Design, Implementation, and Evaluation of Secure Communication for Line Current Differential Protection Systems over Packet Switched Networks

Andreas Aichhorn[a,b], Bernhard Etzlinger[c], Andreas Unterweger[d], René Mayrhofer[a], Andreas Springer[c]

[a] *Institute of Networks and Security, Johannes Kepler University, Linz, Austria*
[b] *Research and Development Department, Sprecher Automation GmbH, Linz, Austria*
[c] *Institute for Communications Engineering and RF-Systems, Johannes Kepler University, Linz, Austria*
[d] *Center for Secure Energy Informatics, Salzburg University of Applied Sciences, Salzburg, Austria*

Abstract

In this work we propose a secure communication concept for the protection of critical power supply and distribution infrastructure. Especially, we consider the line current differential protection method for modern smart grid implementations. This protection system operates on critical infrastructure, and it requires a precise time behavior on the communication between devices on both ends of a protected power line. Therefore, the communication has to fulfill deterministic constraints and low-delay requirements and additionally needs to be protected against cyber attacks. Existing systems are often either costly and based on deprecated technology or suffering from maloperations. In order to allow for both, economical and reliable operation, we present the first holistic communication concept capable of using state-of-the-art packet switched networks. Our solution consists of three parts: (i) we develop a list of design requirements for line current differential protection systems communication; (ii) we propose a communication concept obeying these design requirements by combining cryptographical and physical security approaches; and (iii) we evaluate our solution in a practical setup. Our evaluation shows a clock accuracy of 3 microseconds with a resilience to asymmetric delay attacks down to 8 nanoseconds per second. This demonstrates the secure and fault-free operation of a line current differential protection system communicating over a state-of-the-art network.

Preprint submitted to International Journal of Critical Infrastructure Protection February 19, 2018

Keywords: Power System Protection, Line Current Differential Protection, Clock Synchronization, Network Security, IPsec, Critical Infrastructure Protection, Wide Area Network, Ethernet

1. Introduction

The power grid is responsible to provide electrical energy to meet the needs of the society. Hence, the power grid is a critical infrastructure as referred in the *Official Journal of the European Union* [1] and has to be protected against faults, like an earth fault or short circuit that would have high economical impact if not detected accurately. Basically, three protection principles are used for grid protection according to [2]: overcurrent protection, distance protection, and differential protection. Additionally, these systems need to be secured from malicious, intentional attacks from outside the grid to provide a holistic protection of the critical infrastructure. This work addresses the security issues that arise from such attacks on the communication interface for differential protection.

The influential change of the electrical grid from a hierarchical to a distributed topology causes a variety of consequences, like reverse power flow which disrupts existing power grid protection systems, as discussed in [3, 4]. This change is rooted by introducing Distributed Renewable Energy Sources (DRES), e.g., wind and photovoltaic power plants, which are replacing centralized big scale power plants, e.g., coal and nuclear power plants. Lightner and Widergren [5] previously discussed this grid evolution and the aggravating effect of arising lack of power due to non-controllable environmental situations at decreased wind speed or illumination from the sun. Hence, a power grid including a power control is required to cover the demand of electrical energy in a power grid with DRES. As a consequence, the direction of the power flow is changing depending on environmental factors.

Alvin et al. [3] already discussed the impact of the power flow direction on protection systems and proposed a phase comparison scheme based on the same principle as the differential protection scheme. It is inevitable to adapt the protection schemes to the resulting characteristic of the evolved distributed power grid. To establish safe operation of the grid, a robust and flexible protection system is necessary which can handle bidirectional energy flow, as discussed in [3, 6].

Overcurrent and distance protection are well established protection types, suffering from complex coordination of the relay parametrization in a grid

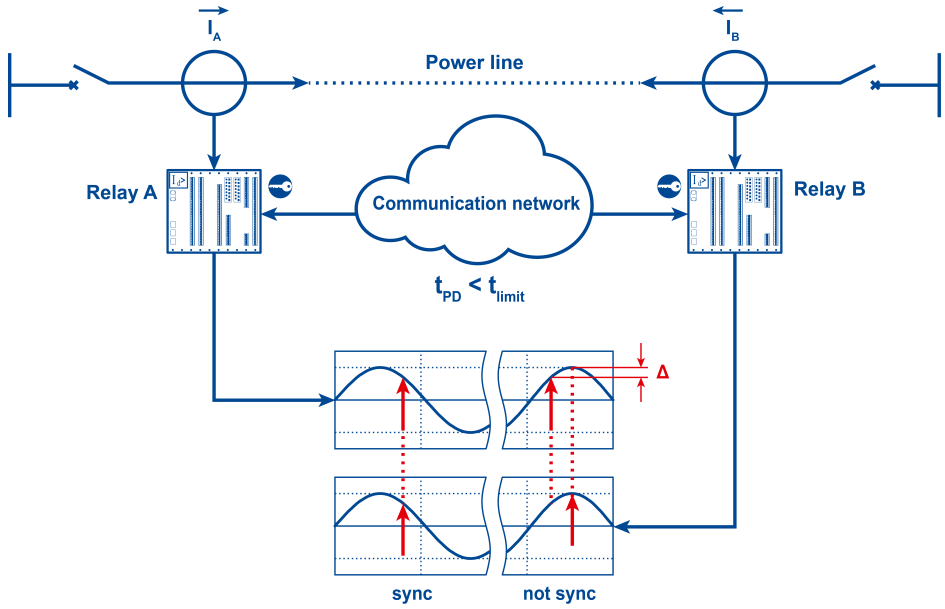

Figure 1: Arrangement of a Line Current Differential Protection (LCDP) system.

with frequent change of the power flow direction. In contrast, the big advantage of a differential protection system is the absolute selectivity in its protection area and its correct function independent of the energy flow direction. This scheme, according to Fig. 1, is proposed to work most efficient in a power grid with increasing penetration level of DRES [4]. Therefore, the importance of differential protection and especially Line Current Differential Protection (LCDP) is increasing in the grid and is considered in this work because of its convincing characteristics.

In this work, LCDP protection relays as discussed in [6] are contemplated, which compare the measured currents between the ends of the power line (e.g., overhead line or cable). According to Kirchhoff's current law, the resulting current must be zero in a non-fault condition. If there is a resulting current above a preset threshold, a fault in the power system is detected. To get an accurate result of the difference current, measurement values from the same point in time have to be compared. Therefore, synchronized sampling at both ends of the line is required to yield proper results.

Fig. 1 shows the basic arrangement of such a system at the top and the diagram on the bottom shows on the left side accurately synchronized samples, whereas resulting difference current caused by poor synchronized

samples is shown on the right side. Therefore, accurate synchronization is inevitable for LCDP systems, otherwise a spuriously calculated difference current is the result. As a matter of the functional principle a communication between the protection relays, i.e., the protection interface, is required to exchange their measurement values. The timing constraint for transferring the measurement value, i.e., path delay t_{PD} along the communication channel, must be lower than the specified limit t_{limit} (cf., Fig. 1).

