DOI: 10.48011/sbse.v1i1.2401

Análise de Redes de Dados Estatísticas para Teleproteção de Linhas de Transmissão de Energia

Luiz F. F. Almeida*. Leonardo H. M. Leite. Ronaldo A. Fernandes**. Roberto S. J. Santos***. Ralph J. Machado*** Wanderson R. da Silva***. Jose R. dos Santos*. Joel J. P. C. Rodrigues*. Antônio M. Alberti***

**Instituto Nacional de Telecomunicações – INATEL*
(luizalmeida@gea.inatel.br; joserodrigo@gec.inatel.br; joeljr@inatel.br; alberti@inatel.br)
***Fundação para Inovações Tecnológicas - FITec*
(lleite@fitec.org.br; rafernandes@fitec.org.br)
**** Companhia Energética de Minas Gerais – CEMIG*
(robseb@cemig.com.br; ralph.machado@cemig.com.br; wanrisi@cemig.com.br)

Abstract: Energy consumption has been growing continuously, supporting the current social model. In this scenario, electric utilities provide means of interconnecting generating sources to end consumers. Systems such as teleprotection are used to ensure that faults in power grids do not affect consumers. Electric utilities have traditionally used Time-Division Multiplexing (TDM) technologies as a means of communication for teleprotection systems, but their inefficient resource allocation and end-of-life cycle have enabled new technologies such as IP-based ones. This work evaluates the statistical network's performance for the teleprotection service, presenting laboratory results with equipment used in the field. The test results show the potential feasibility of using statistical networks to teleprotection operational requirements, constituting an important step for the implementation of field deployments. Further tests will be needed for the definitive proof of viability.

Resumo: O consumo energético vem crescendo continuamente, sustentando o modelo social atual. Neste cenário, as concessionárias de energia proveem meios de interligar as fontes geradoras aos consumidores finais. Sistemas como os de teleproteção são utilizados para garantir que as falhas presentes nas redes elétricas não afetem os consumidores. Tradicionalmente, as concessionárias de energia utilizam tecnologias de multiplexação por divisão de tempo (do inglês, *Time-Division Multiplexing* - TDM), como meio de comunicação para os sistemas de teleproteção, porém a sua ineficiente alocação de recursos e o seu final de ciclo de vida vem possibilitando a utilização de novas tecnologias, tais como as baseadas no protocolo Internet (do inglês, *Internet Protocol*- IP). Deste modo, esse trabalho avalia o desempenho de redes estatísticas para o serviço de teleproteção, apresentando resultados laboratoriais com equipamentos utilizados em campo. Os resultados dos testes indicam uma potencial viabilidade da utilização de redes estatísticas em relação aos requisitos operacionais de teleproteção, constituindo um passo importante para a realização de implementações em campo. No entanto, mais testes serão necessários para a prova definitiva dessa viabilidade.

Keywords: Teleprotection; Deterministic Networks; Statistical Networks; IP Protocol; Hard-Pipe.

Palavras-chaves: Teleproteção; Redes Determinísticas; Redes Estatísticas; Protocolo IP; Hard-Pipe.

1. INTRODUÇÃO

O avanço tecnológico e o advento de soluções cada vez mais complexas nos ramos industriais, comerciais e residenciais exigem que as redes de energia se tornem mais resilientes, seguras e confiáveis, de modo a suprir, com qualidade e segurança, as diversas demandas dos consumidores. Neste cenário, o Sistema Elétrico de Potência (SEP) se apresenta como um habilitador do processo, sendo responsável pela geração, transmissão e distribuição de energia. Os sistemas de controle e proteção da rede de energia são um dos principais pilares do SEP, responsáveis por serviços de missão crítica tais como, teleproteção, auto-cura, comunicação com religadores, entre outros (Silva, 2009).

Os sistemas de proteção, mais especificamente os relacionados a teleproteção, desempenham um papel fundamental nas linhas de transmissão de energia, atuando no seccionamento de partes da rede que se apresentam em situações de risco, garantindo que a falha não se propague pelo sistema. As aplicações de teleproteção se baseiam em tecnologias de telecomunicações, responsáveis por interligar

equipamentos de proteção que se encontram geograficamente distantes. A comunicação entre os equipamentos é realizada através de lógicas que comparam os estados de cada relé localizados nas extremidades da linha de transmissão. A função que converte os sinais e mensagens disponibilizados pelos relés em elementos que possam ser compartilhados pelos canais de telecomunicação e vice-versa, pode ser realizado pelos próprios relés ou por equipamentos dedicados, denominados equipamentos de teleproteção.

