



**XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA**

CB/GTL/25

22 a 25 de outubro de 2017
Curitiba - PR

GRUPO - XV

**GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS
ELÉTRICOS- GTL**

**SEGURANÇA CIBERNÉTICA EM REDES IEC 61850: COMO MITIGAR VULNERABILIDADES DAS
MENSAGENS GOOSE**

Mauricio Gadelha da Silveira (*)
SEL

Paulo Henrique Franco
SEL Engineering Services, Inc

RESUMO

A IEC 61850 é uma norma utilizada para organizar o fluxo de informação dentro de uma SE (Subestação de Energia) através de protocolos de comunicação não proprietários. As mensagens do tipo GOOSE são projetadas para trafegar na camada de enlace do modelo OSI. Devido a necessidade do alto desempenho na troca de informação, as mensagens são privadas de procedimentos de segurança como autenticação do publicador e criptografia das mensagens. Este trabalho, explora as fraquezas implícitas nas mensagens GOOSE (Generic Object Oriented Substation Event) e as formas de mitigação através da utilização de switches gerenciáveis e redes definidas por software (SDN).

PALAVRAS-CHAVE

IEC 61850, GOOSE, SEGURANÇA CIBERNÉTICA, SDN

1.0 - INTRODUÇÃO

Por muito tempo, as subestações de energia elétrica operavam seus esquemas de controle e proteção através de cabos de controles, jogo de contatos e protocolos de comunicação proprietários (Dolezilek, Whitehead, & Skendzik, 2010). O avanço da tecnologia dos equipamentos de proteção e controle permitiu que a informação fosse compartilhada utilizando cabos e hardwares de comunicação. Contudo, a padronização da informação passou a ser necessária para o intercâmbio de informação entre os equipamentos de diferentes fabricantes. A norma IEC-61850 define globalmente como as informações devem ser construídas, processadas e transmitidas através da definição de uma classe comum de dados que permite a construção de uma semântica definida (Ozansoy, 2010), (IEC 61850-7-1, 2003), podendo ser transmitida de forma vertical ou horizontal.

A comunicação vertical, do tipo cliente-servidor, que conectam equipamentos ao sistema SCADA é implementada utilizando o padrão MMS (*Manufacturing Message Specification*) (O'Fallon, Klas, Tibbals, Shah, & S, 2013). O mecanismo multicast, utilizado para o intercâmbio de mensagens de forma horizontal entre os IEDs (*Intelligence Equipment Devices*) é definido através do protocolo GOOSE (*Generic Object Oriented Substation Event*). As mensagens do tipo GOOSE foram projetadas para trafegar na camada de enlace do modelo OSI e sua implementação está descrita na IEC-61850-8-1, (IEC 61850-8-1, 2004).

A necessidade do desempenho elevado para o intercâmbio de mensagens entre os IEDs, exige a abstração de procedimentos de segurança como: autenticação do publicador e criptografia das mensagens. Técnicas de ataque como saturação de redes e manipulação dos quadros Ethernet exploram essa fragilidade e podem ser utilizadas para impedir a correta operação das SE's e até mesmo causar operações indevidas. A técnica de saturação da rede consiste em inundar a rede com mensagens GOOSE com a mesma semântica do publicador, impossibilitando o processamento adequado das reais mensagens enviadas pelo publicador para o dispositivo assinante. A técnica de

manipulação dos quadros Ethernet, tem como intenção, identificar as mensagens GOOSE e alterar o valor dos dados das mensagens, fazendo com que o dispositivo assinante passe a descartar as mensagens reais subsequentes do dispositivo publicador ou faça com que o dispositivo assinante opere de forma indevida.

Melhores práticas de configuração da rede, são utilizadas para mitigar essas e outras forma de ataques que podem ocorrer em subestações de energia, essas práticas utilizam-se da aplicação correta de *Virtual Lans* (VLANs), bloqueio de portas que não estão em uso e de novas tecnologias de gerenciamento de rede definidas por software (SDN) através do controle do fluxo de dados. Portanto essas técnicas de ataque utilizam-se de lacunas que podem ser encontradas em sistemas de automação de subestações e podem ser prevenidas com a correta engenharia da rede dentro da subestação aumentando a performance, a confiabilidade e a segurança do sistema de automação.