An LCDP system is a vital protection approach for the prevailing grids, yet suffering from high interface costs. Todays realizations either use a dedicated Fiber Optical (FO) cable, or a communication network with a Time Division Multiplexing (TDM) method (e.g., Synchronous Digital Hierarchy (SDH)). TDM-based systems served well through the 1990s, but reached end of life, as discussed in [7, 8]. This Wide Area Network (WAN) technology is replaced by Packet Switched Networks (PSNs), like Ethernet [9]. Further literature [10] (Sec. I) also stated that PSNs are increasingly adopted by electrical utilities because of: *"packet-based networks offering several operational benefits; the lack of availability of leased Time-Division Multiplexing (TDM) services; the decline of expertise and availability of legacy technologies; and network infrastructure cost optimisations"*. A secure and efficient communication concept to use Ethernet WANs for the protection interface has not been discussed yet and is proposed in this paper.

Security investigations are of big importance in addition to protecting the grid from system faults in order to maintain a safe operation and high availability. Hansen et al. [11] previously discussed the vulnerability of the power grid to cyber attacks referring to the attacked Ukrainian power grid. Therefore, availability, confidentiality and integrity has to be ensured to provide a secure operation of the protection system. In order to achieve this, well-established protocols are available (e.g., IPsec [12] or Transport Layer Security [13]), to meet the security requirements. Nevertheless, it is not possible to prevent all possible threats (e.g., packet dropping and asymmetric delay attacks).

In the following, we describe related work, the contributions of our work and this paper's structure.

1.1. Related work

To realize an efficient concept that uses Ethernet communication systems for the protection interface, the requirements for the communication have to

be identified first. Operational requirements for LCDP according to standard exist [2, 14], but no holistic summary for the communication interface.

The authors in [15] use the Global Positioning System (GPS) for clock synchronization. GPS is not contemplated in this work by reason of security issues (e.g., GPS spoofing [16]). Another approach focuses on using channel-based clock synchronization, like the Precision Time Protocol (PTP) according to [17], which needs correcting clocks along the communication path and the data transfer is based on Layer 2 Ethernet messages [18]. The use of correcting clocks is costly and most existing infrastructures do not support them. Blair et al. [10] discusses the realization of an LCDP system over an IP-based Multi Protocol Label Switching (MPLS) WAN without sampling synchronization between the protection relays to compensate the influence of the jitter caused by the PSN. The correction of asymmetric latencies or jitter, respectively, is performed by using a feature of special WAN devices called asymmetrical delay control. Their implementation presents a cost-effective solution, but suffers from possible maloperations, i.e., unwanted operation of the protection relay.

[19] and [20] propose clock synchronization algorithms for exponential distributed delays, like they occur in PSNs. No implementation and no measurement was presented in real-life systems so far.

A predestined protocol for securing IP-based Ethernet communication is IPsec [12]. A major security issue for channel-based clock synchronization, which can not be solved by using IPsec, is the asymmetric delay attack. IPsec covers security threads on the IP layer in terms of protecting the content of the message without any focus on timing constraints. The delay attack represents a physical attack on the system, where time sensitive synchronization messages are intentionally delayed in one direction only which yields a distortion of the clock synchronization. In the field of power system protection, especially for LCDP systems, a correct and precise clock synchronization is inevitable. A distortion of the clock synchronization may lead to a malfunction of the protection system and threatens the power system which is a critical infrastructure. Several approaches were published to solve the issue of the delay attack, which is discussed in the following paragraphs, but no such proposed solution can solve this issue for the LCDP system.

Ganeriwal et al. [21] present a threats analysis and propose a secure clock synchronization method for wireless sensor systems. The delay attack is discussed and a countermeasure is proposed to compensate the estimated injected delay to synchronize during such an attack. The basic idea is to

observe the delays from $A \rightarrow B$ and $B \rightarrow A$. A delta delay Δ is introduced to estimate if an attack is performed. The probability to detect a delay attack is increasing if the injected delay increases. For their system, a reliable delay attack detection is reached for an injected delay of $\Delta \geqslant 30\,\mu$s, where the LCDP system already violates the required synchronization accuracy (cf., Sec. 2). Further, the authors of [21] only consider a single step of introduced delay but not a slight incremental injected delay (e.g., 8 ns/s which is discussed in this paper). Therefore, [21] has not investigated the slight but steady increase of the injected delay which is malicious and jeopardizing for LCDP systems.

Moussa et al. [22] propose the use of GPS receiver in addition to the channel-based clock synchronization for a plausibility check of the estimated clock parameter. For this approach it is assumed, that a GPS spoofing attack is not happening at the same time as delay attack and additional GPS receivers are required for the realization. Mizrahi [23] requires multiple communication paths to create a reference for the validation of the received time information to detect anomalies of the clock synchronization. Hence, it is assumed that the used communication paths are not simultaneously affected by a delay attack and more than one active communication channel is required for this approach. Since Moussa et al. and Mizrahi assume that no simultaneous attack is going on and only a single communication path without additional use of GPS is contemplated in this work, these approaches do not provide a sufficient detection method for delay attacks in the application of LCDP systems. We already presented a threats analysis and a relating security concept solving the delay attack problem designed for LCDP systems without an assumption of a non-attacked reference time in [24].

1.2. Contributions

With the increased penetration of Smart Grids, communication infrastructures based on PSN (e.g., Ethernet), is widely available. A secure, accurate and cost-efficient system architecture for the protection interface of an LCDP system using this widespread available infrastructure is the key feature for the broad application of LCDP systems to maintain system safety of state-of-the-art power grids.

In this work, a new communication concept for the protection interface is developed, which fulfills the necessary requirements to realize a secure and accurate working LCDP system which uses the existing Ethernet infrastructures. From [24, 14] we summarize the operational requirements on the

communication and present a suitable solution for the protection interface. The contributions of this paper are:

- A complete set of requirements for the protection interface communication system of an LCDP system communicating over PSN;
- A holistic concept that enables secure and cost-efficient implementation of the protection interface communication system of an LCDP system without the risk of maloperations;
- Verification measurements of the implemented proposed clock synchronization algorithm in an embedded system, tested in real-life PSN infrastructures;

This article includes a comprehensive analysis of some aspects which have previously appeared in [25, 19, 24]. First, the concept bases on the proposed transport protocols from [25] including a channel-based clock synchronization from [19] which is implemented in hardware and tested in active Ethernet WANs under various conditions and the relating results are presented in this paper. Second, the proposed security concept, presented in [24], is enhanced investigated in this work for its interoperability. The holistic concept including the requirements, the implementation and the evaluation is presented in this paper.

1.3. Paper organization

Section 2 specifies all requirements for a PSN-based protection interface communication system of an LCDP system. Section 3 presents a state-of-the-art implementation of the protection interface using PSNs. Section 4 presents the proposed concept of using existing PSNs for fulfilling the specified requirements and Section 5 evaluates it. The conclusion is finally presented in Section 6.

