES PowerAfrica, Accra, Ghana, 27–30 June 2017, pp. 1–6

# PAPER B

## Experimental validation of a new impedance based protection for networks with distributed generation using co-simulation test platform

K. Pandakov, C. M. Adrah, H. K. Høidalen and Ø. Kure,

IEEE Transactions on Power Delivery. doi: 10.1109/TPWRD.2019.2935834

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



# Experimental validation of a new impedance based protection for networks with distributed generation using co-simulation test platform

Konstantin Pandakov, Charles M Adrah, Hans Kristian Høidalen, Øivind Kure

***Abstract*—Combined real-time hardware-in-the-loop simulations and modeling of communication networks (co-simulation platforms) is a powerful testbed for development and validation of relay protection schemes utilizing communication links especially for applications in Smart Grids. This paper introduces laboratory tests in such environment of a new protection scheme for medium voltage networks with distributed generation. It is based on impedance measurements with compensation of remote infeed currents and high fault resistances. Since the scheme utilizes multi-terminal measurements, a communication network emulator has been developed to model Ethernet network impairments. The test method uses Monte-Carlo approach for evaluation of protection dependability. The results demonstrate enhancement of impedance relay performance compared to the conventional protection. Moreover, fault location capability is preserved with sufficient accuracy. Nevertheless, communication network imperfections, such as jitters and data loss, deteriorate scheme functionality.**

***Index Terms*—co-simulation testbed, distributed generation, HIL, IEC 61850, impedance relaying**

## I. Introduction

EXTENSIVE penetration of distributed generation (DG) into distribution networks creates problems for correct operation of the conventional protection mainly based on overcurrent relays. It requires development of new schemes to provide secure network operation.

Impedance (or distance) protection in such case can be an advantageous solution as showed in [1]. [2] demonstrates feasibility of impedance relaying in an actual distribution network. Moreover, it is already a typical practice in several countries [3]. Nevertheless, it is prone to malfunctioning due to underreaching in presence of remote infeed currents from DG and high impedance faults. Hence, the main scope of this study is to present solution for this issue to improve performance of this type of protection in distribution networks.

Impedance protection underreaching was thoroughly investigated in literature with respect to the transmission network where impedance protection is typical. Methods utilizing only local measurements [4]–[9] are of interest since communication technologies and additional equipment is not involved. The methods are aimed at elimination of under- and overreaching issues and offer adaptive settings or error compensation. The main outcome of the methods is possibility to estimate distance to faulty point on the line.

Increased dependability and more accurate results on fault location can be achieved utilizing two-end measurements [4], [10]–[13]. At the same time, synchronized measurements are not necessarily used [12]. A method can also be based on non-fundamental harmonics as in [13].

Special attention is paid to protection of a line between two buses with intertie connection (the third bus) due to difficulties in fault location. Thus, [14] offers adaptive characteristics based on one-end measurements, [15] proposes the scheme utilizing two-end measurements and [16] uses Direct Underreaching Transfer Trip scheme with measurements available from all three terminals. Extensive application of communication links and synchrophasors in a multi-terminal transmission network is considered in [17].

Implementation of these schemes in distribution networks can be problematic because they were mainly developed for high voltage systems with simple configuration (two or three buses), whereas medium voltage (MV) networks have complex topology: several feeders at one substation, side branches and multi-tapped load outfeeds on each feeders, embedded generators. Additionally, performance can also be affected due to: phase of distribution line impedance can reach $45^0$ (unlike transmission systems where resistive part is small); fault impedance can be up to several kilo-ohms in case of falling trees [18] (in transmission systems it is typically negligible).

Differential protection schemes can successfully be implemented in distribution networks with DG, for instance [19]; however, information about fault location cannot be provided as with impedance relaying. Furthermore, impact of load currents and current transformer saturation requires careful analysis.

Thus, having advantages of impedance relaying in MV networks, solutions for elimination of its malfunctioning are necessary for development and involvement of communication links facilitates this task. Reference [20] proposes the scheme based on differential impedance (two-point measurements), [21] presents accurate estimation of distance to fault in presence of DG infeed currents, adaptive settings are examined in [22], and [23] studies compensation of DG impact on fault location. One of the shortages here is assumption that the communication networks utilized for realization of the methods are

K. Pandakov is with Department of Electric Power Engineering, Norwegian University of Science and Technology (NTNU), Trondheim, NO-7491 Norway, e-mail: konstantin.pandakov@ntnu.no.

C. M. Adrah is with Department of Information Security and Communication Technology at NTNU, e-mail: charles.adrah@ntnu.no

H. Kr. Høidalen is a professor in NTNU at Department of Electric Power Engineering, e-mail: hans.hoidalen@elkraft.ntnu.no

Ø. Kure is a professor in NTNU at Department of Information Security and Communication Technology, e-mail: okure@ntnu.no

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



ideal, whereas their impact on protection dependability and security is also required to be considered, as for example in [24]. In general, studies in this direction are still lacking.

The current paper, firstly, proposes a new communication-based impedance protection scheme applicable for multi-tapped distribution networks with DG typical for Norway (small-scale hydro power plants). The scheme is capable of compensation of under-reaching errors of impedance measurements caused by remote infeeds and high fault impedances during phase-to-phase faults (with ground path as well if high impedance system grounding is used) utilizing multi-terminal measurements (required, at least, from DG locations). Secondly, this work demonstrates its laboratory verification using real-time (RT) hardware-in-the-loop (HIL) tests. To improve quality and precision of standard HIL tests, a communication emulator has been developed to run together with the RT HIL testbed and to study impact of communication network impairments on overall protection dependability. Furthermore, to evaluate applicability for a real network, a complex network model has been developed for tests to take into account load variations and imbalances. Thus, a new protective scheme can be assessed in close to real-life conditions.

The rest of the paper is organized as follows: Section II briefly outlines the developed compensation strategy (2 particular cases); Section III presents the laboratory co-simulation platform for testing of the protection scheme that includes the real time simulator OPAL-RT®, ABB impedance relay RED 670® and the communication network emulator; the network model with several load points and DG is described in subsection III-A; functionalities and model algorithms of the network emulator are listed in subsection III-B; Section IV introduces the test method including Monte-Carlo simulations for evaluation of method dependability for different conditions; Section V contains the test results with discussions.

## II. Overview of Communication-Based Impedance Protection Scheme

A new protection scheme is based on impedance measurements with compensation of errors caused by DG infeed currents and/or high fault impedance. Calculation of impedance errors requires measurements from an embedded generator (typically synchronous) and/or from a remote relay. Depending on network configuration, two cases can be considered.

### *A. Equivalent line approach (ELA) for compensation of impedance errors*

A part of a network between an impedance relay and a remote measuring point (e.g. DG) is passive and has only load outfeeds. In such case, this part before fault is represented as an equivalent line with impedance calculated as $z = (U^{\text{pre}} - U_r^{\text{pre}})/I^{\text{pre}}$, see Fig.1. Here, $U$ and $I$ are phase-to-phase voltage and current respectively, 'pre' denotes prefault conditions and 'r' – remote measurements. Hereafter, phasor quantities are implied. Fault produces an additional node on the equivalent line with voltage $U_{\text{err}}$ that is derived from set of equations:

$$\begin{cases} U - U_{\text{err}} = Izk \\ U_r - U_{\text{err}} = I_r z(1-k) \end{cases} \qquad U_{\text{err}} = \frac{UI_r + U_r I - zII_r}{I + I_r}, \quad (1)$$

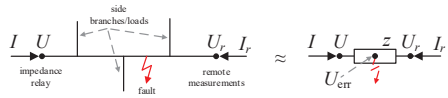



Fig. 1: Example network topology for application of ELA (to the left) and its equivalent (to the right).

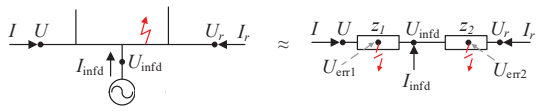



Fig. 2: Example network topology for application of ENA with one infeed source (to the left) and its equivalent (to the right).

where $k$ represents relative distance from the relay to the fault. Current directions are towards the network. The following compensation method of impedance measurements has been proposed:

$$Z_{\text{cps}} = \frac{U - U_{\text{err}}}{I}, \quad (2)$$

where $Z_{\text{cps}}$ is the compensated phase-to-phase impedance calculated by the relay and used for tripping decision. Hereafter, it is assumed that $Z_{\text{cps}}$ is separately calculated for phases a-b, b-c, and c-a.

### *B. Equivalent network approach (ENA) for compensation of impedance errors*

In this approach, a part of a network between two measuring points is active, that is infeed current from DG is present, see Fig.2. As a result, two passive parts of the network before and after infeed point can be represented for pre-fault conditions as equivalent lines with impedances $z_1 = (U^{\text{pre}} - U_{\text{infd}}^{\text{pre}})/I^{\text{pre}}$ and $z_2 = (U_r^{\text{pre}} - U_{\text{infd}}^{\text{pre}})/I_r^{\text{pre}}$, where $U_{\text{infd}}$ and $I_{\text{infd}}$ are measured voltage and current at the infeed source. In this case, two probable faulty nodes can exist with voltage error $U_{\text{err1}}$ or $U_{\text{err2}}$ on each line that can be calculated using the same approach as in (1):

$$U_{\text{err1}} = \frac{U(I_r + I_{\text{infd}}) + U_{\text{infd}} I - z_1 I(I_r + I_{\text{infd}})}{I + I_r + I_{\text{infd}}} \quad (3)$$

$$U_{\text{err2}} = \frac{U_r(I + I_{\text{infd}}) + U_{\text{infd}} I_r - z_2 I_r(I + I_{\text{infd}})}{I + I_r + I_{\text{infd}}}, \quad (4)$$

The smallest among these two determined upon phasor magnitudes is chosen to avoid overcompensation. If $U_{\text{err1}}$ is chosen from the minimum condition, then voltage error in equation (2) is equal to $U_{\text{err}} = U_{\text{err1}}$. If $U_{\text{err2}}$ is chosen, then an additional voltage drop on equivalent line $z_2$ caused by DG infeed current must be considered and then voltage error is:

$$U_{\text{err}} = U_{\text{err2}} + kz_2 I_{\text{infd}} = U_{\text{infd}} - \frac{I}{I_r}\left(U_{\text{err2}} - U_r + I_r z_2\right) \quad (5)$$

Equally, measurements at the infeed source can be taken as $U_r$ and $I_r$ in equations (3)-(5), then the remote measurements become $U_{\text{infd}}$ and $I_{\text{infd}}$. Having possibility of such swap, two

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



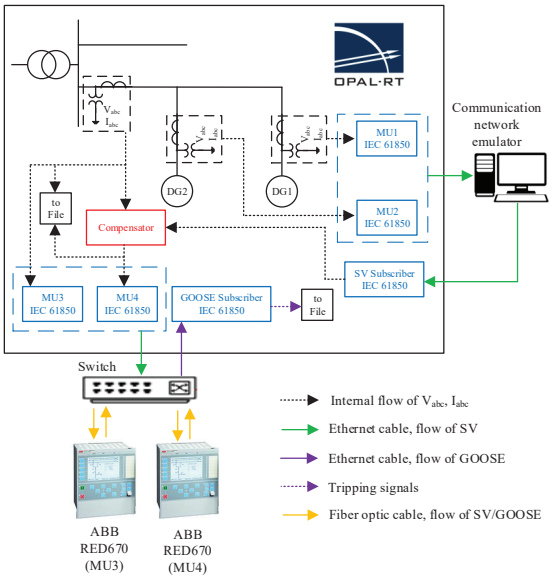



Fig. 3: Laboratory co-simulation testbed: the hardware-in-the-loop testing platform with emulator of communication links.

voltage errors $U_{\text{err}}$ for compensation (2) appear. A minimum value (upon magnitude) must be chosen to avoid overcompensation and to increase fault location precision.

General case with several infeed sources and more details can be found in previous work [25].

### C. Start conditions for compensation

Voltage error $U_{\text{err}}$ is equal to zero during normal conditions in the network, whereas it is nonzero during fault situation recognized upon fulfillment of three conditions together:

1) impedance magnitude measured at relay location falls below a threshold: 80% of what was measured 40 ms ago (two periods). It is expressed as $|U/I| < 0.8|U^{\text{pre}}/I^{\text{pre}}|$.
2) rate of change of this impedance $\frac{\delta|U/I|}{\delta t}$ over the last 5 samples is less than -1 Ohm/ms. Fast collapse indicates a fault.
3) the real part of the impedance is positive that indicates downstream fault (a directional element), real$(U/I) > 0$.

## III. Laboratory Test Setup

Fig.3 shows the full laboratory setup for verification of the proposed method. The previously developed hardware-in-the-loop testing platform [26] is expanded with a communication network emulator [27]. Real time simulations of the network with the DG are executed in OPAL-RT® with 50 $\mu$s time step.

Detailed description of the model with 2 embedded generators and fault scenarios are given in the next subsection.

Three-phase voltage and current measurements at the generators and the substation are formed as sample values (SV) in the merging units (MU) using the standard IEC 61850. SV measured at the substation are directly sent to ABB relay RED 670® via MU3 in order to examine impact of the DG on impedance measurements. SV measured at the generators (MU1-2) are sent to the communication network emulator. It models constant time delays, jitters, data loss and background traffic in the SV flows imitating real time communication links (more details are given in subsection III-B). The emulator sends the obtained SV back to the real time simulator (SV Subscriber). The MUs and the subscribers have 4 kHz sampling rate, quality of SVs is set as good.

The compensator accomplishes calculations described in section II, namely: it determines phasors utilizing the obtained SV from the substation and both generators, calculates $U - U_{\text{err}}$ and converts it into an instantaneous signal. This signal together with the measured current at the substation are formed as SV in MU4 and sent to another impedance relay with the same configuration.

In this work, time stamp on SV is not applied assuming unavailability of GPS signal (non-synchronized measurements). Thus, the compensator takes into account known permanent latencies $t_d$ of the remote measurements superimposed by the emulator: $t_d = 3$ ms for DG1 and $t_d = 2$ ms for DG2 have been chosen based on DG remoteness.

Thus, responses (missing or presence of the tripping signals) of the relays with and without compensation are compared: they send GOOSE messages back to the real time simulator (GOOSE Subscriber). The tripping signals and the SV are written to file for further off-line analysis.

The relay settings have Zone 1 not reaching the DG units to allow keeping the feeder alive during DG internal faults and Zone 2 covering the whole feeder and providing backup protection. Zone 1 has positive sequence impedance 13.5+13.5i Ohm with 20 ms time delay for coordination with load fuses; Zone 2 has 20.5+20.5i Ohm. Its time delay must be bigger than breaking operation at the DG units; however, for simplicity and test quickness, 40 ms is set. The zones' boundaries are depicted in Fig.4. The quadrilateral relay characteristics have forward direction and preset fault resistance 10 Ohm because expected maximal arc resistance estimated on Warrington's formula [28] is 7.5 Ohm.

### A. Test case network

The test case network is illustrated in Fig.4. The network configuration is specially designed to study impact of load points and infeed current sources (as well as their remoteness from the impedance relay) on both compensation approaches. The network model has been realized in Matlab Simulink®, and all model parameters, described in Table I, are taken from a real Norwegian distribution network (modelled network size is comparable with the real).

Lines 'TL' are modeled as PI-equivalents due to short line lengths and interest in slow transients (up to 1 kHz).

Loads 'Ld' have a random level of active power $P$ and imbalance. Load imbalance at the given load point is modeled as phase-to-phase loads with values equal to 100%, 80% and 120% (between randomly determined phases) from $P/3$. Each load point is independently determined. Thus, overall load profile and imbalance on the feeder alternates. Phase voltage

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



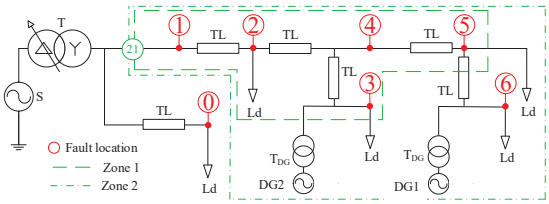



Fig. 4: The test case network.

TABLE I: Network parameters.

| | Matlab Simulink model name: parameters |
|---|---|
| S | Three-Phase Source: 66 kV, 50 Hz, 0.055 H (source inductance) |
| T, $T_{DG}$ | Three-Phase Transformer (Two Windings): 50 Hz, Rm=500 pu, Lm=500 pu (ideal model)<br>T: 20 MVA, Winding 1 [66 kV 0.0045 pu 0.09739 pu], Winding 2 [22·1.05 kV 0.0045 pu 0.09739 pu]<br>$T_{DG}$: 3 MVA, Winding 1 [6.6 kV 0.0066 pu 0.06336 pu], Winding 2 [22 kV 0.0066 pu 0.06336 pu] |
| TL | Three-Phase PI Section Line: 50 Hz, [r1 r0]=[0.36 0.5] Ohms/km, [l1 l0]=[1.146 5.093] mH/km, [c1 c0]=[10.137 4.794] nF/km, length 10 km |
| Ld | Three-Phase Parallel RLC Load: Delta configuration, 22 kV, 50 Hz, power factor 0.98, Qc=0, total active power is randomly set as 1 MW, 2 MW or 3 MW, 80% imbalance (see description below) |
| DG1,2 | Synchronous Machine: 3 MVA, 6.6 kV, 50 Hz, [Xd Xd' Xd" Xq Xq" Xl]=[2 0.22 0.2 1.4 0.2 0.18] pu, [Tdo' Tdo" Tqo"]=[4 0.025 0.1] s (open circuit), Rs=5e-3 pu, [H(s) F(pu) p]=[1 0 2]<br>Excitation System: IEEE type 1 (default parameters), Hydraulic Turbine and Governor: default parameters |

unbalance in the network does not exceed 2% according to EN50160. Randomness is realized using block 'Random Source' with uniform distribution and not repeatable automatic initial seed.

The interconnected generators are operated with zero reactive power production (unit power factor).

Phase-to-phase permanent faults are applied in 7 different locations as shown in Fig.4 with detectable low resistance (an arc with 10 Ohm) and undetectable high resistance (an extraneous object with 50 Ohm causing intentional relay underreach).

### *B. Communication network emulator*

Testing of protection algorithms utilizing inter-substations or even wide area networks requires modeling of communication network impairments to study their impact on overall performance. At the same time, OPAL-RT® has limited capabilities for these purposes. Thus, the communication emulator is proposed to be used together with the RT simulator to mirror behavior and characteristics of communication network properties that tend to have effects in the real-world applications.

The core functionality is to emulate communication network infrastructure between several distant relays exchanging GOOSE/SV packets or messages (fibre-optic point-to-point connections between the substations) so that the communication properties between source relays and destination relays can be varied. These properties are regarded as impairments in the network and include delays, jitters, packet losses, packet corruptions, bandwidth restriction. Additionally, the emulator as a software router can direct packets to actual existing routers and other network elements such as switches, bridges and hubs for integration into real networks. Hence, the emulator is also used to achieve different queuing schemes with different priorities, as well as different router scheduling algorithms.

Network impairments applied in the current work are as follows:

*1) Random delay emulator element:* It is used to emulate jitters and the input is a specific range for random delays expressed further in the paper using DG permanent latency $t_d$. Jitters are referred to as variations in latency of data packets. Two jitter levels are used in the tests: 1) the low level when an actual delay is between $t_d$ and $1.5t_d$); 2) the high level when an actual delay is between $t_d$ and $2t_d$. Normal distribution is used.

*2) Burst packet drop emulator element:* It is used to emulate packet losses. It drops a consecutive number of packets with a given probability. The input is a number of consecutive packets to drop and a probability. Similarly, two data loss levels are used: 1) the low level where 10% on average of packets sending during 1 s are lost; 2) the high level where 20% on average of packets are lost during the same period.

*3) Influence of background traffic and network dimension:* The generated SV of MU1 and MU2 is sent through the emulator combined with a VLAN enabled switch network (HPE 1920) to the OPAL-RT® simulator. A separate background traffic generated as a User Datagram Protocol (UDP) video source is added to the network traffic mix. The network configurations utilizes the IEEE 802.1Q and IEEE 802.1p priority tagging to investigate how prioritizing the background traffic will affect the performance of the received SV from MU1 and MU2.

## IV. Test Method

In order to evaluate dependability and security of the tested protection scheme, a Monte Carlo simulation approach is used that applies several consecutive faults in arbitrary set conditions. The following repeatable sequence with a three-seconds period is utilized for each new fault:

- A random source sets load power $P$ and a separate random source (with different seed) determines phases where load imbalance takes place. Settings are applied to all load points independently with their own random sources.
- After end of the transient period caused by load variation (2 s), a fault is initiated between two randomly determined phases. A different random source determines fault resistance: 10 Ohm or 50 Ohm.
- After another 100 ms the fault is cleared followed by a relaxation period of 900 ms.

