IDENTIFICANDO FALHAS DE SEGURANÇA NA REDE DE COMUNICAÇÃO DE SUBESTAÇÕES DIGITALIZADAS EM REDES ELÉTRICAS INTELIGENTES UTILIZANDO O GEESE 2.0

Julia D. Noce*, Yona Lopes*, Natalia C. Fernandes†, Célio V. N. Albuquerque*, Débora C. Muchaluat-Saade*

*Departamento de Ciência da Computação e de Engenharia de Telecomunicações
Laboratório MídiaCom - UFF
Niterói, RJ, Brasil

Emails: julianoce, yona, natalia, debora@midiacom.uff.br, celio@ic.uff.br

Abstract— The use of IEDs in substations have brought a great improvement in terms of speed, costs, maintenance, and reliability. In this context, the use of IEC 61850 standard appears as one of the main recommendations for substation automation in smart grids that digitally perform the electrical network control and protection. Nevertheless, this improvement may cause several security issues. Therefore, security threats in substation networks must be detected in order to improve cyber security solutions. Thereat, we propose an extension to GEESE generator in order to allow interaction with operator through a graphical interface. GEESE 2.0 allows a cyber security threat validation. We have deployed a substation local network and used GEESE 2.0 to perform an attack. After we analyze the impact of an attack in a protection scheme of a substation .

Keywords— GOOSE, Security, IEC 61850, Cyber Attack, Spoofing

Resumo— A utilização de dispositivos eletrônicos inteligentes nas subestações elétricas trouxe um grande avanço em termos de velocidade, custo, manutenção e confiabilidade. Nesse sentido, a utilização da norma IEC 61850 aparece como uma das principais recomendações para automação de subestações em *smart grids*, que passam a realizar o controle e proteção da rede elétrica de forma digitalizada. Contudo, esse avanço pode causar diversos problemas de segurança. Nesse sentindo é importante que as falhas de segurança nas redes de subestações sejam identificadas e avaliadas para que soluções possam ser implementadas. Com esse objetivo, o gerador de pacotes GEESE foi estendido para permitir a interação com o operador através de uma interface gráfica e assim permitir a validação do impacto que uma falsificação de pacotes pode causar na rede de subestação. Uma rede local real de subestação foi implementada em laboratório e o GEESE 2.0 foi usado para avaliar o impacto que um ataque gera em um esquema de proteção de uma subestação.

Palavras-chave— GOOSE, Segurança, IEC 61850, Ataque Cibernético, Spoofing

1 Introdução

Com o desenvolvimento de novas tecnologias relacionadas a modernização do setor elétrico, os *Intelligent Electronic Device*s (IEDs) têm sido utilizados com maior frequência. A utilização de IEDs ao invés dos dispositivos tradicionais de proteção para subestações apresenta diversas vantagens, tais como: digitalização de informações, maior velocidade, possibilidade de comunicação e redução de custo (Lopes et al., 2012). Contudo, a introdução de um forte suporte ao sistema de proteção por meio de redes de comunicação também traz ao ambiente das subestações diversas ameaças cibernéticas (Hoyos et al., 2012). Problemas de segurança nas redes elétricas tornaram-se muito relevantes, principalmente após a transição de tecnologia analógica para digital. Com a introdução de redes Ethernet para trafegar informações críticas do sistema, tem-se também a possibilidade de invasão nessa rede. Falhas na comunicação, assim como a introdução de mensagens falsas ou adulteradas na rede, podem afetar a estabilidade e a confiabilidade no setor elétrico com um todo (Hoyos et al., 2012). Devido ao sistema elétrico ser todo interligado, o mau funcionamento de uma subestação pode causar efeitos em diversas outras instalações de geração, transmissão ou distribuição, comprometendo o fornecimento de energia e podendo causar grandes perdas financeiras.

Este trabalho estende o gerador de pacotes chamado GEESE (Lopes et al., 2015) para que possa permitir interação com o operador e a realização facilitada de ataques a subestação. O GEESE consiste em um gerador de pacotes *Generic Object Oriented Substation Event* (GOOSE) (Lopes et al., 2015) da IEC 61850 (61850, 2002–2013). O GEESE 2.0 além da interface com o operador possui um módulo de segurança que captura os pacotes e indica os campos que devem ser alterados para o ataque. Para realizar os ataques, uma rede de subestação local foi montada com equipamento reais tais como IEDs e *switches* de mercado[1]. Também foram usados equipamentos para simular o comportamento da rede elétrica e IEDs que permitem o armazenamento de oscilografias para observar a efetividade dos ataques produzidos com o GEESE 2.0.