2. Requirements for the protection interface communication system of LCDP systems

This section summarizes the necessary requirements for the protection interface communication system of an LCDP system. We first provide a general description of LCDP systems, followed by a detailed set of requirements, shown in Sec. 2.1 to 2.7. Sec. 2.8 summarizes the requirements which are subsequently illustrated in Table 1.

The aim of a power system protection relay is to detect and clear faults in a power system. The total clearing time[1] should be as low as possible to minimize the impact of such a fault on the surrounding parts of the grid. The basic arrangement of the protection scheme considered in this research, an LCDP system is, depicted in Fig. 1. As a matter of principle, the data from relay A has to be transmitted to relay B and vice versa to be able to compare against the tripping criterion, i.e., the threshold difference current at which the power line has to be switched off.

The operation of the LCDP system is divided into two protection modes, the main and the back-up protection mode. The main protection mode is the standard operation mode of the LCDP, with the difference current used to build the tripping criterion. If the relays recognize (e.g., by a concept proposed in this work) that the communication system is not trustworthy, the protection device switches over to the back-up protection mode (e.g., overcurrent protection). In this case, the power line is still protected, but suffering from the disadvantages of the implemented protection scheme.

Clock synchronization is inevitable to yield accurate results for the calculated difference current, as demonstrated in the diagrams in Fig. 1. Communication latency, i.e., path delay t_{PD}, must be underneath a certain level to ensure adequate clearing times. If the threshold value for the communication latency is exceeded, the requirement on determinism (see Sec. 2.5) is violated. The necessary bandwidth for transmitting the measurement values has to be provided by the communication network. The used communication network needs to be resilient to maintain a highly available and reliable protection interface. To yield a wide utilization of the system, cost-efficiency is of big importance.
The rest of this section discusses these requirements for the protection interface communication system to operate a proper LCDP system.

2.1. Clock synchronization

To maintain accurate operation of the LCDP system, the measurement data from the local and the remote station (assuming Relay A is the local and Relay B the remote station) have to be allocated a timestamp to be able to compare the measurement values from the same point in time. Therefore,

[1] *"The maximum time between the fault initiation and its clearing such that the power system is transiently stable"*, according to [26]

accurate clock synchronization is required. IEC 61850-90-1 recommends a maximum deviation of 10 μs for LCDP systems if high fault current sensitivity is required [14].

2.2. Security

In order to protect against intentional attacks, like Blackmailing or Nation-State Attacks, security measures have to be conducted. Hansen et al. [11] presents disruptions of the Ukraine's power system in 2015, caused by malicious attacks.

Therefore a security concept for LCDP systems is inevitable. To the best of our knowledge, no previous work apart from [24] is published, which describes the security requirements for the protection interface of an LCDP system in terms of intentional attacks.

The IEEE standard 1686-2013 [27] recommends countermeasures against security vulnerabilities for power system protection devices, whereas LCDP systems, i.e., teleprotection devices, are explicitly excluded. Therefore, we have discussed these requirements including a detailed threats analysis in a previous publication [24], resulting in the need for integrity, confidentiality and availability. While IPsec can ensure a cryptographic security against cyber attacks on the protection interface communication system, it can not protect from physical channel attacks (e.g., delay attack by injecting additional delay) that may yield a malfunction of the system.

For this case, it is necessary to detect if the communication is affected by an attack. Thus, the security measure needs a reliable detection if such physical attacks are happening. In this case, the operation mode of the protection relay has to switch over to the back-up protection mode such that the power line is still protected, albeit with a less favorable protection mode. Therefore, it is also part of the security measure, in addition to a security protocol, to detect unpreventable attacks for maintaining a secure communication and consequently a safe operation of the power line.

2.3. Communication latency

The communication latency t_{PD} is the time it takes for transferring one measurement value to the remote station. It is added to the default tripping time and thus is subject of minimization to maintain a low clearing time. IEC 61850-90-1 [14] recommends a maximum t_{pd} on the communication channel of 5 to 10 ms depending on the voltage level and is limited in this work with 10 ms. In PSN-based communication networks, the path delay t_{PD} depends

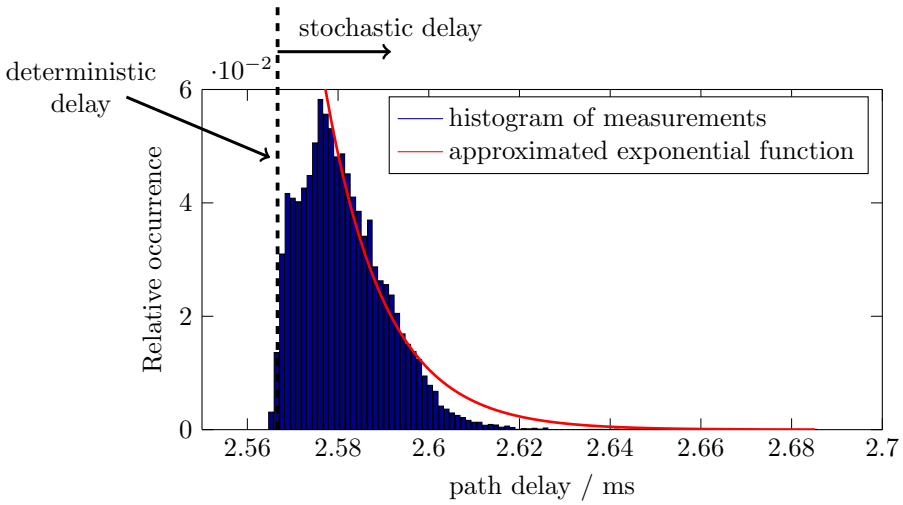

Figure 2: Histogram and approximated exponential function of 20 000 path delay measurements in an MPLS network across 14 hops. FO cable length is approximately 300 km.

on a deterministic and on a stochastic part. The deterministic delay depends on the port speed, packet size, number of switching devices along the route and the FO cable length. The stochastic part depends on the traffic load. Fig. 2 shows a histogram of path delay measurements including the separation of the deterministic and the stochastic part.

2.4. Bandwidth

Besides synchronization data, comprising timestamps, measurement data also has to be transferred over the protection interface. Basically, two different types of measurement data can be used for creating the tripping criterion: sample values or vector data. If vectors of measured values, based on one cycle (e.g., RMS value) are transmitted, only one message has to be sent per cycle per direction, which is equal to 50 data vectors per second in a 50 Hz system like in Europe. Therefore, just every 20 ms new measurement data is transferred to calculate the tripping criterion. To accelerate the reaction time of the protection algorithm and calculate various characteristics, momentary measurement values have to be transmitted. In this specific application the measured samples are transferred with a frequency of 1 kHz.
The required bandwidth for this implementation (in both directions) is 1.57 MBit/s on wire (including packet overhead), consisting of the measured samples and the timestamp exchange. This exchange is performed using IP-based proto-

cols, like SCTP for the measurement data stream and UDP for the timestamp exchange.