2.0 - REVISÃO BIBLIOGRÁFICA

2.1 Mensagens GOOSE

As mensagens do tipo GOOSE são projetadas para serem rápidas e providenciam um mecanismo que permita uma troca de informação entre um ou mais IEDs sobre uma rede IEEE 802.3. As mensagens GOOSE são transmitidas através do mecanismo multicast, e são distribuídas através de uma configuração publicador/assinante, aonde um IED é responsável por criar mensagens (publicador) que são entregues para um grupo de IEDs assinantes, ver **Erro! Fonte de referência não encontrada.**

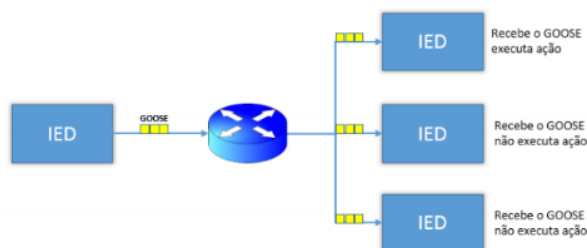


FIGURA 1 – Mecanismo multicast

As informações seguem um datagrama descrito na IEC-61850-8-1 e são mapeadas na camada de enlace do modelo OSI evitando overloads de camadas adjacentes. Portanto não existe suporte para autenticação de mensagens.

2.1.1 Estrutura do datagrama GOOSE

As mensagens GOOSE são projetadas e mapeadas diretamente na camada de enlace do modelo OSI e utilizam a arquitetura Ethernet para a construção do frame, **Erro! Fonte de referência não encontrada.**

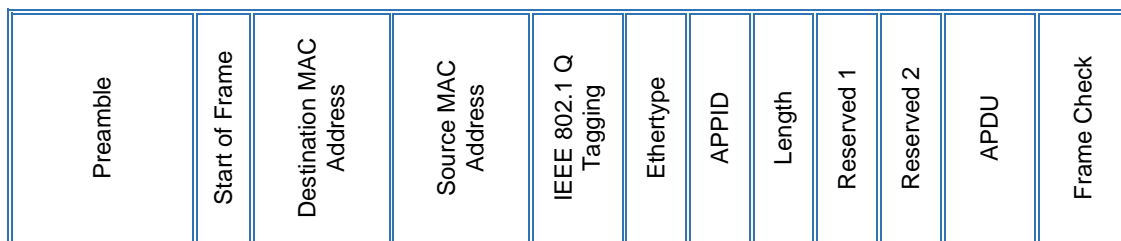


FIGURA 2 – Datagrama GOOSE

Os campos *Preamble* e *Start of frame* são idênticos aos dois primeiros campos do frame ethernet. O campo *Destination MAC address*, corresponde ao endereço multicast. A IEC 61850 define uma faixa para o endereçamento das mensagens que se inicia através dos três primeiros octetos: 01-0C-CD. O quarto octeto simboliza o tipo de datagrama, 01 para GOOSE, 02 para GSSE ou 04 para SV. O quinto e sexto octeto definem o endereço individual da mensagem.

O campo *Source MAC address*, define o endereço unicast da mensagem. As tags IEEE 802.1Q (*VLAN priority tagging*), (IEEE Std. 802.1Q, 2012) definem um mecanismo de seleção e segregação de mensagem. O *Ethertype* GOOSE é definido como 88-B8. O *APPID* identifica o frame. O campo *Length* indica o número total de bytes na mensagem. Os campos *Reserved 1* e *Reserverd 2* são reservados para padronização futuras. Os últimos campos são o APDU (Application Protocol Data Unit) e a checagem sequencial dos frames.

Erro! Fonte de referência não encontrada.

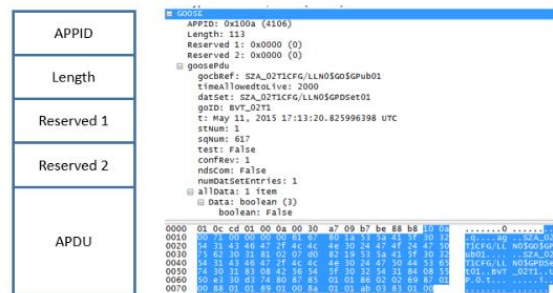


FIGURA 3 – GOOSE APDU

O APDU, descrito no anexo A da IEC 61850-8-1 é uma sequência de 11 parâmetros que carregam as informações que devem ser entregues aos IEDs assinantes. As informações são divididas em:

- **gocbRef**: Identificação singular do APDU contendo o endereço do LNO
- **TimeAllowedtoLive**: Informa o receptor o tempo máximo de espera para a próxima retransmissão
- **DatSet**: Referência de identificação do DataSet
- **gold**: Identificação da mensagem GOOSE
- **t**: estampa de tempo da mensagem
- **stNum**: *State Number*; Contador incrementado a cada novo disparo de mensagem
- **sqNum**: *Sequence Number*; Contador de retransmissão (zerado a cada novo disparo de evento)
- **test**: O parâmetro test indica se a mensagem está em modo teste
- **confRev**: Contador que é incrementado a cada alteração na configuração do DataSet
- **ndsCom**: *Needs Comissioning*, Parâmetro utilizado para informar possível falha na mensagem ou equipamento
- **numDataSetEntries**: Numero de elementos dentro do DataSet
- **allData**: Contém as informações dos LNs armazenadas pelos DataSets

As informações no campo allData, são containers (DataSets) que armazenam as informações representadas pelos LNs. As informações contidas nos DataSets são codificadas através dos mecanismos descritos na IEC 61850 8-1 e distribuídas através de um envelope ethernet (Konka, Arthur, Garcia, & Atkinson, 2011).