Thus, the performed compensation techniques can be applied for different fault parameters and network conditions.

In equations (2) - (5), $U$ and $I$ are always measured at the main substation for device number 21 in Fig.4. $U_r$, $I_r$, $U_{\text{infd}}$, $I_{\text{infd}}$ can belong to either DG1 or DG2 depending on a case below.

The following scenarios are studied:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



- Case 1: no communication impairments are introduced. DG permanent latencies are taken into account by the compensator.
  - Case 1a: test of equivalent network approach (ENA, section II-B). $U_{\text{infd}}$ and $I_{\text{infd}}$ are measured at DG1 (the source of infeed), $U_r$ and $I_r$ are at DG2 (a remote end). 100 consecutive faults are simulated.
  - Case 1b: ENA where $U_{\text{infd}}$ and $I_{\text{infd}}$ are measured at DG2, and $U_r$ and $I_r$ are at DG1 (100 faults).
  - Case 1c: equivalent line approach (ELA, section II-A). $U_r$ and $I_r$ are measured at DG2, and DG1 is disconnected from the grid (100 faults).
  - Case 1d: ELA where $U_r$ and $I_r$ are measured at DG1, and DG2 is disconnected (100 faults).

  Cases 1a-d are repeated for all 7 fault locations, in total 2800 faults for Case 1 have been simulated. Cases 1c and 1d are used to analyze impact of network configuration on ELA fault location precision. Cases 1a and 1b are used for the same purpose for ENA, as well as to verify validity of the criterion for infeed source selection discussed in subsection II-B.
- Case 2 simulates communication link imperfections – the low and the high level of either jitters or data losses. The compensator still applies the predefined DG permanent latencies.
  - Case 2a: ENA with the low (50 faults) and the high (50 faults) jitter level. Infeed source either DG1 or DG2 is automatically specified using the criterion discussed in subsection II-B.
  - Case 2b: ENA with the low (50 faults) and the high (50 faults) data loss level.
  - Case 2c: ELA with disconnected DG1 for the low (50 faults) and the high (50 faults) jitter level.
  - Case 2d: the same as in 2c, but for the low (50 faults) and the high (50 faults) data loss level.
  - Case 2e: repeats 2c, but with disconnected DG2 instead of DG1.
  - Case 2f: repeats 2d, but with disconnected DG2 instead of DG1.

  For analysis, three extreme fault location have been chosen - 1, 3, and 6. In total 1800 faults for Case 2 have been simulated.
- Case 3 studies impact of background traffic on SV delays and packet losses. Faults are not simulated because impact on protection is seen from Case 2. The practical Ethernet switch used in tests has a priority mapping of class of service queues ('pcp' in the text) and the following have been chosen to test: pcp 1 categorizing traffic types as background, pcp 2–best effort and pcp 3–critical applications. Since SV are the time critical traffic, they were tagged with pcp 3. The background traffic was then varied in the network with pcp 1, 2 and 3. Two video files of 3MB and 10MB were used for the tests. Maximum sending speed for them through 1 Gbps Ethernet is 480 Mbps and 710 Mbps correspondingly.

Finally, percentage of successful tripping among all faults in a specific case can be calculated.

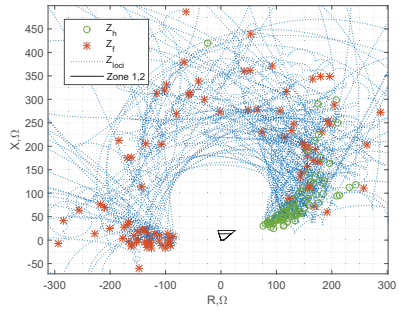



Fig. 5: The impedance loci of faults at location 0 (the adjacent feeder) in test case 1a.

TABLE II: Percentage of successful tripping for Case 1a, 1b.

| | FL[1] | Low-ohmic faults | | | | High impedance faults | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | w/o cps[2] | | with cps[3] | | w/o cps | | with cps | |
| | | Z1[4] | Z2[5] | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 |
| Case 1a | 1 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 2 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 3 | 4 | 2 | 82 | 100 | 0 | 0 | 58 | 100 |
| | 4 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 5 | 83,7 | 87,8 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 6 | 0 | 15,7 | 74,5 | 100 | 0 | 0 | 65,3 | 100 |
| Case 1b | 1 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 2 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 3 | 22,9 | 10,4 | 100 | 100 | 0 | 0 | 96,2 | 100 |
| | 4 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 5 | 96,4 | 100 | 96,4 | 100 | 0 | 0 | 95,6 | 100 |
| | 6 | 0 | 26,5 | 16,3 | 100 | 0 | 0 | 11,8 | 100 |

[1]fault location, [2]without compensation, [3]with compensation, [4]Zone 1, [5]Zone 2.

## V. Results and Discussions

### A. Case 1

*1) Case 1a and 1b:* Firstly, Fig.5 demonstrates impedance loci of faults in the adjacent feeder (location 0) for test case 1a. $Z_{h,f}$ denotes steady-state healthy and faulty impedance correspondingly; upward power flow from the DG can be seen as the negative real part of $Z_f$. Sympathetic tripping (unnecessary disconnection of the healthy feeder) during the tests has not been registered: all impedance loci are out of zones' reach.

Hereafter, this location is out of interest and excluded from the following analysis because tripping signal is not produced by the investigated relay. Security of the protection is not jeopardized because compensator cannot be initialized due to conditions 1 - 3 in section II-C.

Table II shows calculated percentages of successful tripping in test cases 1a and 1b for fault location 1-6 and two different fault resistances compared to relay performance without the compensation strategy.

The colored cells highlight indices indicating problems: red (relay without compensation) or pink (with) shows decreased dependability (less than 100%), orange - decreased security (higher than 0).

It is seen that low-ohmic fault in location 1,2,4 is reliably detected without compensation in both test cases; however, blinding is observed for high impedance fault because all

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



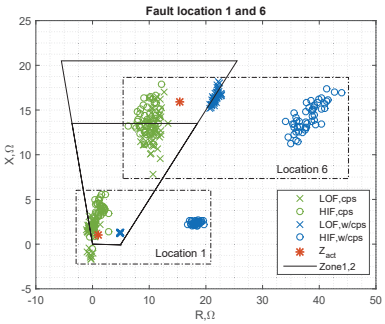



Fig. 6: The measured steady-state fault impedances for low-ohmic (LOF) and high impedance faults (HIF) at location 1 and 6 with compensation (cps) and without (w/cps).

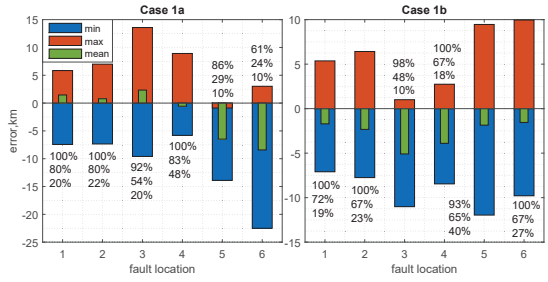



Fig. 7: Fault location errors for Case 1a and 1b (LOF).

locations and cases have 0. At the same time, application of the compensation methods resolves this issue.

We can clearly observe from Table II that relay dependability without compensation is significantly decreased at locations next to the generators (3,5,6). Dependability with compensation is 100% for Zone 2 in all cases, whereas it is not for Zone 1 due to compensation errors that leads to delayed tripping (location 3 for Case 1a and 3,5 for Case 1b).

It is worth noting two main outcomes: 1) Zone 1 must not see faults at location 6 (see Fig.4), whereas in both cases percentage with compensation is not 0 (the orange cells). In other words, the compensated impedance might become smaller than an actual. Since it can lead to a situation when internal faults in DG1 cause unnecessary feeder tripping, the compensator must be blocked to maintain protection selectivity. It can be checked with the same conditions 1 - 3 in subsection II-C applied to measurements at the DG locations: if they are not fulfilled (current is measured towards the monitoring zone), the compensation is not used for the feeder relay; 2) performance of the compensation method in Case 1a is slightly better than in Case 1b for location 5, whereas it is considerably worse for location 3 and 6. As it will be shown further, it is linked with fault location accuracy.

Finally, protection with compensation demonstrates faster operation time: mean value is 40 ms for Zone 1 and 60 ms for Zone 2 irrespectively of fault location and resistance. Without compensation, it can reach 90 ms for problematic locations 3, 5, and 6.

Fig.6 demonstrates the reason for poor relay dependability without compensation and improvements applying ENA (Case 1a is considered) for close-in fault location 1 and far-end location 6. It is seen from the figure that all high impedance faults (HIF) without compensation are out of the zones' reach. Zone 1 can handle all low-ohmic faults (LOF) at close-in location, whereas Zone 2 cannot detect all faults at far-end location due to impact of the DG. '$Z_{act}$' denotes an actual fault impedance. The compensated impedances are inside the zones and they have inherent errors with bigger dispersion due to influence of variable network conditions that is the reason of dependability and security issues in Table II. Though for location 1 not all $Z_{cps}$ are in Zone 1, a corresponding locus crosses it and, therefore, the tripping signal appears.

The main advantage of the strategy compared to differential protection is preserving of fault location capability. It is seen from Fig.6 that $Z_{cps}$ for location 1 and 6 are distinguishable, and it is of interest to analyze impact of the compensation on fault location accuracy for all cases.

There are many different approaches for fault location calculation in distribution networks with distributed generation. In this paper, we use a simple one based on the imaginary part of the compensated impedance discussed in [29]. Combination of the compensation strategy with more complex locating algorithms is out of the scope of this paper.

Error in kilometers can be calculated as $\text{imag}(Z_{cps} - Z_{act})/\text{r1}$, where $\text{r1} = 0.36$ Ohm/km (Table I), and $Z_{cps}$ is registered when the tripping signal from Zone 1 or 2 appears, or just a steady-state value if no response is present.

Fig.7 illustrates maximum, minimum and mean errors for 6 fault locations. LOF is considered because it has better precision. For better insight, number of fault incidents (in % from the total) that have a given precision are given alongside: the upper value is precision $\pm 10$ km, the middle is $\pm 5$ km and the lower is $\pm 2$ km.

It can be seen from the plots that the precision for remote locations 5 and 6 is better (compare corresponding indices and mean values) for Case 1b, whereas Case 1a demonstrates better accuracy for location 3. At the same time, average $U_{err}$ for Case 1a is less than for Case 1b during fault at location 3, and it is less for Case 1b for fault at location 5 and 6. Thus, such criterion based on minimum $U_{err}$ (discussed in subsection II-B) can be applied for infeed selection because it provides higher $Z_{cps}$ and, consequently, better fault location accuracy.

To summarize, the presented results in Table II (the pink and orange cells) and in Fig.7 are in good agreement with theoretical expectations: if DG1 is a source of infeed (Case 1a), then locations 5 and 6 are seen as location 4 that gives better dependability and worse security because location 4 is in Zone 1. However, it leads to bigger fault location errors with a negative sign. At the same time, location 3 is detected with some errors leading to the decreased dependability. The opposite is true if an infeed source is DG2 (Case 1b): location 3 is seen as 4 (therefore errors are higher and dependability is better), and 5 and 6 have better location precision (therefore worse dependability and better security).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



TABLE III: Percentage of successful tripping for Case 1c, 1d.

| FL | | Low-ohmic faults | | | | High impedance faults | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | w/o cps | | with cps | | w/o cps | | with cps | |
| | | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 |
| Case 1c | 1 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 2 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 3 | 74,4 | 67,4 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 4 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 5 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 6 | 0 | 97,7 | 100 | 100 | 0 | 0 | 100 | 100 |
| Case 1d | 1 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 2 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 3 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 4 | 100 | 100 | 100 | 100 | 0 | 0 | 100 | 100 |
| | 5 | 100 | 100 | 100 | 100 | 0 | 0 | 95,8 | 100 |
| | 6 | 0 | 5,7 | 45,3 | 100 | 0 | 0 | 36,2 | 100 |

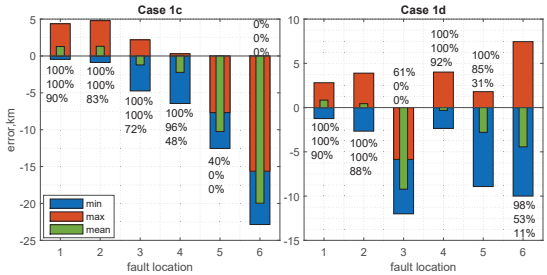



Fig. 8: Fault location errors for Case 1c and 1d (LOF).

*2) Case 1c and 1d:* Table III shows relay dependability in test cases 1c and 1d. Case 1c shows impact of DG2 (DG1 is disconnected) on relay performance without compensation. As a consequence, dependability reduction is seen for fault location 3,6 and HIF gives 0 as in the previous cases. Case 1d illustrates impact of DG1 seen for location 6. Compensation entirely improves indices for Case 1c, whereas HIF at location 5 has some difficulties for detection by Zone 1 in Case 1d. In both cases, relay security is deteriorated for location 6 (non zero indices for Zone 1). The same point about compensation blocking as in the previous cases is applied here. Finally, protection with compensation is also faster.

Fig.8 shows fault location errors. Case 1c has bigger errors for location 5,6 than Case 1d (zero indices mean large error), but better precision for location 3. This is in agreement with theory because if DG1 is disconnected, then locations 5,6 are seen as 4 (therefore large negative errors in Case 1c) and location 3 is correctly determined; therefore, in Table III, security at location 6 is completely disrupted. If DG2 is disconnected, then the opposite situation arises: location 3 is seen as 4 with large negative error (Case 1d), better security at location 6 and worse dependability for 5 is due to better location accuracy.

To summarize, LOF or HIF inside the zone of protection are reliably detected (at least by Zone 2) with application of the equivalent line or network approach. The main advantage compared to differential protection is preserved fault location capability since errors of impedance measurements can be compensated especially for HIF. For both approaches, the main source of location errors is load currents that are not directly compensated by the given method of equivalences. Accuracy can be improved applying the compensated measurements and the methods discussed in [29].

TABLE IV: Percentage of successful tripping for Case 2a, 2b.

| FL | Level | Case 2a (jitters) | | | | Case 2b (data loss) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | LOF | | HIF | | LOF | | HIF | |
| | | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 |
| 1 | no[1] | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | low | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | high | 81,8 | 100 | 85,7 | 100 | 95,5 | 100 | 100 | 100 |
| 3 | no | 100 | 100 | 96,2 | 100 | 100 | 100 | 96,2 | 100 |
| | low | 3,3 | 76,7 | 5 | 65 | 100 | 100 | 100 | 100 |
| | high | 0 | 15 | 0 | 10 | 20,8 | 83,3 | 26,9 | 76,9 |
| 6 | no | 16,3 | 100 | 11,7 | 100 | 16,3 | 100 | 11,8 | 100 |
| | low | 0 | 53,8 | 0 | 62,5 | 82,6 | 95,7 | 11,1 | 100 |
| | high | 0 | 20,7 | 0 | 23,8 | 18,8 | 75 | 14,7 | 55,9 |

[1] no impairments.

TABLE V: Percentage of successful tripping for Case 2c, 2d.

| FL | Level | Case 2c (jitters) | | | | Case 2d (data loss) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | LOF | | HIF | | LOF | | HIF | |
| | | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 |
| 1 | no | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | low | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | high | 100 | 100 | 71,4 | 100 | 100 | 100 | 100 | 100 |
| 3 | no | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | low | 0 | 88,9 | 0 | 82,6 | 14,3 | 91,4 | 13,3 | 66,7 |
| | high | 0 | 50 | 0 | 0 | 42,9 | 100 | 41,4 | 96,6 |
| 6 | no | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | low | 27, 3 | 100 | 0 | 94,1 | 78,6 | 100 | 77,3 | 90,9 |
| | high | 0 | 38,5 | 0 | 0 | 78,3 | 100 | 66,7 | 96,23 |

## B. Case 2

This sections demonstrates impact of communication network imperfections, namely jitters and data packet loss, on performance of the compensation methods. Here, fault locations 1,3 and 6 are only considered as extreme points.

*1) Case 2a and 2b:* Table IV demonstrates performance of the compensation in test cases 2a and 2b compared to similar in Case 1 (without jitters and data loss). The pink colored cells show dependability deterioration compared with cases without communication network distortions, blue - affected security (location 6 only), and the green cells indicate improvements.

Jitter level rise (Case 2a) significantly aggravates relay dependability in locations 3 and 6. Analysis of fault location errors shows that it leads to compensated impedance increase (especially reactive part that deteriorates fault location accuracy) and, consequently, underreaching; therefore, for location 1, influence is not so prominent.

Data loss level rise (Case 2b) has also similar impact – relay dependability falls. Considerable influence is observed for location 3 and 6 for the highest probability.

Improvements are observed for protection security with jitter rise; however, worsening for data loss. At the same time, if the tripping signal appears, operation time is not affected by the communication impairments.

*2) Case 2c and 2d:* Table V shows results for impact of jitters and data loss in test cases 2c and 2d on the equivalent line approach with disconnected DG1. Comparison with the corresponding results in Case 1 are also present.

As it is possible to observe for location 1, dependability is less than 100% only for the high jitter level and HIF. Impact

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPWRD.2019.2935834, IEEE Transactions on Power Delivery



TABLE VI: Percentage of successful tripping for Case 2e, 2f.

| FL | Level | Case 2e (jitters) | | | | Case 2f (data loss) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | LOF | | HIF | | LOF | | HIF | |
| | | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 | Z1 | Z2 |
| 1 | no | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | low | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | high | 95,4 | 100 | 21,4 | 100 | 100 | 100 | 100 | 100 |
| 3 | no | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| | low | 14,8 | 92,6 | 0 | 69,6 | 69 | 100 | 9,5 | 85,7 |
| | high | 0 | 24,1 | 0 | 0 | 100 | 100 | 100 | 100 |
| 6 | no | 45,3 | 100 | 36,2 | 100 | 45,3 | 100 | 36,2 | 100 |
| | low | 0 | 38,9 | 0 | 3,1 | 34,5 | 93,1 | 23,8 | 90,5 |
| | high | 0 | 0 | 0 | 0 | 10,7 | 92,9 | 4,5 | 90,9 |

is less than in Cases 2a,b because only one communication channel is affected. More serious consequences from jitter and data loss level rise are seen for locations 3 and 6. At the same time, clear falling tendency is present with increase of jitter level (Case 2c); however, for data loss (Case 2d), this dependency is not revealed. Finally, location 6 has higher dependability indices due to the applied ELA: it is seen by the fault locating algorithm closer to location 4. In such case, communication network impairments have positive impact on security. Impact of communication link imperfections on location errors is the same as in the previous cases.

*3) Case 2e and 2f:* Table VI illustrates results for the same ELA as before but DG2 is disconnected. Here impact of the jitters on location 1 is seen even for LOF, and it is higher for HIF than in the previous case. The reason is that calculation errors increase with the distance between two measuring points.

Performance at location 3 is better (indices are higher) than in the previous case because location 3 is now seen as 4; however, impact of network impairments for location 6 is considerable compared to the previous case due to calculation errors of the applied ELA. Positive impact on security in such case is also higher.

To summarize, the main reason of dependability issues in the considered cases is the presence of errors during calculation of the compensated impedance caused by non-synchronized remote measurements or information losses. The analysis of cases with jitter level variation (Case 2a,c,e) can be useful for utilities for evaluation of protective scheme dependability and security in case of sudden loss of synchronizing signal or its unavailability (e.g. underground substations). Data losses have overall adverse effect on the protective schemes increasing relay underreach (Case 2b,d,f); therefore, communication network reliability must be sufficient with minimal packet losses. Finally, comparing results in test Case 2 and Case 1, it is possible to see that even with unreliable communication, protection performance with compensation is superior than without especially for HIF and for LOF in case of low level impairments.

### C. Case 3

Fig.9 shows results for test Case 3: end-to-end time delays as mean values over 400000 SV packets with the standard deviation (denoted as 'std') and percentage of lost packets measured between the substations for DG1 and DG2 merging units (MU1 and MU2 respectively) for the two background

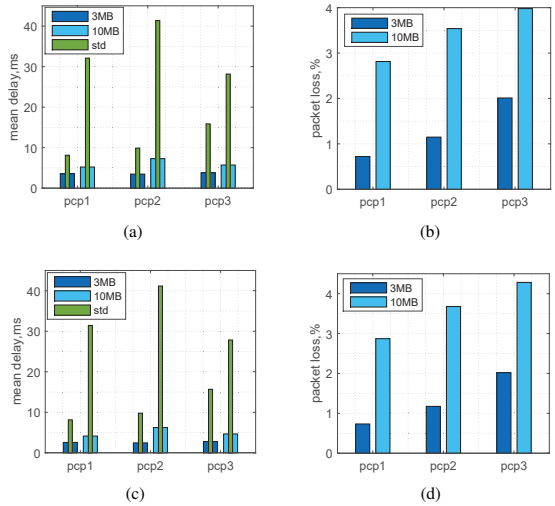



Fig. 9: Impact of 3MB and 10 MB background traffic set with priority (pcp) 1, 2 and 3 on a) end-to-end delays (MU1), b) percentage of lost packets (MU1), c) end-to-end delays (MU2), d) percentage of lost packets (MU2).

sources used in the tests, i.e. 3 MB (maximum 48% traffic occupancy) and 10MB (maximum 71% traffic occupancy) video file sizes, while varying the priority tags of the background traffic as previously explained.

