Modelling and Analysis of Asymmetrical Latency in Packet-Based Networks for Current Differential Protection Application

Steven M. Blair, *Member, IEEE*, Campbell D. Booth, Bram De Valck, Dominique Verhulst, and Kin-Yee Wong

***Abstract*—Current differential protection typically requires symmetrical communications channels—with equal latency in each direction—for correct operation. Conventionally, this has been delivered using protocols such as IEEE C37.94 over a Time-Division Multiplexing (TDM) wide-area network (WAN). Modern packet-based WANs offer improvements in efficiency, flexibility, and cost-effectiveness for utility applications. However, jitter is unavoidable in packet-based networks and, in extreme cases, jitter inevitably results in substantial asymmetrical latency in communications paths. This paper clearly defines how a new source of asymmetry arises due to the use of "de-jitter" buffers, which can jeopardize critical protection services. This is demonstrated using an analytical modelling approach, which precisely quantifies the degree of risk, and through real-time demonstration with actual devices, involving current differential protection over an IP/MPLS WAN. Using a novel method of real-time manipulation of Ethernet traffic to emulate large WANs, the modelling approach has been validated. It is shown how the sensitivity of relays to asymmetry depends on the protection settings and the magnitude of the measured load current. To address the risk of protection maloperation, a new approach for compensating for asymmetrical latency has been comprehensively validated. These developments will be of immediate interest to utilities operating, or migrating to, a packet-based infrastructure.**

***Index Terms*—Communications, current differential protection, IEEE C37.94, IP/MPLS, power system protection, teleprotection, time synchronization, wide-area networks.**

I. Introduction

PACKET-BASED networks are being increasingly adopted by electrical utilities for monitoring, controlling, and protecting critical grid infrastructure [1], [2]. This is due to: 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 [3]. However, many protection relays installed in transmission and distribution system substations worldwide still use TDM-based protocols such as IEEE C37.94 [4] for delivering current differential protection (often referred to as teleprotection) rather than packet-based methods such as using IEC 61850 [5]. These legacy installations must continue to be supported for many years, and therefore must integrate with packet-based wide-area networks (WANs)—without adversely affecting protection performance.

In many cases, accurate time synchronization methods—such as using a GPS clock or distributing time with the IEEE 1588 Precision Time Protocol (PTP)—are not available, and would be impractical or too expensive to deploy. Instead, a simpler method for time synchronization, using the same communications channel as for protection data, must be used; as shown in this paper, this method has a significant weakness when applied in modern packet-based WANs.

Jitter is unavoidable in practical packet-based communications networks [6], due to variable queuing latency and other factors. Jitter results in fluctuating differences between the "forward" and "reverse" latency, i.e., it creates the presence of asymmetrical latency. Although, packet-based technologies such as Multiprotocol Label Switching (MPLS), along with careful traffic engineering and the use of standardized Circuit Emulation Services (CESs), can minimize jitter and the associated asymmetrical latency, there are still cases where jitter can cause subtle issues which can disrupt protection schemes, as explained and demonstrated fully in this paper. This can potentially lead to a degraded operational state of the protection scheme or, in the worst case, result in the accidental tripping of cables or transmission lines during benign, non-fault conditions.

The main contribution of this paper is to isolate and analyse a new source of communications asymmetry which caused by the use of de-jitter buffers. This work will thereby provide confidence for electrical utilities seeking to provide teleprotection services over packet-based WANs, by clearly illustrating the potential problems arising from jitter, quantifying the impact, and validating this work using real-time simulation with a representative IP/MPLS WAN. The paper builds on the contributions of [7]. One of the key findings is that jitter is a significant issue during the initialization of a CES over packet networks, and the buffers associated with a CES must be carefully monitored and adjusted. Similarly, CES restoration after a connection failure in the communications network can be prone to the same jittery conditions, potentially inducing latency asymmetry. It should be noted that the method described in this paper does not eliminate jitter or asymmetry from the communications network; instead, the paper demonstrates how to provide a high level of resilience to even extreme levels of of jitter or asymmetry.

Although the examples presented in this paper are based on UK transmission systems and conventions, this phenomenon

S.M. Blair and C.D. Booth are with the Institute for Energy and Environment, Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, G1 1RD, UK (e-mail: steven.m.blair@strath.ac.uk).
B. De Valck and D. Verhulst are with Nokia, Antwerp, Belgium.
K. Wong is with Nokia, Ottawa, Ontario, Canada.

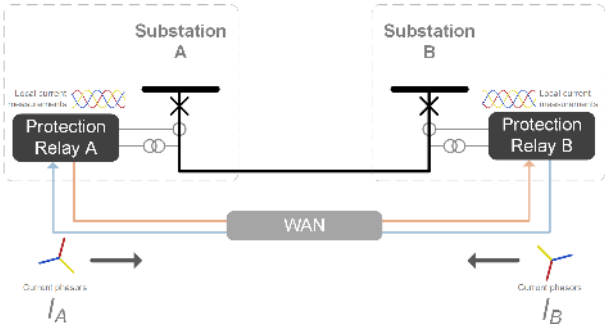


Fig. 1: Illustrative two-terminal differential protection scheme

has applicability to utilities worldwide wishing to efficiently integrate teleprotection services using modern packet-based networks. The term "false trip" is used in this paper to denote these conditions where protection maloperation could occur; however the specific protection policy and available equipment (such as the provision of a redundant backup primary protection system) will define the actual result.