Tradicionalmente, as concessionárias de energia utilizam redes de telecomunicações baseadas em tecnologias determinísticas TDM, como Rede óptica síncrona *(*do inglês, *Synchronous Optical Network* - SONET), Hierarquia digital síncrona *(*do inglês, *Synchronous Digital Hierarchy* - SDH) e Hierarquia Digital Plesiocrônica *(*do inglês, *Plesiochronous Digital Hierarchy* - PDH) para suportar os serviços de missão crítica. A utilização dessas tecnologias se deve ao fato de atenderem aos rigorosos requisitos demandados pelos sistemas de teleproteção, tais como, latência, *jitter*, simetria, e recuperação de canal. Apesar de seus benefícios, as tecnologias TDM são ineficientes em relação à utilização do meio de comunicação, apresentando, em muitos casos, elevada ociosidade, devido ao não compartilhamento do canal com outras aplicações ou serviços.

Com o avanço das Redes Inteligentes de Energia (do inglês, *Smart Grids*), motivado pela modernização do SEP, as concessionárias de energia vêm se adaptando as novas necessidades demandadas por funções avançadas de automação, que requerem infraestrutura de comunicação cada vez mais abrangente, capilar, resiliente e que atenda, de forma agregada, a um conjunto de serviços operativos e em uma perspectiva de melhor custo benefício. Muitas destas aplicações possuem características de tráfego em "rajadas", consumindo momentaneamente uma grande largura de banda e desocupando o canal para outras aplicações logo que o tráfego de dados é finalizado. Nesse contexto, as redes determinísticas se apresentam ineficientes, abrindo portas para novos tipos de tecnologias.

Embora as redes TDM sejam bem aceitas do ponto de vista operacional, a necessidade de evolução faz-se necessária, devido à diversas vantagens de outros tipos de redes, em especial as redes estatísticas ou por comutação de pacotes. A evolução das redes de telecomunicações tem como premissa melhorar o custo-benefício das redes de transporte e o aumento de eficiência de transmissão e segurança nas aplicações, bem como integração das diversas tecnologias desenvolvidas para atender as demandas, serviços, e funcionalidades. O surgimento e crescimento acelerado das redes baseadas em comutação de pacotes, chamadas também de redes estatísticas, impulsionada mundialmente pela utilização da Internet, proporcionou o avanço de pesquisas e desenvolvimento de protocolos de comunicação e aplicações para integração dos serviços demandados com diversos requisitos operacionais e comerciais.

Este trabalho, desenvolvido em um projeto de Pesquisa e Desenvolvimento (P&D), tem o objetivo de apresentar os resultados de análise de desempenho da utilização de redes de comunicação de dados baseadas em comutação de pacotes (estatísticas), aplicáveis ao serviço de teleproteção das redes de transmissão de energia da Companhia Energética de Minas Gerais (CEMIG). A validação do cenário proposto ocorre a partir do estudo e da implementação prática de topologias de rede em diferentes cenários de teleproteção, realizados em um ambiente de laboratório.

O restante deste artigo está dividido da seguinte forma. A Seção 2 apresenta uma revisão de trabalhos que abordam o assunto discutido. A Seção 3 realiza uma abordagem mais detalhada sobre os requisitos de teleproteção de linhas de transmissão. A Seção 4 apresenta a metodologia e o *setup* de testes implementado. A Seção 5 apresenta a análise crítica dos resultados a partir dos cenários de testes. Por fim, a Seção 6 apresenta as conclusões do trabalho realizado.

2. TRABALHOS RELACIONADOS

Outros trabalhos que complementam a abordagem de tecnologias IP nos cenários de teleproteção de infraestruturas de energia podem ser observados na literatura. Blair *et al.* (2016) avaliaram a utilização dos protocolos IP e *MultiProtocol Label Switching* (MPLS) na proteção diferencial de corrente. Um método de compensação de atraso assimétrico e um método de criptografia foram apresentados, sendo estes validados através de experimentos em laboratório.

Bächli *et al.* (2017) apresentaram um estudo avaliando a utilização de tecnologias de pacotes para teleproteção. Os cenários de proteção diferencial e de distância foram implementados. Para a validação do estudo, resultados de aplicações em campo e testes em laboratório foram utilizados. Rahman *et al.* (2018) reportam os resultados de testes utilizados na preparação da migração das redes que interligam relés de proteção da subestação *San Diego Gás & Electric* (SDG&E) de SONET para MPLS. Os testes apresentados foram realizados tanto em laboratório, quanto em modelo de simulação usando o *Real Time Digital Simulator* (RTDS). O artigo apresenta os requisitos para teleproteção e destaca como o MPLS fornece técnicas para garantir mínima assimetria, roteando e transmitindo caminhos de teleproteção sobre os mesmos nós da rede de dados. Uma metodologia de como aplicar MPLS em teleproteção é fornecida. Os autores concluem que as redes MPLS são um meio de comunicação viável para o tráfego de telecomunicações entre relés de proteção, se projetadas adequadamente, considerando a latência, a assimetria, *failover*, e a disponibilidade.