It can be seen that the background traffic with different priority increases end-to-end delays because the mean values are higher than preset (3 ms for MU1 and 2 ms for MU2). Moreover, the 10MB video file as a background traffic source resulted in a generally higher increase in average network delays and standard deviation compared to the 3MB video file. Setting the background traffic with different priority tags has resulted in different packet delay variations; however, a strict regularity is not observed due to randomness nature of packet delays.

Influence of the background traffic on packet losses is seen from Fig.9b and Fig.9d: the 10MB video background traffic generally resulted in more packet losses compared to the 3MB video file. Unlike the previous case, a correlation between pcp and lost packets is prominent. Thus, setting the background traffic as critical messages with pcp = 3, same as the SV traffic for DG1 and DG2, has resulted in the highest percentage of lost packets in the network for both background traffic cases, i.e. MU1 (2.01%, 3.98%) and MU2 (2.01%, 4.28%).

## VI. Conclusion

The current paper, firstly, presents a new communication-assisted impedance-based protective scheme for distribution grids with DG and, secondly, its comprehensive laboratory tests using the developed co-simulation platform that includes a real time hardware-in-the-loop testbed and a network emulator. The latter creates controlled communication network

parameters for protection testing in close to real life environment.

The protection scheme aims at elimination of underreaching errors during impedance measurements associated with DG and high impedance faults. It demonstrates promising results with ideal communication links improving dependability compared to the conventional distance relaying. The test results also reveal negative impact of communication network impairments, such as uncompensated jitters or data losses, leading to underreaching errors especially for far end fault locations. Hence, the main limitation of the developed protection scheme is communication links quality and reliability.

Though the tests show that unbalanced and dispersed load currents have impact on fault location accuracy, faulty points can be differentiated due to utilization of prefault measurements in the method and large synchronous generator fault currents exceeding load currents. The latter means that in networks with inverter-integrated DG fault location errors might be bigger, but since it leads to relay overreaching, protection scheme dependability should stay high. Further investigations in this direction are required.

ELA can only be applied for a passive network between two-point measurements (Fig.1). If a network becomes active, ENA is used (Fig.2) since multiple-point measurements are required. As it is seen from the analysis, the main disadvantage of both approaches is recognition of faults in lateral branches in false locations (on the feeder). If more precise fault discrimination is needed, additional measurements in these branches can be provided. Therefore, a large network with complex topology and scattered DG sources is divided into several zones of protection where ELA or ENA can be applied. In order to select a correct (i.e. that gives the best fault location precision) remote relay for calculation of $Z_{\text{cps}}$ in both approaches, the criterion of minimum $U_{\text{err}}$ or maximum $Z_{\text{cps}}$ must be applied. Finally, the results reveal that ELA demonstrates better fault location accuracy than ENA and less susceptibility to communication network imperfections, therefore it must be prioritized.

## REFERENCES


[1] A. Sinclair, D. Finney, D. Martin, P. Sharma. (2014). Distance Protection in Distribution Systems: How It Assists With Integrating Distributed Resources. *IEEE Transactions on Industry Applications. 50(3)*, pp. 2186 – 2196.

[2] K. Pandakov, H. Kr. Høidalen, J.I. Marvik, "Implementation of distance relaying in distribution network with distributed generation", *13th International Conference on Development in Power System Protection (DPSP)*, 2016, pp. 1 – 7.

[3] Joint Working Group B5/C6.26/CIRED. (2015) *Protection of Distribution Systems with Distributed Energy Resources*.

[4] M. M. Saha, J. Izykowski, E. Rosolowski, M. Bozek, "Adaptive Line Distance Protection with Compensation for Remote End Infeed", *IET 9th International Conference on Developments in Power System Protection (DPSP)*, 2008, pp. 1 – 6.

[5] V.H. Makwana, B. Bhalja. (2012). New digital distance relaying scheme for phase faults on doubly fed transmission lines. *IET Generation, Transmission & Distribution. 6(3)*, pp. 265 – 273.

[6] V. H. Makwana, B. R. Bhalja. (2012). A New Digital Distance Relaying Scheme for Compensation of High-Resistance Faults on Transmission Line. *IEEE Transactions on Power Delivery. 27(4)*, pp. 2133 – 2140.

[7] Y. Zhong, X. Kang, Z. Jiao, Z. Wang, J. Suonan. (2014). A Novel Distance Protection Algorithm for the Phase-Ground Fault. *IEEE Transactions on Power Delivery. 29(4)*, pp. 1718 – 1725.

[8] Z. Y. Xu, G. Xu, L. Ran, S. Yu, Q. X. Yang. (2010). A New Fault-Impedance Algorithm for Distance Relaying on a Transmission Line. *IEEE Transactions on Power Delivery. 25(3)*, pp. 1384 – 1392.

[9] Q. K. Liu, S. F. Huang, H. Z. Liu, W. S. Liu. (2008). Adaptive Impedance Relay With Composite Polarizing Voltage Against Fault Resistance. *IEEE Transactions on Power Delivery. 23(2)*, pp. 586–592.

[10] M.M. Eissa. (2006). Ground distance relay Compensation based on fault resistance calculation. *IEEE Transactions on Power Delivery. 21(4)*, pp. 1830 – 1835.

[11] T. G. Bolandi, H. Seyedi, S. M. Hashemi, P. S. Nezhad. (2015). Impedance-Differential Protection: A New Approach to Transmission-Line Pilot Protection. *IEEE Transactions on Power Delivery. 30(6)*, pp. 2510 – 2518.

[12] Z.Li, X. Lin, H. Weng, Z. Bo. (2012). Efforts on Improving the Performance of Superimposed-Based Distance Protection. *IEEE Transactions on Power Delivery. 27(1)*, pp. 186 – 194.

[13] C. J. Lee, J. B. Park, J. R. Shin, Z. M. Radojevie. (2006). A new two-terminal numerical algorithm for fault location, distance protection, and arcing fault recognition. *IEEE Transactions on Power Systems. 21(3)*, pp. 1460 – 1462.

[14] J. Ma, X. Xiang, P. Li, Z. Deng, J. S. Thorp. (2017). Adaptive distance protection scheme with quadrilateral characteristic for extremely high-voltage/ultra-high-voltage transmission line. *IET Generation, Transmission & Distribution. 11(7)*, pp. 1624 – 1633.

[15] Y. Lin, C. Liu, C. Yu. (2002). A new fault locator for three-terminal transmission lines using two-terminal synchronized voltage and current phasors. *IEEE Transactions on Power Delivery. 17(2)*, pp. 452 – 459.

[16] S. Sarangi, A. K. Pradhan. (2015). Adaptive Direct Underreaching Transfer Trip Protection Scheme for the Three-Terminal Line. *IEEE Transactions on Power Delivery. 30(6)*, pp. 2383 – 2391.

[17] N. A. Al-Emadi, A. Ghorbani, H. Mehrjerdi. (2016). Synchrophasor-based backup distance protection of multi-terminal transmission lines. *IET Generation, Transmission & Distribution. 10(13)*, pp. 3304 – 3313.

[18] N. I. Elkalashy, M. Lehtonen, H. A. Darwish, M. A. Izzularab, A. I. Taalab. (2007). Modeling and experimental verification of high impedance arcing fault in medium voltage networks. *IEEE Transactions on Dielectrics and Electrical Insulation. 14(2)*, pp. 1 – 9.

[19] H. Gao, J. Li, B. Xu. (2017). Principle and Implementation of Current Differential Protection in Distribution Networks With High Penetration of DGs. *IEEE Transactions on Power Delivery. 32(1)*, pp. 565 – 574.

[20] W. Huang, T. Nengling, X. Zheng, C. Fan, X. Yang, B. J. Kirby. (2014). An Impedance Protection Scheme for Feeders of Active Distribution Networks. *IEEE Transactions on Power Delivery. 29(4)*, pp. 1591-1602.

[21] S. Biswas, V. Centeno, "A communication based infeed correction method for distance protection in distribution systems", *North American Power Symposium (NAPS)*, 2017, pp. 1 – 5.

[22] J. Ma, J. Li, Z. Wang, "An adaptive distance protection scheme for distribution system with distributed generation", *5th International Conference on Critical Infrastructure (CRIS)*, 2010, pp. 1 – 4.

[23] J. I. Marvik, H. K. Høidalen, A. Petterteig, "Localization of short-circuits on a medium voltage feeder with distributed generation", *20th International Conference and Exhibition on Electricity Distribution (CIRED 2009) - Part 1*, 2009, pp. 1 – 4.

[24] A. C. Adewole, R. Tzoneva. (2017). Co-simulation platform for integrated real-time power system emulation and wide area communication. *IET Generation, Transmission & Distribution. 11(12)*, pp. 3019-3029.

[25] K. Pandakov, H. Kr. Høidalen. "Distance Protection with Fault Impedance Compensation for Distribution Network with DG", *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, pp. 1-6.

[26] Z. Liu, H. K. Høidalen. "An adaptive inverse time overcurrent relay model implementation for real time simulation and hardware-in-the-loop testing", *13th International Conference on Development in Power System Protection 2016 (DPSP)*, 2016, pp. 1-6.

[27] C. M. Adrah, Ø. Kure, Z. Liu, H. Kr. Høidalen. "Communication network modeling for real-time HIL power system protection test bench", *IEEE PES PowerAfrica*, 2017, pp. 1-6.

[28] V. D. Andrade, E. Sorrentino. "Typical expected values of the fault resistance in power systems", *Transmission and Distribution Conference and Exposition: Latin America (T&D-LA), 2010 IEEE/PES*, 2010, pp. 1-8.

[29] B. D. S. Jose, P. A. H. Cavalcante, F. C. L. Trindade, M. C. de Almeida. "Analysis of distance based fault location methods for Smart Grids with distributed generation", *IEEE PES ISGT Europe*, 2013, pp. 1-5.

# PAPER C

## A Methodology to Implement and Investigate Performance of Sampled Values for Wide-Area Protection

C. M. Adrah, Ø. Kure, J. R. A. K. Yellajosula, S. Paudyal, and B. Mork,

2018 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC), Kuala Lumpur, 2018, pp. 84-90.

# PAPER D

## An IP Multicast Framework for Routable Sample Value Communication in Transmission Grids

C. M. Adrah, J. R. A. K. Yellajosula, Ø. Kure, D Palma, and P. E. Heegaard,

Journal of Communications vol 14 (9) (2019) 765–772.

# An IP Multicast Framework for Routable Sample Value Communication in Transmission Grids

Charles M. Adrah[1], Jaya R. A. K. Yellajosula[2], Øivind Kure[1], David Palma[1], and Poul E. Heegaard[1]
[1] NTNU, Trondheim N-7491, Norway
[2] MTU, Houghton, Michigan - 49931, USA
Email: charles.adrah@ntnu.no

***Abstract*** —The growth and deployment of digital substations based on IEC 61850 in power utility industry will spawn new opportunities for wide area systems. These include monitoring, protection and control applications that will require suitable communication architectures and technologies. Techniques such as bridging and tunneling have been recommended for encapsulating and de-encapsulating messages between substations. These methods are however point-to-point solutions and are not suitable for wide area applications, involving multiple substations at the same time. In this paper, we propose using Protocol Independent Multicast- Source Specific Multicast (PIM-SSM), an IP multicast routing protocol for routable Sampled Value transmission in decentralized wide area systems. IP multicast is a technology tailored for one-to-many and many-to-many communications, such as wide area protection applications requiring multiple substations receiving R-SV messages in a single transmission from another substation in the power grid. We first show how PIM-SSM can be realized in a transmission grid communication network and present a qualitative analysis of effects on multicast when link failures occur. We then present a quantitative study to evaluate the performance of PIM-SSM, on selected communication network topologies. Our results show that the communication technology will play a critical role in efficient delivery of routable Sampled Value data in a multicast framework. Furthermore, they show that improvements in the networking infrastructure design leads to better performance of the multicast delivery.

***Index Terms***—IP Multicast, networking topologies, IEC 61850, transmission grid

## I. Introduction

In power systems, wide area application systems have been implemented using phasor measurement units (PMUs). PMUs acquire high-resolution measurements or data of voltage, current, phase angle and frequency from the different parts of the grid, which are transmitted to a Phasor Data Concentrator (PDC), and then to a control center. Historically, only centralized control was possible, because only at this higher level could computers and communication support be technically and economically justified [1].

IEC 61850 has emerged as the leading22 communication standard for power utility automation [2]. It provides a comprehensive model for power system devices to organize data, configure objects and map them to protocols, so that they are consistent and inter-operable. Due to this new paradigm, there has been the need to define an information model of an IEC 61850 compliant PMU [3], [4]. The result is the so-called routable sample values (R-SV) in wide area systems. R-SV measurements will be produced from devices called merging units (MUs) which will replace PMUs, while PDCs will be replaced by intelligent electronic devices (IEDs) acting as R-SV measurement subscribers. The opportunities of IEC 61850 in the utility grid will lead to exponential growth in the number of deployed IEC 61850 compliant PMUs, as well as new types of monitoring, control and protection applications. Hence, the currently centralized communication and computing architecture is envisaged to become much more distributed and decentralized [5].

Both centralized and decentralized wide area monitoring, protection and control (WAMPC) applications require reliable and high-performance communication infrastructure to meet the real time requirement needs. In a typical IEC 61850 smart grid, as illustrated in Fig. 1, communication between substations can occur by two means; 1) inter-substation communication at the networking layer 2 (i.e., L2 connected switches) and wide area communication based on IP (i.e., routers connected). The underlying communication medium however could be any combination of optical, copper, wireless and power line with optical fiber recommended to be used in transmission grids.

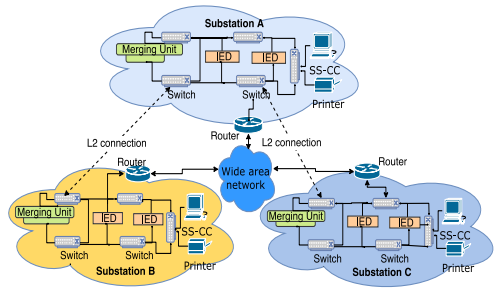



Fig. 1. Wide-Area communication framework.

The decentralized WAMPC applications of group communication among PMUs and PDCs can be addressed by point-to-point unicast communication.

Manuscript received November 22, 2018; revised August 2, 2019.
Corresponding author email: charles.adrah@ntnu.o.
doi:10.12720/jcm.14.9.765-772

However, this approach is not economical due to redundant copies of R-SV data existing on shared links. Conversely, one- to-many or many-to-many multicasting solutions, in which the receivers are connected to the source in a tree topology, are much more cost-efficient choices [6].

IP multicast technology, a method of sending IP data to subscribed receivers in a single transmission, has primarily been used to support multimedia applications. Support for multicast routing can be achieved through the Protocol Independent Multicast (PIM) of which several variants exists [7], [8]. In [9], IP multicast PIM-SSM (Source Specific Multicast) was proposed as an architecture to transport PMU data in wide area monitoring and protection applications in order to provide optimal delivery paths for low latency traffic. However, the architecture was at a high level and generic without considerations for utility grid networking topologies and impacts on achieving optimal delivery paths.

In this paper, we propose using Protocol Independent Multicast-Source Specific Multicast (PIM-SSM) for R-SV in wide area transmission networks. We analyze the impact of multicast tree costs and network delays in different communication network topologies suitable for WAMPC. The rest of this paper is organized as follows: Section 2 describes the architectures for routable sample values in the wide area and their typical communication infrastructures. In Section 3, we define the IP multicast architecture based on PIM-SSM and show how multicast groups are mapped from the transmission grid. Section 4 presents the performance evaluation of IP multicast impact on defined topologies. Finally, section 5 presents the conclusion for this research.

## II. Routable Sample Value Applications and Communication Architectures

In this section, we show the current centralized and future decentralized applications and communication architecture of PMU networking based on IEC 61850 concepts.

### A. Centralized R-SV Application

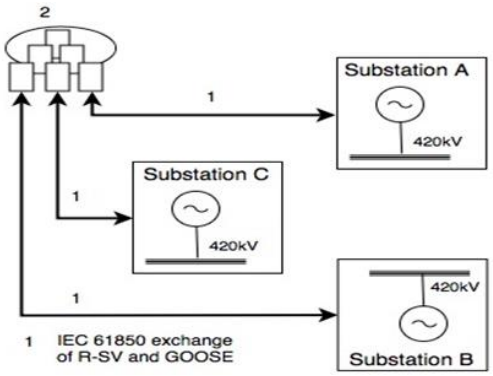



Fig. 2a. Centralized R-SV architecture.

The centralized application consists of R-SV data generated at substations and an R-SV subscriber IED located in the control center of the utility grid. Fig. 2(a) shows a 3-terminal network where R-SV measurements from each substations A, B and C are sent to a centralized R-SV subscriber IED with built-in estimator and protection relay functions. The IED can then run application software to analyze the measurements and take control actions.

The communication framework usually deployed for the centralized application is hierarchical. In Kim & Kim [10], the proposed communication network has three levels of 1) generation, 2) substation and 3) control center to mirror the hierarchy of the power system. This is a centralized architecture with the different levels of the utility power grid aggregating data which is sent to the control center.

### B. Decentralized R-SV Application

In the decentralized application, each substation generates R-SV data and in addition, has a R-SV subscriber IED. Fig. 2(b) illustrates a 3-terminal network consisting of substations A, B and C. B will receive R-SV data from A and C as well as send R-SV data to both A and C. B, will then initiate local control and protection actions based on received measurements from A and C. This is a major benefit of the decentralized architecture since distributed protection and control actions can be quickly initiated in the local substation, unlike the centralized approach where actions can only be effected from the control center.

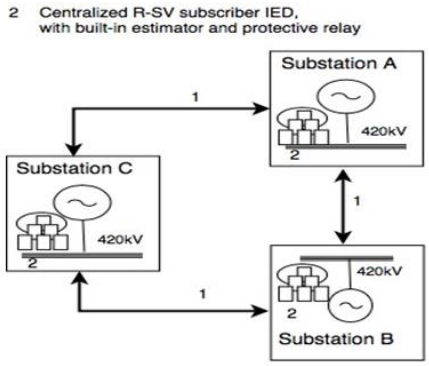



Fig. 2b. Decentralized R-SV Architecture.

The type of communication architecture for the decentralized R-SV application will involve a group communication system since multiple groups of R-SV data to R-SV subscriber IEDs can be formed. Multicast communications or multicast overlay networks provide solutions to enable this kind of communication architecture. WAMPC systems have delay constraints on protection and control actions, hence constructing a network architecture that satisfies Quality of Service requirements of low latency, availability and path redundancy is challenging [11].

## III. IP Multicast Architecture for WAMPC

Deng *et al*. [12] proposed a network structure where substations in the same regional area of a physical grid were connected on a backbone ring as shown in Fig. 3. In this work, the built communication infrastructure for the IEEE 39-bus transmission system [13], which is a reference test system shown in Fig. 4, is defined such that the resulting topology is based on backbone rings supported by a mesh core network. In addition, our motivation for choosing ring structure is that, it provides a redundant path for data to be sent in the opposite direction when a link failure occurs.

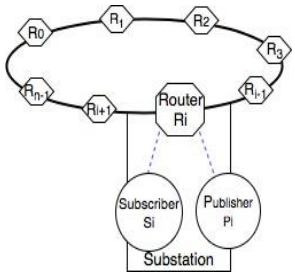



Fig. 3. Ring communication structure for transmission systems [12].

### A. IP Multicast

Using an IP multicast routing architecture to disseminate R-SV measurements in wide area seeks to be a suitable solution to enable R-SV from one substation to reach multiple substations. This architecture ensures that a substation produces a single source of the R-SV measurements while the networking infrastructure ensures the delivery of these measurements to the other interested substations.

Considering a transmission grid that spans a wide area, we propose using source specific multicast (PIM-SSM) routing architecture for sharing R-SV measurements. PIM-SSM scales well in wide area links and supports multicast groups to use shortest path trees [8]. It uses reverse path forwarding to construct shortest path trees rooted at the source, and a soft-state approach is employed by periodically refreshing the multicast forwarding states [14].