II. Problem Definition

A. Time Synchronization Requirements

Current differential protection systems, as illustrated in Fig. 1, require 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. If necessary, relays "rotate" the current phasors received from the remote end(s) of the scheme, by an amount corresponding to the communications latency. Because of the polarity of connected current transformers (CTs), the two measured current phasors are 180° out of phase under normal load conditions, such that the vector sum would be close to zero [8].

Many teleprotection schemes use the simple "ping-pong" protocol to estimate the communications path latency [9]. The required timing information is transmitted along with the current phasor data [3]. This approach calculates the average of the round trip latency, and it therefore assumes symmetrical latency; the presence of asymmetrical latency will introduce an error in the estimated path latency. The reliance on the ping-pong protocol—which must be supported for many years—is the critical mechanism which can lead to false trips, and underpins the rest of the work presented in this paper.

The use of GPS to provide a better quality of time synchronization—eliminating the issue of asymmetrical latency—is often not reliable [10] or is susceptible to jamming or other interference [11]–[13]. The IEEE 1588 Precision Time Protocol (PTP) can be used as an alternative but requires hardware support, such as transparent or boundary clock functionality within every node, throughout the entire communications network to be effective. Therefore, PTP can be relatively expensive to implement if not supported by the existing network infrastructure, and if a network overhaul is not due in the short term.

B. Characteristics of Packet-Based Networks

Assuming a WAN is correctly configured to use appropriate Quality of Service (QoS) and traffic engineering techniques to ensure forward and reverse traffic use the same path, there are still opportunities for jitter—i.e. variation in packet latency over time—to occur [7], [14]. The causes include:

- Head-of-line (HOL) blocking [15], where a high-priority packet is delayed due to another packet which is already being transmitted on the same egress port. This impact on random latency is worsened by the presence of large packets and by links with relatively low data rates. For example, a 10 Mbps Ethernet link could potentially experience an order of magnitude greater jitter compared to a 100 Mbps Ethernet link when HOL blocking occurs.
- Networks where part of the underlying communications infrastructure includes TDM-based links, e.g., transporting MPLS over E1. This means that packets must wait for the next available TDM time slot before being transmitted, resulting in random latency.

To absorb jitter in packet networks, a CES such as Structure-Agnostic TDM over Packet (SAToP) [16] and Circuit Emulation Service over Packet Switched Network (CESoPSN) [17], must be established across the WAN. This requires the use of special "de-jitter" buffers to regulate the flow of data. The de-jittter buffer is used to control the egress of data from the WAN to the protection relays, to ensure that a consistent stream of data is delivered, and mimicking a circuit-switched connection. However, asymmetrical latency can still occur in these arrangements. The de-jitter buffer must be initialized, or "primed", with data when the teleprotection service is started. Any communications jitter (i.e., random deviations from the mean latency) experienced during this initialization period can be critical, and may result in the buffer "playing-out" data too early or too late. This is because buffers will play out when half-full, and "bursty" traffic resulting from excessive jitter may result in the egress buffer initiating its data output slightly early. Accordingly, there can be an inconsistency in the buffer residency time for the forward and reverse directions, which would be present until the service was stopped and reinitialized, resulting in a permanent asymmetry—which is clearly unacceptable for a teleprotection service. If the difference in the forward and reverse buffer residency times was substantial, a false trip could occur due to the latency asymmetry. Therefore, counter-intuitively, the buffering required by the CES can actually cause additional asymmetry.

Fig. 2 illustrates this process, in a simplified manner, for two data streams: without jitter, and with jitter. Without jitter, at stage t_1 the buffer reaches its halfway point and begins outputting data to the receiving protection relay; with jitter, this occurs slightly later. Therefore, the time that the first packet spends in the buffer depends on the random delay (within certain limits) caused by jitter. This phenomenon is explained in further detail in [15], and is noted for SONET applications in [18]. This effect can also occur due to clock drift, where a clock frequency error at either edge router in the WAN causes a phase error to be accumulated over time, as demonstrated

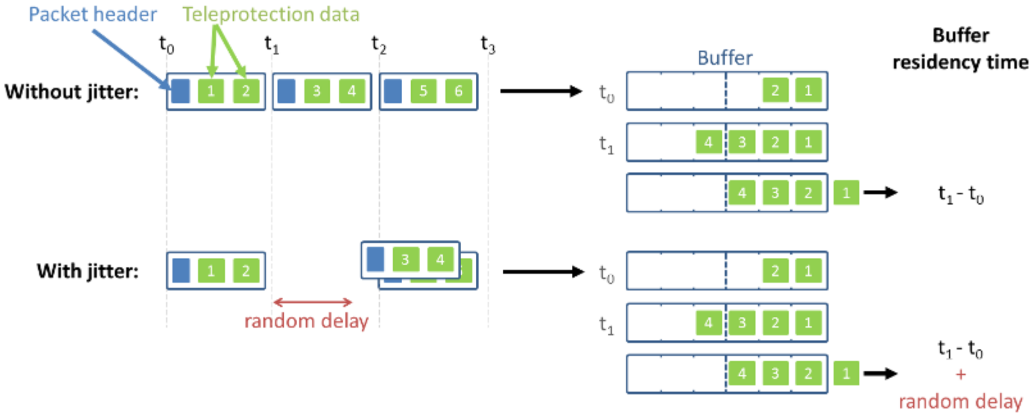


Fig. 2: Example of jitter causing degraded state of a CES de-jitter buffer

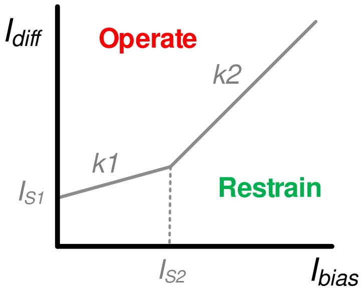


Fig. 3: Typical current differential protection characteristic

in [7]. Note that this is different to the issue of excessive instantaneous jitter over- or under-filling a de-jitter buffer; this is assumed to be controlled by correctly engineering the buffer size during commissioning, and is not the primary concern of this paper.

