GRUPO GPC
GRUPO DE ESTUDO DE PROTEÇÃO, MEDIÇÃO E CONTROLE EM SISTEMAS DE POTÊNCIA - GPC

Solucionando problemas de automação com redes SDN: Lacunas de configuração das mensagens GOOSE

ROMULO FABRICIO CORNA (3); MAURICIO GADELHA DA SILVEIRA (3); WELLINGTON OLIVEIRA (3);

RESUMO

Atualmente a engenharia de projetos de arquitetura de rede Ethernet de comunicação tem demostrado muitos desafios de desempenho, determinismo, topologia e validação. O objetivo deste trabalho é apresentar uma alternativa utilizando a solução através de redes definidas por software SDN (do ingles Software Defined Network), com o objetivo de contornar os atuais desafios existentes na segregação das redes de automacao em subestações, em especial para mensagens GOOSE (Generic Oriented Object Substation Event).
Tais dificuldades são frequentemente encontradas em projetos de proteção, controle e automação de subestações de energia elétrica.
Além disso, ressalta as características técnicas e os benefícios que esta tecnologia pode agregar na aplicação de sistemas eletricos de potência (SEP).

PALAVRAS-CHAVE
SDN, GOOSE, SEGREGAÇÃO, REDE

1.0 - INTRODUÇÃO

A comunicação entre equipamentos de Subestações de Energia Elétrica (SEs) ou plantas industriais através de redes *Ethernet*, traz diversos benefícios técnicos e econômicos (3), (5). Um exemplo é a utilização de mensagens do tipo *Generic Object Oriented Substation Events* (GOOSE) (9) que permite o intercâmbio de informações entre dispositivos na rede de comunicação, contribuindo com esquemas de proteção (como exemplo, seletividade lógica das funções proteção) (1).

O maior impacto está no aumento da confiabilidade, além de reduzir os custos de cablagem. Para que essas mensagens cumpram seus objetivos, é exigido um alto desempenho nas questões de disponibilidade e latência da rede, sendo assim o projeto e a implantação de redes *Ethernet* devem ser concebidos com a garantia de cumprimento de todos os requisitos. Técnicas conhecidas de projetos como em (11) e (2), contribuem com a melhoria de confiabilidade, integridade e disponibilidade da rede de dados, porém demandam engenharia prévia dos switches e dos hosts de comunicação. Há diversos tipos de protocolos de comunicação nas SEs, cliente-servidor, que utilizam todas as camadas do modelo OSI (Open System Interconnection), além de endereçamento unicast, essa estrutura de comunicação garante que os dados sejam direcionados para um equipamento especifico na rede. Por outro lado, há protocolos que utilizam somente as duas primeiras camadas OSI e utilizam o endereçamento multicast para a transmissão de dados. As mensagems são replicadas para todos os equipamentos da rede de automação, oferecendo riscos como excesso de trafego na rede, travamento de portas de comunicação e buffer overflow nos equipamentos de proteção, controle e automação.

Há inumeras vulnerabilidades presentes nos protocolos de camada 2 que podem ocasionar falhas no sistema de proteção, controle e automação (12). Esses problemas podem ser contidos ou minimizados utilizando técnicas como VLANs (*Virtual Local Area Network*), filtros MAC (*Media Access Control*). e protocolos de redundância. A dificuldade para a aplicação dessas técnicas é a necessidade de implantação na fase inicial do projeto. Na hipótese de um sistema já em operação necessitar implementar essas técnicas, certamente será complicado e custoso garantir o funcionamento.