PIM-Sparse Mode (PIM-SM), is another approach that scales well in wide area usage. However, it builds per group shared tree which is rooted at a designated node called the rendezvous point. This approach is not suitable for sharing R-SV data in wide area. R-SV is critical data requiring low latency, hence multicast trees should be formed based on shortest path routing to avoid the longer delays instead of single shared tree [15].

Moreover, it is possible to deploy PIM-SSM alone in the network without protocol support for inter-domain PIM-SM since SSM does not require rendezvous point mechanisms. In the case of already configured PIM-SM networks, this option can also be adopted by simply upgrading the last hop routers (i.e., receiver connected routers) to support SSM while the remaining routers run PIM-SM in SSM range [16]. Finally, the flooding of multicast PIM-SSM traffic is reduced when compared against PIM-Dense Mode, since it is a receiver-initiated protocol and therefore there is a more efficient use of the network bandwidth [17].

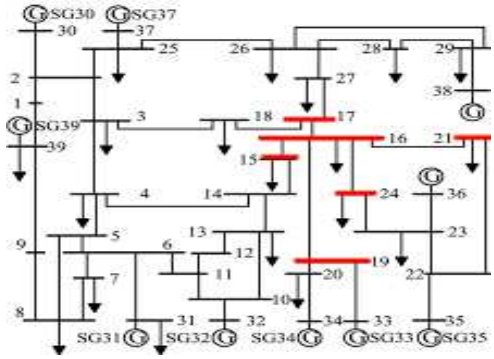



Fig. 4. IEEE 39 Bus Transmission System [13].

### B. PIM-SSM realized for R-SV in WAN

In the decentralized R-SV transmission for wide area state estimation and protection, a substation is interested in sending and receiving measurements from only a subset of substations from the grid topology at a time. This subset is defined by the number of physically connected substations to it. For example, based on the reference test system shown in Fig. 4, bus 16 has connection points to buses 15, 17, 19, 21 and 24 (highlighted in red). This means that bus 16 will receive R-SV from the five connected buses while transmitting its local R-SV measurements to each of the five buses simultaneously.

PIM-SSM requires classifying a group of multicast hosts by the multicast group address G, and a specific source S. The (S, G) network service group is called a "channel". The SSM channel is unique and therefore allows different sources to use the same group address. SSM is best applicable to dissemination-style applications with one or more senders whose identities are known before the application begins [8]. This means that the multicast sources need a method to predetermine the initial configuration. This fits our use case, and WAMPC systems in general, since the physical grid topology is already known, and therefore the multicast sources can be predetermined.

In our use case for the IEEE 39-bus system, we assign R-SV data to be distributed to R-SV subscriber IEDs in only the immediately connected substations. Using an adjacency matrix, we transform the IEEE test bus to show the connections between the substations and determine the multicast groups source/destination pairs. Table I shows the defined multicast groups. The source, S and receivers, R are the substation bus number with an R-SV MU. The sources, S, is root of the multicast tree, while the set of receivers, R represent the interested receivers of the multicast traffic from the corresponding source. The

multicast group size is the size of the multicast group size, |R|. The table is presented with distinct colors and in the order of increasing multicast group size.

TABLE I: MULTICAST GROUPS SORTED IN INCREASING GROUP SIZE

| Source, $S$ | Receivers, $R$ | Source, $S$ | Receivers, $R$ | Source, $S$ | Receivers, $R$ |
|---|---|---|---|---|---|
| 30 | 2 | 15 | 14,16 | 11 | 6,10,12 |
| 31 | 6 | 18 | 3,17 | 13 | 10,12,14 |
| 32 | 10 | 20 | 19,34 | 14 | 4,13,15 |
| 33 | 19 | 21 | 16,22 | 17 | 16,18,27 |
| 34 | 20 | 24 | 16,23 | 19 | 16,20,33 |
| 35 | 22 | 27 | 17,26 | 22 | 21,23,35 |
| 36 | 23 | 28 | 26,29 | 23 | 22,24,36 |
| 37 | 25 | 39 | 1,9 | 25 | 2,26,37 |
| 38 | 29 | 3 | 2,4,18 | 29 | 26,28,38 |
| 1 | 2,39 | 4 | 3,5,14 | 2 | 1,3,25,30 |
| 7 | 6,8 | 5 | 4,6,8 | 6 | 5,7,11,31 |
| 9 | 8,39 | 8 | 5,7,9 | 26 | 25,27,28,29 |
| 12 | 11,13 | 10 | 11,13,32 | 16 | 15,17,19,21,24 |

### C. Network Failure Analysis in Rings

PIM-SSM depends on the unicast routing information hence whenever there is a change in the unicast routing database, the multicast routing information also needs to be updated. The result of this rebuilding process is known as tree recovery [18]. Two techniques of multicast recovery initiation are the periodic recovery and the triggered recovery. The former involves periodic polling of the unicast routing tables while the latter involves the unicast routing state sending a notification of event change. Events leading to changes in the unicast routing, and hence reforming multicast trees, can be broadly classified as [18]:

- Topology reduction (link failure, removal or node failure);
- Topology enrichment (link recovery or adding a new link);
- Dynamic routing change (link metric change).

When the event of topology reduction occurs, there is consequential packet losses at multicast receiver ends. This is because some time is taken to detect the events, and additional time to reconstruct the multicast tree after a link or a node fails.

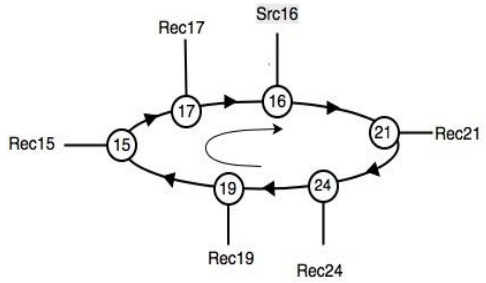



Fig. 5. A 6-node ring topology for failure analysis.

In Fig. 5, we consider multicast traffic for 6 nodes organized in a Ring, with node 16 as the sourced and the rest of the nodes as receivers. A unicast routing protocol for ring topologies, such as Ethernet Ring Protection [19], could be deployed on the ring as an alternative to spanning tree protocol and its family of related protocols. This would enable PIM-SSM to detect port- status changes during failures with less complex computations, provision overhead and excessive information exchange, achieving protection switching under 50 *msec*.

When a link failure occurs, (e.g., between node 16 and 21), the multicast tree is broken, and no data is delivered until a link restoration is done or traffic starts flowing in the alternate direction. In this case, data traffic flows to Rec21 through nodes 16 − 17 − 15 − 19 − 24 − 21. The time taken for the multicast traffic to flow after the link break is dependent on how fast the protection switching works to establish this alternative route. If the link between 16 and 21 is restored, the original distribution tree is also restored, which could lead to additional packet losses of undelivered packets on the alternative route.

## IV. PERFORMANCE EVALUATION

The performance evaluation is based on the IEEE 39-bus system, with the aim to evaluate the efficiency of multicast trees based on shortest-path trees, constructed among the defined multicast groups in different network topologies. Shortest-path trees or source-based trees tend to minimize the cost of each path from source to any destination [20]. Based on each defined topology, we run the Dijkstra's algorithm [21] to evaluate the performance of the multicast trees. The following metrics were used in our evaluation:

- *average shortest path tree length* (ASPTL): The ASPTL is the average number of physical links in the paths from source to each receiver of the multicast tree per multicast group. This metric was chosen because in creating an efficient shortest path tree for a ring with core mesh communication topology, we want to know which nodes and how many nodes per ring need to be connected to the core mesh.
- *end-to-end delay*: We determine the end-to-end delay for each multicast tree by calculating the average total number of hops between source and receiver for each multicast group defined.
- *hop count per source-receiver*: We assume there will be a threshold on the number of nodes the R-SV data can be routed through, between a source and receiver, in order to keep delay within acceptable limits. In addition, we investigate which topology incurs the lowest hop count per source-receiver path in each multicast group, giving a maximum hop threshold to be five.

We did not consider constraints on the designed network topologies and assume that all links have equal link costs and nodes have equal processing capacities. In addition, we assume that a ring has a unidirectional flow of data. We define a set of communication topologies based on the following criteria:

- The node connections to the core mesh.
- The number of rings the 39 nodes (representing the substation routers) are partitioned into.

### A. Node Connections to the Core Mesh

In determining the criteria of which nodes and how many to connect to the core mesh, we first determine the Betweenness Centrality, BC(v) [22] for all nodes in the IEEE 39-bus topology. U. Brandes [22], defines the Betweenness Centrality of a vertex v ∈ V as:

$$BC(v) = \sum_{s,t \in V} \frac{\sigma(s,t|v)}{\sigma(s,t)}$$

where:

- $\sigma(s,t|v)$ is number of shortest paths from vertex s to vertex t, where $v \neq (s,t)$.
- $\sigma(s,t)$ is number of shortest paths from vertex s to vertex t.

The calculated BC(v) is normalized by a factor $(N-1)(N-2)/2$, where $N = 39$, is the total number of nodes in the grid. The criteria to construct the topologies based on node connections to the core mesh were determined as follows:

- For each ring, the top two nodes ranked by BC(v), are connected to the mesh core.
- For each ring, the top three nodes ranked by BC(v) (if they exist) are connected to the mesh core.

TABLE II: NETWORK TOPOLOGIES

| Topology | Description | Legend |
|---|---|---|
| T1 | Four rings, two nodes per ring are connected to the core mesh | 4R2C |
| T2 | Four rings, three nodes per ring are connected to the core mesh | 4R3C |
| T3 | Seven rings, two nodes per ring are connected to the core mesh | 7R2C |
| T4 | Seven rings, three nodes per ring are connected to the core mesh | 7R3C |

### B. Creating Rings for the Topology

In designing the networking rings to be connected to the core mesh, the IEEE 39-bus needs to be partitioned carefully. Consideration for proximity of buses to form regional areas were taken into account. In addition, the following criteria were also considered;

- A bus/node with only one node as neighbor should be in the same ring as the neighbor node with more than one neighbor node.
- Rings are partitioned at points where a bus/node has a minimum of three neighbor nodes connected.

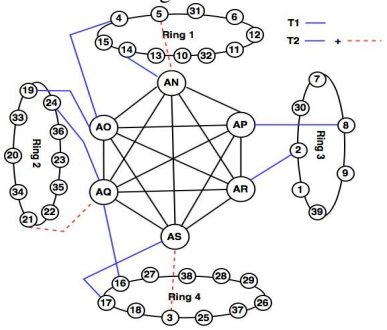



Fig. 6a. Network topologies - T1 & T2.

With these criteria, we construct the topologies constituting of four and seven rings for the evaluation. Having chosen the number of rings and the nodes to be connected to the mesh, the following four topologies emerge as described in Table II. Fig. 6a and Fig. 6b show the placement of the substation buses in the constructed topologies.

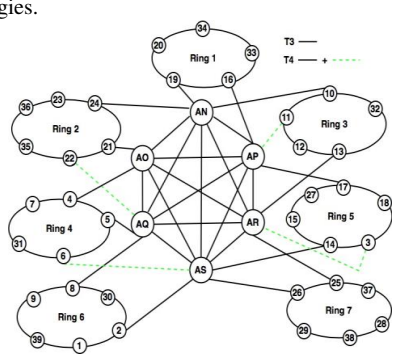



Fig. 6b. Network topologies – T3 & T3.

### C. Results and Discussion

We plot the results of the ASPTL cost per multicast group for the four topologies in Fig. 7(a). The results were organized by the size (i.e., number of interested receivers) for each multicast group. It was observed that T1 had the highest average cost with an expectation, μ = 4.818 and variance, σ2 = 6.594, while T4 had the lowest average cost with μ = 2.154, σ2 = 0.917.

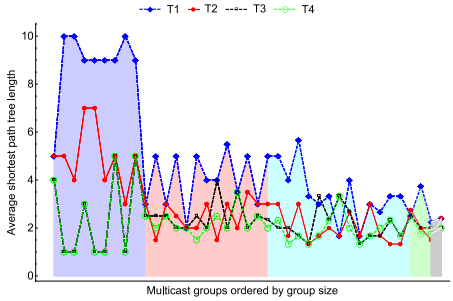



Fig. 7a. ASPTL cost per multicast group.

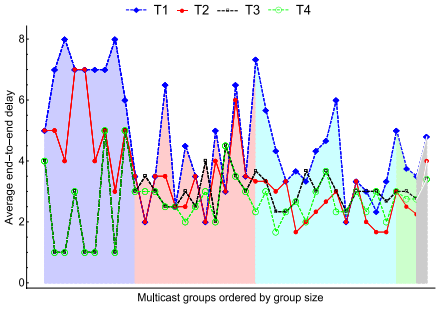



Fig. 7b. End-End delays of multicast trees per multicast group.

T2 had a significantly lower cost than T1 (40% reduction in mean ASPTL) with μ = 2.889, σ2 = 2.09236.

T3's cost of μ = 2.312, σ2 = 0.917 only has about 6.8% higher mean value. This shows that adding extra links to the core mesh from a node with the next highest betweenness centrality reduces the average multicast tree cost.

Fig. 7(b) shows the end-to-end delays of the multicast trees per multicast group for topologies T1-T4. T1 had the highest delay with μ = 10.179 and σ2 = 24.099, while T4 had the lowest delay of μ = 6.3846 and σ2 = 11.401. With T2 μ = 7.2051 and σ2 = 9.6937, there was reduction of 30% in the mean delay compared to T1. T3's delay recorded was μ = 7.00 and σ2 = 12.842.

A cumulative frequency plot of hops required to form multicast trees in each topology. As can be observed in the Fig. 8, T4 had a 100% multicast tress formed with maximum of 5 hops for source-receiver pairs. Given a threshold of 4 hops, it is seen that T4 has 88% of multicast trees formed while T2 and T3 have 78%, and T1 having only 50%. The equivalent performance of T2 and T3 shows how improvement in networking infrastructure design can lead to better performance of multicast delivery. In terms of delay, when a threshold for the source-to-receiver hop count is set, it is possible to determine which topology will fail for the multicast trees and if further improvements in the design can be achieved.

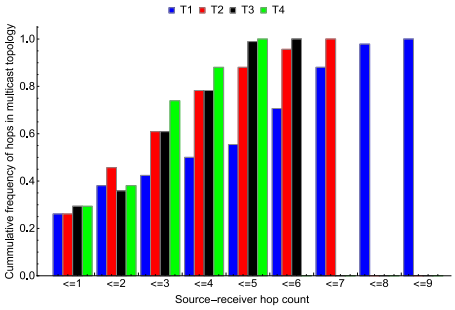



Fig. 8. Cumulative frequency of maximum hops to construct multicast trees for T1(4R2C), T2(4R3C), T3(7R2C), T4(7R3C).

For example, for a threshold of 5 hops, T2 has 88% and T3 has 98.9%. Improvement using cross connects can be considered for T2 and T3, to keep their source-to-receiver hop count below 5.

The results above show that the choices in the design of communication network topologies using the substation nodes will affect the efficiency of multicast trees for the multicast groups. Forming topologies with large rings (high number of nodes per ring, i.e., T1 and T2), will require connecting nodes with high betweenness centrality to the core mesh to reduce the mean shortest path tree length and delay.

For topology T2, simply identifying extra nodes with high betweenness centrality and connecting them to the core mesh resulted in significant reduction in the metric costs and achieving comparable performance to T3 and T4. Topologies with rings constructed with a smaller number of nodes per ring (T3 and T4) enabled nodes with high betweenness centrality to be selected and connected to the core. This reduced the ASPTL as well as the end-to-end delay. Hence, there will be trade-offs between choosing topologies for efficient multicast trees can be evaluated by considering the betweenness centrality of nodes in the physical grid topology.

## V. Conclusion

The deployment of digital substations in wide area networks for applications such as routable sample values transmissions will require appropriate communication technologies and infrastructures. In this paper, we conducted a study on how an IP multicast routing protocol, the PIM-SSM, can be used to enable R-SV transmission in wide area. We constructed communication network topologies to support the formation of multicast groups and used the IEEE 39-bus transmission test system to evaluate our method.

The performance of the suggested topologies is evaluated with respect to the end-to-end delays and length of the multicast trees which were created by using PIM-SSM. The results show that the multicast tree performance strongly depends on the underlying communication network topologies. In our case study, selecting the right topology resulted in 4 times reduction in shortest path lengths and 3 times lower delays. Furthermore, by analyzing the nodes' betweenness centrality, the addition of a single extra link to the core mesh network results in a 4-ring topology with a performance comparable to a 7-ring topology.

## References

[1] M. Begovic, D. Novosel, D. Karlsson, C. Henville, and G. Michel, "Wide-Area protection and emergency control," *Proceedings of the IEEE*, vol. 93, no. 5, pp. 876-891, May 2005.

[2] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *Proc. IEEE PES Power Systems Conference and Exposition*, Atlanta, GA, 2006, pp. 623-630.

[3] I. Ali, S. M. S. Hussain, and A. Aftab, "Communication modeling of phasor measurement unit based on IEC 61850-90-5," in *Proc. Annual IEEE India Conference (INDICON)*, New Delhi, 2015, pp. 1-6.

[4] S. R. Firouzi, L. Vanfretti, A. Ruiz-Alvarez, H. Hooshyar, and F. Mahmood, "Interpreting and implementing IEC 61850-90-5 routed-sampled value and routed-GOOSE protocols for IEEE C37.118.2 compliant wide-area synchrophasor data transfer," *Elsevier Journal of Electric Power Systems Research*, vol. 144, pp. 255-267, March 2017.

[5] A. Chakrabortty, "Handling the data explosion in Tomorrows power systems," *IEEE Smart Grid Newsletter*, Sep. 2011.

[6] Y. Xin and A. Chakrabortty, "A study on group communication in distributed wide-area measurement system networks in large power systems," in *Proc. IEEE Global Conference on Signal and Information Processing*, Austin, TX, 2013, pp. 543-546.

[7] C. H. R. Oliveira and A. P. Bowen, "Iec 61850 goose message over wan," in *Proc. International Conference on Wireless Networks (ICWN'12)*, 2012.
[8] H. Holbrook and B. Cain, Source-Specific Multicast for IP, RFC 4607, August 2006.
[9] M. Seewald, "Building an architecture based on IP-Multicast for large phasor measurement unit (PMU) networks," in *Proc. IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, 2013, pp. 1–5.
[10] K. Do-Young and Y. Kim, "Design and performance evaluation of hierarchical communication network for wide area measurement system," in *Proc. IEEE International Conference on Smart Energy Grid Engineering*, Oshawa, ON, 2015, pp. 1-5.
[11] A. Bose, "Smart transmission grid applications and their supporting infrastructure," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 11-19, June 2010.
[12] Y. Deng, H. Lin, A. G. Phadke, S. Shukla, J. S. Thorp, and L. Mili, "Communication network modeling and simulation for Wide Area Measurement applications," in *Proc. IEEE PES Innovative Smart Grid Technologies*, Washington, DC, 2012, pp. 1-6.
[13] A. Pai, *Energy Function Analysis for Power System Stability*, Norwell, MA, USA: Kluwer, 1989.
[14] L. Lao, J. H. Cui, M. Gerla, and D. Maggiorini, "A comparative study of multicast protocols: top, bottom, or in the middle?" in *Proc. IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, Mar. 2005, pp. 2809-2814.
[15] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C. Liu, and L. Wei, "The PIM architecture for wide-area multicast routing," *IEEE ACM Transactions on Networking*, vol. 4, no. 2, April 1996.
[16] Cisco Systems, Inc., IP Multicast: PIM Configuration Guide, Cisco IOS XE Release 3E, 2013.
[17] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), RFC 4601, Aug. 2006.
[18] T. Cicic, S. Gjessing, and Ø. Kure, "Tree recovery in PIM sparse mode," Research Report 293, University of Oslo, Department of Informatics, March 2001.
[19] J. D. Ryoo, H. Long, Y. Yang, M. Holness, Z. Ahmad, and J. K. Rhee, "Ethernet ring protection for carrier ethernet networks," *IEEE Communications Magazine*, vol. 46, no. 9, pp. 136-143, September 2008.
[20] B. Y. Wu and K. Chao, "Shortest-paths trees," in *Spanning Trees and Optimization Problems*, 2340. CRC Press, 2004.
[21] E. W. Dijkstra, A Note on Two Problems in Connection with Graphs, Numerische Math. 1, 269-271, 1959.
[22] U. Brandes, "On variants of shortest-path betweenness centrality and their generic computation," *Social Networks*, vol. 30, pp. 136-145, 2008.