C. Modelling the Impact of Asymmetrical Latency

Although there is some guidance on asymmetrical latency for protection applications in the literature—such as maintaining asymmetry <200-750 µs in [19], or <500 µs as given in [20]—there is no agreement on the precise level of allowable asymmetry for a particular utility's requirements, and no existing analytical approach to clearly define the issue. Similar analysis is given in [21] and [8] (for the alpha-plane current differential method), but not in the context of packet-based networks. This section formally addresses this, by generically deriving the theoretical maximum asymmetrical latency that can be tolerated for any given utility deployment of current differential protection.

The well-known characteristic for current differential protection is illustrated in Fig. 3 [9]. More advanced characteristics have been proposed [8], [22], but Fig. 3 represents the commonly-implemented approach. In this arrangement, I_{diff} is the vector sum of the local and remote current phasors, and I_{bias} is the sum of the local and remote current magnitudes divided by two. There are four protection settings which will be selected based on the requirements for a particular scheme. Table I gives typical settings for a 400 kV transmission line protection scheme in the UK.

TABLE I: Current differential protection settings

Setting name	Symbol	Typical value	Value for high sensitivity to asymmetrical latency
Minimum pickup current	I_{s1}	400 A	400 A
Bias current threshold (breakpoint)	I_{s2}	4000 A	4000 A
Lower percentage bias setting (slope)	$k1$	30%	0%
Higher percentage bias setting (slope)	$k2$	150%	150%

The following analytical method determines the sensitivity of a protection scheme to asymmetrical delay caused by degraded de-jitter buffers as explained in Section II-B. Current phasors I_A and I_B (see Fig. 1) can be defined as follows (for simplicity, only a single phase is considered but the method applies to three-phase schemes):

$$\begin{aligned} I_A &= I_{A_m}\angle I_{A_\theta} &= I_{A_m}\cos I_{A_\theta} + jI_{A_m}\sin I_{A_\theta} \\ I_B &= I_{B_m}\angle I_{B_\theta} &= I_{B_m}\cos I_{B_\theta} + jI_{B_m}\sin I_{B_\theta} \end{aligned}$$

I_{diff} is the magnitude of the vector sum of I_A and I_B, which can be calculated from the real (*re*) and imaginary (*im*) components as follows:

$$\begin{aligned} I_{diff} &= \sqrt{\left(re\left(I_A\right)+re\left(I_B\right)\right)^2+\left(im\left(I_A\right)+im\left(I_B\right)\right)^2} \\ &= \sqrt{\begin{matrix}\left(I_{A_m}\cos I_{A_\theta}+I_{B_m}\cos I_{B_\theta}\right)^2 \\ +\left(I_{A_m}\sin I_{A_\theta}+I_{B_m}\sin I_{B_\theta}\right)^2\end{matrix}} \end{aligned}$$

Protection Relay A is used as a reference and therefore I_A has a phase of 0°; by convention, under normal operation, the phase of I_B should be 180° such that I_{diff} is close to zero. Therefore, I_{diff} can be simplified as follows:

$$I_{diff} = \sqrt{\left(I_{A_m}+I_{B_m}\cos I_{B_\theta}\right)^2+\left(I_{B_m}\sin I_{B_\theta}\right)^2}$$

Asymmetrical latency only affects the phase of the current measurements, and therefore it can also be assumed that both

I_A and I_B have the same magnitude, i.e., $I_{A_m} = I_{B_m}$. Therefore, I_{diff} can be further simplified as given below:

$$\begin{aligned} I_{diff} &= \sqrt{\left(I_{A_m} + I_{A_m} \cos I_{B_\theta}\right)^2 + \left(I_{A_m} \sin I_{B_\theta}\right)^2} \\ &= \sqrt{{I_{A_m}}^2 \left(2 \cos I_{B_\theta} + 2\right)^2} \\ &= \sqrt{4\, {I_{A_m}}^2 \cos^2\left(\frac{I_{B_\theta}}{2}\right)} \\ &= 2 I_{A_m} \left|\cos\left(\frac{I_{B_\theta}}{2}\right)\right| \end{aligned}$$

Assuming the load current is within the first region of the differential protection characteristic (i.e., $I_{A_m} < I_{s2}$) and that $k1 = 0\%$, a trip will occur when $I_{diff} \geq I_{s1}$, as follows:

$$2 I_{A_m} \left|\cos\left(\frac{I_{B_\theta}}{2}\right)\right| \quad \geq \quad I_{s1}$$

This expression can be rearranged to a simple equation for calculating the exact value of I_{B_θ} which would result in a trip, as follows:

$$I_{B_\theta} \quad \geq \quad 2 \cos^{-1}\left(\frac{I_{s1}}{2 I_{A_m}}\right) \tag{1}$$