Switches com a tecnologia SDN solucionam problemas com vantagens de poder ser implementadas em qualquer fase, desde a fase de implementação, passando pela fase de operação até a fase de expansões futuras. Por meio delas, é possível criar fluxos e filtros de mensagens nas quatro primeiras camadas do modelo OSI. Ao criar um fluxo, cria-se também um redundante, essa restrição de possibilidades permite gerenciar o fluxo de dados

(*) Avenida Pierre Simon de Laplace, n° 633 – TechnoPark – CEP 13.069-32 - Campinas, SP, – Brasil
Tel: (+55 19) 3515-2000 – Fax: (+55 19) 3515-2001 – Email: marketing_br@selinc.com

da subestação. Uma particularidade dessa tecnologia é ser baseada no descarte de mensagens (deny-by-default), por essa razão, qualquer outro dado que chegue ao switch e não esteja habilitado nos fluxos, será descartado. Devido a otimização do número de equipamentos na rede, proporciona vantagens econômicas para o projeto.

Por essas razões, a rede SDN proporciona a solução de inúmeras dificuldades de redes já em operação e possibilita expansão segura do sistema de automação.

2.0 - SOFTWARE DEFINED NETWORKS - SDN

O processo de implantação de uma rede convencional inicia-se na topologia, seguida pela configuração dos dispositivos de rede e, por fim, a configuração dos serviços de rede. Com o objetivo de otimizar, a rede deve ser configurada com o intuito de evitar loops, priorizar aplicações e garantir a convergência para roteadores, obtendo ganho de velocidade. A complexidade no gerenciamento decorre de que cada dispositivo de rede (switch ou roteador) tem lógica de controle e encaminhamento de dados integrados.

Os caminhos determinados pelo protocolo de roteamento são codificados em tabelas de encaminhamento de pacotes (10). Com tal característica, o plano de controle em uma rede tradicional é distribuído por seus dispositivos, assim sendo, alterar o comportamento de encaminhamento de dados na rede envolveria alterar a configuração de muitos dispositivos de rede, eventualmente todos (6).

Os switches tradicionais através de sua arquitetura de controle descentralizada, possuem o plano de dados e o plano de controle compartilhados em um mesmo hardware. O plano de dados realiza a entrega e a recepção dos pacotes pelas portas de comunicação, enquanto o plano de controle realiza o gerenciamento, descarte e aceitação do pacotes (6).

SDN é uma nova abordagem para gestão, configuração e operação de sistemas de rede. Ela permite que uma plataforma de controle altere, gerencie e monitore de modo contínuo. A mudança fundamental é a dissociação dos sistemas que decidem o tráfego, no caso o plano de controle do sistema que executam o encaminhamento do tráfego na rede, sendo esse o plano de dados. SDN é uma nova arquitetura em rede que simplifica o gerenciamento de rede, através da abstração do plano de controle do plano de encaminhamento de dados.

O plano de controle é um software que determina como os dados devem fluir pela rede. O plano de dados consiste nos equipamentos de rede, como switches e roteadores, que encaminham dados, que atravessam a rede. Esses dois planos necessitam de um meio de comunicação, pois o software de controle, comunica o dispositivo de rede, sobre quais tarefas deve executar. O protocolo OpenFlow (8), uma interface padronizada e gerenciada pela Open Networking Foundation (ONF), e utilizada por vários fabricantes. Contudo, há outros protocolos com a mesma capacidade no mercado. Diversos serviços podem ser disponibilizadas através de uma rede SDN, sendo que os controladores expõe esses serviçoes através de *application programming interface* (API), Figura 1, e existem softwares de controle específicos para o setor elétrico, com aplicações dedicadas. Dentro das aplicações é possivel encontrar além do controle da rede, monitoramento do desempenho da rede e aplicações de segurança cibernética (10).