2.5. Real-time / Determinism

Besides the communication latency, real-time constraints have to be fulfilled. In general, real-time requirements can be classified into levels [28], the highest being Hard real-time – if the timing requirement cannot be met, the correct behavior of the entire system is jeopardized. Since the protection system is responsible to protect the power grid, which is a critical infrastructure, *hard real-time* is necessary in this safety-critical application.

2.6. Availability

The functional principle of the LCDP system requires measurement data from the local and the remote device to build the tripping criterion. Hence, the protection interface communication is required for the operation of the LCDP system in the main protection mode. Therefore, the availability of the protection system in main mode is depending on the availability of the contemplated communication system.

The occurrence as well as the duration of communication errors are relevant to define the availability of the whole protection system. Primarily, the parts of the communication system (e.g., switch or router with its electronic components) need to provide high system stability, which define the Mean Time Between Failures (MTBF). Secondarily, if a communication failure occurs, the failure time also influences the availability of the LCDP system. The average time until the LCDP is again in regular operation is defined as the Mean Time To Recover (MTTR). The attributes MTBF and MTTR are defined according to [29]. Consequently, the communication system has to be designed with highest priority to maximize MTBF and minimize MTTR, i.e., optimize the availability of the protection system [18].

Therefore, a communication system with best possible availability with maximum possible MTBF and a minimum of MTTR is required in order to achieve a highly available protection system according to [18].

2.7. Cost-efficiency

Besides all technical relevant requirements for the protection interface communication system, a concept enabling cost-efficient operation is a decisive requirement to enable a widespread use. Therefore, the installation and operating costs for the protection interface communication system needs to

Table 1: Summary of LCDP requirements and evaluation results.

		Proposed Method	
Attribute	**Required Limit / Definition**	**Measured / Concluding**	**Fulfilled**
Synchronization accuracy	$10\,\mu$s	$< 3\,\mu$s	✓
Communication latency	10 ms	< 2.7 ms	✓
Necessary bandwidth	1.57 MBit/s	provided bandwidth > 10 MBit/s	✓
Real-Time	Hard Real-Time	no violation of timing constraints	✓
Security	Integrity, Confidentiality and Availability	Provided by IPsec plus delay attack detection	✓

be as low as possible. If a concept enables the use of existing Ethernet-based WANs (e.g. IP/MPLS according to [30]), the economic factor is increased compared to protection interface communication systems realized over a dedicated FO cable.

2.8. Summary

Table 1 summarizes all technical quantifiable requirements for the protection interface (communication system) of an LCDP system. The attributes availability and cost-efficiency are not listed in the table, because these values depend on the application specification of the individual operator of such a system and can not be generalized.

3. State-of-the-art implementation of the protection interface

Since a dedicated fiber optical cable would be the best solution from the technical point of view, whereas the economic point of view is not supporting this solution. Considering a distance of hundreds of kilometers between the

protection relays, it is very costly to place a dedicated fiber for only this application. In real-life, FO cables are used to connect WANs, Ethernet-based nowadays, with a high bandwidth utilization to increase the cost-efficiency. Ethernet is using packet switching to yield bandwidth efficiency and is therefore not deterministic by its nature. The following paragraph describes the state-of-the-art implementations and their shortcomings for using Ethernet as protection interface communication system.

3.1. Transport protocol

Power system communication has been already performed by using Layer 2 Ethernet messages, like the standardized Generic Object Oriented Substation Event (GOOSE) messages described in [31]. Liu et al. proposed to use GOOSE messages for an LCDP system [15].

3.2. Clock synchronization over Ethernet-based networks

Clock synchronization is not provided by standard Ethernet services. Therefore, additional services are required, either external timing sources (e.g., GPS receiver or 1 pulse-per-second signal) or a channel-based clock synchronization approach. Synchronization using external timing sources are not contemplated in this work because of additional effort and uncertain security characteristics.

A predestined and standardized protocol for channel-based clock synchronization with achievable accuracy limits of less than $1\,\mu$s is PTP [17]. An obstacle for using this protocol is that the whole infrastructure has to support this standard. In this case, all network devices, i.e., switches and/or routers, along the synchronization path, require correcting clocks. This is costly and thus not a cost-efficient solution which would be accepted by the energy provider. In addition, to secure the clock synchronization, PTP messages have to be encrypted. Since these synchronization messages need corrections from the correcting clocks, the network device has to be able to read the content of the synchronization message. Consequently, the encrypted message has to be de- and encrypted at each network node, which weakens the whole security concept. The whole security system is broken as soon as only one single network device is compromised. The strongest concept would be to establish an End-to-End encryption for synchronization messages, which is not possible by using state-of-the-art methods so far.

3.3. Real-Time capability of Ethernet-based networks

Real-time requirements can not be fulfilled by using PSN Ethernet without additional services, since at high channel utilization messages are stored in a queue and processed according the First-In-First-Out principle. By implementing Quality of Service (QoS) according to [32], data packets can be prioritized. A proper engineering of the network decreases the stochastic part of the network delay behavior (cf., Fig. 2) for dedicated subscriber or packets, respectively. Important for the LCDP system is that the measurement value is transmitted within the maximum allowed communication latency of 10 ms, depending on the applied voltage level. Therefore, a well engineered setting is able to maintain a sufficiently deterministic data transfer. The problem of using PSNs for LCDP systems is the occurring jitter which depends on the traffic load. Therefore, a proper concept is required.

3.4. Cost-efficiency

Gowan [7] shows the cost-efficiency difference between legacy TDM-based SDH systems and state-of-the-art PSN-based communication technology, like Ethernet, referred to as packet-optical platform. The whitepaper illustrates the cost savings by a case study of a data processing service center. There, only 3 bays of a packet-optical platform are necessary compared to the 60 bays required for a comparable SDH system. Therefore, floor space savings are evident, as well as reduction of electric power consumption by the network devices, which save up to 92%. Consequently, installation and operational costs are convincing economic factors to use packet based systems. Ref. [8] also stated, that the cost efficiency is increased by PSN systems compared to TDM systems whereas this factor is not quantified in that report. Further, Blair et al. [10] also states that packet-based WANs improve cost-effectiveness for utility applications.

3.5. Summary

Since Ethernet-based WANs are to be used for the protection interface and state-of-the-art implementations do not fulfill the requirements, a concept fulfilling them has to be developed.