**Charles M. Adrah** received the BSc. degree from the Kwame Nkrumah University of Science and Technology (KNUST), Ghana, in 2008, in Electrical Engineering, and the MSc. degree from the Norwegian University of Science and Technology (NTNU), Trondheim, in 2012, in Telematics (Services and Systems Engineering). He is currently pursuing the Ph.D. degree with the Department of Information Security and Communication Technology, NTNU. His research interests include quality of service and performance evaluation in smart grid communication networks.

**Jaya R.A.K. Yellajosula** received the B.Eng. degree from the Andhra University, India, in 2007. He has worked for 6 years in the field of substation automation, protection and design. He received Master of Science in Electrical Engineering from Michigan Technological university (MTU), in 2016. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering at MTU. His research interests include smart grid protection, real-time simulations, hardware-in-the-loop simulations, and power system communications.

**Øivind Kure** is a professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim. He got his Ph.D. from the University of California, Berkeley in 1988. His current research interest is in various aspects of QoS performance analysis, multicast protocols, and ad hoc networks.

**David Palma** is an Associate Professor at the Department of Information Security and Communication Technology, from the Norwegian University of Science and Technology (NTNU). He was an H2020 Marie Sklodowska-Curie Postdoctoral fellow at NTNU and has worked in the past as a Researcher and Project Manager at OneSource, as well as an invited Assistant Professor at the University of Coimbra. He holds a PhD in Information Science and Technology received from the University of Coimbra. His current research interests are on Cognitive IoT, Networking in Remote Areas, Routing, Cloud-Computing and Software-Defined Networks, subjects on which he has authored and co-authored multiple papers in refereed conferences and journals.

**Poul E. Heegaard** is a Professor at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU). Since 2006, Heegaard has been a faculty member at NTNU, and Head of Department in the period 2009-2013. From 1989- 1999 he was Research Scientist and Senior Scientist at SINTEF, and from 1999 to 2009 a Senior Re- search Scientist at Telenor R&I. He is now Principal Investigator in the CINELDI (Centre for Intelligent Electricity Distribution), a Centre for Environment- friendly Energy Research (FME) where he is responsible for smart grid operation. His research interests include performance, dependability and survivability assessment, with focus on communication networks (such as 5G, NFV, SDN) and services, and communication system as part of a digital ecosystem, including interaction with other critical infrastructures (such as Smart Grid).

# PAPER E

## A Network Design Algorithm for Multicast Communication Architectures in Smart Transmission Grids

C. M. Adrah, D Palma, Ø. Kure, and P E Heegaard

in Electric Power Systems Research Journal, doi: 10.1016/j.epsr.2020.106484

Electric Power Systems Research 187 (2020) 106484

Contents lists available at ScienceDirect

Electric Power Systems Research

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

# A network design algorithm for multicast communication architectures in smart transmission grids

Charles M. Adrah*[a], David Palma[a], Øivind Kure[b], Poul E. Heegaard[a]

[a] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, NTNU, Trondheim, Norway
[b] Department of Technology Systems, University of Oslo, UiO, Oslo, Norway

ARTICLE INFO

*Keywords:*
Smart transmission grids
Heuristics algorithms
Communication networks
Multicast
Wide-area networks
Substation automation

ABSTRACT

In future smart transmission grids, there are distributed applications that will benefit from the deployment of Internet Protocol (IP) multicast technology for communication. Sharing of Routable-Sample Values (R-SV) and Routable-GOOSE among the digital substations for wide-area monitoring, protection, and control (WAMPAC) applications will be needed. Using multicast for distribution of R-SVs is resource-efficient and offers a simpler configuration with only the interested substations needing reconfiguration. However, the demands for such concurrent delivery of R-SV data will put constraints on the underlying supporting networking infrastructure. For example, it must be ensured that the paths taken to route data traffic are within the bounds of delay to achieve the aims of the WAMPAC application. In this paper, we look at the problem of network topology augmentation through link additions. We present a heuristic algorithm that finds a set of links to be added to a network topology such that the multicast distribution tree for a multicast configuration is bounded by latency, which is set as the hop-count threshold. Our results show that by adding a few new links to the network topology, the delay incurred by the multicast traffic from sources to destinations can be reduced.

## 1. Introduction

Critical infrastructures such as the smart transmission grid (STG) will depend on supporting communication networking infrastructures. In STG operations, deploying Internet Protocol (IP) multicast technologies as a solution for wide-area monitoring, protection, and control (WAMPAC) applications have been proposed [1,2]. This will become increasingly common and relevant as more substations adopt the IEC 61850 standardization in substation automation [3,4]. The IEC technical report 61850-90-5 [5] specifies how the data models of Generic Object Oriented Substation Events (GOOSE) and Sampled Values (SV) can be routed beyond the substation into wide-area networks, with the addition of UDP/IP headers. These new data models are referred to in the literature as Routable-GOOSE (R-GOOSE) and Routable-Sampled Values (R-SV) messages.

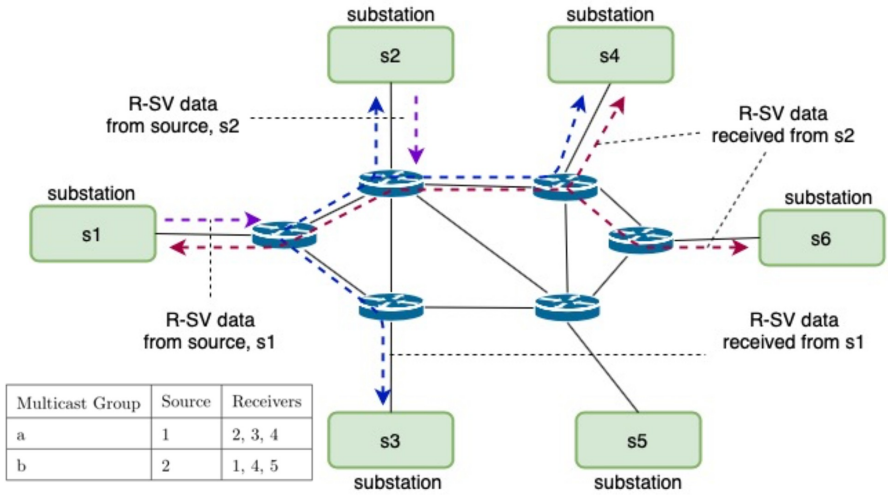
From the Information and Communication Technology (ICT) network perspective, multicast offers several benefits. One of these is bandwidth efficiency as only one copy of R-SV is sent over a link into the network from a source substation to the numerous interested receivers, instead of sending multiple copies from the source substation. R-SVs have delay restrictions to satisfy WAMPAC application requirements. Hence, quality of service (QoS) guarantees, such as multicast admission control and resource reservation techniques, will be needed [6]. Therefore, there is a better utilization of the network resources as maintaining one reservation for the one copy of R-SV sent over the link instead of maintaining reservation for each of the multiple copies. Also, there is the benefit of simplified network configurations. With multicast, only the interested receivers need to change their configurations whenever they want to join or leave a multicast session. The source substation does not need to alter its configurations. If unicast were used, both the source substation and interested receivers would have to be reconfigured whenever a new receiver is interested in R-SVs.

Fig. 1 illustrates how multicast technology is deployed for a WAMPAC application in the STG. It depicts a transmission grid consisting of some substations interconnected by a supporting wide-area communication infrastructure. The substations will want to share and receive R-SV data from other substations. For example, multicast group $a$ with substation $s1$ as a multicast source publishes R-SV data into the network, which are transparently shared using IP multicast to substations $s2$, $s3$, and $s4$. Similarly, substation $s1$ subscribes to receive R-SV data from multicast group $b$, with substation $s2$ as the multicast source.

There are challenges however as to how the communication network should be designed for such multicast deployments. This is as a

* Corresponding author.
*E-mail address:* charles.adrah@ntnu.no (C.M. Adrah).

https://doi.org/10.1016/j.epsr.2020.106484
Received 5 December 2019; Received in revised form 10 May 2020; Accepted 18 June 2020
Available online 27 June 2020




| Multicast Group | Source | Receivers |
|---|---|---|
| a | 1 | 2, 3, 4 |
| b | 2 | 1, 4, 5 |

**Fig. 1.** WAMPAC application deploying IP multicast in the smart transmission grid.

result of the strict QoS requirements such as latency, packet delay variations, packet losses, availability and path redundancy, imposed on the WAMPAC applications [7,9,8]. Constraints such as delays incurred through different link costs or processing delays on nodes become limitations affecting the latency path for the multicast traffic, which must be addressed.

A method to address delay constraints is to augment the network topology by adding new links to the topology. This can ensure that the delay incurred on the multicast traffic from the source(s) to their destinations is limited to a maximum number of hops. The approach known as *network topology design* has received significant attention in graph theory and network science communities. The challenges of minimizing the diameter of such graphs or network topologies by the insertion of edges or links of bounded costs are problems that exist in practical application fields such as telecommunication networks, information networks, road networks, and flight scheduling [10,11].

In this paper, we look at the problem of network topology augmentation through link additions. We present a heuristic algorithm that finds a set of links to be added to a network such that the multicast distribution trees formed from multicast configurations are bounded by latency. Here, the latency is set as the number of hops in the shortest paths (i.e., hop-count threshold). The algorithm minimizes the maximum shortest path lengths from a group of multicast destinations to one or more multicast sources. We evaluate the performance of our algorithm over some ICT network topologies for an IEEE-39 transmission grid. The results show that only a few new links are needed to be added to the topologies to meet set delay requirements. Hence, communication network design through topology augmentation can improve the delivery of multicast traffic in smart transmission grids.

The rest of the paper is organized as follows: We present related work on network design in Section 2. Our heuristic algorithm is presented in Section 3, and we show how the algorithm works with an example network topology. Performance evaluation of ICT topological data-sets for an IEEE-39 transmission grid is presented in Section 4. We present discussions in Section 5 and finally give concluding remarks in Section 6.

## 2. Related work

Network graph or topology design and optimization involve improving the network design with some defined objectives, either be rewiring while maintaining constant edges or by adding new links to improve the connectivity of the networks [12,13]. This is shown to be an NP-hard problem [14]. Adding a set of links or nodes to the graph to optimally maximize a certain graph property is known in the literature as graph augmentation [15–17]. Research works have focused on augmentation of network topologies for two purposes. The first involves improving fault tolerance and robustness of networks [18–20]. The second involves analyzing information flow properties such as minimization of eccentricity and diameter [21,22], and average shortest path length [23]. The scope of our work addresses the latter, where we minimize the end-to-end delays of groups of multicast sources and destinations.

In [21], the problem of designing a composite network to minimize the maximum of shortest path lengths from a traffic source to its specified destinations by adding up to $B$ edges to the information flow structure is addressed. The set of possible added edges is a subset of the edges in a complement graph where a complement graph is the all edges not in the initial network. The maximum of the shortest path lengths from a traffic source to its destinations is the maximum of the delay, or hops, required for traffic propagation. Thus, minimizing this maximum implies reducing the end-to-end delay suffered by the message. The approach used in determining the new edges to be added to the network shows that the newly added edges are incident on the source such that any shortest path from source will use at most one of the newly added edges.

In [22], a clustering algorithm (see Section 4.1) is used to minimize the diameter of a network using up to $B$ constant shortcut edges, with the set of allowable edges added being edges in the complementary graph. With a clustering algorithm to minimize edges from a single source, new-formed edges are incident on the source. Also, edges are formed by connections from the source to the center of the formed cluster(s). Furthermore, the paper shows that solving the single source eccentricity minimization problem, as well as the multicast version, can be done with this same approach.

In [23], the problem of adding $k$ shortcut edges of small fixed length to a graph to minimize the weighted average shortest path distance over all pairs of vertices was studied. In the single source version for this, it is shown that there exists an optimal set $F^*$ such that each edge, $e \in F^*$, is incident on the source $s$, hence for all other vertices, $v \in V$ there exists a shortest $s \leftrightarrow v$ path that uses at most one edge in $F^*$.

From the reviewed works, the methods that have been suggested in

minimizing the eccentricity or diameter of a graph are done mostly by forming new edges that are incident on the source nodes. In minimizing the diameter for multiple single-source multicast groups defined in the same graph, this approach may not always produce the best approximations since there might be links which are not incident on the sources that can better minimize the eccentricity for the multicast groups. The algorithm proposed in this paper suggests new links for multiple single-source multicast configurations defined over a topology without always finding a solution incident on the sources.

## 3. Minimizing end-to-end delay in the network

In this section, we present a heuristic algorithm, which we call *reduction over minimum set cover* (ROMSC). ROMSC algorithm improves a given network topology end-to-end delay through topology augmentation. As such, the delay incurred in the delivery of multicast traffic in the network is reduced. The algorithm's objective is to find a set of best link(s) to be added in a topology network design to enable the delivery of multicast traffic within delay bounds. The delay is defined as the maximum number of hops (hop-count threshold) in the shortest paths trees that can exist in the multicast distribution tree between a source node and the destination nodes. The end-to-end delay in a network is characterized by several delay components such as transmission, propagation, queuing, and processing delays. Hence, setting a limit on the number of routers passed will reduce the end-to-end delay experienced by the multicast traffic. The algorithm finds the best link(s) for a network that has several single-source multicast configurations deployed.

### 3.1. Algorithm

ROMSC uses the greedy approximation technique for the minimum set cover problem [24] to find the minimum set of links. There are three inputs used in our algorithm: an input network topology, $G_i$, multicast configurations, *MC*, and the hop-count threshold value, *thresh*. The input topology is defined by nodes and links, while the multicast configuration is the sets of multicast source and destination nodes. This algorithm uses three functions: find_exceeding_pairs(), find_candidate_links() and find_new_links(). The pseudo-code is presented in Algorithm 1.

The function find_exceeding_pairs() takes an input topology $G_i$, multicast configurations *MC*, hop-count threshold *thresh*, and returns the set of source-destination pairs that exceed *thresh* in all multicast configurations. Multicast trees are built using the reverse shortest path that builds shortest paths from multicast destinations towards the multicast source. We use a Breadth-First Search (BFS) algorithm [25], which is a graph traversal algorithm to find destination nodes that exceed the hop-count threshold. We call the set of source-destination pairs found with this function, the universal set *U*.

The function find_candidate_links() returns a set of candidate links, *C*, from which we find the final solution of new links to be added to our topology. The candidate links are formed by either connecting links directly between the exceeding pairs in *U* or their neighbor nodes. Firstly, the function stores in a table the distances (i.e., number of hops) of all neighbor nodes for all the unique elements in *U*, which are within the hop-count threshold. That is for all neighbor nodes, *i*, that are within the hop-count threshold for each node, *i*, in *U*, we find the distances, *val*, The value of the distances are stored as such; $distMap[i][j] = val$. Secondly, the function forms candidate links from the table for an exceeding pair *k* in *U*, satisfying the condition;

- $distMap[a][k.\ src] + distMap[b][k.\ dest] < thresh$.

Fig. 2 illustrates how candidate links are formed. That is for an exceeding pair *k* in *U* with a multicast source *k.src* and multicast destination *k.dest*, a candidate link $a \leftrightarrow b$ is formed. The nodes *a* and *b* are either the source and destination nodes, i.e., *k*, or their neighbor nodes

**Result**: S:= list of links to be added to topology
**input** : $G_i$ := input network topology; *MC*:= multicast configurations or groups; *thresh* := hop-count threshold;
`Functions` (*find_exceeding_pairs(), find_candidate_links(), find_new_links()*)
**begin**
    $U$ = find_exceeding_pairs($G_i$, thresh, *MC*);
    $C$ = find_candidate_links($G_i$, $U$);
    $S$ = find_new_links($U$, $C$);
    return $S$
**end**
**Function** `find_new_links(U, C)(F)`**:**
    $S = \{\}$ ▷ empty solution list
    **while** *U is not empty* **do**
        select a link, $l_i$, in $C$ that covers most elements $e$, in $U$, starting with the element, $e$, with the highest hop-count away from the source; $S$.add($l_i$); **for** *e in U covered by* $l_i$ **do**
            remove $e$ in $U$
        **end**
    **end**
    return $S$
**End Function**

**Algorithm 1.** ROMSC algorithm.

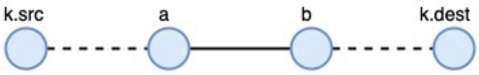



**Fig. 2.** Formation of candidate links.

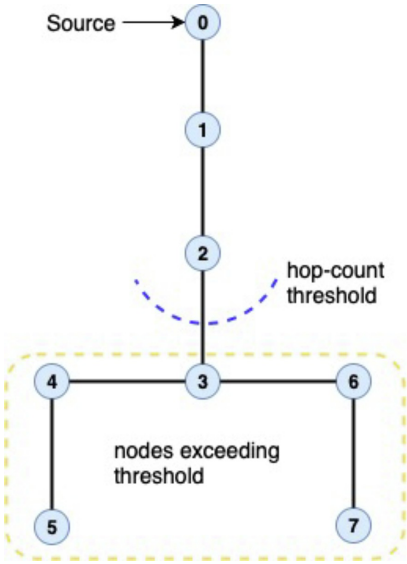



**Fig. 3.** 8 node network.

within the hop-count threshold.

The find_new_links() function returns the set of new links that can be added to the topology to satisfy all the source-destination node pairs exceeding the set threshold, i.e., *U*. The strategy used is the minimum set cover approximation, starting by finding a solution for source-destination pairs having the highest hop-count from the sources. This is followed by the link that covers the source-destination pair with the next highest hop-count and the remaining elements in *U*. The process is repeated until all elements in *U* are covered, and a set of links returned as the solution.

### 3.2. ROMSC algorithm evaluation

In this section, we explain how the ROMSC algorithm works by deploying it on a small size topology. Fig. 3 shows a network topology consisting of 8 nodes and 7 edges. Let us assume the hop-count threshold is set as 2 and that a multicast configuration is defined as follows; source node is 0, and destinations nodes are {1, 2, 3, 4, 5, 6, 7}.

First, by using the function *find_exceeding_pairs()* the list of destination nodes exceeding the threshold returned is: {3, 4, 5, 6, 7}. Hence, the universal set of source-destination pairs exceeding the threshold is:

- $U = \{(0, 3), (0, 4), (0, 5), (0, 6), (0, 7)\}$

Second, we use the function *find_candidate_links()*. This function first creates the table of distances of neighbor nodes within the hop-count threshold for each unique element in *U*. Let us call the set of all unique elements from *U* as $U_{flattened}$. This table takes each element in $U_{flattened}$ and finds distances of neighbor nodes that are within the hop-count threshold, i.e., the elements {0, 3, 4, 5, 6, 7} are used to create this table. Table 1 shows a square matrix of the 8-node network, which

**Table 1**
$distMap[i][j] = val$, where $i$ is a neighbour node of $j$, $j$ is a node in $U_{flattened}$, $val$ is hop-count from $j$.

| i \ j | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 4 | 5 |
| 1 | 1 | 0 | 1 | 2 | 3 | 4 | 3 | 4 |
| 2 | 2 | 1 | 0 | 1 | 2 | 3 | 2 | 3 |
| 3 | 3 | 2 | 1 | 0 | 1 | 2 | 1 | 2 |
| 4 | 4 | 3 | 2 | 1 | 0 | 1 | 2 | 3 |
| 5 | 5 | 4 | 3 | 2 | 1 | 0 | 3 | 4 |
| 6 | 4 | 3 | 2 | 1 | 2 | 3 | 0 | 1 |
| 7 | 5 | 4 | 3 | 2 | 3 | 4 | 1 | 0 |

illustrates how the table is generated. For example, node 0 from $U_{flattened}$ has neighbor nodes 1 and 2 with distances 1 and 2 stored. Another example is node 7, which has neighbor nodes 3 and 6 with distances 2 and 1 respectively stored in the table. Each node in $U_{flattened}$ has also the distance 0 from itself stored in the table. The function then next finds the candidate links of each source-destination pair in *U*. For example, taking the pair (0,3) from *U*, we form candidate links, (*i, j*), if:

- $distMap[i][0] + distMap[j][3] < 2$

Using this condition produces candidate links that can satisfy the pair (0,3); 0↔2, 0↔3, 0↔4, 0↔6 and 1↔3. Table 2 shows all candidate links for the topology, and the exceeding pairs covered in *U* by adding such a link.

Third, we use the function *find_new_links()* to find the solution of the best links to be added to the network topology. With the universal set, $U = (0, 3), (0, 4), (0, 5), (0, 6), (0, 7)$, the function uses a set cover approximation strategy to find a set of links that covers the elements in *U*, starting first with elements with the highest hop-count.

From Fig. 3, nodes 5 and 7 have the highest hop-count (i.e., 5), away from the source, 0. Hence, taking node 5, we find that the link 0↔4 will cover elements (0,3),(0,4),(0,5). The remaining elements in *U* are then (0, 6), (0, 7). Again we find a solution for the node with the next highest hop-count away from the source. It is node 7. Hence, we find the best link that covers the remaining elements in *U*, inclusive of the pair {0, 7}. The link 0↔6 is selected to cover the rest of the elements in *U*. The final solution of new links to be added to the network graph will thus be 0↔4 and 0↔6.