Foi realizado um ataque *spoofing* onde pacotes foram interceptados e o conteúdo alterado sem que os envolvidos, IEDs e supervisores da rede,

[1] *Switches* para subestações diferem consideravelmente de *switches* tradicionais de redes, pois precisam de toda uma proteção devido ao ambiente severo de subestações a que estão propícios, altas temperaturas, interferências eletromagnética, alta periculosidade, etc.

percebam. Com a interface gráfica e o módulo de segurança, a realização de testes em laboratório foi facilitada permitindo que o ataque fosse realizado e avaliado. Observou-se, de fato, que os IEDs atuam indevidamente mediante o ataque gerado a partir do GEESE 2.0. Com isso, verificou-se a atuação indevida de equipamentos elétricos e a vulnerabilidade das subestações foi comprovada, para que possa vir a ser corrigida.

O artigo é apresentado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha a mensagem GOOSE. A Seção 4 apresenta o GEESE 2.0 e o seu funcionamento. A Seção 5 demonstra os testes do gerador de pacotes GEESE 2.0, o ataque realizado aos IEDs na prática e a avaliação. Finalmente, a Seção 6 conclui o artigo e aponta os trabalhos futuros.

2 Trabalhos Relacionados

Geradores de pacotes são úteis para testes de segurança e desempenho. Diferentes tipos de geradores estão disponíveis, seja para criar um número muito grande de pacotes ou ainda para testar as funcionalidades de uma rede de forma mais simples que com as ferramentas de debug tradicionais de redes (Emmerich et al., 2015; Zeng et al., 2014).

O uso de geradores de pacotes para avaliar problemas de segurança em redes também é uma prática bem conhecida. Por exemplo, o mecanismo *packet vaccine* utiliza um gerador de pacotes para identificar *exploits* em redes tradicionais (Wang et al., 2006). Outro exemplo, dentro da área de segurança em redes de automação industrial, faz a geração de pacotes do protocolo DNP3, específico para esse tipo de rede de comunicação e também usado em subestações tradicionais. Nesse caso, o gerador era usado para descobrir os elementos da rede e causar, na sequência, ataques contra os elementos-chave (Rodofile et al., 2016).

Hoyos et al. explicitam as consequências de um ataque em camada dois em redes de subestação e desenvolvem um script de ataque (Hoyos et al., 2012). Contudo, esse estudo limita-se ao fato de realizar ataques e não apresenta uma ferramenta que flexibilize os testes.

Especificamente relacionado ao uso do IEC 61850 em *smart grids*, existem alguns trabalhos que avaliam o impacto de ataques na subestação. Nivethan et al., em 2013, propõem um modelo teórico para avaliar o RTT em redes IEC 61850 por meio de simulações (Nivethan et al., 2013). Isso é importante, pois a norma define atrasos máximos no encaminhamento de pacotes. Caso esses atrasos máximos sejam desrespeitados, o funcionamento correto do sistema de proteção elétrico poderá ser prejudicado. Nessa mesma linha, em 2014, analisam ataques em subestações IEC 61850 por meio de simulação que possam causar sobrecarga nos enlaces através da injeção de pacotes falsos, fazendo com que os atrasos máximos especificados pela norma não sejam respeitados (Nivethan et al., 2014).

O GEESE foi desenvolvido como um gerador de pacotes GOOSE para avaliar o funcionamento de subestações baseadas na norma IEC 61850. As mensagens GOOSE são a parte central para o sistema de proteção de subestações digitalizadas com base na norma IEC 61850, pois são utilizadas para enviar alertas e comandos entre IEDs. O GEESE permite que o tráfego padrão dessas subestações seja injetado por emulação, de forma a permitir avaliar todos os parâmetros de Qualidade de Serviço- *Quality of Service* (QoS) da rede de comunicação da subestação (Lopes et al., 2015).

Um outro trabalho muito interessante é o de Kush et al. Os autores desenvolveram um gerador de mensagens GOOSE mal formadas. O objetivo dessas mensagens é gerar ataques de negação de serviço - *Denial of service* (DoS) contra IEDs, que param de processar as mensagens legítimas ao receber uma mensagem com um número de estados superior ao esperado (Kush et al., 2014).

Este artigo possui a finalidade de estender e oferecer uma interface gráfica ao gerador GEESE (Lopes et al., 2015). O GEESE 2.0 permite a emulação de pacotes que gerem ataques em redes IEC 61850 e é mais flexível que a proposta de Kush et al, pois permite a emulação de qualquer tipo de ataque usando mensagens GOOSE. No GEESE 2.0, todos os campos da mensagem podem ser alterados/configurados pela interface gráfica de forma a permitir a criação de novos tipos de ataques viabilizando um estudo mais profundo sobre segurança em subestações.

3 GOOSE: Detalhamento e Análise

3.1 Mensagem GOOSE

A estrutura do quadro GOOSE é mapeada em um quadro Ethernet e faz o uso de *Virtual Local Area Network*s (VLANs) e de *tags* de prioridade. Essa prioridade contribui para filtrar as mensagens, sobretudo, quando o enlace de comunicação está com uma alta taxa de uso. A Figura 1 exemplifica a estrutura da mensagem GOOSE.