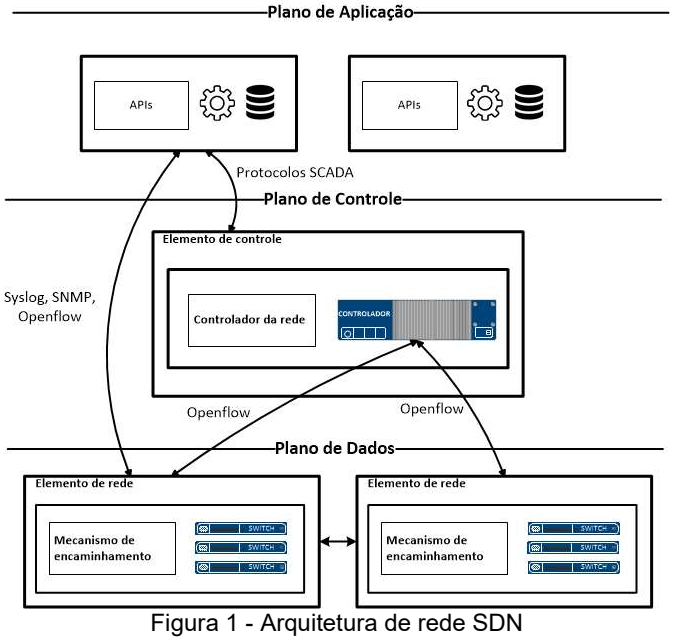

Figura 1 - Arquitetura de rede SDN

As redes SDN utilizam inspeção de pacotes através das camadas do modelo OSI de 1 a 4. As informações de cabeçalhos são utilizadas para a filtragem das mensagens e criação de regras de controle de fluxos. É necessário conhecer as aplicações e os protocolos que trafegam na rede dados e para o correto funcionamento da rede SDN. Essa estratégia aumenta a eficiência e a segurança do sistema, pois é necessário habilitar o fluxo de dado para cada porta dos switches. A Tabela 1 apresenta a distribuição de alguns protocolos e

possíveis regras de aplicação da a filtragem e configuração de rotas de dados. As mensagens GOOSE podem utilizar as informações presentes nas camadas física e de enlace, portanto, é possível selecionar e direcionar as mensagens através das informações de porta de ingressos, endereços MAC e tipo de mensagens. Os protocolos DNP3, TELNET, SSH e SNTP utilizam informações presentes nas camadas física, enlace, rede e transporte.

Tabela 1 - Correlação dos protocolos com as Camadas OSI 1 a 4
** Endereço bidirecional (requisição e resposta)

Camada OSI	Campo de Correlação (Match Field)	IEC 61850 - GOOSE	DNP3	TELNET / SSH	SNTP / NTP
Física	Porta de ingresso	Porta 01			
Enlace	EthDst	Endereço multicast			
Enlace	EthSrc	Endereço físico			
Enlace	EthType	GOOSE (0x88b8)	IPv4 (0x800)	IPv4 (0x800)	IPv4 (0x800)
Enlace	Vlan Id	Endereço VLAN			
Enlace	Vlan PCP	Prioridade VLAN			
Rede	IpProto		TCP	TCP	UDP
Rede	IPv4Dst		Endereço IP	Endereço IP	Endereço IP
Rede	IPv4Src		Endereço IP	Endereço IP	Endereço IP
Transporte	TcpSrc		Porta configurada pelo usuário	22/23**	
Transporte	TcpDst		Porta configurada pelo usuário	22/23**	
Transporte	UdpSrc				123**
Transporte	UdpDst				123**
Enlace	ArpOp				
Enlace	ArpSpa				
Enlace	ArpTpa				

Dessa forma é possível definir regras para cada aplicação e protocolo, independente de rótulos externos como as VLANs. A criação desses fluxos dedicados é fundamental para conter trafego espúrio de outras aplicações e otimizar o desempenho da rede de dados da subestação.

3.0 - PROBLEMAS DE SEGREGAÇÃO EM REDES ETHERNET

As mensagens do tipo GOOSE são amplamente utilizadas nas redes locais das subestações e possibilitam a criação de redes com inteligência distribuída entre os equipamentos de proteção, controle e automação. Os IEDs publicadores disponibilizam a informação na rede, e é de responsabilidade do assinante assiná-las ou descarta-las, sendo que em ambas as situações o IED deverá processar a informação. A transmissão das mensagens é feita de forma periódica e distribuída para todas as portas do switch de comunicação. O comportamento de um switch submetido ao trafego de mensagens do tipo GOOSE está representado na Figura 2.