2.1.2 Dinâmica de transmissão da mensagem GOOSE

A performance das mensagens GOOSE estão descritas na IEC 61850-5 (IEC 61850-5, 2003) e são enquadradas nos tipos 1 e 1A. As mensagens do tipo 1 (Mensagens Rápidas), tipicamente contém um conteúdo binário, porém podem carregar grandezas analógicas. As mensagens do tipo 1A são mensagens críticas em uma subestação cujo requisito de performance exige uma transmissão na ordem de 3ms no caso mais crítico.

61850-8-1, possui uma dinâmica de retransmissão de mensagens mostrada na **Erro! Fonte de referência não encontrada..**

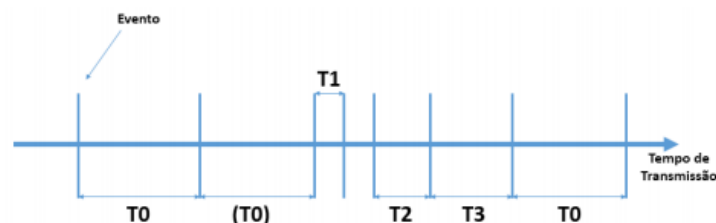


FIGURA 4 – Mecanismo de transmissão da mensagem GOOSE

Os eventos são gerados na aplicação local do IED, mapeados nos Datasets e envelopados nas mensagens GOOSE. Caso não ocorra nenhuma variação nas variáveis do container *allData*, as mensagens trafegam em regime constante, de forma periódica e respeitando o tempo de retransmissão T0.

A transição do estado da informação, representada por um LN, organizada em DataSets, aciona o mecanismo de retransmissão rápida da mensagem GOOSE. O tempo (T0) representa a transição do estado em regime contínuo para o regime de retransmissão rápida. O tempo T1 é a transmissão mais rápida após a ocorrência de um evento. Os tempos T2 e T3 são os tempos associados a recomposição das mensagens em regime permanente. O tempo e a forma de retransmissão T1 pode variar de acordo com o tipo de fabricante.

A cada transmissão de mensagens pelo publicador, o contador SqNum é incrementado até que ocorra o disparo de um novo evento, aonde o contador é zerado. O contador StNum é atualizado a cada novo evento. Os contadores SqNum e StNum estão diretamente ligados ao funcionamento de mecanismo de mensagem GOOSE. Através da variação dos parâmetros dos contadores é possível analisar o comportamento das mensagens GOOSE.

2.1.3 Vulnerabilidade das mensagens GOOSE

As mensagens GOOSE carregam informações importantes dentro de uma SE. Sinais de aberturas, fechamentos e TRIPs muitas vezes fazem partes do escopo das mensagens. Portanto, as mensagens GOOSE influenciam diretamente no comportamento da SE. Contudo, as mensagens do tipo GOOSE e SV não implementam nenhuma recomendação de segurança a nível de enlace nas suas transmissões multicast.

A latência inserida, pela criptografia e autenticação de mensagens é a principal barreira para implementação a nível de enlace. A IEC-62351 define métodos computacionais de baixo consumo, porém não são suficientes para atender os requisitos de performance exigidos pela IEC-61850-5 (Hoyos, Dehus, & Brown, 2012). A IEC-61850-5 define um tempo mínimo de transmissão de 3ms para mensagens do tipo 1A que não podem ser atendidos utilizando os métodos de segurança a nível de frame (criptografia e autenticação de mensagens). Portanto as mensagens GOOSE são intrinsecamente vulneráveis desde sua concepção.

A vulnerabilidade é considerada baixa apenas para redes LAN isoladas, sem a comunicação com o mundo externo. A atual situação das SEs, aonde as informações são compartilhadas com os centros de operação, através de gateways e links de comunicação compartilhados, não podemos mais afirmar que as redes multicast são intrinsicamente isoladas.

As mensagens GOOSE, apesar de não possuírem nenhum mecanismo de segurança, podem ser preservadas através de técnicas de configuração de redes ethernet e manipulação do fluxo de informação. Utilizando a correta engenharia de rede é possível preservar a performance e a integridade da rede de dados. Isolando a rede do tráfego indevido é uma boa opção de segurança utilizando redes IEC 61850.