Por fim, Tan & Cole (2018) apresentam um estudo sobre o transporte do tráfego de teleproteção sobre MPLS em uma rede física compartilhada com outros serviços. Este estudo retrata a experiência realizada por uma empresa de energia australiana (ActewAGL). Através dele, todo o cenário utilizado para a adaptação e validação da tecnologia MPLS aplicada ao serviço de teleproteção foi descrita, comprovando que sua utilização compartilhada com outros serviços é

Tabela 1- Requisitos de teleproteção entre subestações.

Requisitos	Valores	Observações
Latência/Teleproteção	< 10 ms	Nos meios de comunicação.
Canal de dados de telecomunicações	Distintos e redundantes	Rota principal e alternada distintas e com equipamentos idênticos por rota, quando comparado a ponta A e B.
Taxa de erro de pacotes	→ BER mínimo de 10-3 bps [1] → 0 [2] → BER mínimo de 10-9 bps [3]	[1] Período de 10 segundos consecutivos ITU-T G.821/ G.826; [2] Medidas durante 15 (quinze) minutos, para taxas de transmissão igual ou superior a 64 Kbps, em, pelo menos, uma medida entre três realizadas (aplicável a todos os serviços do ONS) [3] C37.94 (aplicável à fibra óptica).
Jitter (UIpp) – Unidade de intervalo – peak to peak amplitude ITU-T G.823	64kbps (0,25 UIpp) [1] 64kbps (0,05 UIpp) [2] 2Mbps (1,5) UIpp) [3] 2Mbps (1,5) UIpp) [4]	(20 a 20 kHz) [1] ; (3 to 20 kHz) [2] ; (20 a 100 kHz) [3] ; (18 a 100kHz) [4] Measurement bandwidth, −3 dB frequencies (Hz) 64 kbit/s: 1 UI = 15.6 µs 2048 kbit/s: 1 UI = 488 ns
Simetria do canal	< 4 ms	IEC 60834-1
Confiabilidade	Alta	IEC 60834-1 e Report 192 do JWG34/35.11
Segurança	Baixa a média para comandos de bloqueio Alta para comandos diretos	IEC 60834-1 e Report 192 do JWG34/35.11

possível sem maiores impactos no que se refere a qualidade dos serviços prestados.

3. REQUISITOS PARA TELEPROTEÇÃO DE LINHAS DE TRANSMISSÃO

O bom desempenho do sistema de proteção é alcançado quando os requisitos de segurança, confiabilidade e velocidade do sistema de teleproteção são atingidos. Assim, cada esquema de teleproteção possui diferentes exigência quanto ao canal de comunicação para garantir seu bom funcionamento e atender o desempenho desejado do sistema de proteção.

Os principais requisitos de teleproteção segundo o Operador Nacional do Sistema Elétrico - ONS (Operador Nacional do Sistema Elétrico, 2011), a norma IEC 60834 (International Electrotechnical Commission, 1999) e o *Report* 192 do JWG34/35.11 do Cigré (Cigré Joint Working Group 34/35.11, 2001) estão sumarizados na Tabela 1.

4. REDES ESTÁTISTICAS PARA TELEPROTEÇÃO

Especificamente, para o atendimento aos serviços de missão crítica, como teleproteção, associado à evolução das redes de transporte, os protocolos MPLS, MPLS - *Transport Profile* (MPLS-TP) e MPLS - *Traffic Engineering* (MPLS-TE) tem se mostrado potencialmente adequados para atender os requisitos técnicos e operacionais exigidos. Para a validação da solução foi concebido em laboratório um *setup* de testes de acordo com a topologia apresentada na Figura 1. A disponibilização física dos equipamentos do laboratório pode ser observada na Figura 2.

Para a implementação desta topologia foram utilizados uma maleta de comandos de teleproteção, desenvolvida pelos funcionários da CEMIG, responsável por reproduzir os comandos enviados pelos relés, dois equipamentos de teleproteção DIP 5000 da empresa Alstom (ALSTOM Grid, 2011), dois roteadores NE08E-S6E (PE-01 e PE-02) do fabricante Huawei (Huawei, 2020), responsáveis por formar o *link* principal de comunicação entre os equipamentos de teleproteção e dois roteadores NE05E-S2 (P-01 e P-02) e NE05E-SQ (CORE-01 e CORE-02) (Huawei, 2020),

responsáveis por simular um *link* secundário (proteção do *link* primário) de comunicação com 6 *hops* em anel.