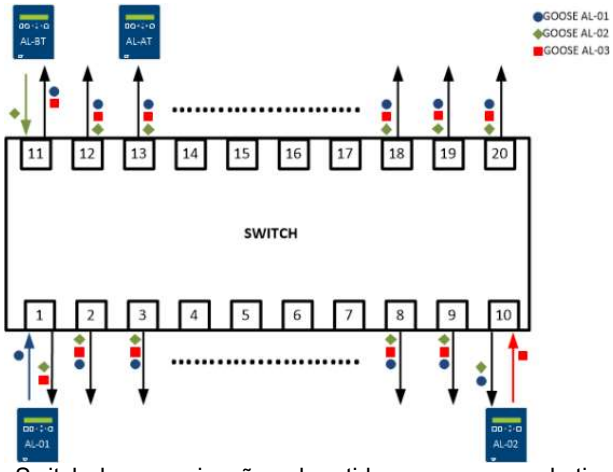

Figura 2 - Switch de comunicação submetido a mensagens do tipo GOOSE

3.1 Seletividade Lógica

A Figura 3, representa um esquema de automação utilizando GOOSE, os alimentadores (AL-01, AL-02, AL-03 e AL-04) enviam sinais de bloqueio para o IED da baixa do transformador (AL-BT), em casos de defeitos, onde os níveis de curto-circuito do ramal e da barra são equivalentes é possível bloquear a atuação do AL-BT evitando a interrupção de energia para os outros ramais. As mensagens dos IEDs AL-01 e AL-02 são publicadas e assinadas pelo IED AL-BT que efetua o processamento da informação.

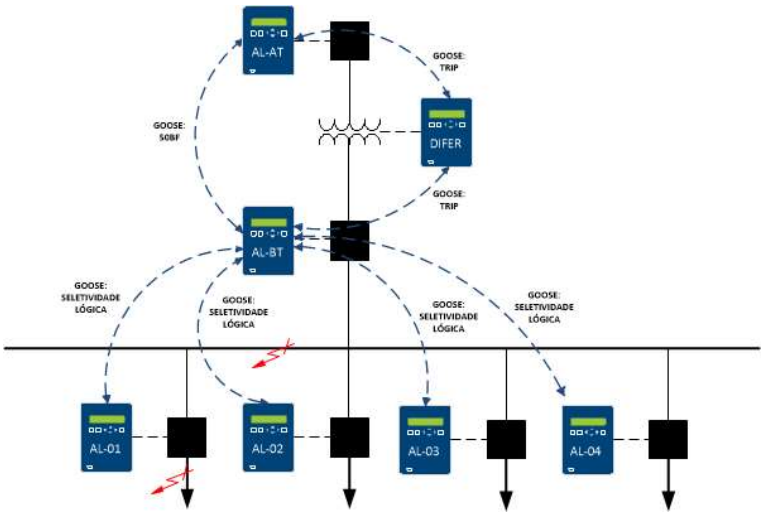

Figura 3 - Esquema de seletividade lógica

Na situação de uma falha de disjuntor o IED AL-BT publica uma mensagem GOOSE que é assinada pelo IED AL-AT, porém o IED AL-AT também recebe mensagens dos IEDs AL-01 e AL-02 que são descartada pelo equipamento. Alguns IEDs recebem mensagens, processam essas informações e depois as descartam, por não assinarem. Como exemplo temos o IED AL-01 que recebe as mensagens GOOSE dos IEDs AL-02 e AL-BT e também temos o IED AL-02 que recebe as informações do IEDs AL-01 e do AL-BT. Ambos os IEDs devem consumir processamento, somente para descartar essas mensagens. A Tabela 2 resume as mensagens GOOSE que são utilizadas e processadas por cada IED.