3.0 - ATAQUE CIBERNÉTICO UTILIZANDO MENSAGENS GOOSE

3.1 Ataque cibernético: Vetores, técnicas e consequências

A realização de um ataque cibernético depende de três pilares: motivação, vetor e técnica. Um ataque pode ser motivado pelo medo, demonstração de vulnerabilidade de um sistema e especulação financeira. Os vetores são os caminhos de acesso a um computador ou uma rede. A técnica de ataque pode variar de acordo com a arquitetura da rede, composição dos frames e dinâmica de transmissão da mensagem. A técnica explorada para esta aplicação é baseada nas vulnerabilidades da camada 2 do modelo OSI (Kush, Ahmed, Branagan, & Foo, 2014).

O vetor pode ser descrito como o meio de acesso a rede de computadores. O acesso a rede pode ser obtido através de um malware instalado em um dispositivo usb, algum equipamento infectado, uma pessoa mal-intencionada com acesso a rede da subestação ou um hacker capaz de invadir a rede a distância. O programa ou malware não necessita ter acesso direto aos equipamentos publicantes e assinantes. Porém ele deve ter a capacidade de analisar, identificar e reproduzir mensagens GOOSE.

A técnica deve ser escolhida de acordo com o alvo do ataque. Devido à natureza do protocolo GOOSE é possível desenvolver técnicas capazes de explorar vulnerabilidades na camada de enlace: *VLAN Hopping*, *MAC flood attack*, *DHCP attack*, *ARP attack* e *Spoofing attack* (Senecal, 2009). Portanto o desenvolvimento da técnica demanda um estudo minucioso dos protocolos em questão.

As consequências de um ataque cibernético dentro de uma SE podem causar danos irreversíveis a uma subestação de energia elétrica. O mal funcionamento da rede de dados pode implicar no funcionamento incorreto dos esquemas de proteção e controle e na atuação indevida de equipamentos primários como disjuntores e seccionadoras. Podendo gerar prejuízos materiais e financeiros.

3.2 Técnica de saturação da rede com mensagens GOOSE

O cenário de testes, Figura 5, consiste em dois IEDs, um switch gerenciável e um computador para simulação do invasor e medição da rede de dados. Os três equipamentos foram conectados as portas do switch através de cabos

de rede. O switch foi configurado de forma transparente, não possuindo nenhuma regra ou bloqueio de portas. Os IEDs operam com uma placa de rede capaz de gerenciar uma largura de banda de 100mb/s.

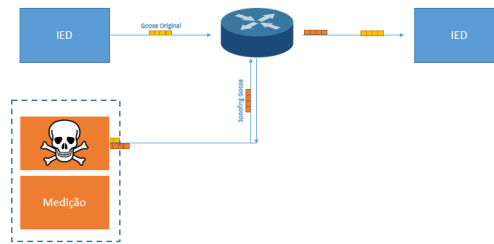


FIGURA 5 – Cenário de testes

Os IEDs foram configurados para a realização de um teste ping-pong. O teste consiste em um IED transmissor publicar uma informação booleana na rede, o IED assinante, ao receber a informação, devolve a resposta para a rede. O IED transmissor não assina a mensagem do IED assinante. O tempo de retransmissão em regime permanente é de 1000ms e o tempo de transmissão durante uma variação é de 4ms.

As mensagens enviadas pelo malware são mensagens GOOSE clonadas e adulteradas do IED transmissor, ver Figura 6. O datagrama GOOSE clonado foi adulterado afim de manter o *stNum* e o *sqNum* com valores fixos e carregar os dados com padding bytes, portanto não influenciando na decisão lógica do IED.

```
F Frame 910: 1488 bytes on wire (11904 bits), 1488 bytes captured (11904 bits) on interface 0  
Ethernet II, Src: Switch_00:b6:0e:bc:(00:30:a7:0b:b6:be), Dst: Tsc-7c:f1:80:13 (81:8c:dc:01:80:13)  
# 6005E  
APVDF: 0x103 (4115)  
Length: 132  
Reserved: 1: 0xb0000 (0)  
Reserved: 2: 0xb0000 (0)  
# goosPdu  
gcchbf: ABA40U_005_ICD_ICF/LNMS05goos0Gdt5  
lsmalmsmclives: 2000  
dctat: ABA40U_005_ICD_ICF/LNMS05dt5  
gid: SubIsay1  
t: Jul 4, 2016 18:03:12.332397460 UTC  
sthM: 1234  
sqM: 0  
test: False  
confRev: 1  
nbsCon: False  
msdsEntries: 1  
# allData: 1 item  
# Data: bit-string (24)  
Padding: 1  
bit-string: <0ESSND>
```

FIGURA 6 – APDU gerado pelo malware

3.3 Perfil de comunicação de saturação de rede para 40 % de carregamento

O experimento pretende analisar a performance do IED assinante durante uma condição de intenso tráfego GOOSE. O malware é responsável por gerar o tráfego. Os pacotes foram manipulados para não interferirem na decisão lógica do IED.