4. Proposed communication concept for the protection interface using PSNs

According to Sec. 3, it is not possible to fulfill all necessary requirements for the protection interface of an LCDP system by using Ethernet with state-

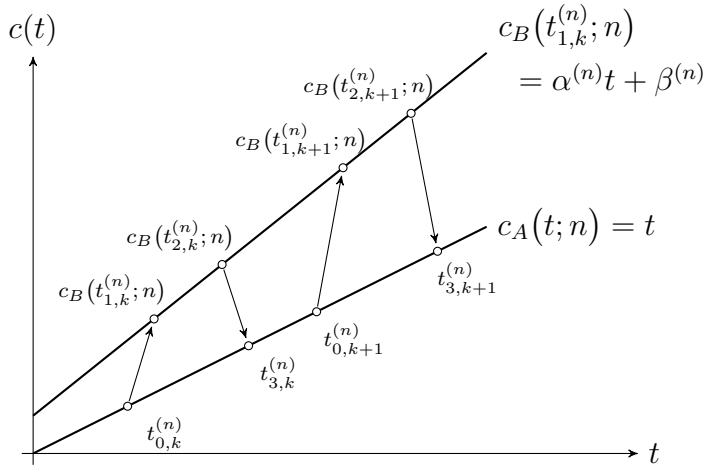

Figure 3: Clocks $c_A(t;n)$ and $c_B(t;n)$ of the protection relays A and B in the nth time interval, where $c_A(t;n)$ has slope = 1 and $c_B(t;n)$ slope = $\alpha^{(n)}$. The arrows between the counter function indicate the packet rounds for $k = 1, ..., K$ in time interval n.

of-the-art methods. The aim of this research is to solve these open issues to enable the use of existing Ethernet WANs for the protection interface of LCDP system, which is also applicable to other secure real-time measurement data exchange applications. This section describes the proposed architecture of the protection interface extending our previous work [25, 19, 24].
Sec. 4.1 discusses the proposed transport protocol which is the basis of the communication concept. Sec. 4.2 presents the clock synchronization algorithm for a PSN without correcting clocks. Sec. 4.3 presents the corresponding security concept.

4.1. Transport protocol

For LCDP systems, it is advantageous to make use of IP-based protocols, instead of using Layer 2 protocol messages like GOOSE, to be routable over an Ethernet network across several network router. In addition, IP-based protocols enable the possibility of continuous encryption between the protection devices, i.e., End-to-End encryption.

4.2. Clock synchronization

Accurate clock synchronization is of fundamental importance for LCDP systems with PSN-based communication system for the protection interface that the occurring jitter on the network does not influence the protective

function. To achieve the synchronization accuracy requirement of $10\,\mu$s stated in Table 1, and to observe the communication latency, usually either a GPS receiver or PTP synchronization is used. However, as stated in [10], those are non-favorable solutions due to vulnerabilities of GPS and extensive upgrade costs of existing network infrastructure to be PTP capable and its lack of End-to-End encryption.

In this work, we use a clock synchronization scheme, originally introduced in [19], that enables End-to-End encryption. It (i) estimates the clock parameters of offset and skew, (ii) tracks their values over time, and (iii) adjusts the local clocks to achieve a synchronous state. Additionally, the algorithm returns an estimate of the channel delay, which is assumed to be symmetric in distribution in both directions. This synchronization scheme only depends on measured packet transmission and arrival times at the two relays as depicted in Fig. 3, i.e., it does not require specific capabilities of the communication network.

In the nth time interval, the packet exchange is illustrated in Fig. 3. Relay A is considered as clock master, and relay B as clock slave with a clock phase $\beta^{(n)}$ and a clock frequency offset (skew) $\alpha^{(n)}$ relative to relay A. The relation of the counter values $c_A(t;n)$ and $c_B(t;n)$ at the kth packet transmission and reception are

$$c_B(t_{1,k}^{(n)};n) = \alpha^{(n)} t_{0,k}^{(n)} + \beta^{(n)} + \Delta^{(n)} + \delta_{AB,k}^{(n)}, \tag{1}$$

$$t_{3,k}^{(n)} = \frac{c_B(t_{2,k}^{(n)};n) - \beta^{(n)}}{\alpha^{(n)}} + \Delta^{(n)} + \delta_{BA,k}^{(n)}\,. \tag{2}$$

This model assumes a deterministic delay $\Delta^{(n)}$ that is the same in both directions, and a stochastic delay $\delta_{AB,k}^{(n)}$ and $\delta_{BA,k}^{(n)}$. The stochastic delay can be modeled according to relevant measurements, depicted in Fig. 2, as exponential distribution. The measurements were collected in a real-life network operated by an Austrian energy provider, in which the communication link was comprised of 14 switches and approximately 300 km FO cable. Based on this model, an algorithm that estimates the clock parameters in every time interval n, adjusts the local clock of relay B accordingly, is derived [19].

The algorithm assumes symmetric conditions of the deterministic delay $\Delta^{(n)}$, i.e., the delay is the same on the path from relay $A \to B$ and $B \to A$. Therefore, the network path has to be routed over the same path for both directions, which can be easily done by proper network engineering. However, the synchronization accuracy and hence the operation of the LCDP

can be distorted by injecting asymmetric delays. For example, an attacker introduces additional delay in one direction. As the synchronization procedure depends on time measurements that need to be exchanged between the nodes, the synchronization can be distorted if this information is corrupted. In the following section, those issues are considered to ensure a holistic security concept.

4.3. Security concept

So far, the basic architecture of the protection interface to provide system safety is presented. To protect against intentional attacks on the communication, security measures are indispensable. In [24] we presented a detailed threats analysis, which is summarized in the following enumeration:

1. **Packet interception:** The attacker captures and reads the content of messages.
2. **Packet manipulation:** The attacker captures and modifies the content of messages.
3. **Reordering:** The attacker captures and changes the order of sending messages.
4. **Delay attack:** The attacker delays certain messages.
5. **Packet dropping:** The attacker drops messages.
6. **Replay attack:** The attacker resends captured messages.

Threat 1 yields a loss of confidentiality, threats $2-4$ yield a loss of integrity and threats $5-6$ yield a loss of integrity and availability. Standard encryption protocols can handle threats $1-3$ and 6. Since IP-based transport protocols are used, IPsec is used as countermeasure for these threats. Threat 3, reordering of packets, will only have a consequence on the system if timing constraints are violated as a result. Threats 4 and 5, delay attacks and packet dropping can not be covered by using IPsec. If packets are dropped, the application initiates a retransmission after a pre-defined timeout expires. If the measurement data is received within the required communication latency (cf., Table 1), even though triggered by a retransmission, these threat does not influence the protection function. As soon as the timing constraints are violated, the protection system has to switch over to the back-up protection. Therefore, the attack has an influence on the system, but the power line is still protected by the back-up protection.

Delay attacks have to be divided into symmetric and asymmetric delay attacks. With symmetric delay attacks, messages in both directions are sent with additional delay introduced by an attacker. Since the condition is symmetric for the message exchange, synchronization accuracy is not affected. There is no consequence on the system safety if the latency requirements are not violated. Asymmetric delay attacks are hazardous, since they distort the clock synchronization. If the sampling at the protection relays is not working synchronously anymore, a spurious difference current is calculated (c.f., Fig. 1 not synchronized mode) and a maloperation of the protection interface is the consequence in the worst case. To avoid this, we developed a delay attack detection algorithm [24].

Fig. 4 shows the influence of such an asymmetric delay attack in a real WAN. In this specific case a steady increase of 80 ns/s was injected on the link from relay A to B. The diagram on the top shows the measured path delay from both directions. The diagram on the bottom shows the influence of the asymmetric delay. The application does not recognize that the synchronization is not working properly anymore, indicated by the blue line. However, by applying an external measurement system, the time offset can be measured (red line) and it can be seen that the synchronization accuracy is violated. It is not possible to prevent this kind of attack, like packet interception, but it has to be detected, so that the protection device is able to switch over to the back-up protection to avoid maloperations in the worst case.