Tabela 2 - Descarte e processamento das mensagens GOOSE

IED	Mensagem Publicada	Mensagem Utilizada / Processada	Mensagem Descartada
AL-01	GOOSE AL 01	N.A	GOOSE AL-02 E GOOSE AL-BT
AL-02	GOOSE AL 02	N.A	GOOSE AL-01 E GOOSE AL-BT
AL-BT	GOOSE AL-BT	GOOSE AL 01 E GOOSE AL-2	N.A
AL-AT	N.A	GOOSE AL-BT	GOOSE AL-01 E GOOSE AL-02

SDN é aplicada para segregar a rede LAN, criando os fluxos entre os dispositivos, evitando a transmissão de mensagens broadcasts e multicast para a rede, poupando o excesso de processamento desnecessário, que cada IED teria que fazer. Os pacotes GOOSE podem ser filtrados pelo seu endereço multicast (EhtDst) e direcionados para as portas de interesse, sem a necessidade da utilização de mensagens marcadas com VLANs. Uma outra vantagem atrelada está no fato de não ser necessário atualizar o arquivo CID dos IEDs, pois todas as vezes que há a necessecidade de alterar a VLAN de algum IED, devemos enviar o arquivo CID para todos os envolvidos na publicação e na assinatura da mensagem GOOSE, caso contrário haverá alarmes de falha GOOSE. A Figura 4 apresenta os fluxos de mensagens GOOSE filtrados pela rede SDN.

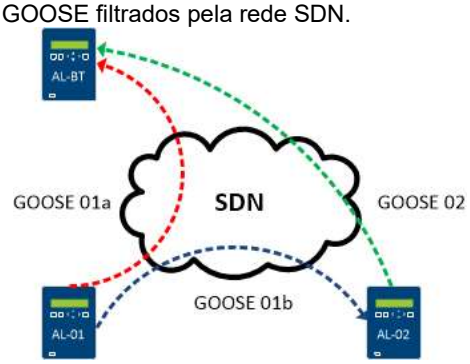

Figura 4 - Rede SDN com Seletividade Lógica

3.2 Conexão entre subestações

Em um projeto envolvendo muitas SEs, deve-se atentar aos endereçamentos de cada IED, tanto para a camada 3 quanto para a camada 2. Na situação de não se dar o cuidado de configurar a camada 2 de modo que as informações não se repitam em outras subestações. No caso de conexão entre elas, há risco de as informações atreladas mensagens GOOSE como MAC, Appid, VLANid e DATASET serem os mesmos. Nessa hipótese poderá ocorrer conflitos de endereçamento MAC causando falha na comunicação.

Outro problema atrelado a essa situação, é que além dos IEDs terem que descartar mensagens GOOSE que não assinam da própria subestação, também terão de descartar as mensagens GOOSE que não assinam dos

IEDs de outra subestação, dessa forma os IEDs passam a realizar operações de descarte desnecessárias, gerando problemas como travamento de portas de comunicação e mal funcionamento dos equipamentos de proteção. O problema pode ser solucionado com a utilização de VLANs e filtros MAC, porém, para o correto funcionamento, essas configurações devem ser testadas durante as etapas de projeto e comissionamento da planta, sendo muito difícil e arriscado a implementação futura desse tipo de tecnologia.

Observa-se na Figura 5, que se não for configurado corretamente os endereços MAC para as mensagens GOOSE, e for configurado o mesmo endereço em diferentes subestações, existindo o link entre elas, haverá erro de operação devido a confusão de mensagens GOOSE entre as subestações.

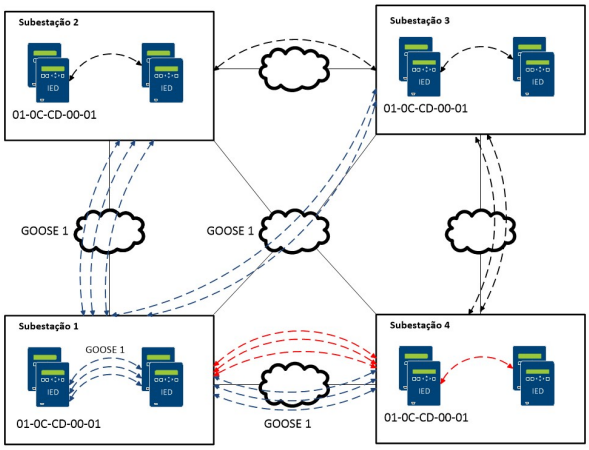

Figura 5 - Rede entre subestações

Esse problema é facilmente resolvido pelo SDN devido sua característica deny-by-default, pois mesmo ao realizar a conexão física entre as redes, não haverá a proliferação de todas as mensagens multicast. Sendo assim só será permitido que um GOOSE chegue a uma SE, se for realizado o fluxo para essa mensagem.