A Erro! Fonte de referência não encontrada. - (a), mostra o perfil das mensagens GOOSE antes e durante o início do ataque de saturação. O ataque se inicia entre os instantes 10s e 20s.

A Erro! Fonte de referência não encontrada. - (b), mostra o comportamento do IED receptor. As mensagens são repetidas a uma frequência constante de 1000ms, o atributo *stNum* se manteve constante e apenas o atributo *sqNum* é incrementado.

A Erro! Fonte de referência não encontrada. - (c), representa os pacotes GOOSE enviados pelo malware, foi fixado o contador stNum em um valor fixo e o parâmetro sqNum em zero. A taxa de envio foi controlada até atingir um valor de 40Mbps, o que representa uma mensagem a cada 400µs aproximadamente.

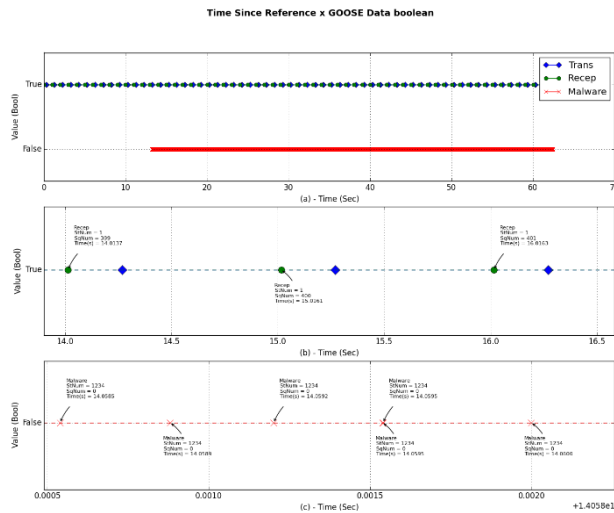


FIGURA 7 – (a) – Perfil de comunicação GOOSE antes e durante o ataque; FIGURA 7 – (b) – Perfil de comunicação GOOSE durante o ataque; FIGURA 7 – (c) – Perfil de comunicação do malware durante o ataque

A **Erro! Fonte de referência não encontrada.** mostra a largura de banda utilizada durante o ataque. Durante a operação pré-ataque, a banda utilizada pela rede é de aproximadamente 2 Kbps. Durante o ataque a largura de banda registrada foi de 40Mbps, devido ao carregamento gerado pelo malware.

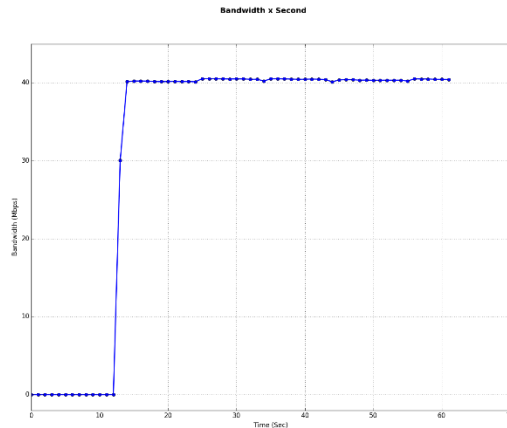


FIGURA 8 – Largura de banda de 40Mbps registrada durante o ataque

Ao iniciar o ataque o IED receptor identifica que existe uma mensagem fora de sequência e uma mensagem corrupta sendo enviada. A mensagem fora de sequência é reconhecida devido o parâmetro *stNum* do malware, fixado em um valor fora da sequência natural do IED transmissor. O IED receptor identifica que a informação contida no APDU não é esperada pelo algoritmo de recepção e efetua o descarte. Após o descarte da mensagem, o algoritmo de recepção assume a próxima mensagem como sendo a nova sequência válida. O perfil de comunicação das mensagens GOOSE durante esta simulação de ataque foi satisfatório, não observando nenhuma perda de pacotes.

3.4 Perfil de comunicação de saturação de rede para 85 % de carregamento

O Ataque continua com o aumento da taxa de transmissão das mensagens GOOSE pelo malware, até atingir um nível de 85Mbps.