Definida pela RFC 7625, a solução proprietária da empresa Huawei prevê a divisão da rede física em 2 planos paralelos, sendo eles *Hard-Pipe* e o *Soft-Pipe* (Hao *et al.* 2015). O *Hard-Pipe* prevê o fornecimento de serviços de alta prioridade para os clientes, garantindo baixos valores de latência e alta largura de banda. Enquanto o *Soft-Pipe* executa serviços básicos para o cliente, implementando a qualidade de serviço do MPLS para o compartilhamento da banda.

A solução prevista na RFC 7625 trabalha com a premissa de que os planos sejam isolados um do outro, de forma que um congestionamento nos serviços prestados pelo *Soft-Pipe* não afete os serviços localizados no *Hard-Pipe*. Apesar deste isolamento, a solução oferece a possibilidade de ajuste nas capacidades de largura de banda de ambos os planos, a qualquer momento.

O *software Jperf*, (Dugan *et al*. 2020), foi utilizado para a geração de tráfego na rede, sendo o cliente interligado ao roteador PE-01 e o servidor conectado ao roteador PE-02. A ligação entre os roteadores foi realizada através de *links* de fibra óptica de 1 Gbps, sendo 10 Mbps para o *Hard Pipe* e 990 Mbps para o *Soft Pipe*. Os parâmetros de *Jitter Buffer* e compensação de latência foram configurados para 1 ms nos roteadores. Os equipamentos DIP 5000 foram interligados aos roteadores PE-01 e PE-02 via interface G.703 *Codir* 64 kbps (ITU-T, 2016). Por fim, a maleta de comandos, que simula os reles de proteção, foi interligada aos equipamentos DIP 5000, através de interfaces I/O.

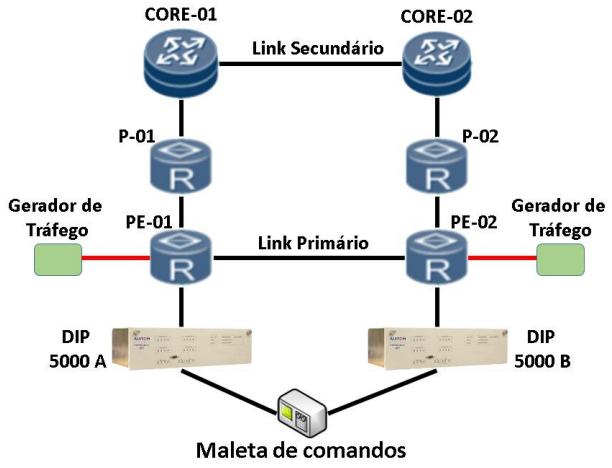

Figura 1 - Topologia utilizada para a validação do sistema.

A maleta foi configurada para o envio de 200 amostras do equipamento de teleproteção A para o equipamento B. Cada uma das amostras possuindo 4 comandos (2 diretos e 2 de bloqueio), espaçados por um período de 1 segundo entre o envio de cada amostra.

4. 1 Procedimentos dos Testes

Os testes realizados durante os experimentos foram os de tempo de operação dos equipamentos de teleproteção, operação da rede sem congestionamento, operação da rede congestionada com tráfego de 500 Mbps, falha de canal e assimetria de canal. A seguir, um breve detalhamento sobre cada teste será fornecido.

Inicialmente, foi realizada a configuração da rede de telecomunicações. Para isto, os roteadores foram configurados com os protocolos IP/MPLS e o protocolo de roteamento *Open Shortest Path First* (OSPF) (Moy, 1998) como pode ser observado na Figura 3 .O sincronismo da rede foi realizado através de Clock interno, *Synchronous Ethernet* (SyncE) (ITU-T, 2019) e 1588v2 (PNCS - Precise Networked Clock Synchronization Working Group, 2008).

Posteriormente, foi realizado um teste para a definição do tempo de operação dos equipamentos de teleproteção, com o objetivo de determinar o tempo gasto para envio e processamento dos comandos pelos equipamentos DIP 5000, sem considerar o tempo gasto pelo transporte na rede de telecomunicações. A topologia adotada, predefinia a interconexão de um equipamento diretamente ao outro (*Back-to-Back*). Através deste teste foi possível a obtenção do valor do atraso médio aplicado pelos equipamentos no sistema.