Using this equation, for a load current magnitude of 3900 A (i.e., I_{A_m} = 3900 A), a value of I_{B_θ} of 185.88º or 174.12º (i.e. a phase error of 5.88º) would cause a trip. At a 50 Hz nominal frequency (with a period of 20 ms), this equates to a time error of 326.6 µs (= 5.88° × 20 ms ÷ 360°). However, for the relays to erroneously rotate current vectors by a given angle, the actual asymmetry (or the aggregate of the asymmetry in each path) must be twice the value obtained using (1). This is because the "ping-pong" time synchronization algorithm used by the relays calculates the total round-trip latency, which is divided by two to estimate the propagation latency in one direction [23]. Therefore, including this aspect, the time threshold for a false trip due to asymmetry in one direction, t_{asym}, can be calculated as follows (with angles expressed in radians):

$$\begin{aligned} t_{asym} &= 2 \frac{0.02}{2\pi} \left(\pi - 2 \cos^{-1}\left(\frac{I_{s1}}{2 I_{A_m}}\right)\right) \\ &= 0.02 \left(1 - \frac{2}{\pi} \cos^{-1}\left(\frac{I_{s1}}{2 I_{A_m}}\right)\right) \qquad (2) \end{aligned}$$

Therefore, for the "high-sensitivity" settings given in Table I, an asymmetrical latency of approximately 653 µs would result in a false trip. It should be stressed that these are not practical settings, but have been selected to better illustrate the problem in Section III. Note that the current bias has been ignored in the above analysis (because $k1$ = 0%), but the full expression is given in (3) (where F_{nom} is the nominal system frequency) which can be simplified to (4) under the assumption that $I_{bias} = I_{A_m}$. Note that other factors, such as line charging current, can contribute to the apparent asymmetry and therefore, in practice, the value for t_{asym} which can be tolerated is the total of all such factors.

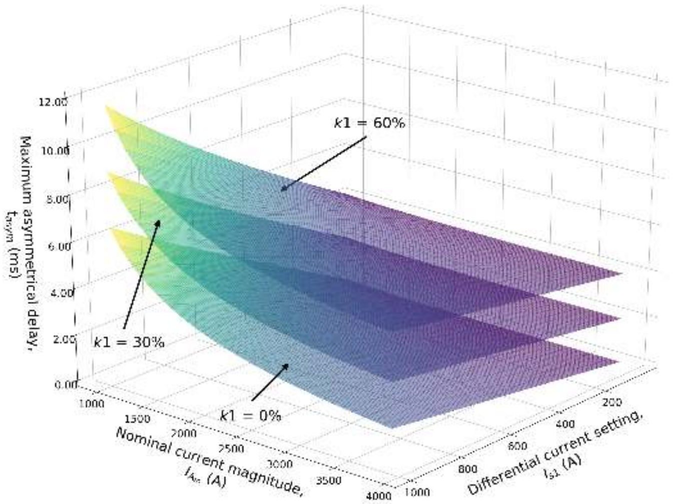


Fig. 4: Behavior of t_{asym} for various I_{s1}, I_{A_m}, and $k1$ values

$$\begin{aligned} t_{asym} &= \frac{1}{F_{nom}} \left(1 - \frac{2}{\pi} \cos^{-1}\left(\frac{k1\, |I_{bias}| + I_{s1}}{2 I_{A_m}}\right)\right) \qquad (3) \\ &= \frac{1}{F_{nom}} \left(1 - \frac{2}{\pi} \cos^{-1}\left(\frac{k1\, I_{A_m} + I_{s1}}{2 I_{A_m}}\right)\right) \\ &= \frac{1}{F_{nom}} \left(1 - \frac{2}{\pi} \cos^{-1}\left(\frac{1}{2}\left(k1 + \frac{I_{s1}}{I_{A_m}}\right)\right)\right) \qquad (4) \end{aligned}$$

Fig. 4 illustrates the behavior of t_{asym} for various I_{s1}, I_{A_m}, and $k1$ values. In summary, a small ratio of $\frac{I_{s1}}{I_{A_m}}$ (i.e. the ratio of setting value to the current magnitude) will tend to be sensitive to asymmetrical latency. It is especially important to note that the level of risk of relay maloperation is dependent on the magnitude of measured load current; at times of higher loading—but below the I_{s2} setting—the system is more susceptible to maloperation due to asymmetry or other factors such as current transformer (CT) saturation errors.

The method provides a very clear and simple way for utilities, system integrators, and other contractors to calculate the risk of protection maloperation under different conditions, for both existing and planned schemes.

III. Real-Time Validation

A. Overview

To validate the model for asymmetrical latency presented in Section (II-C) under realistic conditions, real-time simulations with hardware-in-the-loop equipment have been performed. The use of real-time testing, rather than using a communications simulator such as OMNET++ [24], guarantees that all elements of the system—including the protection relays, WAN routers, and protocol encoding—behave exactly as would occur in a practical application.

The laboratory demonstration arrangement is shown in Fig. 5. This includes a Real Time Digital Simulator (RTDS) to realistically simulate a representative power system (as given in Fig. 1) in real-time, and commercially-available IP/MPLS routers and protection relays. The RTDS supplies analogue current waveforms to the protection relays. This is described further in the following subsections.