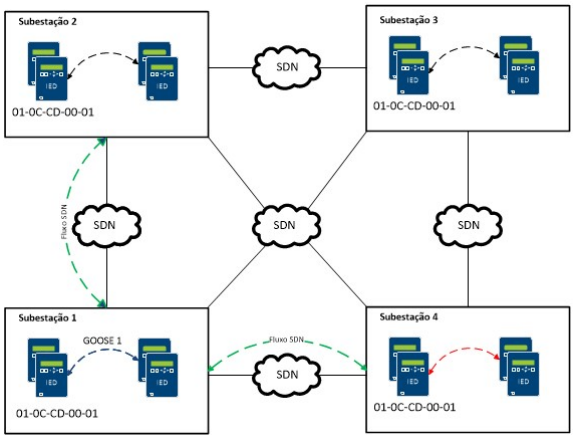

Figura 6 - Rede entre SEs com SDN

Essa característica é eficaz, quando temos um sistema existente, no qual em sua fase de projeto, não foi previsto utilização de ferramenta de segregação como VLANs e filtros MAC. Quando isso ocorre há excesso de mensagens processadas indevidamente, e esse comportamento é potencializado devido a conexão das subestações.

3.3 Redundância de rede

A norma IEC 61850-5-1(4), define tempos de transferência entre os IEDs, sendo que a transferência de dados deve respeitar classes de desempenho para as redes de distribuição e de transmissão. Mensagens do tipo 1, mais críticas, tem tempo de transmissão de 4 milissegundos. O protocolo GOOSE é uma mensagem do tipo 1, também possui o método de disseminação via multicast, e projetado para circular em uma LAN, também não possui técnicas de garantia de entrega dos pacotes, ou roteamento. Geralmente contém informações críticas para o funcionamento do sistema de proteção, controle e automação, tais como: fechar, abrir, ordem de religamento, bloqueio, desbloqueio. Dessa forma, havendo a redundância, certamente haverá um aumento da disponibilidade do sistema.

Segundo (13), podemos chamar de escuridão da rede o tempo em que a rede não está disponível para entregar pacotes, isso pode ocorrer devido a uma ruptura das conexões, ou algum equipamento falhou. Quando

ocorre uma falha da rede, pacotes que foram enviados podem não chegar ao destino, sendo assim teríamos uma falha na comunicação. Nesse caso, seria necessária uma retransmissão da informação, na expectativa de que essa informação chegue ao destino por um caminho alternativo. Com relação as retransmissões, cada protocolo tem o seu mecanismo de retransmissão, no caso do protocolo GOOSE a última retransmissão ocorre 16 milissegundos após a ocorrência do evento. Após as retransmissões, o protocolo GOOSE publica novamente a mensagem, porém em um período maior, insuficiente para atender qualquer lógica de seletividade (13).

Com o objetivo de zerar os tempos de escuridão da rede, foram desenvolvidos protocolos de redundância da rede, definidos pela norma IEC 62439-3 (7). Para que a rede tenha uma alta disponibilidade a norma estabelece duas soluções o Parallel Redundancy Protocol (PRP) e o High-availability Seamless Redundancy (HSR) com o intuito de garantir a redundância da rede. A característica principal de rede em PRP é ser criado duas redes completamente isoladas, e que em nenhum momento podem ser conectadas, ou seja, elas devem ser duplicadas fisicamente.