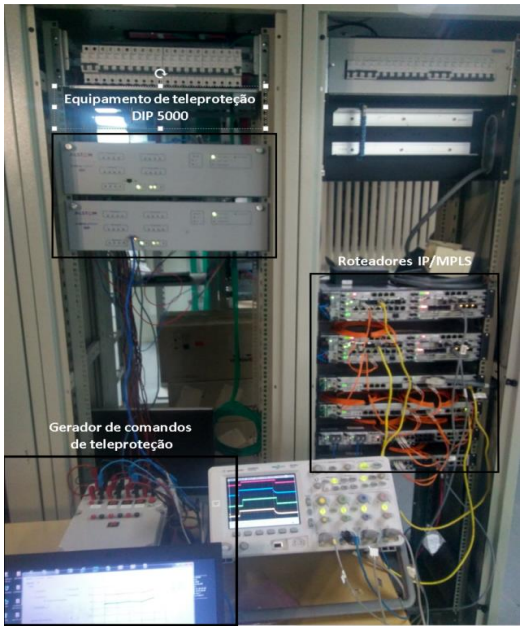

Figura 2 - Disponibilidade física dos equipamentos no laboratório.

```
#
interface GigabitEthernet0/2/7
 mtu 9000
 undo shutdown
 ip address 10.0.0.1 255.255.255.252
 ospf network-type p2p
 ospf enable 1 area 0.0.0.0
 mpls
 mpls te
 mpls rsvp-te
 mpls rsvp-te hello
 mpls ldp
 dcn
 clock synchronization enable
 clock priority 5
 ptp enable
```

Figura 3 - Configuração do MPLS e do protocolo OSPF para a interface GigabitEthernet 0/2/7 do CORE-01

Testes sem e com a geração de tráfego para congestionamento da rede também foram realizados. O *software Jperf* foi utilizado para a aplicação de 500 Mbps no roteador PE-01. Neste cenário, o tráfego e os comandos também foram enviados pelo *link* principal. Em ambos os casos os valores de atraso médio da rede de telecomunicações e do sistema completo foram obtidos.

Realizou-se o teste de falha de canal com o intuito de avaliar o desempenho do sistema quando o caminho principal utilizado para o tráfego do serviço de teleproteção falhar (caminho direto entre os roteadores PE-01 e PE-02) e o sistema comutar o caminho principal para um caminho secundário (tráfego por 6 roteadores). Neste teste, após o envio de 50 amostras o *link* principal foi derrubado e o restante das amostras foi trafegada pelo *link* secundário, registrando-se os valores do atraso médio da rede de telecomunicações e do sistema.

Para a avaliação de assimetria de canal, foi realizada a comparação da latência entre os equipamentos de teleproteção A e B e a latência do equipamento B para o A. A média entre os valores encontrados para cada comando foi realizada para obtenção de um valor de assimetria final.

Por fim, um teste foi realizado para a validação de um dos principais pontos, em comparação as redes TDM e garantido pelo fabricante, na qual a solução prevê a isolação do tráfego entre o *Soft-Pipe* e o *Hard-Pipe*. Para avaliá-lo, o limite de tráfego suportado pelo *Hard-Pipe* foi excedido com o auxílio do gerador de tráfego. Em um primeiro momento, foi realizado o dimensionamento do *Hard Pipe* para 800 Mbps e o *Soft Pipe* para 200 Mbps. Posteriormente, o *Hard Pipe* foi dimensionado para 980 Mbps e o *Soft Pipe* para 20 Mbps.

5. RESULTADOS E ANÁLISES

Nesta seção, são apresentados os resultados alcançados para cada um dos cenários avaliados. Os resultados gráficos foram obtidos através do *software* da maleta de comandos e da ferramenta Matlab.

Inicialmente, são abordados os resultados provenientes do teste de avaliação do tempo de operação dos equipamentos de teleproteção interligados via *back-to-back*. Após o envio de 200 amostras da maleta de comando, como já descrito na Seção 4, os resultados para os comandos diretos (A e B) e os comandos de bloqueio (C e D) foram obtidos. A representação do comando A pode ser observado na Figura 4. Por meio do *software* da maleta de comandos, os valores de atraso médio para os comandos A, B, C e D são de, respectivamente, 7,45, 7,44, 5 e 4,99 ms. A interface gráfica da maleta pode ser observada na Figura 5.

Os resultados de atraso médio do sistema com rede IP para os comandos A B, C e D nos demais testes são reproduzidos na Tabela 2. A Figura 6 comprova os valores de atraso encontrados para o sistema com rede IP e sem a inclusão de tráfego.