In [24] we proposed to use the estimated clock skew in combination with the estimated path delay, which is the output of our proposed clock synchronization algorithm. By setting a limit on the estimated path delay and observing the characteristics of the estimated clock skew, we are able to detect the injection of an asymmetric delay. The limit for the path delay criterion is derived from the required accuracy which is set to 10 μs. The criteria for the clock skew observation has to be individually set depending from the oscillator quality and the filter parameters of the clock synchronization algorithm.

5. Evaluation / Results

The evaluation of the proposed system architecture for the protection interface was performed in a real-life MPLS network of an Austrian utility company by using various topologies, routed across several network devices,

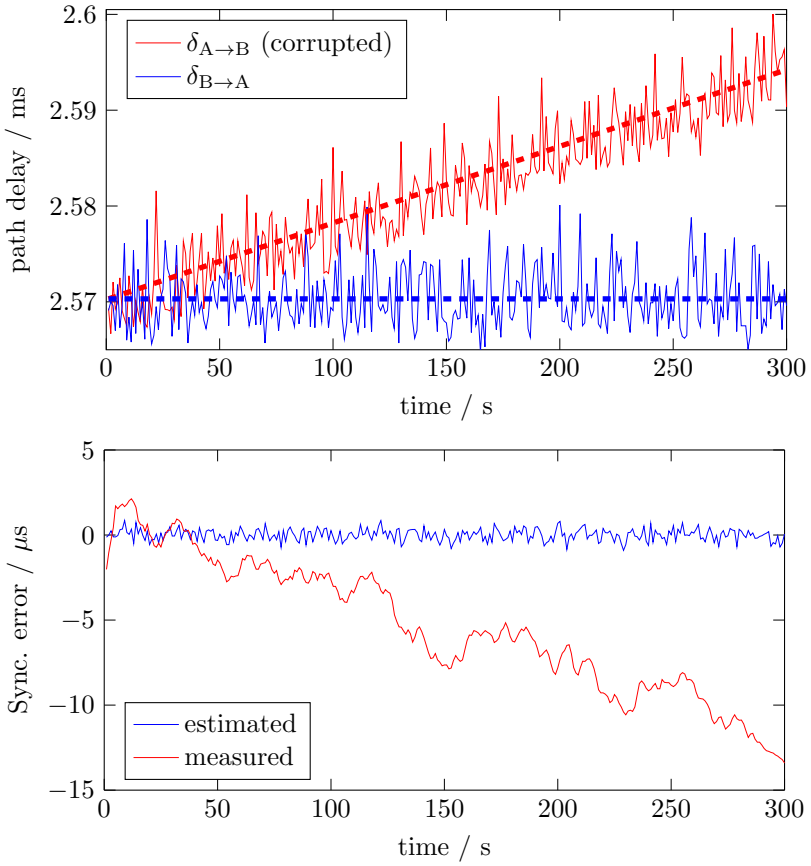

Figure 4: Influence of an asymmetric delay attack on the synchronization accuracy. (top) Measured path delays with an asymmetric delay attack on the link from relay A→B. (bottom) Estimated clock offset versus measured synchronization accuracy.

i.e., hops. To keep the measurement setup for the evaluation of the clock synchronization and the channel latency / path delay measurement as simple as possible, the interfaces for both protection relays are routed to the same substation. If the devices would be placed at different locations, the complexity of the measurement setup would increase whereas the accuracy of it would decrease. To evaluate the clock synchronization accuracy, the pulse-per-second output of both protection relays was compared. The path delay was measured by synchronously capturing the packets at both relays using a Hilscher NET ANALYZER-NXANL 50-RE card with a time resolution of 10 ns.

The link speed of the used network was 1 GBit/s with 10 MBit/s being reserved for our test. According to the requirements in Sec. 2 the necessary bandwidth is equal to 1.57 MBit/s on wire (including packet overhead). The following subsections present measurement results from the developed components.

5.1. Clock synchronization

Two different topologies are investigated to evaluate the clock synchronization accuracy: Topology A, consisting of 8 hops and a total FO cable length of 100 km, and topology B, consisting of 10 hops with a FO cable length of 250 km. Fig. 5 illustrates the histograms of the path delay, depicted on the top of the figure, whereas the bottom diagram illustrates the relating clock synchronization accuracies.

The measurement results demonstrate that the proposed synchronization algorithm yields the desired accuracy, even within a range of 3 μs. The necessary clock synchronization accuracy according to Sec. 2 is 10 μs. So, this quantity fulfills the requirement.

5.2. Security / Delay attack detection

The proposed countermeasure facing against delay attacks is to observe the estimated clock skew and the estimated path delay, as stated in Sec. 4-C. Various profiles of asymmetric delay attacks can be performed, whereas the worst case is a slight, but steady incremental injected asymmetric delay which has no significant change in the clock skew during the attack. Fig. 6 illustrates the effect on the characteristic clock synchronization quantities, performing such an attack with an increment of 8 ns/s. This test was performed on a setup consisting of 2 network switches and insignificant FO cable length which results in a lower total path delay of 20.6 μs in the steady state

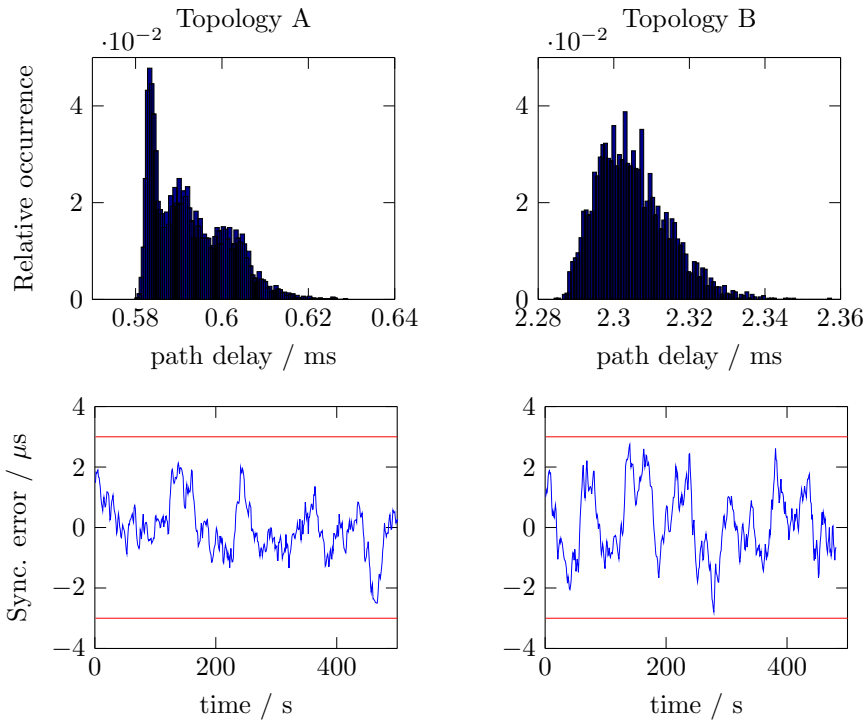

Figure 5: (top) Histogram of the measured path delays and (bottom) the resulting clock synchronization accuracy in between a limit of 3 μs.