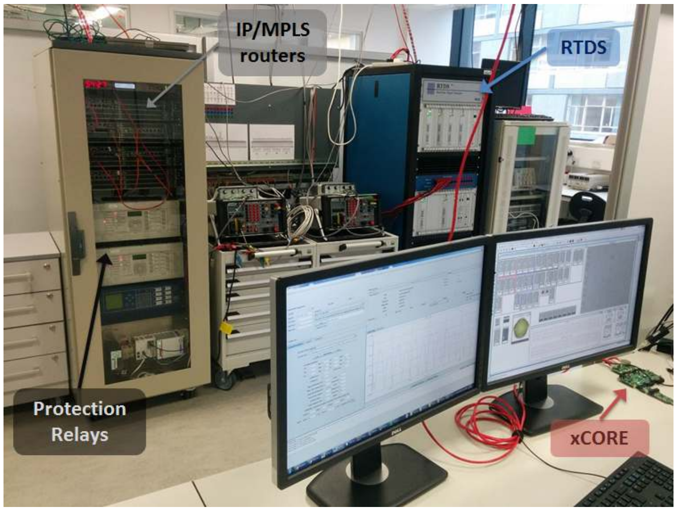


Fig. 5: Laboratory demonstration arrangement

B. Real-Time Jitter Injection

To deliberately induce jitter and asymmetry, it is required to manipulate packets in real-time during initialization of a teleprotection CES. The packet manipulation has been performed using two methods:

1) Forcing static asymmetrical paths, with a fixed, controlled latency in each direction. I.e. the asymmetry is gradually increased until the relays (falsely) trip. This simple method allows the theoretical asymmetry limit which results in false trips (which can be readily calculated, as given in Section II-C) to be validated directly.
2) Delaying each packet by a random amount, according to a given distribution. For simplicity, a Gaussian distribution is assumed in this paper; for improved realism, other distributions or approaches could be used, such as the method described in [25]. This means that, unlike Method 1, each direction of traffic experiences the same mean latency, but can experience instantaneous asymmetry. This should better approximate realistic network conditions, albeit with significant jitter, compared to Method 1.

For both methods, the XMOS xCORE embedded platform [26] has been used to precisely control packet latency in real-time. This platform uses a specialized mircocontroller architecture which multiplexes the CPU between multiple logical cores, but with dedicated hardware CPU registers per core. Therefore, extremely low event response times are possible, which is essential for enabling deterministic applications. The platform also has the benefit of being cost-effective and allows multiple Ethernet interfaces to be connected and controlled [27].

As described in [7], other methods can be used for artificially creating asymmetrical latency in an actual IP/MPLS network, but are not required in this paper:

1) Traffic congestion due to multiple CESs over shared TDM-based E1 links, with limited bandwidth. However, this is unrealistic because the competing services should not have the same priority in a properly configured network.

TABLE II: Comparison of theoretical and measured maximum asymmetry

Setting	Theoretical max asymmetry, t_{asyn} (ms)	Measured max asymmetry (ms)
$k1$ = 0%	0.653	0.604
$k1$= 30%	2.58	2.62

2) Clock drift due to deliberate loss of frequency synchronization between MPLS nodes. However, this approach is time-consuming to repeat.

Furthermore, for both alternative approaches, it is difficult to measure the asymmetry being injected.

C. Automated Testing Methodology

Due to the stochastic nature of the impact of jitter on a teleprotection CES, multiple test iterations (e.g. 100 iterations) must be performed to check for false trips using Method 2. Therefore, the laboratory devices shown in Fig. 5 need to be controlled automatically. This has been achieved by using a Python script to control and monitor the testing over many iterations, as illustrated in Fig. 6. Commands are sent to the IP/MPLS routers using Secure Shell (SSH) to configure the CESs with different settings, and to repeatedly disable then re-enable the CESs. The open source “rapid61850” library [2], [28], which supports the Python programming language, is embedded within the script to decode received the GOOSE trip messages. The GOOSE messages could be sent directly by the protection relays, rather than the RTDS, but this approach enables integration of legacy relays which do not support IEC 61850 communications. To significantly speed up the process over many iterations, the SSH commands to each edge router are executed in parallel in separate threads. In all results given in this paper, the IEEE C37.94 “n” value, which corresponds to the number of 64 kbps slots being used, is set to n = 1.

D. Method 1: Static Asymmetrical Paths

Table II compares the theoretical t_{asyn} values (calculated using Eq. (4)) to values obtained by real-time testing with static asymmetrical paths. The total Ethernet frame latency (calculated from the difference between the hardware time-stamping of egress and ingress times) can be conveniently monitored using the xCORE development software. The level of asymmetry can also be estimated by monitoring the differential current calculated by the each protection relay. The experimental measurements are close to the theoretical values; the difference can be attributed to the inherent inaccuracy of the ping-pong algorithm implementation used by the protection relays which has an error of approximately 0.1 ms (in ideal conditions).

E. Method 2: Real-Time Ethernet Jitter Injection

The network impairment generator, implemented using the xCORE platform and illustrated in Fig. 6, has been configured to apply additional latency to the packet flow in each direction, according to a Gaussian distribution. This allows jitter, according to the defined statistical distribution, to be “injected” into the Ethernet link carrying teleprotection traffic. Fig. 7