A **Erro! Fonte de referência não encontrada.** – (a) mostra o perfil das mensagens GOOSE durante o ataque de saturação. O ataque começa no instante 0s. A taxa de envio pelo malware foi controlada até atingir um valor de 85Mbps, o que representa uma mensagem a cada 190μs aproximadamente.

A **Erro! Fonte de referência não encontrada.** – (b) mostra 2 pacotes pertencentes ao receptor. O parâmetro *stNum* se manteve constante nos dois pacotes indicando que são pertencentes a mesma ordem de variação. O *sqNum* sofreu um incremento de 1 durante um intervalo de 1000ms. Porém a mensagem do transmissor não foi registrada durante 5 segundos.

A **Erro! Fonte de referência não encontrada.** – (c) representa um pacote perdido pelo receptor no instante 9.5.

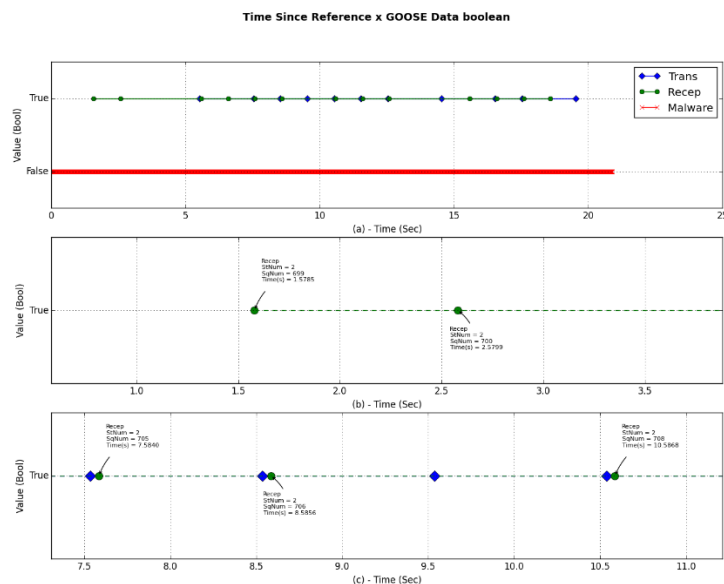


FIGURA 9 – (a) – Ataque GOOSE para 85% da largura de banda; FIGURA 9 – (b) – Perda de pacotes do IED transmissor; FIGURA 9 – (c) – Perda de pacote pelo receptor

A **Erro! Fonte de referência não encontrada.** representa a largura de banda de 85 Mbps registrada durante o ataque.

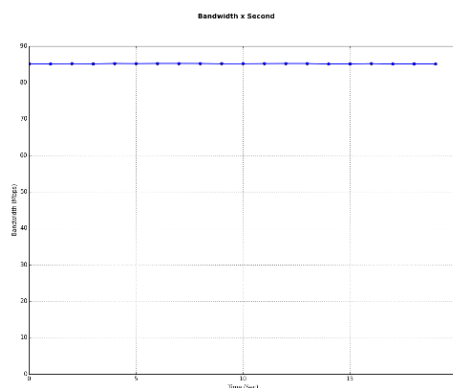


FIGURA 10 – Largura de banda de 85Mbps registrada durante o ataque

Os IEDs continuaram a registrar as mensagens fora de sequência e corrompidas. Contudo foi possível verificar o incremento de mensagens perdidas devido a saturação do receptor, demonstrado pela perda de pacotes do receptor e do transmissor. O perfil de transmissão foi claramente corrompido devido ao aumento do tráfego inserido pelo malware. Portanto é possível concluir que a rede não é mais confiável para o tráfego de qualquer tipo de mensagem ou medição de dados nesta situação, colocando à mostra a vulnerabilidade da rede.

4.0 - SEGURANÇA CIBERNÉTICA PARA SUBESTAÇÕES DE ENERGIA ELÉTRICA

4.1 Gerenciamento de camada 2 utilizando tags IEEE 802.1Q

As subestações modernas, oferecem facilidades e melhoras na implementação de funções utilizando a rede de comunicação. Quando implementadas de forma segura oferecem confiabilidade e eficiência. Porém se implementadas de forma equivocada e com lacunas na segurança, podem oferecer vulnerabilidades para ataques e falhas no sistema de automação diminuindo a confiabilidade e a eficiência da instalação, (Ewing, 2010).

Virtual Local Area Networks (VLANs) são redes particionadas e isoladas na camada de enlace do modelo OSI. As VLANs utilizam a tecnologia IEEE 802.1q que define a normatização do sistema de tags sobre o frame ethernet, (IEEE Std. 802.1Q, 2012). A Figura 11, apresenta um esquemático do tráfego de mensagens gerenciadas pelo switch. Utilizando tags IEEE 802.1Q nos frames ethernets é possível gerenciar o fluxo de dados através da camada de enlace do modelo OSI.