(at no attack). The dashed line in Fig. 6 represents the starting point of the attack. Before the attack the system was in a steady state without any attack. After 950 s the attack started injecting 8 ns/s. The estimated path delay by the slave clock increases by half of the injected delay due to the assumption of symmetric paths, t_{PD} is basically calculated by $t_{PD} = (t_A \rightarrow t_B + t_B \rightarrow t_A)/2$. Hence, by observing the increased path delay the attack can be easily detected by simply setting a threshold, in this case set to 10 μs, according the required synchronization accuracy. Fig. 6 illustrates on the top the consequence of the delay attack on the estimated path delay by the slave clock. So, it would be possible to detect asymmetric delay attacks by just using the path delay criteria but with the drawback that the attack is detected as soon as the consequence already affected the synchronization accuracy at the limit of the accuracy requirement. Observing the estimated clock skew already exhibits a change in its characteristic after starting the attack. The diagram in the second row of Fig. 6 represents the actuating value of the clock, the skew. By creating histograms, in the steady state (at no attack) and during the attack, the change of its characteristic is clearly visible. At no attack a major tight peak at $\overline{\alpha} = 1.305\,\text{ppm}$ with a variance of $\sigma^2 = 4.05 \cdot 10^{-4}\,\text{ppm}^2$ can be seen. The histogram created during the attack illustrates a peak with a mean value of $\overline{\alpha} = 1.303\,\text{ppm}$, which is approximately equal to the peak at no attack, but an increased variance of $\sigma^2 = 5.45 \cdot 10^{-4}\,\text{ppm}^2$. Since the skew is the actuating value for the clock control, this quantity expresses the consequence of such an attack. For this particular attack scenario, the increase of the variance illustrates a significant change and the attack can be detected.

If the delay attack would be performed by a steeper incremental injected asymmetric delay, the characteristic of the clock skew would also change according to the intensity of the attack. Simply observing mean values of the clock skew may be not reliable for small delay attacks since the skew is influenced as well by disturbing values like ambient temperature variations.

The evaluation above presents the challenging scenario of slight but steady increases which influence the clock parameters and sets the most challenging scenario of such kind of attack. If the injected delay would be decreased, the influence on the clock skew will be decreased as well, but the estimated path delay still represents the deviated clock accuracy independent from the increment of the delay attack.

So, by simultaneously observing the estimated path delay and the clock skew, a reliable criteria to detect asymmetric delay attacks is established. If

such an attack is detected, the protection system switches over to the back-up protection mode, where no communication between the relays is necessary, to prevent maloperations in the power system with basic functionality. The here presented solution describes an approach that validates the plausibility of the received time information without the use of a reference channel, which significantly improves over related work (e.g., [23] and [22]). Thus, no additional reference channel is required of which a secure operation has to be guaranteed as well.

The big advantage of this presented approach is that no reference channel is necessary, which additionally needs to be guaranteed unattacked, for a reliable delay attack detection by a plausibility check of the estimated clock synchronization parameter.

5.3. Real-time capability

The path delay measurements, illustrated in Fig. 2, represents the results from a topology consisting of 14 network devices along the path, and a FO cable length of approximately 300 km. The maximum measured path delay corresponds to 2.685 ms. Therefore, all measurement values reached the remote station within the time limit of 10 ms, according to Sec. 2. As long as the resulting path delay does not exceed the delay limit, the timing requirements are not violated.

5.4. Summary

The concept proposed in Sec. 4 provides a protection interface fulfilling the requirements specified in Sec. 2. The measurement results presented in this section illustrate a proper working system within the required limits. Table 1 summarizes the requirements and the measured values, tested in a real-life environment. Therefore, a safe operation of the power line is maintained by using the proposed concept.

6. Conclusion

This paper presents a holistic concept for the protection interface of an LCDP system communicating over a packet switched network and its evaluation results from a real-life environment. The proposed concept provides a protection interface fulfilling the stringent requirements summarized in Table 1. The presented measurements illustrate a proper working system within the required limits. Particularly, the synchronization algorithm enables this

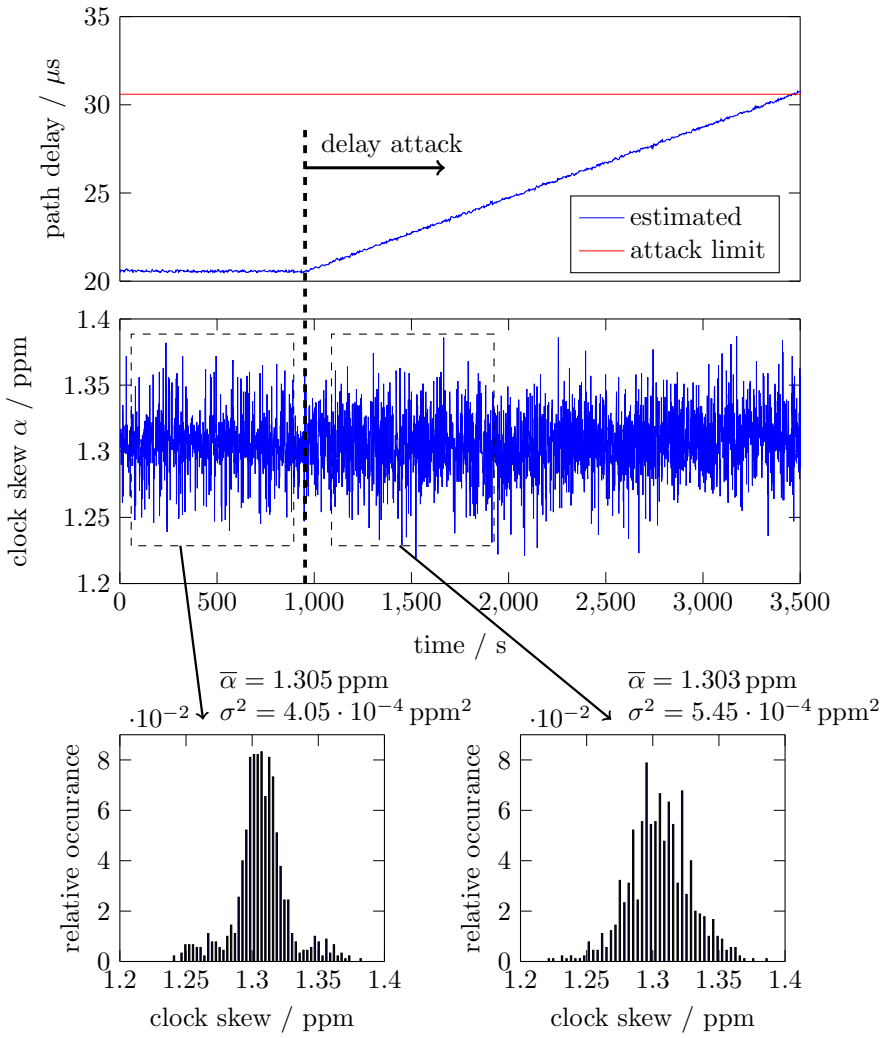

Figure 6: Impact of an asymmetric delay attack by 8 ns/s. The diagram on the top illustrates the impact on the path delay, the diagram in the 2nd row represents the resulting actuating value of the clock, the clock skew α, and the diagrams on the bottom illustrate the histogram of the clock skew at no attack and during the attack.