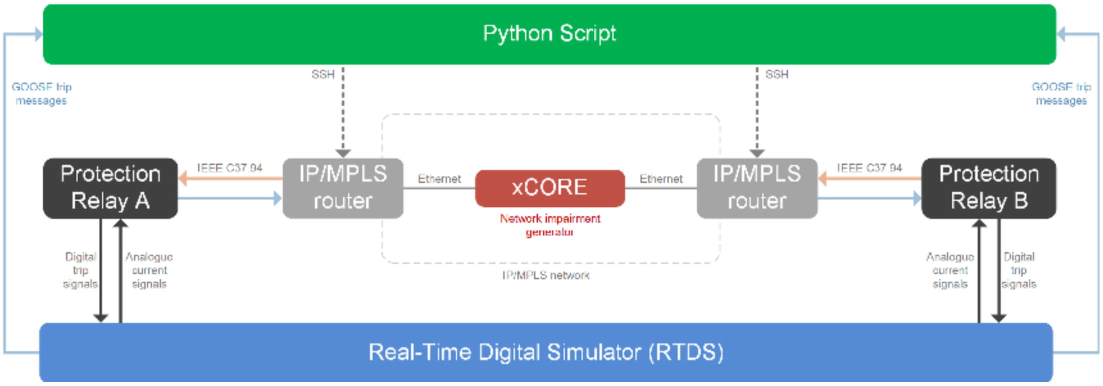


Fig. 6: Overview of automated process used for validation

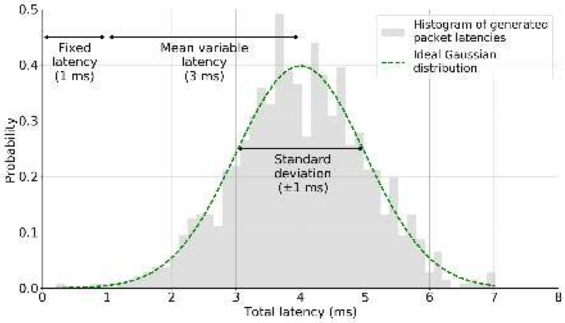


Fig. 7: Example packet latency injection profile

illustrates a typical packet latency distribution. The random latency is applied independently for each direction of traffic. Other distributions could also be applied, but the important point is not the shape of the latency distribution; instead, it is only required that, during the laboratory experiments, the presence of some jitter triggers asymmetry during initialisation of the de-jitter buffers.

Table III provides the results for a selection of test configurations with different parameters. To illustrate the effect of asymmetry, a sensitive setting value of $k1 = 0\%$ has been used. Although this value is impractical, it has been chosen deliberately to ensure that the method described in Section IV was tested under extremely undesirable conditions, and to prove that maloperations do occur without this method enabled. For each test, 100 iterations have been executed to force re-initialization of the de-jitter buffers. In all tests, the jitter is significant enough to result in some false trips. To reiterate, this is caused by instantaneous jitter causing the de-jitter buffers to be initialized incorrectly when the CES is activated, as described in Section II-B. It is important to note that there is a degree of chance involved, which is why many iterations need to be performed, as summarised in Table III. Furthermore, even if a false trip does not occur instantly upon starting the teleprotection service, the de-jitter buffers may be initialized into a degraded state which makes the teleprotection service more susceptible to maloperation due to other factors (such as charging current or CT saturation). There are many options when configuring a teleprotection CES; the results in Table III highlight that the de-jitter buffer size and the MPLS payload size options do not significantly affect the probability of false trips.

Note that to test this phenomenon in isolation, the de-jitter buffers must be large enough to be able to absorb the worst-case jitter after the teleprotection service has been initialized; otherwise the service may fail due to the separate issue of de-jitter buffer under-run or over-run, which would distort the results.

F. Probability of Protection Maloperation

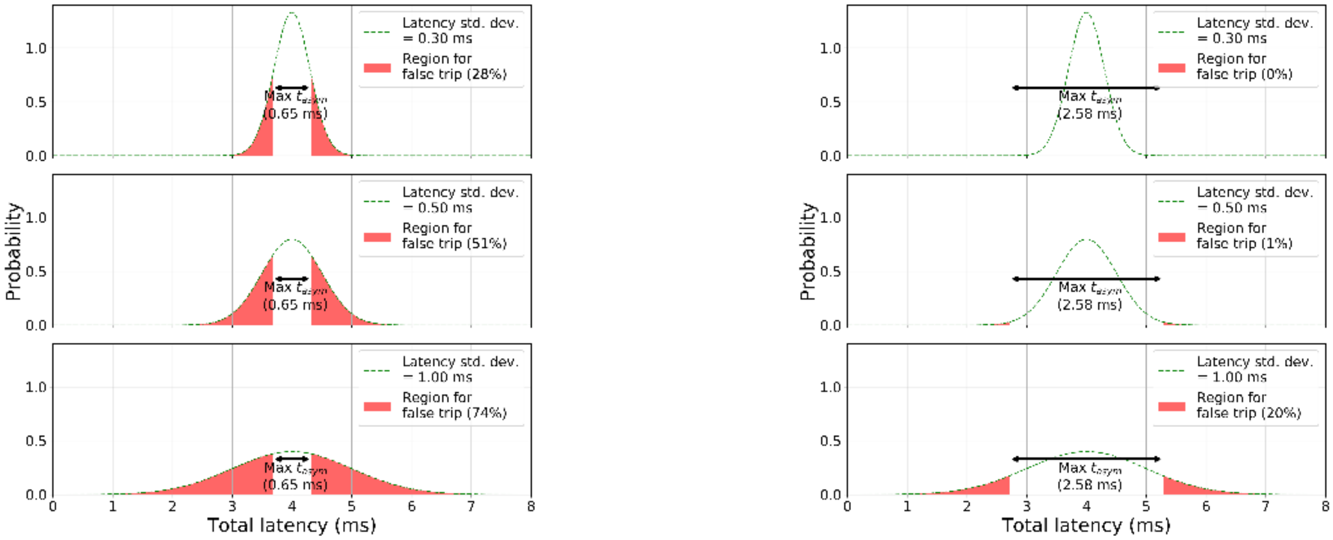
The method given in [21] can be used to calculate the probability of false trips during teleprotection service initialization, with the results given in Fig. 8a (for $k1 = 0\%$) and Fig. 8b (for $k1 = 30\%$). With $k1 = 0\%$, the protection scheme is highly susceptible to false trips caused by packet jitter. Fig. 8b highlights that, even for typical protection setting values, a moderate jitter with std. dev. of 1 ms can result in a 20% probability of false trips during CES initialization; however, note that jitter of 1 ms would exceed the existing guidelines described in Section II-C. The slight mismatch between the theoretical probabilities and the experimental results given in Table III can be attributed to the measured propagation time error (as noted in Section III-D) and the fact that only 1000 samples are used, resulting in a non-perfect normal distribution, as illustrated in Fig. 7.