## 4. Performance evaluation and discussion

In this section, we apply our algorithm presented in Section 3.1 by

**Table 2**
Candidate links (C) and exceeding pairs (U) satisfied.

| C \ U | (0,3) | (0,4) | (0,5) | (0,6) | (0,7) |
|---|---|---|---|---|---|
| 0↔2 | x | | | | |
| 0↔3 | x | x | | x | |
| 0↔4 | x | x | x | | |
| 0↔5 | | x | x | | |
| 0↔6 | x | | | x | x |
| 0↔7 | | | | x | x |
| 1↔3 | x | | | | |
| 1↔4 | | x | | | |
| 1↔5 | | | x | | |
| 1↔6 | | | | x | |
| 1↔7 | | | | | x |

evaluating sets of communication network topologies that can be deployed in the STG. The physical power grid for transmission networks is usually well planned, and as such, operations involving WAMPAC applications in the grid should be carefully planned before deployment. Therefore, when deploying multicast configurations, the sources of multicast traffic (i.e., substations sending R-SV data), and the multicast traffic receivers (i.e., substations receiving R-SV data) should also be predetermined.

The evaluation is done by setting different values of hop-count thresholds required to achieve multicast delivery for a multicast configuration in a network topology. Our algorithm, ROMSC, determines the number of links to be added to the network topology to meet the latency demands for the delivery of multicast traffic. We compare ROMSC and clustering algorithm from Demaine et al. [22] in our evaluations. Both algorithms were implemented in C++ and our code compiled with gcc-5.4.0. The tests were done on a 32 *bit* Ubuntu Linux machine equipped with 8 *GB* RAM, and a 2.2 *GHz* Intel core. A summary of the clustering algorithm and its implementation is presented next.

### 4.1. Clustering algorithm (CLUS)

Given a distance or hop-count $dist(x) \geq 0$, the CLUS algorithm [22] involves partitioning the vertices, $V$, and edges, $E$, of an undirected weighted graph, $G = (V, E)$ into clusters of diameters at most $2x$. A subset of vertices $S$, from $G$, is selected as the centers of the clusters. The set $S$ satisfies the following properties; 1) the distance between any pair of vertices in $S$ should be greater than $2x$. 2) for every vertex $u \ni S$, there should be a vertex $v \in S$ whose distance to $u$ is at most $2x$, where $dist(u, v)$ is the distance between $u$ and $v$. Otherwise, vertex $u$ is added to the set $S$ as a cluster center.

In the implementation of the single-source version of the multicast problem, only a subset of the nodes is minimized. That is for the subset of vertices, $V' \subseteq V$, and a source node $s$, we want to add $k$ shortcut edges to minimize the maximum distance between the nodes in $V'$ from the source $s$. In this case, the centers of the clusters are selected from the vertex set $V'$. Hence any vertex outside is not chosen as a center in the algorithm. The CLUS stops when all vertex nodes of the set $V'$ are exhausted or cannot be selected.

### 4.2. IEEE 39-bus transmission grid and communication network topology

In Adrah et al. [2], we defined a method of constructing physical-level communication topologies for an IEEE 39-bus transmission test system. These were assumed fiber-level topologies having a general structure of substations grouped into rings connected to a common core network. Each substation is represented by an edger router that connects to other substation edge routers to form the wide-area communication topology. Four different communication topologies were defined, as shown in Figs. 4 and 5, and will be used in our evaluation. The main differences between these topologies are the number of groups of rings formed, and the additional links added to the core node for improved connectivity.

Also, we define two sets of multicast configurations to be deployed on these topologies. The first multicast configuration (MC-1) consists of all 39 nodes acting as multicast sources, and multicast receivers defined as all neighbor nodes directly connected to a multicast source. The average number of receivers per multicast group is 2. For the second multicast configuration (MC-2), 39 nodes acting as multicast sources and the multicast receivers are defined to include all nodes that are at most 2 nodes away from their respective multicast sources. MC-2 has the average number of receivers per multicast group as 6. The details of the topologies with the number of nodes, links, the average number of hops per multicast configuration, and maximum candidate links of the topologies are presented in Table 3. The defined multicast configurations are shown in the Appendix (Tables 4 and 5).

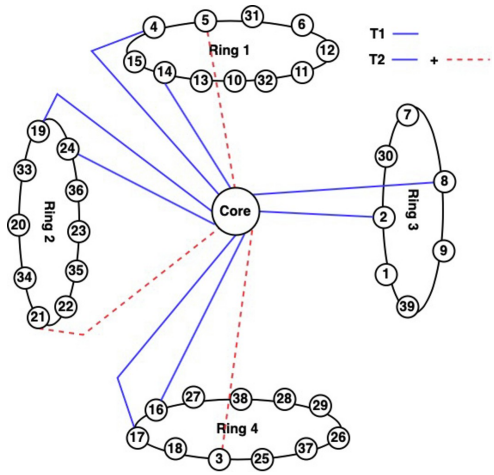



**Fig. 4.** Communication network topologies T1 and T2.

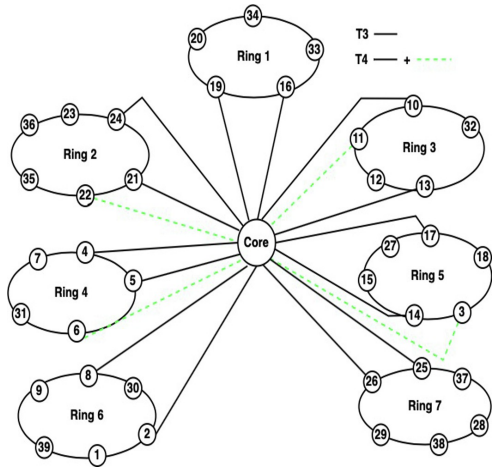



**Fig. 5.** Communication network topologies T3 and T4.

**Table 3**
Topological Data-set.

| Network | Nodes | Links | Avg. Degree | Avg. no. of hops | | Candidate links |
|---|---|---|---|---|---|---|
| | | | | MC-1 | MC-2 | |
| T1 | 40 | 47 | 2.35 | 1.91 | 2.79 | 733 |
| T2 | 40 | 50 | 2.5 | 1.69 | 2.44 | 730 |
| T3 | 40 | 53 | 2.65 | 1.69 | 2.38 | 727 |
| T4 | 40 | 57 | 2.85 | 1.65 | 2.29 | 723 |

### 4.3. Results

Figs. 6 and 7 show plots of the minimum number of links to be added to the four network topologies deployed with multicast

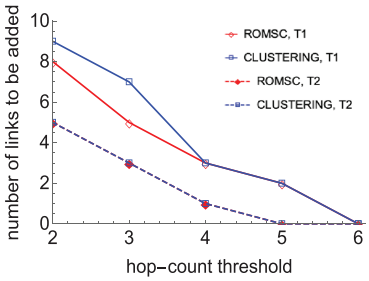



**Fig. 6.** T1 and T2 with MC-1.

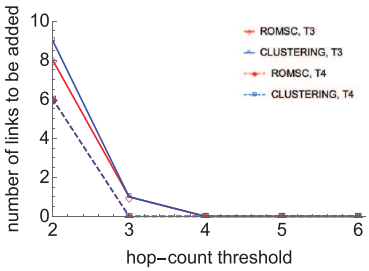



**Fig. 7.** T3 and T4 with MC-1.

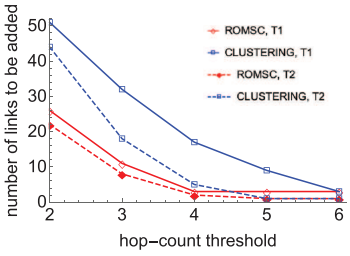



**Fig. 8.** T1 and T2 with MC-2.

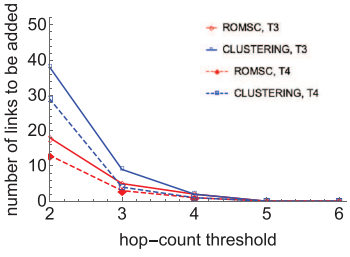



**Fig. 9.** T3 and T4 with MC-2.

configuration 1 (i.e., Table 4). The number of hops in the shortest path or hop-count threshold is varied from 2 to 6. As can be seen, ROMSC performs better than or equal to the CLUS in approximating the number of links to be added for all values of the hop-count threshold. The topologies T2 and T4 are improvements of T1 and T3, respectively, in terms of design, and were observed to have equal performance using both algorithms. This can be attributed to the additional links in T2 and T4, which improved their average degree compared to T1 and T3.

We also evaluate the performance of ROMSC and CLUS over the same topological data-set deployed with multicast configuration 2 (i.e., Table 5). Figs. 8 and 9 show the number of minimum links to be added with the hop-count threshold varied from 2 to 6. Similarly, we observe that ROMSC performs better than or equal to the CLUS. However, the difference in the number of minimum links suggested by ROMSC and CLUS is more significant in these cases. This is because of the complexity of the multicast configuration used. MC-2 is more complex than MC-1, having a higher average number of multicast receivers per group. MC-2, when deployed on the topologies generally resulted in a higher number of links required to be added to the network, compared to using MC-1. It is observed that ROMSC suggests a significantly fewer number of links compared to CLUS for small hop-count thresholds. For example, when the hop-count threshold is 2 ROMSC gives 26 links against 51 links with CLUS for T1 and likewise ROMSC gives 22 links against 44 links with CLUS for T2. A similar trend is observed with T3 and T4, where ROMSC gives 18 and 13 links against 38 and 29 links using the CLUS.

With a more complex multicast configuration, the percentage of the number of new links to all source-destination pairs exceeding the hop-count threshold is less for ROMSC compared to CLUS. For T1 with MC-2, source-destination pairs $U$, was 109 when the hop-count threshold was set to 2. ROMSC generated 23.85% new links per $U$ while CLUS generated 46.79% new links per $U$.

Furthermore, the underlying physical topology also influenced the number of new links to be added to the network topology. For topologies with a higher average degree of connectivity, there were fewer new links needed to be added for improved multicast delivery. In our analysis, T4 had the highest average degree. Using the ROMSC algorithm, when T4 was deployed with MC-1, and hop-count threshold = 3, no new links were required to achieve the end-to-end delay of multicast traffic. When T4 was deployed with MC-2, and hop-count threshold = 4, only 1 link was needed to be added to the topology. It is also noticeable that the performance of both algorithms tends to converge as the hop-count threshold increases.

### *4.4. Analysis of IEEE-39 bus communication network with no initial core*

In this section, we consider a utility whose communication network topology is without a core network. For such a scenario, we assume the communication network topology of the utility grid is geographically grouped into ring structures. We aim to find the minimum number of links to be added to enable connectivity among the rings for the multicast groups to achieve the desired end-to-end delay paths. We do this by modifying the topologies T1, having four-rings and T3, having seven-rings, which are the groupings of the substation edge routers. All links from the ring structures going towards the core network are removed. We call the modified T1 and T3: *T1-no-core* and *T3-no-core* respectively. We deploy multicast configurations MC-1 and MC-2 on *T1-no-core* and *T3-no-core*. Both ROMSC and CLUS algorithms are used in

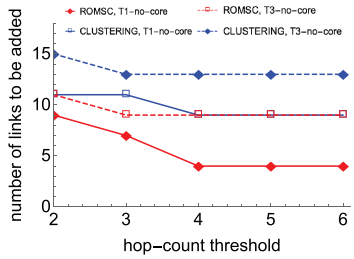



**Fig. 10.** T1-no-core and T3-no-core with MC-1.

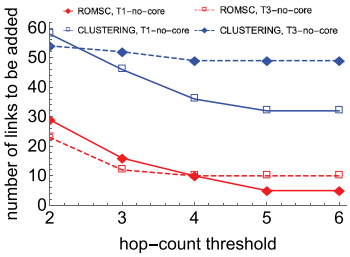



**Fig. 11.** T1-no-core and T3-no-core with MC-2.

the evaluations.

Figs. 10 and 11 show the number of minimum links added to the topologies when deployed with MC-1 and MC-2, respectively. Again the results show that ROMSC performs better than the CLUS in producing the number of minimum links to be added to the network. We compare the performance of ROMSC on T1-no-core and T3-no-core to study the effects of ring sizes. For MC-1, T1-no-core with a four ring structure consistently produced the minimum number of links for all hop-count thresholds compared with T3-no-core with a seven ring structure. For MC-2, T3-no-core performed better than T1-no-core for the hop-count threshold between 2 and 4. Beyond hop-count = 4, it is observed that T1-no-core produced a minimum number of links as compared to T3-no-core.

## 5. Discussion

The ICT topologies used in our evaluation were based on IEEE 39-bus STG. Since the STG used in actual deployments are of a limited size, the range of ICT topologies will be equally limited. Our use-case topologies, and cost metric of a hop-count threshold, provide an insight on the expected performance of our algorithm in actual deployment. From the evaluations, the performance of ROMSC is always the same or better, and in some cases, significantly better than the CLUS in reducing the number of links to be added to the network topology.

In our analysis in Section 4.4, with the 39 substation edge routers used to form groups of ring structures, we observed the most significant reduction in the number of added links using ROMSC. Therefore for transmission grid networks that already have existing supporting communication infrastructures, using ROMSC provides a method of finding the minimum links to augment the topology to attain the required end-to-to delay for the multicast traffic in the network. However, such augmented topologies may be sub-optimal. In cases where the network topology is designed just for multicast delivery, it may be possible to achieve fewer links needed to satisfy the latency requirements without consideration for an already existing core network.

Furthermore, the size of the topology ring structures to be created for such networks, together with the multicast configuration complexity, will also affect the number of links required for the topology augmentation. For small multicast configurations of less complexity, large groupings of nodes in rings tend to produce the fewer number of links. With more complex multicast configurations, and for high end-to-to end delay requirements (i.e., small hop-count threshold), the smaller sized rings performed better. However, with lower delay thresholds (i.e., large hop-count threshold), it is observed that the large-sized rings tend to perform better than the small sized ring networks.

In ROMSC, the set of candidate links is reduced. This is because we generate the candidate links only from nodes exceeding the hop-count threshold and their close neighbor nodes that are within the hop-count threshold. The set of all possible candidate links is calculated by $\frac{n(n-1)}{2} - k$ [18], where $n$ is the number of nodes in the topology and $k$ is the existing links in the initial topology. In our 8-node example network with 7 existing links shown in Fig. 3, the maximum number of candidate links is 21. With ROMSC, the candidate links size is reduced to 11, as shown in Table 2. For topology T1 running MC-1, the number of maximum candidate links is 733 since the existing network already has 47 links. When the hop-count threshold is set for the values {2, 3, 4, 5}, ROMSC reduces the candidate link size needed to find the minimum links to {48, 110, 148, 180}, respectively.

Using a brute force approach to obtain the number of minimum links is computationally expensive. If the number of candidate links is $n$, with existing links $k$, the maximum iteration to find the number of minimum links using brute force is $\sum_{k=1}^{l} \frac{n!}{(n-k)!k!}$, with a computational complexity of $O(n^n)$. For example, in our 8-node case topology, approximately 2.1 million running iterations will be required with a brute force approach. It was shown in [21] that a brute force enumeration algorithm that determined the eccentricity for a 75-node graph, on adding up to 4 edges and higher, took months to run on the provided hardware.

## 6. Conclusion

Current and future networking topologies for transmission grids will need to be re-designed as the demand for more complex power system applications arise. For example, WAMPAC applications that require synchronous operations will largely leverage IP multicast technology as a communication solution.

In this paper, we have presented a novel heuristic algorithm, ROMSC, that adds a minimum number of links to the network topology. When we assume a constant delay per hop, the maximum delay for a multicast configuration running in the network can be set. It is shown that by adding a few new links to the network topology, the hop-count threshold is fixed for all multicast traffic in the network.

We demonstrate that ROMSC is more efficient when compared to a CLUS algorithm. Also, ROMSC finds minimum links for multiple multicast configurations defined over the network topology. Hence, it better approximates a minimum number of links to be added to the network. Furthermore using ROMSC, larger network topologies can be easily augmented, which will enable the concurrent delivery of multicast traffic for WAMPAC applications.

## CRediT authorship contribution statement

**Charles M. Adrah:** Conceptualization, Methodology, Investigation, Software, Writing - review & editing. **David Palma:** Conceptualization, Validation, Writing - review & editing. **Øivind Kure:** Conceptualization, Methodology, Writing - review & editing. **Poul E. Heegaard:** Conceptualization, Supervision, Writing - review & editing.

## Declaration of Competing Interest

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

## Appendix A

**Table 4**
Multicast configuration 1 (MC-1) with sources *S*, and receivers *R*.

| *S* | *R* | *S* | *R* | *S* | *R* |
|---|---|---|---|---|---|
| 30 | 2 | 15 | 14,16 | 11 | 6,10,12 |
| 31 | 6 | 18 | 3,17 | 13 | 10,12,14 |
| 32 | 10 | 20 | 19,34 | 14 | 4,13,15 |
| 33 | 19 | 21 | 16,22 | 17 | 16,18,27 |
| 34 | 20 | 24 | 16,23 | 19 | 16,20,33 |
| 35 | 22 | 27 | 17,26 | 22 | 21,23,35 |
| 36 | 23 | 28 | 26,29 | 23 | 22,24,36 |
| 37 | 25 | 39 | 1,9 | 25 | 2,26,37 |
| 38 | 29 | 3 | 2,4,18 | 29 | 26,28,38 |
| 1 | 2,39 | 4 | 3,5,14 | 2 | 1,3,25,30 |
| 7 | 6,8 | 5 | 4,6,8 | 6 | 5,7,11,31 |
| 9 | 8,39 | 8 | 5,7,9 | 26 | 25,27,28,29 |
| 12 | 11,13 | 10 | 11,13,32 | 16 | 15,17,19,21,24 |

**Table 5**
Multicast configuration 2 (MC-2) with sources *S*, and receivers *R*.

| *S* | *R* | *S* | *R* | *S* | *R* |
|---|---|---|---|---|---|
| 34 | 20,19 | 29 | 25,26,27,28,38 | 11 | 5,6,7,10,12,13,31,32 |
| 37 | 25,2,26 | 28 | 25,26,27,29,38 | 15 | 4,13,14,16,17,19,21,24 |
| 32 | 10,11,13 | 7 | 5,6,8,9,11,31 | 14 | 3,4,5,10,12,13,15,16 |
| 33 | 19,16,20 | 8 | 4,5,6,7,9,39 | 26 | 2,17,25,27,28,29,37,38 |
| 38 | 29,26,28 | 18 | 2,3,4,16,17,27 | 19 | 15,16,17,20,21,24,33,34 |
| 35 | 22,21,23 | 10 | 6,11,12,13,14,32 | 3 | 1,2,4,14,17,18,25,30 |
| 36 | 23,22,24 | 23 | 16,21,22,24,35,36 | 24 | 15,16,17,19,21,22,23,36 |
| 31 | 6,5,7,11 | 1 | 2,3,9,25,30,39 | 5 | 3,4,6,7,8,9,11,14,31 |
| 30 | 2, 1,3,25 | 22 | 16,21,23,24,35,36 | 4 | 2,3,5,6,8,13,14,15,18 |
| 39 | 1,2,8,9 | 21 | 15,16,17,19,22,23,24 | 25 | 1,2,3,26,27,28,29,30,37 |
| 20 | 16,19,33,34 | 27 | 16,17,18,25,26,28,29 | 2 | 1,3,4,18,25,26,30,37,39 |
| 9 | 1,5,7,8,39 | 13 | 4,10,11,12,14,15,32 | 17 | 3,15,16,18,19,21,24,26,27 |
| 12 | 6,10,11,13,14 | 6 | 4,5,7,8,10,11,12,31 | 16 | 14,15,17,18,19,20,21,22,23,24,27,33 |

## References


[1] M. Seewald, Building an architecture based on ip-multicast for large phasor measurement unit (pmu) networks, 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), (2013), pp. 1–5.

[2] C.M. Adrah, J.R.A.K. Yellajosula, Ø. Kure, D. Palma, P.E. Heegaard, An IP multicast framework for routable sample value communication in transmission grids - Volume 14, no. 9, september 2019 - journal of communications, J. Commun. 14 (9) (2019) 765–772.

[3] R.E. Mackiewicz, Overview of iec 61850 and benefits, 2006 IEEE PES Power Systems Conference and Exposition, (2006), pp. 623–630.

[4] IEC, IEC TR 61850-90-1:2010, Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations, Technical Report, IEC, 2010.