Essas características podem também trazer algumas complicações, que a rede SDN pode ajudar a resolver, dessa forma ao invés de utilizarmos o protocolo PRP sobre uma LAN convencional, utilizariamos o PRP sobre um LAN com SDN. Uma das complicações que o PRP sobre uma LAN convencional pode trazer seria um maior investimento econômico justamente pelo fato de ter que ser construido duas redes completamentes isoladas, outra situação seria no momento em que o sistema já esteja em operação algum usuário equivocadamente conectar as redes, isso traria problemas para o funcionamento da LAN, pois teriamos pacotes duplicados na mesma rede. Além dessas duas situações temos também a dificuldade de solução em caso de uma falha dupla, Figura 7, nessa situação não haveria mais comunicação entre os equipamentos..

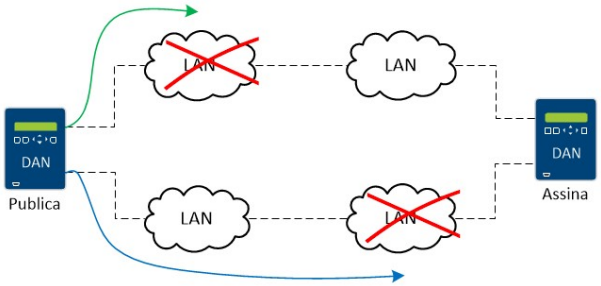

Figura 7 - Falha Dupla

Isso ocorre pois não há mais opções de caminho, todas as situações são facilmente resolvidas pelo SDN, no cenário de um usuário conectar as redes, isso já não é um problema pois a rede SDN, como já comentado, é uma rede deny-by-default, sendo assim em caso de link entre as redes, não haverá fluxos configurados, consequentemente não haverá nenhum pacote circulando.

Caso se apresente uma falha dupla, a rede SDN contorna esse problema pela característica de separar o plano de dados do plano de controle, criando fluxos para as duas redes independentes, no mesmo switch, permitindo assim a conexão de todos os switches envolvidos, Figura 8. Dessa forma o isolamento que o PRP necessita é suprido por uma segregação lógica das redes, e não mais física. Assim sendo os mesmos switches podem criar várias opções de caminhos para a arquitetura de rede, proliferando as alternativas de links entre os IEDs, suportando facilmente uma falha dupla.

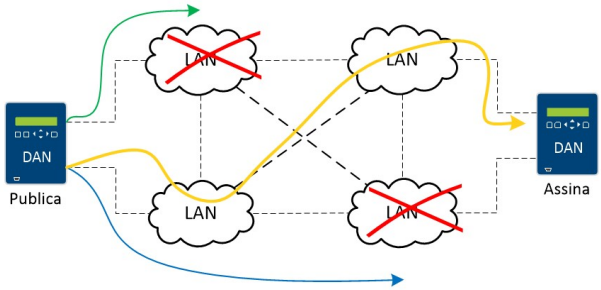

Figura 8 - Diversos Caminhos

Conjuntamente, se existem alternativas de caminhos, sem aumentar o número de equipamentos da rede, certamente isso trará também uma vantagem econômica, uma vez que não se faz mais necessário duplicar fisicamente toda uma solução.

4.0 - CONCLUSÃO

O estudo elucida a utilização da tecnologia SDN como meio de transporte para interconectar redes que utilizam o protocolo GOOSE. Embora existam outras tecnologias disponíveis, o objetivo de utilizar SDN é tornar a infraestrutura mais confiável e robusta aumentado a disponibilidade do sistema. As mensagens GOOSE, por serem de camada 2 e multicast, necessitam de outras ferramentas para que seu desempenho e sua utilização, não prejudique outras comunicações. Por essa razão foi possível constatar que utilizar a rede SDN em conjunto

com GOOSE é uma excelente escolha pelas vantagens apresentadas.