IV. Solution to Compensate for Asymmetrical Latency

A feature called Asymmetrical Delay Control (ADC) [7] has been developed for IP/MPLS networks to directly address the main issue presented in this paper. ADC analyses the behavior of traffic entering and leaving de-jitter buffers over time. ADC can therefore adjust the de-jitter buffer residency time accordingly to compensate for deviations from the correct value. Specifically, if the mean measured residency time with a de-jitter buffer is different from the engineered value, a byte is dropped from or added to the data stream, which brings the buffers in each direction into alignment. This will cause one relay message to fail a Cyclic Redundancy Check, and be discarded. However, relays typical tolerate a 25% loss of messages within a 100 ms window before the differential scheme starts running in a “Degraded Mode” with a consequent latency applied to the tripping time [14];

TABLE III: Results for real-time testing using Method 2

Fixed latency (ms)	Variable latency mean (ms)	Variable latency std. dev. (ms)	De-jitter buffer size (ms)	MPLS payload size (bytes)	Theoretical probability of false trip (%) (see Section III-F)	Recorded false trip occurrence (%)
1	3	0.3	10	32	28	28
1	3	0.3	16	32	28	19
1	3	0.3	10	16	28	20
1	3	0.3	16	16	28	33
1	3	0.5	10	32	52	46
1	3	0.5	16	32	52	53
1	3	0.5	10	16	52	51
1	3	0.5	16	16	52	47
1	3	1	10	32	75	74
1	3	1	16	32	75	76
1	3	1	10	16	75	65
1	3	1	16	16	75	58



(a) For $k1$ = 0% (not a practical value)

(b) For $k1$ = 30%

Fig. 8: Theoretical probability of false trip during various jitter characteristics

therefore adding or dropping one byte will not disrupt the protection functionality.

Method 2 (see Section III-E) has been repeated for a wide variety of CES configurations, but with the ADC feature enabled. In all cases, there were no false trips during buffer initialization, regardless of the jitter profile applied, and the protection function remained stable (unlike the results given in Table III). This provides strong evidence that it is possible to avoid the disruptive effects of jitter by carefully managing the CES buffering process.

V. Conclusions

This paper has provided the first clear explanation of the issues of asymmetrical latency for teleprotection services in modern packet-based networks, backed by theoretical analysis and real-time demonstration with actual substation hardware. A novel and cost-effective approach for manipulating WAN traffic in real-time has been used to validate the contributions of the paper and quantify the risk of protection maloperation for various sets of circumstances and parameter values. Although the issues presented in this paper can be resolved through dissemination of a high-quality timing reference, e.g. using PTP, this is not practical or cost-effective in many situations. Legacy protection relays with TDM-based interfaces must continue to be supported by utilities for many years.

This work will help utilities to quantify requirements for teleprotection services in various configurations, and determine the risk of maloperation. One of the key findings is that jitter is a significant issue during the initialization of a CES over packet-based networks, and the buffers associated with a CES must be carefully monitored and adjusted. Although protection relays may not (falsely) trip immediately following initialization of the CES, the asymmetry caused by misaligned de-jitter buffers will make the protection more sensitive to other sources of error leading to apparent asymmetry, such the circuit charging current; this may cause a false trip at a later time.

The following recommendations can be made:

- This issue will not occur in all networks, but should be considered if part of the packet-based WAN infrastructure is delivered over TDM links or if there is any other factor which can result in packet jitter.
- If there is significant variation in load current over time, particularly if the load current is expected to be below the I_{s2} setting, there is increased susceptibility to false trips due to asymmetry. The protection settings could be revised to avoid this situation, but this may affect the protection sensitivity.
- In networks with the potential for significant jitter, it is prudent to ensure that—in addition to the proper configuration of QoS and traffic engineering—the buffers associated with CES for teleprotection are managed correctly (as shown in Section IV) to avoid degraded, asymmetrical states.
- It is important that system integration testing explicitly forces re-initialization of the teleprotection CES many times, whilst monitoring the differential current reported by protection relays—ideally using field testing with the actual deployment network—to verify the potential for this issue.

REFERENCES

[1] P. Beaumont, F. Kawano, A. Kawarada, T. Kase, H. Sugiura, F. Lam, J. Hurd, P. Worthington, D. Richards, and P. Merriman, "Performance evaluation of current differential relays over a wide area network," in *11th IET Int. Conf. Dev. Power Syst. Prot. (DPSP 2012)*. IET, 2012, pp. 152–152.

[2] S. M. Blair, F. Coffele, C. D. Booth, and G. M. Burt, "An Open Platform for Rapid-Prototyping Protection and Control Schemes with IEC 61850," *IEEE Trans. Power Deliv.*, vol. 28, no. 2, pp. 1103–1110, 2013.

[3] S. M. Blair and C. D. Booth, "Real-time teleprotection testing using IP/MPLS over xDSL," Glasgow, 2013. [Online]. Available: https://pure.strath.ac.uk/portal/files/26184600/001{_}DSL{_}Testing.pdf

[4] IEEE, "C37.94-2002 - IEEE Standard for N Times 64 Kilobit Per Second Optical Fiber Interfaces Between Teleprotection and Multiplexer Equipment," 2003.