[5] IEC, IEC standard for communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasors information according to IEEE C37.118 IEC 61850-90-5 TR Ed 1.0, Technical Report, IEC, 2012.

[6] A. Neto, E. Cerqueira, A. Rissato, E. Monteiro, P. Mendes, A resource reservation protocol supporting qos-aware multicast trees for next generation networks, 2007 12th IEEE Symposium on Computers and Communications, (2007), pp. 707–714.

[7] P. Kansal, A. Bose, Bandwidth and latency requirements for smart transmission grid applications, IEEE Trans. Smart Grid 3 (3) (2012) 1344–1352.

[8] Y. Deng, H. Lin, A.G. Phadke, S. Shukla, J.S. Thorp, L. Mili, Communication network modeling and simulation for wide area measurement applications, 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), (2012), pp. 1–6.

[9] S.M. Blair, C.D. Booth, B. De Valck, D. Verhulst, K.-Y. Wong, Modeling and analysis of asymmetrical latency in packet-based networks for current differential protection

application, IEEE Trans. Power Delivery 33 (3) (2018) 1185–1193.
[10] S. AhmadBeygi, A. Cohn, Y. Guan, P. Belobaba, Analysis of the potential for delay propagation in passenger airline networks, J. Air Transp. Manage. 14 (5) (2008) 221–236.
[11] F. Frati, S. Gaspers, J. Gudmundsson, L. Mathieson, Augmenting graphs to minimize the diameter, Algorithmica 72 (4) (2015) 995–1010.
[12] A. Sydney, C. Scoglio, D. Gruenbacher, Optimizing algebraic connectivity by edge rewiring, Appl. Math. Comput. 219 (10) (2013) 5465–5479.
[13] H. Wang, P. Van Mieghem, Algebraic connectivity optimization via link addition, Proceedings of the 3rd International Conference on Bio-Inspired Models of Network, Information and Computing Sytems, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 22.
[14] J.M. McQuillan, Graph theory applied to optimal connectivity in computer networks, ACM SIGCOMM Comput. Commun. Rev. 7 (2) (1977) 13–41.
[15] K.P. Eswaran, R.E. Tarjan, Augmentation problems, SIAM J. Comput. 5 (4) (1976) 653–665.
[16] M. Papagelis, F. Bonchi, A. Gionis, Suggesting ghost edges for a smaller world, Proceedings of the 20th ACM International Conference on Information and Knowledge Management, CIKM '11, ACM, New York, NY, USA, 2011, pp. 2305–2308.
[17] N. Parotsidis, E. Pitoura, P. Tsaparas, Selecting shortcuts for a smaller world, SIAM International Conference on Data Mining 2015, SDM 2015, Society for Industrial and Applied Mathematics, Philadelphia, PA, 2015, pp. 28–36.
[18] M.J. Alenazi, E.K. Çetinkaya, J.P. Sterbenz, Network design and optimisation based on cost and algebraic connectivity, International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, IEEE, 2013, pp. 193–200.
[19] M.J. Alenazi, E.K. Cetinkaya, J.P. Sterbenz, Cost-Efficient network improvement to achieve maximum path diversity, Proceedings of 2014 6th International Workshop on Reliable Networks Design and Modeling, RNDM 2014, IEEE, 2014, pp. 202–208.
[20] M.J. Alenazi, J.P. Sterbenz, Evaluation and comparison of several graph robustness metrics to improve network resilience, Proceedings of 2015 7th International Workshop on Reliable Networks Design and Modeling, RNDM 2015, IEEE, 2015, pp. 7–13.
[21] S. Perumal, P. Basu, Z. Guan, Minimizing eccentricity in composite networks via constrained edge additions, Proceedings - IEEE Military Communications Conference MILCOM, IEEE, 2013, pp. 1894–1899.
[22] E.D. Demaine, M. Zadimoghaddam, Minimizing the diameter of a network using shortcut edges, in: H. Kaplan (Ed.), Algorithm Theory - SWAT 2010, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 420–431.
[23] A. Meyerson, B. Tagiku, Minimizing average shortest path distances via shortcut edge addition, Proceedings of the 12th International Workshop and 13th International Workshop on Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX '09 / RANDOM '09, Springer-Verlag, Berlin, Heidelberg, 2009, pp. 272–285.
[24] V. Chvatal, A greedy heuristic for the set-covering problem, Math. Oper. Res. 4 (3) (1979) 233–235.
[25] C.Y. Lee, An algorithm for path connections and its applications, IRE Trans. Electron. Comput. EC-10 (3) (1961) 346–365.

# PAPER F

## Fusion Networking for IEC 61850 Inter Substation Communication: Use Case Applications

C. M. Adrah, S. Bjørnstad, and Ø. Kure,

Journal of Communications vol 12 (9) (2017) 510-517.

# Fusion Networking for IEC 61850 Inter Substation Communication: Use Case Applications

Charles M. Adrah, Steinar Bjørnstad, and Øivind Kure
NTNU, Trondheim N-7491, Norway
Email: {charles.adrah; steinar.bjornstad; okure}@ntnu.no

***Abstract*** —In this paper, Fusion networking technology is proposed as a solution for transporting time critical traffic in wide area network power system protection applications among utility substations, to attain deterministic low delay, zero packet loss and ultra-low packet delay variation. Use case applications are explained for communication between two substations and more than two substations using the Fusion networking technology. In addition, the requirements for inter substation communications are presented with focus on the IEC 61850 protocols of Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SMV) and their adaptability to the traffic classes of guaranteed service transport (GST) and statistically multiplexed (SM) in Fusion networking technology.

***Index Terms***—Communication, power systems protection, IEC 61850, Hybrid networks, circuit-switched, packet-switched

## I. Introduction

In recent years, traditional relay protection devices are being replaced with digital relays called Intelligent Electronic Devices (IEDs) in the substations. The IEDs are built on advanced communication technologies to develop communication-assisted protection schemes within the smart grid context. The IEC 61850 [1] is the resultant standardization efforts in substation automation and to address the issues in communication for protection purposes.

The scope of IEC 61850 was originally specified for communication within the substation. It includes two real-time, peer-to-peer communications protocols that are designed particularly for protection applications: Generic Object Oriented Substation Event (GOOSE) messages and Sampled Values (SV) messages [2]. GOOSE and SV messages are link layer protocols that use a publisher/subscriber architecture. This multicast structure works by sending to the multiple subscribed nodes fast and reliable messages.

GOOSE is event driven and supports the point-to-point communication among multiple nodes. The high speed and reliability requirements makes it impractical to use confirmation services in its protocol. GOOSE solves this with a pragmatic approach by assuming subscribers did not receive the message and hence retransmit quickly notwithstanding the reality. This retransmission mechanism also increases the dependability of the protocol. SV is not event driven but sampled whereby configurable datasets are transmitted on a multicast basis from a publisher to multiple subscribers. Although the initial scope of IEC 61850 was within the substation, it is now seen as the future for digital substation as well as inter-substation automation. IEC 61850 90-1 [3] has defined specifications for communication between substations.

Furthermore, IEC 61850 is deployed with Ethernet technology. IEEE 802.1Q [4] specifies functions of Virtual LAN tagging of Ethernet packets and the methods used by network switches to handle packets such that GOOSE and SV messages flooding the wide area networks can be avoided. To lower the latencies of protection application messages which are mostly higher priority traffic, priority scheduling in addition to techniques of Quality of Service (QoS) prioritization are recommended for communication between substations. However, these techniques do not provide hard QoS of a dedicated circuit, e.g. like a dedicated wavelength light-path in an optical wavelength routed optical network [5].

When transporting protection application messages across two or more substations, over provisioning of bandwidth is one method to lower delay. Transporting other kinds of traffic such as IP-telephony, video, metering, Supervisory Control and Data Acquisition (SCADA) will lead to demand for increased bandwidth which presents challenges in cost-efficiency. Maximizing the bandwidth utilization while maintaining the strict QoS requirements for protection applications messages therefore provides a motivation in improving the network throughput in addition to reducing the cost per bit for utilities.

Fusion networking technology is an implementation of Integrated Hybrid Optical Networks (IHONs) [6]. This seeks to combine the circuit and packet networks in the same wavelength to achieve circuit quality transport of high priority services referred to as guaranteed service transport (GST) streams, and statistical multiplexing of best effort services referred to as Statistical Multiplex (SM) streams enabling the high throughput efficiency of packet networks. In [7], an experiment using two Ethernet based Fusion nodes with dedicated interface support for both high priority GST and lower priority SM streams was performed. It was demonstrated that GST enables connections with circuit-switched QoS of no

Manuscript received May 20, 2017; revised September 25, 2017.
Corresponding author email: charles.adrah@ntnu.no.
doi:10.12720/jcm.12.9.510-517

packet loss and ultra-low Packet Delay Variation (PDV) with the unutilized capacity being filled through statistical multiplexing of streams from lower priority SM class.

In this paper, Fusion networking technology is proposed as a solution to transport time critical power system protection data with hard QoS requirements mixed with other types of traffic that are typically running between substations. In addition, we propose an architecture of mixed traffic priorities on the aggregation and deaggreation interfaces, and estimate and analyze the performance on the time critical protection data.

The rest of the paper is structured as follows; Section II summarizes the requirements in the standardization efforts for inter substation communication specified in [3]. Section III introduces the Fusion networking concept. In section IV, scenarios are presented to show the application of fusion nodes in transporting protection application messages in inter substation communication and in addition, how protection messages can be classified. Section V explains the principles of the combining mixed traffic on Fusion nodes and we evaluate performance of a chosen scenario and finally conclusions are presented in section VI.

## II. Requirements For Substation-To-Substation Communication

### A. Background

The need to exchange standardized information directly between substations for power system protection purposes is increasing. IEC 61850 protocol originally made for exchange of information among devices within a substation provides features which can be used to extend beyond substations. It is expected that IEC 61850 will become the bedrock for a globally standardized utility communication network.

The different kinds of protection applications impose different communication constraints such as communication channel failure, timing, propagation delay, reliability, redundancy, data synchronization (e.g. less than 0.1ms), frequency of data exchange, data bandwidth to transmit three-phase current/voltage data, and data size.

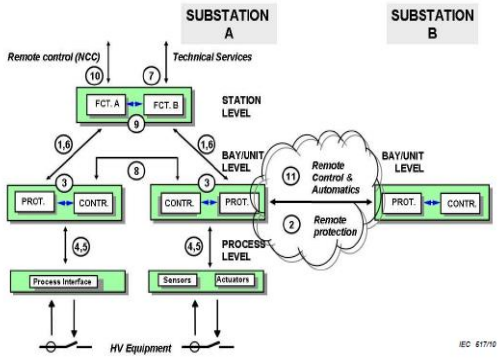



Fig. 1. Logical allocation of functions and interfaces [3].

A substation-to-substation (SS-SS) communication refers to functions in Substation Automation Systems (SASs) that are either distributed between two substations or functions in one substation that require some information from another substation. Fig. 1 shows the logical allocation of functions and interfaces in an SAS. Interface 2 and 11 are the focus of SS-SS communication. Protection related functions are defined on interface 2 and includes analogue data for line differential protection applications as well as digital data for line distance protection applications. The control related functions are defined on interface 11 and are mainly digital data for interlocking functions or inter-substation communication data. Both interfaces are expected to be dedicated communication paths for their respective functions.

### B. Message Types and other Performance Requirements

Due to the different requirements of the functions in and between substations, IEC 61850 message types are divided into Message Performance Classes (MPC). Table I shows the message performance classification of different kinds of traffic that can exist between substations. MPC Type 1 are the high-speed messages that typically contain simple binary information of a short or simple message such as "Trip", "Reclose order", "Start". These message types are mission critical for the performance of the supported application function hence the receiving IED needs to act immediately upon receipt of such message. An MPC specialized Type 1A is mostly used to send "Trip" binary signal which is the most important fast binary message.

Table I: IEC 61850 Message Types [3].

| Traffic (By protocol) | Type | Applications | Performance Class | Transfer times |
|---|---|---|---|---|
| GOOSE | 1A | Fast messages "Trip" | P1 | 10 *ms* |
| | | | P2/P3 | 3 *ms* |
| | 1B | Other fast messages | P1 | 100 *ms* |
| | | Normal messages | P2/P3 | 20 *ms* |
| SV | 4 | Raw Data | P1 | 10 *ms* |
| | | | P2/P3 | 3 *ms* |
| Others (e.g. TCP/IP) | 2 | Medium speed | | 100 *ms* |
| | 3 | Low speed | | 500 *ms* |
| | 6 | File transfers | | 1000 *ms* |

The transfer times for Type 1A varies depending on supported application function between 3 *ms* to an upper limit of 10 *ms*. Type 1B is another MPC that is for both fast and normal messages relevant for automation functions but with less stringent requirements compared to Type 1A. For this MPC, transfer time requirements are between 20 *ms* to 100ms. MPC Type 4 which are raw data messages including SV messages or phasors also have stringent transfer times between 3 *ms* and 10 *ms*.

MPC Types 2, 3 and 6 for medium speed, low speed and file transfers can be messages such as commands and

reports like station level database update, update of the single line display at a screen, update of alarm and event lists. Transfer times for these kinds of messages are between the bounds of 100 *ms* to 1000 *ms*.

### C. Integrity, Security and Dependability

The communication link between SS-SS has high requirements on bit-error-ratio and signal-to-noise ratio. Three integrity classes have been specified for different types of messages in the standard IEC 60870 [8]. Protection safety related messages which are the most time critical messages, i.e. MPC type 1A, have the highest integrity class 3 prescribed. All other messages can be transmitted with lower data integrity in a class 2.

Security and dependability requirements are very high as well. Security "S", against unwanted commands, i.e. unwanted trips of protection if they are not requested by the protection scheme in the actual situation. Hence given $P_{uc}$ as the probability for unwanted commands, then Security, $S = 1 - P_{uc}$. It is recommended that protection application in the tripping IED should have $P_{uc} < 10^{-8}$, and blocking schemes $P_{uc} < 10^{-4}$.

Dependability "D" means the dependability against "missing commands" i.e. for protection missing trips if these are requested from the protection scheme in the actual situation. Given probability for missing commands as $P_{mc}$, $D = 1 - P_{mc}$. It is prescribed a $P_{mc} < 10^{-4}$ within a 10ms duration. Table II lists the security, dependability and bit-error-ratio metrics recommended for GOOSE and SV traffic types.

TABLE II: SECURITY, DEPENDABILITY AND BER METRICS

| Traffic Type | Security | Dependability | Error rate (BER) |
|---|---|---|---|
| GOOSE | $<10^{-8}$ | $<10^{-4}$ | $<10^{-6}$ |
| SV | $<10^{-8}$ | $<10^{-4}$ | $<10^{-6}$ to $<10^{-8}$ |

### D. Ethernet Communication for IEC 61850

Tele protection systems rely on telecommunication channels that provide a deterministic signal transmission delay and have a constant bandwidth or bit rate over time, without any delay variation [9]. Legacy technologies of SONET/SDH and PDH have been used by utilities to build wide-area communications networks for inter substation communication. Ethernet technology with its statistical multiplexing transmission mechanism and use of bandwidth-on-demand or "best effort" techniques have brought challenges to the performance requirements that protection applications must conform. Statistical multiplexing, which offers the main benefit of exploiting the network capacity efficiently, also imposes a crucial drawback: Ethernet networks are high bandwidth-delay product networks. Delay and packet delay variations (PDV) are normally imposed on the traffic because buffering is needed for handling the statistical variations in the traffic pattern. While the high-throughput is welcomed by bandwidth hungry applications and data centric technologies, the delay and PDV characteristic is not well- fitted for the transport of time-sensitive information [5].

IEC 61850 is deployed on an Ethernet Local Area Network (LAN). Traffic dependability problems emanate from congestion that arise from competing Ethernet packets for a network path. A solution for this is to use several priority-dependent queues at each egress port to lower the latencies of the higher-priority traffic. Another solution to address the security and dependability issues using Ethernet, is to avoid GOOSE packets flooding the wide area networks. This is achieved by configuring flow restrictions using Virtual LANs (VLANs). VLAN identifiers (VIDs) are configured between all IEDs needing certain messages or belonging to a certain application working with a specific kind of message hence using different VLANs for a substation internal traffic and substation-to-substation inter traffic.

[3] lists recommendations for using Ethernet for communication between substations as follows:

- If the Ethernet telecommunication network is outside the utility's "security perimeter", the Ethernet links through such equipment should be secured through technology such as "L2TP" (layer 2 tunneling protocol) to create a "VPN".
- Ethernet should recover (restore traffic) from a fiber failure within 10ms, unless dual-port IEC 61850 IEDs are used with physically separate paths.
- All the network switches "drop" ports connected to IEC 61850s should be configured for memberships only in the VLANs supported by the connected IEDs.
- All network switches "drop" ports shall be configured to block ingress traffic with VIDs for the critical VLANs.
- Probability of a GOOSE packet taking more than 10ms to traverse the network should be constrained to less than $10^{-4}$ by limiting the number of switches on the longest path and limiting the traffic loading.

## III. FUSION NETWORKING CONCEPT

Fusion is a technology solving the problem of providing packet networks with the advantages of circuit switched networks [10]. The technology is built on the architecture of integrated hybrid optical Networks (IHON).

### A. Introducing Integrated Hybrid Optical Networks

IHON is a concept that attempts to bring packet and circuit network domains together. IHON supports two main classes of service: the circuit- service class referred to as guaranteed service transport (GST) offering hard quality of service (QoS) and packet-service class referred to as statistically multiplexed (SM) with lower QoS [11]. The two classes of service share the same physical wavelength resource. The GST traffic offers hard QoS including: zero packet jitter, zero packet loss, and low deterministic delay while the SM traffic is statistically multiplexed, accepting lower priority QoS.

Provisioning circuits of wavelength granularity leads to the well-known issue of low resource utilization in optical circuit switching and wavelength routed optical networks (WRONs) [7] because statistical multiplexing is not available. Therefore, to optimize the wavelength capacity, IHON uses the established GST wavelength to transport SM traffic whenever there is an idle time gap between GST packets. The GST traffic is not affected by this technique since the SM traffic is only added in between vacant gaps not used by the GST packets.

### B. Introducing Fusion Node

The TransPacket H1 prototype node [12], is a Fusion networking add-drop Ethernet muxponder which enables Ethernet packet transport of the two types of traffic classes; GST with circuit QoS and the statistically multiplexed SM class for high wavelength capacity utilization. TransPacket H1 10 Gigabit Ethernet (GE) add/drop Fusion muxponder introduces high density 10x1GE channels with transparent Ethernet transport, ultralow delay and zero packet loss. While the processing in the node follows the Fusion principle, all data signals into and out of the node is Ethernet compliant.

## IV. SS-SS Communication Usng Fusion

In this section, we show the application of Fusion nodes in a first scenario as a direct link between two substations. We then show a second scenario involving more than two substations. We also show how traffic exchanged between substations can be classified using the Fusion traffic classes.

### A. Fusion Node as Direct Link betweeen Two Substations

In the first scenario shown in Fig. 2, a Wide Area Network (WAN) communication setup between two substations is established. We assume that there is a direct Ethernet connection between the two substations hence the substations use the tunneling approached described in [3] for SS-SS communication. Tunneling is a method that connects multiple substation networks by allowing "direct access" to functions in a remote station. The station network becomes extended to include the remote station. Higher bandwidth is normally required to achieve low delay. Even for low data volume of GOOSE traffic, a higher bandwidth of the communication mechanism correlates with lower delay [3]. Tunnels are normally established by means of network switches or routers.

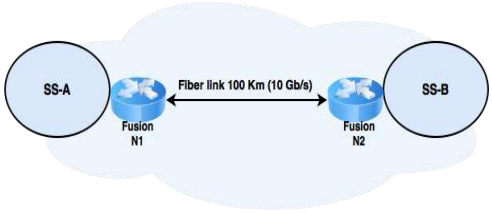



Fig. 2. SS-to-SS communication structure with fusion nodes

In each substation, we consider a Fusion node connected through a fiber link with a 10 Gb/s Ethernet wavelength. The 10Gb/s link is configured as the trunk port that connects the two substations. It is assumed that messages enter input ports of 1 Gb/s on each node and are then aggregated into the 10 Gb/s Ethernet output link. The Fusion node acts as a Substation Edge Node (SEN) coupling the WAN connection between the two substations. The SEN aggregates different traffic streams from each substation.