5.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) S. Kimura, A. Rotta, R. Abboud, R. Moraes, E. Zanirato e J. Bahia. Aplicação do IEC 61850 no Mundo Real: Projeto de Modernização de 30 Subestações Elétricas, 1st Annual Protection, Automation and Control World Conference,Dublin, Irlanda, 2010.

(2) D. Dolezilek, J. Dearien, A. Kalra e J. Needs. Appropriate Testing Reveals New Best-in-Class Topology for Ethernet Networks, 13th International Conference on Developments in Power System Protection, 2016.

(3) N. Moreno, M. Flores, L. Torres, J. Juarez e D. Gonzalez. Case Study: IEC 61850 as Automation Standard for New Substations at CFE, Practical Experiences, 12th Annual Western Power Delivery Automation Conference, 2010.

(4) IEC 61850-5, Communication Networks and Systems in Substations - Part 5: Communicantion requirements for functions and device models. 2013, pp. 65-72.

(5) D. Dolezilek, D. Whitehead e V. Skendzic. Integration of IEC 61850 GSE and Sampled Value Services to Reduce Substation Wiring, 47th Annual Minnesota Power Systems Conference, 2011.

(6) Q. Yang e R. Smith. Improve protection communication network reliability through software-defined process bus, SEL website, 2018.

(7) IEC 62439-3, Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). 2016.

(8) ONF TR-535. ONF SDN Evolution, 2016.

(9) TC 57 - Power systems management and associated information exchange, IEC 61850-8-1: Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, 2011.

(10) BOBBA, Rakesh et al. Software-Defined Networking Addresses Control System Requirements. 2014.

(11) G. Leischner e C. Tews. Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability, 9th Annual Western Power Delivery Automation Conference, 2007.

(12) M. G. Silveira e P. H. Franco. Segurança cibernética em redes IEC 61850: Como mitigar vulnerabilidades das mensagens GOOSE," Seminário Nacional de Produção e Transmissão de Energia Elétrica, 2017.

(13) S. Chelluri, D. Dolezilek, J. Dearien, A. Kalra, Z. Korkmaz and A. Ali. Validating mission-critical ethernet networks for protection, automation, and control applications, 2014 Saudi Arabia Smart Grid Conference (SASG), Jeddah, 2014, pp. 1-9.

Rômulo Fabricio Corna nascido em Curitiba-PR, em 1985. Possui graduação em Engenharia Elétrica pela UTFPR (2010), especialização em Teleinformática e Redes de Computadores pela UTFPR (2015) e mestrando em Desenvolvimento de Tecnologia pelo LACTEC (2019). Tem interesse nas áreas de automação, engenharia elétrica, rede de computadores, segurança cibernética. Empresa: Schweitzer Engineering Laboratories, desde 2014.

Mauricio Silveira formado em Engenharia Elétrica pela Universidade Estadual Paulista, atuou em projetos de P&D voltados para sistemas elétricos de potência antes de se juntar a equipe da SEL em 2014. Iniciou sua carreira na equipe de Engenharia e Serviços como Engenheiro de Proteção, em seguida assumiu os estudos avançados em tempo real utilizando o RTDS. Em 2016 se juntou a equipe de R&D na SEL-USA atuando no desenvolvimento de equipamentos voltados para aplicação da norma IEC 61850-9-2 (Sampled Values). Retornou ao Brasil fazendo parte da equipe de Engenharia de Aplicação da SEL, atuando nas áreas de Automação, Redes e Segurança Cibernética. Atualmente trabalha na sede da SEL em Pullman-WA no departamento de Pesquisa de Desenvolvimento como Engenheiro de Integração e Automação.

Wellington Oliveira nascido em Salvador-BA em 1982 possui graduação em Engenharia Elétrica e Especialização em Automação de sistemas Elétricos de potência e conta com 19 anos de experiencia na área de automação de SEP. O histórico profissional conta passagens por Cia de eletricidade e fabricante de equipamentos de proteção e automação. Colaborador da Schweitzer Engineering Laboratories desde 2012 e possui interesse nas áreas de automação, protocolos de comunicação, segurança cibernética e logicas IEC 61131-3.