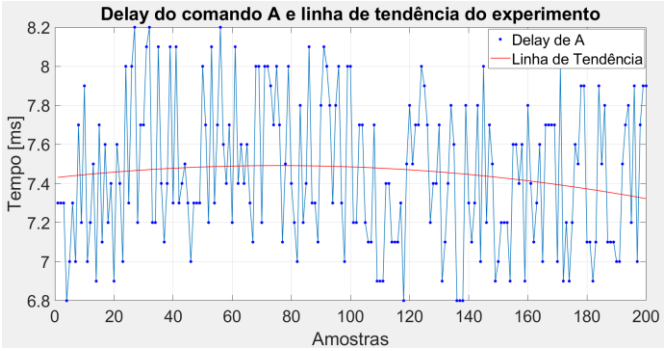

Figura 4 - Resultados obtidos para o comando direto A na topologia Back to Back.

O tempo gasto para o envio dos comandos na rede de telecomunicações foi obtido através da subtração entre o tempo do sistema e o tempo de operação dos equipamentos de teleproteção. Neste cenário, o atraso médio da rede para os comandos A, B, C e D nos testes apresentados na Seção 4 podem ser observados na Tabela 3.

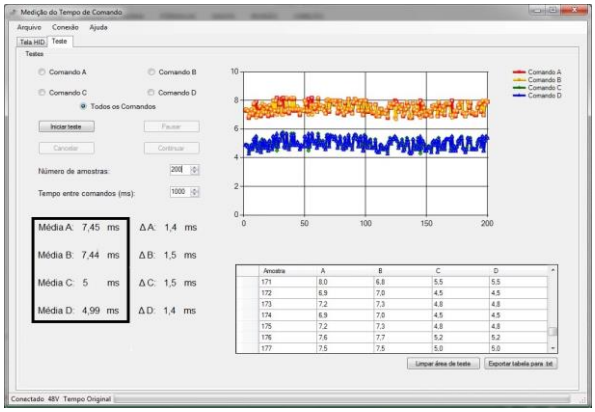

Figura 5 - Valor médio dos comandos referentes a topologia *back-to-back*.

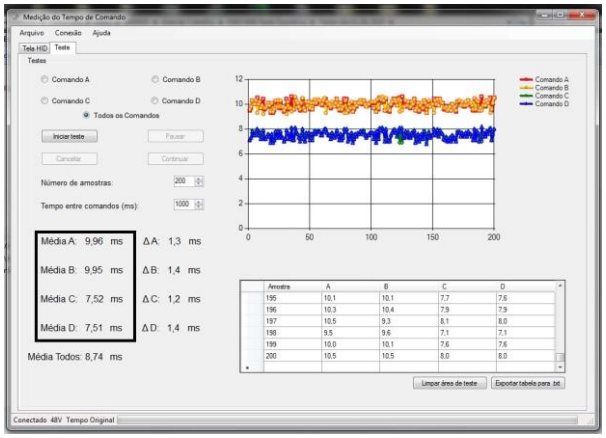

Figura 6- Valor médio dos comandos referentes ao cenário com rede IP e sem a inserção de tráfego.

Tabela 2 - Atraso médio do sistema com rede IP para os comandos de teleproteção (ms).

Teste	A	B	C	D
Rede sem Tráfego	9,96	9,95	7,52	7,51
Rede com Tráfego	9,94	9,91	7,48	7,48
Falha de Canal	9,99	9,9	7,5	7,53
Latência de A para B	9,88	9,86	7,39	7,42
Latência de B para A	9,95	9,94	7,5	7,49

Tabela 3 - Atraso médio da rede para os comandos de teleproteção (ms).

Teste	A	B	C	D
Rede sem Tráfego	2,51	2,51	2,52	2,52
Rede com Tráfego	2,49	2,47	2,48	2,49
Falha de Canal	2,54	2,46	2,5	2,54
Latência de A para B	2,43	2,42	2,39	2,43
Latência de B para A	2,5	2,5	2,5	2,5

A partir dos valores apresentados nas Tabelas 2 e 3, pode-se realizar uma análise comparativa com os requisitos de teleproteção fornecidos na Seção 3. Os resultados referentes ao atraso dos comandos de teleproteção se mantiveram, em média, dentro do limite de 10 ms estabelecidos nos requisitos da norma IEC 60834, tanto para os comandos diretos como os de bloqueio. No entanto, foi possível verificar a ocorrência de algumas amostras com valores de atraso superiores aos 10 ms nos testes de comandos diretos (A e B). Isso pode ser comprovado através dos valores de desvio padrão, os quais são valores máximos de oscilação tanto positivos, quanto negativos em torno do atraso médio, para os comandos A, B, C e D nos testes executados, como mostra a Tabela 4.