concept, also to establish a strong End-to-End security concept which combines physical and cryptographical security. Therefore, the grid as a critical infrastructure can be protected from system faults without complex protection strategies, by simply using the principle of differential protection and is additionally protected from cyber attacks. The evaluation provides measurements from a real-life environment which demonstrates the practicability of the proposed concept. Therefore, a safe operation of the power line is maintained by using the proposed concept. This enables the use of widespread available Ethernet-based WANs without the necessity of correcting clocks in the network infrastructure and can therefore be realized in a cost-effective manner providing system safety.

Acknowledgments

This work was supported in part by the research project SmartProtect, supported by The Austrian Research Promotion Agency (FFG), project no. 848911, and in part by the LCM in the framework of the Austrian COMET-K2 program. The financial support by the Austrian Federal Ministry of Science, Research and Economy and the Austrian National Foundation for Research, Technology and Development is gratefully acknowledged.

References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), Official Journal of the European Union L345 (2008) 75–82.

[2] IEEE Guide for Protective Relay Applications to Transmission Lines, IEEE Std C37.113-2015.

[3] T. G. M. Alvin, I. Z. Abidin, H. Hashim, A. A. Z. Abidin, Phase comparison protection for distribution networks with high PV penetration, in: ISGT ASIA, 2014, pp. 216–221.

[4] A. F. Sarabia, Impact of distributed generation on distribution system, Master's thesis, Aalborg University, Denmark (2011).

[5] E. M. Lightner, S. E. Widergren, An Orderly Transition to a Transformed Electricity System, IEEE Transactions on Smart Grid 1 (1) (2010) 3–10.

[6] E. Sortomme, S. S. Venkata, J. Mitra, Microgrid Protection Using Communication-Assisted Digital Relays, IEEE Transactions on Power Delivery 25 (4) (2010) 2789–2796.

[7] B. Gowan, White paper: SONET/SDH Network Modernization is long overdue, Tech. rep., ciena® corporation (Jun. 2013).
URL http://www.ciena.com/

[8] White paper: TELEPROTECTION OVER MPLS WIDE-AREA NETWORKS, Tech. rep., CISCO™and SIEMENS (Jan. 2017).
URL http://www.cisco.com/

[9] K. Parikh, J. Kim, TDM Services over IP Networks, in: MILCOM 2007 - IEEE Military Communications Conference, 2007, pp. 1–10.

[10] S. M. Blair, C. D. Booth, B. D. Valck, D. Verhulst, K. Y. Wong, Modelling and Analysis of Asymmetrical Latency in Packet-Based Networks for Current Differential Protection Application, IEEE Transactions on Power Delivery, in press.

[11] A. Hansen, J. Staggs, S. Shenoi, Security analysis of an advanced metering infrastructure, International Journal of Critical Infrastructure Protection 18 (Supplement C) (2017) 3 – 19.

[12] S. Frankel, S. Krishnan, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, RFC 6071 (Feb. 2011).
URL http://www.rfc-editor.org/rfc/rfc6071.txt

[13] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol, RFC 5246 (Aug. 2008).
URL http://www.rfc-editor.org/rfc/rfc5246.txt

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

[15] S. V. Muddebihalkar, G. N. Jadhav, Analysis of transmission line current differential protection scheme based on synchronized phasor measurement, in: PCCCTSG, 2015, pp. 21–25.

[16] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner Jr, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, in: ION GNSS international technical meeting of the satellite division, 2008.

[17] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002).

[18] Y. Liu, H. Gao, W. Gao, N. Li, M. Xiang, A design scheme of line current differential protection based on IEC61850, in: PEAM, Vol. 2, 2011, pp. 520–523.

[19] A. Aichhorn, B. Etzlinger, R. Mayrhofer, A. Springer, Accurate clock synchronization for power systems protection devices over packet switched networks, Computer Science - Research and Development 32 (1) (2017) 147–158.

[20] J. Li, D. R. Jeske, Maximum likelihood estimators of clock offset and skew under exponential delays, Applied Stochastic Models in Business and Industry 25 (4) (2009) 445–459.

[21] S. Ganeriwal, C. Pöpper, S. Čapkun, M. B. Srivastava, Secure time synchronization in sensor networks, ACM Trans. Inf. Syst. Secur. 11 (4) (2008) 23:1–23:35. doi:10.1145/1380564.1380571.
URL http://doi.acm.org/10.1145/1380564.1380571

[22] B. Moussa, M. Debbabi, C. Assi, A detection and mitigation model for PTP delay attack in a smart grid substation, in: SmartGridComm, 2015, pp. 497–502.

[23] T. Mizrahi, A game theoretic analysis of delay attacks against time synchronization protocols, in: 2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings, 2012.

[24] A. Aichhorn, B. Etzlinger, S. Hutterer, R. Mayrhofer, Secure communication interface for line current differential protection over Ethernet-based networks, in: IEEE Manchester PowerTech, 2017.

[25] A. Aichhorn, R. Mayrhofer, H. Krammer, T. Kern, Realization of Line Current Differential Protection over IP-based networks using IEEE 1588 for synchronous sampling, in: DPSP, 2016.

[26] Proposed Terms & Definitions for Power System Stability, IEEE Transactions on Power Apparatus and Systems PAS-101 (7) (1982) 1894–1898.

[27] IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Std 1686-2013.

[28] M. Chetto, A. Queudet, Energy Autonomy of Real-Time Systems, Energy Management in Embedded Systems Set, ISTE Press Ltd. and Elsevier Ltd., London and Oxford, 2016.

[29] L. Hughes, The effects of event occurrence and duration on resilience and adaptation in energy systems, Energy 84 (2015) 443 – 454. doi:https://doi.org/10.1016/j.energy.2015.03.010.
URL http://www.sciencedirect.com/science/article/pii/S036054421500300X

[30] S. Blair, C. Booth, Real-time teleprotection testing using IP/MPLS over xDSL, University of Strathclyde, 2013.

[31] IEEE Guide for Power System Protective Relay Applications Over Digital Communication Channels, IEEE Std C37.236-2013.

[32] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin, Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification, RFC 2205 (Sep. 1997).
URL http://www.rfc-editor.org/rfc/rfc2205.txt