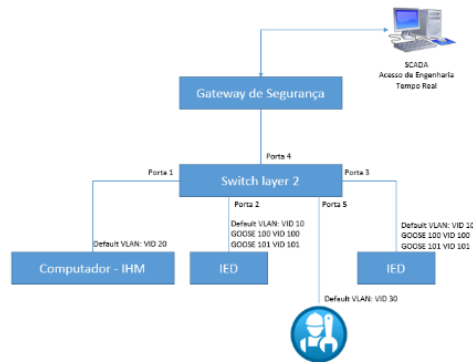


FIGURA 11 – Diagrama de rede utilizando VLANs

O acesso entre as VLAN ID 10, 20, 30 é realizada através do Gateway de Segurança e um firewall gerencia a inspeção dos pacotes, os níveis de acesso. Portanto o fluxo de informação com as tags 10, 20, 30 é direcionada para a porta 4 e distribuído para as portas de interesse e o sistema SCADA. As VLANS 100 e 101 são específicas para mensagens GOOSE e não é necessário o roteamento pelo gateway de segurança. As mensagens GOOSE trafegam exclusivamente pelas portas 2 e 5. Portanto apenas os equipamentos de interesse compartilham da informação.

O gerenciamento da rede através de VLANS possibilita isolar a rede de dados apenas para aqueles equipamentos de interesse, dificultando acesso por pessoas não autorizadas e otimizando a performance da rede de comunicação uma vez que o tráfego multicast é dividido.

4.2 Software Defined Network: SDN

SDN é uma arquitetura de rede estática baseada na tecnologia de tabelas de pesquisas, é ideal para performance da rede reduzindo a largura de banda através do controle de fluxo por software. SDN é uma abordagem que utiliza protocolos abertos, como o OpenFlow que permitir controle de fluxo em equipamentos de fronteira como switches (Open Networking Foundation, 2016).

A arquitetura SDN possui 3 níveis: Aplicação, controlador de fluxo e infraestrutura de rede. A Figura 12 mostra a interação entre os 3 níveis. A camada de aplicação possui 3 principais funções: Operação, administração e gerenciamento do sistema (*Operation, administration, management* –OAM). O controlador de fluxo é a aplicação central que permite a visualização da rede e instrui o sistema como tratar os pacotes. A infraestrutura de rede são os equipamentos que recebem as instruções do controlador e direcionam os pacotes para os seus respectivos destinos.

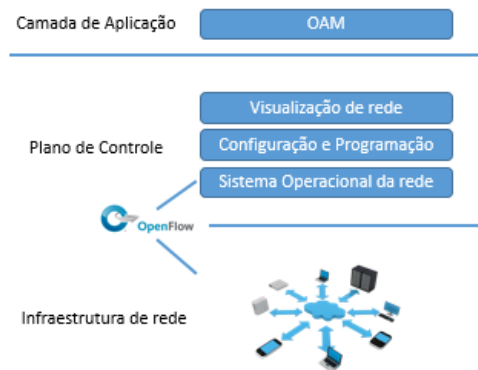


FIGURA 12 – Arquitetura da rede SDN

O OpenFlow utiliza valores contidos em uma tabela verdade para o controle do fluxo através da rede e para o processamento interno do switch. Uma entrada da tabela verdade contém informações presentes no header da mensagem. Para as mensagens GOOSE, as entradas das tabelas verdades, podem ser qualquer informação do header ethernet como a tag IEEE 802.1q ou o endereço MAC de destino.

O switch compara as entradas adquiridas com cada entrada na tabela verdade procurando por uma regra válida. O pacote então é aplicado para a saída de ação e o switch encaminha o pacote para a porta especificada ou para o descarte da mensagem.

Uma vez feita a engenharia da rede SDN o switch irá se comportar como configurado pelo usuário, eliminando possíveis rotas de invasão e de sobrecarga na rede de dados. As redes SDN apresentam um grande avanço para a segurança e performance nas redes das subestações.

5.0 - CONCLUSÃO

A norma IEC 61850, oferece recursos interessantes para automação de subestações de energia elétrica. As mensagens GOOSE podem ser utilizadas para compartilhar sinais de bloqueios, abertura e fechamento para equipamentos dentro de uma SE. Devido à alta necessidade de performance, procedimentos de autenticação e segurança são abstraídos da dinâmica de transmissão, tornando as mensagens GOOSE intrinsecamente vulneráveis. Técnicas de ataques como: manipulação dos frames ethernet e saturação da rede de dados, podem comprometer o desempenho dos equipamentos envolvidos no sistema de proteção e controle. Melhores práticas de configuração de redes ethernet e novas tecnologias como gerenciamento de redes por software (SDN) podem minimizar os riscos de ataques e aumentar a performance da rede de dados.