Tabela 4 - Desvio padrão para os comandos de teleproteção (ms).

Teste	A	B	C	D
Rede sem Tráfego	0,322	0,33	0,319	0,319
Rede com Tráfego	0,336	0,341	0,344	0,34
Falha de Canal	0,347	0,377	0,367	0,354
Latência de A para B	0,362	0,35	0,353	0,362
Latência de B para A	0,349	0,362	0,345	0,352

Para exemplificar, o teste de rede IP sem inserção de tráfego resultou em valores de latência média dos comandos A, B, C e D de, respectivamente, 9,96, 9,95, 7,52 e 7,51 ms. Ao consultar a Tabela 4 nesse respectivo cenário, os valores de desvio padrão são de 0,322, 0,33, 0,319 e 0,319, respectivamente. Com isso, pode-se verificar que os valores das amostras obtidas podem apresentar atrasos entre 9,638 e 10,282 ms para o comando A. Deste modo, verifica-se que há ocorrência de valores acima dos 10 ms estabelecidos como requisito. Esse comportamento se repete em todos os experimentos para os comandos diretos A e B. Já os comandos de bloqueio C e D apresentaram uma pequena margem de distância em relação ao requisito, se mantendo dentro do esperado.

Os valores de atraso médio para os comandos nos testes de rede com e sem tráfego se mantiveram próximos, de forma a comprovar que a inserção de tráfego na rede estatística não afeta o serviço de teleproteção, sendo isso comprovado posteriormente com o teste de validação da solução *Hard-Pipe*.

Através do teste de falha de canal, foi comprovado que uma possível falha do *link* primário (forçando os comandos a serem enviados pelo *link* secundário), não apresenta grandes impactos aos sistemas de teleproteção mantendo os valores, em média, próximos aos obtidos para o teste de rede sem inserção de tráfego. Vale destacar que para este cenário experimental, a distância entre os roteadores pode ser considerada nula, uma vez que um roteador está conectado ao outro, localmente, através de fibra óptica.

A assimetria de canal foi analisada enviando comandos do equipamento de teleproteção A para o equipamento B e do equipamento B para o A através do *link* principal. Em média, o valor encontrado foi de 0.5825 ms estando abaixo dos 4 ms estabelecidos pela norma IEC 60834 (International Electrotechnical Commission, 1999).

Para a validação da solução *Hard-Pipe*, foi realizada a inserção de tráfego no *Soft-Pipe* e verificado se o sistema realmente apresentava uma isolação entre os canais. Inicialmente, com a utilização do *software Jperf* e o auxílio de 3 computadores foi possível a geração de um valor de tráfego de 500 Mbps. Esse tráfego foi direcionado ao *Soft Pipe* que, neste cenário, foi configurado para 200 Mbps. A solução avaliada confirmou a isolação prevista, permitindo que pouco mais que 200 Mbps trafegassem pelo *link* como pode ser observado na Figura 7.

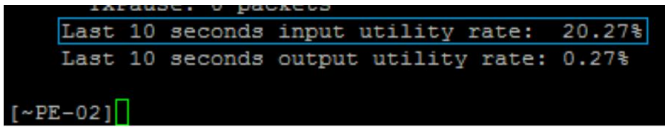

Figura 7 - Resultados obtidos para o primeiro cenário no servidor interligado ao roteador PE-02.

Em um segundo momento, a solução *Hard-Pipe* foi dimensionada para 980 Mbps e o *Soft-Pipe* para 20 Mbps. Com um tráfego de um 500 Mbps sendo direcionado ao *Soft-Pipe*, a solução avaliada permitiu que pouco mais do que 20 Mbps trafegassem pelo *link*. Esse cenário pode ser confirmado através da Figura 8.

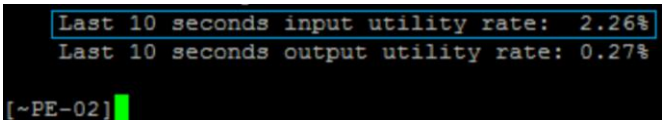

Figura 8 - Resultados obtidos para o segundo cenário no servidor interligado ao roteador PE-02.