[5] S. M. Blair, F. Coffele, C. Booth, B. De Valck, and D. Verhulst, "Demonstration and analysis of IP/MPLS communications for delivering power system protection solutions using IEEE C37.94, IEC 61850 Sampled Values, and IEC 61850 GOOSE protocols," in *CIGRE Paris Sess. B5*, aug 2014.

[6] E. O. Schweitzer, D. Whitehead, K. Fodero, and P. Robertson, "Merging SONET and Ethernet Communications for Power System Applications," in *38th Annu. West. Prot. Relay Conf.*, 2011.

[7] S. M. Blair, C. D. Booth, B. De Valck, D. Verhulst, C. Kirasack, K. Y. Wong, and S. Lakshminarayanan, "Validating Secure and Reliable IP/MPLS Communications for Current Differential Protection," in *Dev. Power Syst. Prot.*, 2016.

[8] H. Altuve, "Transmission line differential protection with an enhanced characteristic," in *Eighth IEE Int. Conf. Dev. Power Syst. Prot.*, vol. 2004. IEE, 2004, pp. 414–419.

[9] Alstom Grid, *Network Protection & Automation Guide*. Alstom Grid, 2011.

[10] Wen An, N. Tart, D. Barron, M. Bingham, and A. Hackett, "A transmission utility's experience to date with feeder unit protection systems," in *11th IET Int. Conf. Dev. Power Syst. Prot. (DPSP 2012)*. IET, 2012, pp. 31–31.

[11] P. Beaumont, G. Baber, I. Hall, M. Saga, and H. Ito, "Line Current Differential Relays Operating over SDH/SONET Networks," *PAC World Mag.*, 2008.

[12] K. Fodero, C. Huntley, D. Whitehead, and B. Kasztenny, "A novel scheme for wide-area time synchronization," in *10th IET Int. Conf. Dev. Power Syst. Prot. (DPSP 2010). Manag. Chang.* IET, 2010, pp. 132–132.

[13] J. Kelly, M. Stockton, and M. Mohemmed, "Optimisation of protection IED user interaction and implementing self-monitoring protection schemes," in *13th Int. Conf. Dev. Power Syst. Prot. 2016*. Institution of Engineering and Technology, 2016.

[14] J. Jesus, C. Diago, R. Lobo, S. M. Blair, and B. De Valck, "MPLS networks for inter substation communication for current differential protection applications in digital substations," in *PAC World Conf.*, Zagreb, 2014. [Online]. Available: http://strathprints.strath.ac.uk/48807/1/PP021.pdf

[15] Nokia, "Mission-critical communications networks for power utilities," Tech. Rep., 2016. [Online]. Available: http://resources.alcatel-lucent.com/?cid=180690

[16] A. Vainshtein and Y. Stein, "Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)," Internet Requests for Comments, Tech. Rep., 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4553.txt

[17] A. Vainshtein, I. Sasson, E. Metz, T. Frost, and P. Pate, "Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)," Internet Requests for Comments, Tech. Rep., 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5086.txt

[18] B. Kasztenny, N. Fischer, K. Fodero, and A. Zvarych, "Communications and Data Synchronization for Line Current Differential Schemes," in *38th Annu. West. Prot. Relay Conf.*, 2011.

[19] IEC TC 57, "Communication networks and systems for power utility automation - Part 90-12: Wide area network engineering guidelines," Tech. Rep., 2015.

[20] Cisco and Siemens, "Teleprotection over MPLS Wide-Area Networks," 2014. [Online]. Available: https://www.cisco.com/c/dam/en{_}us/solutions/industries/energy/partner-utilities-teleprotection-over-mpls.pdf

[21] Y. Wu, M. Li, Y. Tang, R. Fu, and M. Ni, "Reliability Analysis Models for Differential Protection Considering Communication Delays and Errors," *Energies*, vol. 8, no. 4, pp. 2454–2472, mar 2015.

[22] H. Miller, J. Burger, N. Fischer, and B. Kasztenny, "Modern line current differential protection solutions," in *2010 63rd Annu. Conf. Prot. Relay Eng.* IEEE, mar 2010, pp. 1–25.

[23] S. Roesler and R. Lobo, "Proving viability of line current differential over packet switched networks," in *2014 67th Annu. Conf. Prot. Relay Eng.* IEEE, mar 2014, pp. 542–551.

[24] OpenSim Ltd., "OMNeT++ Network Simulation Framework," 2016. [Online]. Available: http://www.omnetpp.org/

[25] C. Huang, F. Li, T. Ding, Y. Jiang, J. Guo, and Y. Liu, "A Bounded Model of the Communication Delay for System Integrity Protection Schemes," *IEEE Trans. Power Deliv.*, vol. 31, no. 4, pp. 1921–1933, aug 2016.

[26] G. Martins, D. Lacey, A. Moses, M. J. Rutherford, and K. P. Valavanis, "A case for I/O response benchmarking of microprocessors," in *IECON 2012 - 38th Annu. Conf. IEEE Ind. Electron. Soc.* IEEE, oct 2012, pp. 3018–3023.

[27] S. M. Blair, A. J. Roscoe, and J. Irvine, "Real-time compression of IEC 61869-9 sampled value data," in *2016 IEEE Int. Work. Appl. Meas. Power Syst.* IEEE, 2016, pp. 1–6.

[28] S. M. Blair, "rapid61850," 2012. [Online]. Available: https://github.com/stevenblair/rapid61850