As mensagens GOOSE são definidas pelas IEC 61850-8-1 e mapeadas sobre o frame ethernet. O APDU possui uma série de parâmetros utilizados para análise de erros e recepção dos dados. Parâmetros como *stNum* e *SqNum*, podem ser utilizados pelos IEDs para verificar e processar as mensagens GOOSE. Porém sem um mecanismo de autenticação da fonte da mensagem esses parâmetros de confirmação podem facilmente serem mascarados e utilizados de forma maliciosa.

A técnica de saturação da rede de dados, explorada nesse artigo, mostrou como a dinâmica de transmissão multicast pode ser usada de forma maliciosa e influenciar na performance dos equipamentos conectados na rede de dados. Ao atingir um limite próximo da capacidade de dados foi possível observar a perda de pacotes de ambos os equipamentos, transmissor e receptor. A rede de dados foi comprometida devido ao ataque e não é mais possível garantir a entrega dos pacotes.

Melhores práticas de redes podem ser utilizadas para mitigar possíveis ataques e garantir a integridade da troca de mensagens. A utilização da tecnologia IEEE 802.1Q garante a segregação de redes na camada de enlace através da configuração dos switches e da inserção de tags nos frames ethernet. As redes SDN são cyber seguras pela concepção da tecnologia. A topologia estática das redes SDN permite um controle de acesso e fluxo preciso nas portas dos controladores de redes, prevenindo assim qualquer forma de ataque dentro das subestações.

6.0 - REFERENCIAS

Dolezilek, D., Whitehead, D., & Skendzik, V. (2010). *Integration of IEC 61850 and Sampled Values services to reduce substation wiring*. Pullman, Washington: Schweitzer Engineering Laboratories.

Ewing, C. (2010). *Engineering Defense-in-Depth Cybersecurity for the Modern Substation*. Spokane, Washington: 12th Annual Western Power Delivery Automation Conference.

Hoyos, J., Dehus, M., & Brown, T. (2012). *Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure*. Boulder, Colorado: University of Colorado Boulder.

IEC 61850-5. (2003). *Communication networks and systems in substation - Part 5: Communication requirements for functions and device models*. Geneva, Switzerland: IEC.

IEC 61850-8-1. (2004). *Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*. Geneva, Switzerland: IEC.

IEEE Std. 802.1Q. (2012). *IEEE Std. 802.1Q, Virtual Bridge Local Area Network*. IEEE.

Konka, J., Arthur, C., Garcia, F., & Atkinson, R. (2011). *Traffic Generation of IEC 61850 Sampled Values*. Glasgow, Scotland: University of Strathclyde.

Kruger, C., Behardien, S., & Retonda-Mo, J. (2013). *A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system*. INT J COMPUT COMMUN.

Kush, N., Ahmed, E., Branagan, M., & Foo, E. (2014). *Poisoned GOOSE: Exploiting the GOOSE protocol*. Auckland, New Zealand: Queensland University of Technology.

O'Fallon, L., Klas, A., Tibbals, T., Shah, & S. (2013). *IEC 61850 MMS SCADA network optimization for IEDs*. Pullman, Washington: Schweitzer Engineering Laboratories.

Open Networking Foundation. (01 de 08 de 2016). *OpenFlow*. Fonte: OpenFlow: <https://www.opennetworking.org/sdn-resources/openflow>

Ozansoy, C. (2010). *Modelling and Object Oriented Implementation of IEC 61850, The New International Standard on Substation Communication and Automation*. Lambert Academic Publishing.

Senecal, L. (2009). Understanding, preventing, and defending against layer 2 attacks. Cisco Expo. Wireshark. (1 de 7 de 2016). *Wireshark*. Fonte: <https://www.wireshark.org/>

7.0 - DADOS BIBLIOGRAFICOS

Mauricio Gadelha da Silveira nasceu em Monte Aprazível, SP, em 29 de Janeiro de 1988. Graduou-se em Engenharia Elétrica pela Universidade Estadual Paulista (UNESP) no ano de 2013. Atualmente faz parte da equipe de Engenharia e Serviços da Schweitzer Engineering Laboratories (SEL), onde ocupa o cargo de Engenheiro de Proteção.

Paulo Henrique Franco nasceu em Piracicaba, SP, em 03 de Março de 1981. Graduou-se em Engenharia Elétrica pela Universidade Estadual Paulista (UNESP) no ano de 2004. Atualmente faz parte da equipe Special Protection Systems da SEL Engineering Services (SEL-USA), onde ocupa o cargo de Engenheiro de Automação.