6. CONCLUSÕES

Com a realização dos experimentos foi possível verificar que a latência média dos comandos de teleproteção, foi inferior a 10ms, quando conectados via interface G.703 codir 64 kbps. Porém, algumas amostras de comandos direto ultrapassaram os valores estabelecidos pela norma IEC 60834-1. Conclui-se que os resultados indicam potencial viabilidade, entretanto mais testes são necessários para a prova de conceito definitiva. Uma possível alternativa seria a realização de novos testes utilizando interfaces mais rápidas entre os equipamentos de teleproteção e roteadores, como por exemplo G.703 2 Mbps. Outra medida que pode ser adotada para a redução dos valores de latência, está na utilização de sistemas de proteção que dispensem o uso de equipamentos teleproteção (ou seja, conectar os relés diretamente aos equipamentos de rede), uma vez que grande parte da latência atribuída ao sistemas se encontra nos mesmos (comprovado pela análise dos valores obtidos no teste de avaliação do tempo de operação dos equipamentos de teleproteção).

Os valores obtidos para a latência da rede IP foram de aproximadamente 2,46 ms. Foi constatado que a inserção de tráfego não afetou o desempenho do circuito de teleproteção configurado no *Hard-Pipe*, concluindo que o os roteadores permitiram trafegar no *Soft-Pipe* apenas a diferença entre o tráfego injetado e o tráfego reservado no túnel *Hard-Pipe*, constatando a reserva de banda e comprovando um comportamento "similar ao determinístico".

AGRADECIMENTOS

Os autores agradecem a CEMIG, FAPEMIG, Inatel e a FITec, empresas executoras desse trabalho e também a ANEEL – Agência Nacional de Energia Elétrica, por proverem as informações e os recursos necessários para sua a realização. Esse artigo é parte do Projeto D0640 - Modelo de Referência para a Rede Operativa de Dados.

REFERÊNCIAS

ALSTOM Grid. (2011). e-terra gridcom DIP: High-reliability multi-support teleprotection.

Bächli, R., Häusler, M., & Kranich, M. (2017). Teleprotection solutions with guaranteed performance using packet switched wide area communication networks. 2017 70th Annual Conference for Protective Relay Engineers (CPRE), 1-6.

Blair, S. M., Booth, C. D., De Valck, B., Verhulst, D., Kirasack, C., Wong, K. Y., & Lakshminarayanan, S. (2016). Validating secure and reliable IP/MPLS communications for current differential protection. 13th International Conference on Development in Power System Protection 2016 (DPSP), 1-6.

Cigré Joint Working Group 34/35.11. (2001). Protection using telecommunications. Paris: CIGRE.

Dugan, J., Elliott, S., Mah, B., Poskanzer, J., & Prabhu, K. (s.d.). Acesso em 16 de março de 2020, disponível em iPerf - The ultimate speed test tool for TCP, UDP and SCTP: https://iperf.fr/

Hao, J. T., Maheshwari, P., Huang, R., Andersson, L., & Chen, M. (2015). RFC 7625: Architecture of an IP/MPLS Network with Hardened Pipes. Internet Engineering Task Force.

Huawei. (16 de Março de 2020). Série NE05E/08E . Fonte: https://e.huawei.com/br/products/enterprise-networking/routers/ne/ne05e-08e

International Electrotechnical Commission. (1999). IEC 60834-1: Teleprotection equipment of power systems - Performance and testing: Part 1: Command systems. Geneva.

ITU-T. (2016). G.703 : Physical/electrical characteristics of hierarchical digital interfaces. International Telecommunication Union.

ITU-T. (2019). G.8261/Y.1361: Timing and synchronization aspects in packet networks. Geneva: International Telecommunication Union.

Moy, J. (1998). RFC 2328: OSPF Version 2. Internet Engineering Task Force.

Operador Nacional do Sistema Elétrico. (2011). Submódulo 2.6: Requisitos mínimos para os sistemas de proteção e de telecomunicações.

PNCS - Precise Networked Clock Synchronization Working Group. (2008). IEEE 1588 v2: Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. IEEE- institute of electrical and electronics engineers.

Rahman, T., Moralez, J., Ward, S., Udren, E. A., Bryson, M., & Garg, K. (2018). Teleprotection with MPLS ethernet communications - Development and testing of practical installations. 2018 71st Annual Conference for Protective Relay Engineers (CPRE), 1-18.

Silva, W. (2009). Experiência em implementação/ manutenção de equipamentos de teleproteção digital e analógica abordando o novo cenário proposto aos equipamentos de teleproteção a partir das novas resoluções do ONS descritas no procedimento. XX SNPTEE - Seminário Nacional de Produção e Transmissão de Energia Elétrica.

Tan, V., & Cole, J. (2018). Teleprotection over Multiprotocol Label Switching (MPLS): Experiences from an Australian Electric Power Utility. CIGRE - Session Papers & Proceedings.