### B. Three or More SS - Optical Ring Add/Drop

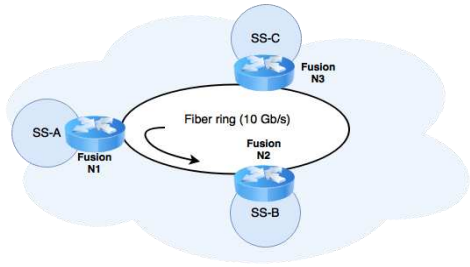



Fig. 3. SS-to-SS communication structure with 3 substations

In our second scenario, we extend the setup shown in Fig. 2 with an additional substation. Using the Fusion nodes, a ring topology is implemented such that the Fusion nodes acts as add/drop multiplexers, with large aggregate capacity suitable for a wide area network architecture. Using Fusion nodes for add/drop, aggregation rings with low delay and ultra-low PDV can be implemented, avoiding unnecessary routing or switching at intermediate nodes. In Fig. 3, the substations A, B, and C are connected by a 10 Gb/s fiber ring. Traffic directed from SS-A to SS-C will pass through an intermediate node, N2 at SS-B. N2 acting as a bypass node. Directed traffic to SS-B will be dropped at N2. In addition, traffic from SS-B can be added at N2, onto the 10 Gb/s aggregate link and routed to SS-C or SS-A based on the protection application requirements.

### C. Use Case 1 – Protection vs Non-Protection Traffic.

TABLE III: MAPPING BETWEEN SS-SS TRAFFIC AND IHON TRAFFIC

| SS-SS traffic types | IHON traffic types |
|---|---|
| Protection traffic - GOOSE (Type 1A 1B – fast, normal) and SV Type 4 | GST |
| Non-protection traffic - Other traffic (TCP/IP) | SM |

In the first use case, two types of traffic between substations are defined. All the protection traffic i.e. GOOSE and SV, as one type of traffic. The second type of traffic are non-protection traffic which may be client-server communications running on TCP/IP. This is the simplest case of traffic segregation where all data for protection applications between the two substations are considered to offer time critical services. The protection

traffic entering the Fusion node will be classified as GST streams while the non-protection traffic will be classified as SM streams. A mapping of the defined traffic types between the substations and supported classes by Fusion nodes is shown in Table III.

### D. Use Case 2 – Clasification by Message Performance Classes

I the second use case, we consider the different IEC 61850 message performance classes for the protection traffic between substations shown in Table I. The messages are marked as either GST or SM streams on arrival at the Fusion node. The reason for classification of traffic types is based on the transfer time requirements for such message types. Table IV shows a mapping of the classes of services supported by the Fusion nodes and the IEC 61850 traffic types defined between substations.

The GOOSE Type 1A and Type 4 SV messages are classified as GST when entering the port of the Fusion node. These messages are the most time critical of the protection traffic, hence are marked as such. The GOOSE Type 1B (fast and normal), control messages or other traffic types running on TCP/IP that are exchanged between the two substations are classified as SM. We consider these traffic types to be less demanding on transfer time requirements for our use case, hence are marked as such.

TABLE IV: MAPPING BETWEEN IEC 61850 MESSAGE TYPES AND IHON TRAFFIC TYPES

| SS-SS traffic types | IHON traffic types |
|---|---|
| GOOSE Type 1A | GST |
| SV Type 4 | GST |
| GOOSE Type 1B - fast | SM |
| GOOSE Type 1B - normal | SM |
| Other traffic (TCP/IP) | SM |

In Fusion, the high priority traffic (GST) is given a fixed delay through the node corresponding to the duration of a maximum sized SM frame. The purpose of the delay is the ability of detecting gaps in the GST traffic sufficiently large to insert a maximum sized SM packet. In this configuration, the fixed delay δ is set to 1.21$\mu s$ to accommodate an SM maximum-length lower priority packet of 1518 bytes. The aim is to show that we can achieve aggregation of GST connections, transport and deaggregation with circuit QoS: low deterministic delay, ultralow PDV, and no packet loss.

## V. COMBINING TRAFAFIC PRIORITIES ON INTERFACES, EVALUATION AND DISCUSSION

In this section, we explain the principles of the proposed combination of mixed traffic classes on aggregate nodes and evaluate performance effects on the GST traffic class. Furthermore, we discuss the effects the classification choices have on the GST streams and SM performance.

### A. Combining Traffic Priorities on Interfaces

In the field trial setup in [7], the experiment considered nodes of dedicated traffic for the different traffic classes of GST and SM streams as shown in Fig. 4.

In our proposed architecture, traffic arriving and departing a node could be from a mix of different priority classes. Fig. 5 shows the mechanism of combining traffic priorities at the interfaces of the nodes. Suppose we have two 1 Gb/s ports of N1, with mix traffic priorities arriving on their ports, i.e. GST1/SM1 on *ge0* and GST2/SM2 on *ge1,* for the aggregation process into the 10GE wavelength channel. After deaggregation by N2, it is expected a different mix of traffic priorities at the corresponding ports, i.e. GST2/SM1 on *ge0* and GST1/SM2 on *ge1*.

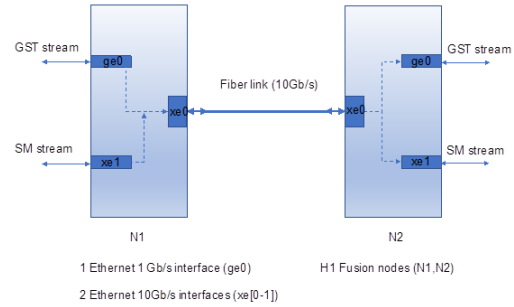



Fig. 4. Dedicated interface for traffic priorities [7].

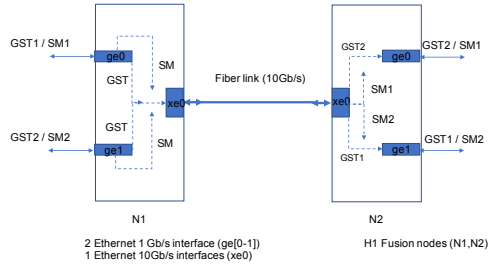



Fig. 5. Setup with mixed traffic at aggregation and deaggregation interfaces.

The aggregation scheme in N1 for the proposed architecture will behave similarly as shown in [7]. The SM streams from ports *ge0* and *ge1* are filtered into internal buffers from where they are scheduled only if they fit into the available of unutilized GST capacity. The GST packets received at the 10GE input interface pass through to the other 10GE output interface with absolute priority and light processing in the node [7].

In the deaggregation process, a mix of traffic priorities are expected on the interfaces of *ge0* and *ge1*. An additional delay will be incurred on the GST packets when combining with SM traffic on 1GE output, for achieving zero PDV from contending packets. The delay is fixed and influenced by the maximum packet length of the SM packet.

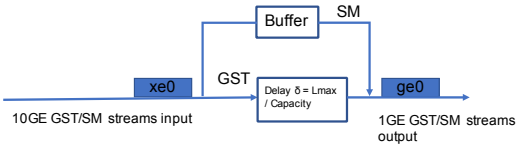



Fig. 6. Deaggregation from 10Gb/s to 1Gb/s.

In addition, since the deaggregation is from a 10 Gb/s port interface to a 1 Gb/S interface ports, it will take 10 times slower to clock out a packet on the 1 Gb/s ports. Fig. 6 shows a schematic of the deaggregation process and mechanism of combining mixed traffic on the 1Gb/s interface.

### B. Performance Analysis on GST Traffic

To estimate the delay budget for the scenario in Fig. 2, we consider the following equation:

$$C_D = N\ x\ (N_D + T_{ProD})$$

$C_D$, is the delay budget. $N$, is the number of nodes. $N_D$, is the nodal delays which consists of transmission delay, processing delays and queuing delays. $T_{ProD}$, is the propagation delay.

The propagation delay for a fiber link is estimated to be *5us* per km [13]. We consider the SS-SS link in Fig. 2 to be of a transmission grid spanning 100 Km. A fixed delay δ is incurred by the GST packets before accessing the 10 Gb/s and 1 Gb/s output channels in both the aggregation and deaggregation process. This fixed delay is determined by the channel capacity C and the maximum length SM packet $L_{max}$, i.e. $\delta = L_{max} / C$. Assuming the maximum SM packet size of 1518 bytes, the GST marked packets will experience a fixed delay of 1.21 *us* during the aggregation process into the 10 Gb/s channel port and add fixed delay of 12.1 *us* due to combining traffic priorities on the 1 Gb/s channel ports of N2. The total end-to-end fixed delay for GST streams will then be 13.31 *us.*

The rest of the delay budget is constituted by propagation delay of 500 *us* (100 *Km* x 5 *us/Km*) plus some nodal processing delays. In the field trial demonstrated in [7], the end-to-end nodal processing delay recorded was 43.3 *us.* The total delay budget using Fusion with the proposed mix of traffic on interfaces will be:

$$C_D = (13.31 + 43.3 + 500)\ us = 556.6\ us$$

IEC 61850-90-1 [3] states that the requirements for the transfer time i.e. the communication performance are basically the same in one bay, between bays and between substations. Therefore, the same classification scheme shall be used for all links compliant with IEC 61850. For digital communication beyond the substation, transfer times ≤ 10 *ms* may be accepted according to the message performance class TR2 [14]. In addition, other less demanding performance classes may be acceptable if the protection application function will work with these transfer times. Hence from the delay budget of 556.6 *us* estimated when using Fusion, it can be a suitable solution in the transport of protection traffic between substations.

It was also shown in [7] that, the average delay of the GST streams will be deterministic independent of the amount of GST or SM load. The principle allows packet delay variation of the GST streams to be zero, but some PDV is added due to imperfect implementation issues in the node. The peak-to-peak PDV for GST in the experiment of [7] was however shown to have an average of 320 *ns.*

### C. Discussions

The estimated delay budget obtained for the GST traffic will be the same for the traffic classification use cases explained in Sec. IV, C and D. Marking all protection traffic as GST and non-protection traffic as SM in one case versus only some message performance class as GST will not affect the delay performance of the GST traffic. This is because the only influence the Fusion node has on the GST circuit stream is that bypassing packets are given a fixed delay δ corresponding to the transmission time of the maximum length SM Ethernet packet [5].

Deciding on how to classify substation traffic either as GST or SM stream depends on what data is viewed as performing time-critical service. In addition, it depends on the total amount of data exchanged between the substations i.e. total network load. If a higher portion of total network load between the substations are classified as time-critical and hence marked as GST streams, this will have a corresponding effect on the offered load of SM traffic. This is because there will be a higher bandwidth utilization by the GST traffic which could lead to lower offered load of SM streams. Therefore, it is important to consider this before marking streams as either GST or SM.

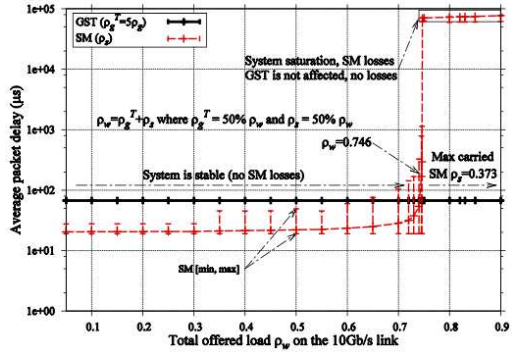



Fig. 7. Packet delays as function of the normalized offered load on the 10 Gb/s Ethernet wavelength [7].

In [7], it was shown that when the total offered load $\rho_W$ is equally offered by the GST aggregate and SM such that $\rho_T = \rho_G + \rho_S$, $\rho_G = \rho$, the system goes into saturation at a point where SM traffic starts experiencing packet delays and losses. Illustrated in Fig. 7 are end-to-end delay results for GST and SM traffic. The minimum and

maximum boundary, plus their averages, SM delay values are plotted to show how the increase in GST load influences the SM performance. It is seen that as both GST and SM loads increase, the GST average delay is constant. At 0.75 of $\rho_T$ with 0.38 GST, the system saturates and the end-to-end delay of the SM traffic increases. It was also observed SM traffic experienced congestion and packet losses.

## VI. Conclusion

This paper presents the requirements in the IEC 61850 90-1 standard for communication between substations and proposes the use of Fusion networking technology based on the IHON architecture, for transporting time critical power system protection traffic together with other types of traffic between substations. The application of Fusion nodes in a wide area network setting was demonstrated in a first scenario involving two substations and a second scenario using more than two substations. In addition, two use cases showed how protection application traffic can be classified per the Fusion traffic classes. In one use case, classification of messages as GST or SM are based on the message performance classes of IEC 61850. GOOSE Type 1A and Type 4 SV messages are marked as GST streams which maintain the stream characteristic with zero packet loss, low delay and ultralow PDV. This provides circuit-switching properties with a low deterministic delay. The other IEC 61850 message types, i.e. Type 1B (fast and normal) plus traffic types running on TCP/IP which we consider less time critical are marked as SM streams and are statistically multiplex on to the same wavelength. This enables an efficient utilization of the wavelength.

Furthermore, we proposed an architecture of mixed traffic priorities on the aggregation interfaces and estimated the delay values incurred on GST streams in combining different traffic priorities on interfaces of both arrival and departure nodes. The delay is different for combined GST and SM within one interface versus dedicated GST and SM on two different interfaces, i.e. when traffic priorities are combined within the same interface there is an additional delay incurred due to the combination process. In a network architecture scenario including 100 km transmission distance it was found that a delay of 556.6 *us* for the GST traffic, significantly lower than the acceptable transfer time of maximum 10 *ms*, can be reached.

Applying the Fusion concept is therefore found to be a feasible solution for transport of time critical data across substations with guaranteed QoS of low deterministic delay and ultra-low PDV. In future, we intend to investigate the effect on offered load of SM traffic due to the combined traffic priorities on the proposed aggregation interface.

## References


[1] R. E. Mackiewicz, "Overview of IEC 61850 and Benefits," in *Proc. IEEE PES Power Systems Conference and Exposition*, Atlanta, GA, 2006, pp. 623-630.

[2] I. Xyngi and M. Popov, "IEC61850 overview - where protection meets communication," in *Proc. 10th IET International Conference on Developments in Power System Protection*. *Managing the Change*, Manchester, 2010, pp. 1-5.

[3] IEC/TR 61850-90-1, Communication Networks and Systems for Power Utility Automation – Part 90-1: Use of IEC 61850 for the Communication between Substation.

[4] IEEE Standard for Local and metropolitan area networks, Virtual Bridged Local Area Networks, IEEE 802.1Q-2005, December 2005.

[5] R. Veisllari, S. Bjornstad, K. Bozorgebrahimi, and N. Stol, "Providing ethernet circuit quality of service and high bandwidth efficiency through fusion networking," *Norsk Informatikkonferanse NIK*, 2013.

[6] S. Bjornstad, D. R. Hjelme, and N. Stol, "A packet switched hybrid optical network with service guarantees," *IEEE J. Sel. Areas Commun*., vol. 24, no. 8, pp. 97–107, 2006.

[7] R. Veisllari, S. Bjornstad, J. P. Braute, K. Bozorgebrahimi and C. Raffaelli, "Field-trial demonstration of cost efficient sub-wavelength service through integrated packet/circuit hybrid network [invited]," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 7, no. 3, pp. A379-A387, March 2015.

[8] IEC 60870-4, Telecontrol Equipment and Systems, Part 4: Performance Requirements, 1990.

[9] Advanced Power Grid Protection Next Generation Tele Protection Solutions. [Online]. Available: http://studylib.net/doc/8743237/advanced-power-grid-protection

[10] Fusion networking explained. TransPacket White Paper [Online]. Available: http://subsystems.transpacket.com/wpcontent/uploads/2016/09/White_paper_fusion_intro_12062012.pdf

[11] R. Veisllari, N. Stol, S. Bjornstad, and C. Raffaelli, "Scalability analysis of SDN-controlled optical ring MAN with hybrid traffic," in *Proc. IEEE International Conference on Communications*, Sydney, NSW, 2014, pp. 3283-3288.

[12] TRANSPACKET H1: A fusion networking add-drop mux-ponder. TransPacket White Paper [Online]. Available: http://www.transpacket.com/fusionh1/fusion‐ethernet‐h1/

[13] Application Considerations of IEC 61850/UCA 2 for Substation Ethernet Local Area Network Communication for Protection and Control, IEEE PSRC H6: SPECIAL REPORT.

[14] C. H. R. de Oliveira and A. P. Bowen, "Iec 61850 goose message over wan," in *Proc. International Conference on Wireless Networks*, 2012.

**Charles M. Adrah** was born in Ho, Ghana, in 1986. He received the B.S. degree from the Kwame Nkrumah University of Science and Technology (KNUST), Ghana, in 2008, in Electrical Engineering, and the M.S. degree from the Norwegian University of Science and Technology (NTNU), Trondheim, in 2012, in Telematics. He is currently pursuing the Ph.D. degree with the Department of Information Security and Communication Technology, NTNU. His research interests include smart grid communication networks, quality of service and performance evaluation.

**Steinar Bjørnstad** is a professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim. He is also with TransPacket AS, Oslo 0277, Norway. His research interests include optical networks, performance evaluation, QoS, wireless networks.

**Øivind Kure** is a professor with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Trondheim. He got his Ph.D. from the University of California, Berkeley in 1988. His current research interest is in various aspects of QoS performance analysis, multicast protocols, and ad hoc networks.

# PAPER G

## Achieving Guaranteed Performance for Protection Traffic in Smart Grids Wide-Area Networks

C. M. Adrah, A. K. Kamath, S. Bjørnstad, and M. P. Tahiliani,

2019 IEEE International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2019, pp. 42-47.

# Secondary Papers

# PAPER H

## Hardware-in-the-loop testing of impedance protection with compensation of fault impedance and DG in feed current

K. Pandakov, C. M. Adrah, Z. Liu, H. Kr. Høidalen, and Ø. Kure,
The Journal of Engineering, vol. 2018, no. 15, pp. 1018-1022, 10 2018.

The standard impedance protection deployed in distribution networks can malfunction due to underreach errors caused by fault impedances and remote infeed currents from embedded generators (becoming more and more widespread). This paper introduces a compensation method aiming at elimination of these issues and enhancement of relay dependability. As an advantageous outcome, compensated measurements can be utilised for accurate fault location. The method is verified on ABB RED 670 relay in the loop with an OPAL-RT real-time simulator. As the method is based on multipoint measurements, the test setup also contains a communication network emulator for modelling network delays and imperfections. The laboratory tests verify applicability of the method with proper appearance of the tripping signals from the relay. The fault location results based on synchronised data show overreaching inaccuracy rising with fault resistance. Though communication network delays and imperfection of the channels lead to underreaching, it has been revealed that not strict requirements for data synchronisation can be applied to specific measurements.

# PAPER I

## Fusion Networking for IEC 61850 Inter Substation Communication

C. M. Adrah, S. Bjørnstad, and Ø. Kure,
2017 IEEE International Conference on Smart Grid and Smart Cities(ICSGSC), Singapore, 2017, pp. 152-156.

This paper explains how Fusion networking technology can be used as a communication mechanism between utility substations for transporting time critical traffic in wide area power system protection applications to attain deterministic low delay, zero packet loss and ultra-low packet delay variation. The requirements for inter substation communications are presented with focus on the IEC 61850 protocols of Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SMV) and their adaptability to the traffic classes of guaranteed service transport (GST) and statistically multiplexed (SM) in Fusion networking technology.

# PAPER J

## A Method for Performability Study on Wide Area Communication Architectures for Smart Grid

T. Amare, C. M. Adrah, and B. E. Helvik
2019 7th International Conference on Smart Grid (icSmartGrid), Newcastle, Australia, 2019, pp. 64-73.

An extensive use of ICT is a key feature in the development of next generation smart grids. The ability of the ICT system to meet the real time requirements of the powers system, even when it is degraded due to failures, is essential. This simultaneous study of dependability (reliability) and performance are referred to as performability. This paper presents a method for a performability study on ICT support system of smart grid. It looks into how performance associated properties (timing failures) can be modelled together with properties affecting dependability such as omission or conventional component failures. A two tier model using ns-3 and SAN is developed to study the peformability of an IEC 61850 based communication infrastructure for a protection application. For illustration, a simulation is conducted to study the reliability and unavailability of an IEC 61850 based communication architecture, where the impact of both timing failures and omission failures are investigated and compared. The result revealed that the availability and reliability is highly dependent on the requirements for the protection application, maximum delay per packet and maximum number of consecutive delayed packets the protection application can tolerate. It also shows that timing failures have a higher impact than omission failures for a protection application with shorter time requirement.

ISBN 978-82-326-4850-4 (printed ver.)
ISBN 978-82-326-4851-1 (electronic ver.)
ISSN 1503-8181

Doctoral thesis
Charles Mawutor Adrah

Doctoral theses at NTNU, 2020:251

Charles Mawutor Adrah

# Communication Networks for Protection Systems in Smart Transmission Grids

Doctoral theses at NTNU, 2020:251

**NTNU**
Norwegian University of Science and Technology
Thesis for the degree of Philosophiae Doctor
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

NTNU
Norwegian University of Science and Technology

NTNU
Norwegian University of Science and Technology