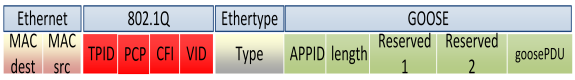

Figura 1: Estrutura da mensagem GOOSE (Lopes et al., 2015).

O campo `ethernet` especifica o endereço *Media Access Control* (MAC) de origem, especificando o IED que envia a mensagem, e o endereço MAC Multicast de destino que é o grupo para o qual essa mensagem é enviada.

O campo `802.1Q` especifica uma *tag* de VLAN acrescentada ao quadro Ethernet, o que permite a utilização de VLANs com diferentes prioridades nas mensagens. O seu tamanho é de 4 bytes. O campo `ethertype` indica que esse pacote é o GOOSE e possui o valor de 0x88B8. Seu tamanho é de 2 bytes. O campo *Application Identifier (APPID)* serve para selecionar a mensagem GOOSE e distingui-la da aplicação, ocupa o tamanho de 2 bytes. Já o *length* determina um octeto representando o total do tamanho da *Goose Protocol Data Unit (goosePDU)* mais 8 bytes do APPID e do Ethertype. Os campos *Reserved* são para futuras aplicações e são atribuídos com o valor 0. Após o *Reserved* tem-se os campos que formam o goosePDU, conforme mostra a Figura 2 que exibe a captura de um pacote GOOSE utilizando o software Wireshark [2].

```
802.1Q Virtual LAN, PRI: 4, CFI: 0, ID: 1
GOOSE
  APPID: 0x1002 (4098)
  Length: 114
  Reserved 1: 0x0000 (0)
  Reserved 2: 0x0000 (0)
  goosePdu
    gocbRef: SEL_451CFG/LLN0$GO$GooseDSet13
    timeAllowedtoLive: 2000
    datSet: SEL_451CFG/LLN0$DSet13
    goID: Sub1Bay2
    t: Mar 15, 2016 12:29:39.473267853 UTC
    stNum: 2
    sqNum: 12849
    test: False
    confRev: 1
    ndsCom: False
    numDatSetEntries: 1
    allData: 1 item
```

Figura 2: Captura do Pacote GOOSE pelo Wireshark ressaltando os campos GOOSE.

Segundo as definições da norma IEC 61850 (61850, 2002–2013), o campo `gocbRef`, de GOOSE Control block reference, dá a referência para o caminho do bloco de controle do GOOSE. Já o `timeAllowedtoLive` representa o tempo que o IED receptor espera receber a próxima mensagem GOOSE daquela retransmissão. O `datSet` é uma String que descreve o nome do Data Set [3]. O `goID` é um identificador do IED que envia a mensagem. `t` é um marcador de data e hora do momento em que a mensagem foi enviada. O `stNum` do nome *State Number* representa o evento, com isso ele incrementa toda vez que tem-se um evento que resulte em uma mudança de valor em um atributo do data set. Já o `sqNum` (*Sequence Number*) possui um contador que incrementa toda vez que um pacote daquele mesmo evento (stNum) é enviado. O campo `test` indica se a mensagem está sendo usada apenas para teste. O `confRev` (*Configuration Revision*) é um versionamento usado nos projetos que indica em qual versão aquela configuração está. O `ndsCom` indica a necessidade de revisão na configuração entre origem e destino, indicando que o `gocbRef` precisa ser atualizado e assume o valor de *True* quando o Data Set está vazio. O `numDatSetEntries` (*Number of Data Set Entries*) é o número de elementos que compõem essa *Data Set* específico. Finalmente, o `allData` é o elemento que possui a informação da mensagem GOOSE.

3.2 Regras de codificação ASN1

Os campos que compõem a mensagem GOOSE seguem a norma de codificação *Abstract Syntax Notation One (ASN.1)* (ASN1, 2002–2015). A ASN.1 define uma notação formal utilizada para dados transmitidos em protocolos de telecomunicações. A codificação do protocolo GOOSE não se baseia rigorosamente na ASN.1/BER original, mas sim em uma adaptação da codificação ASN.1 para o protocolo *Manufacturing Message Specification* (MMS) (Kriger et al., 2013), que também é usado da norma IEC 61850. Essa norma possui a finalidade de promover especificações de codificação e decodificação para a sintaxe do protocolo que é enviado pela rede. Além disso, os valores codificados pelo ASN.1 sempre possuem o formato de uma TAG, LENGTH, seguido por um VALOR (Content).

4 GEESE 2.0: Nova versão do gerador de pacotes GEESE

Com a necessidade de tornar mais fácil e flexível a utilização da ferramenta, e permitir a realização de testes de segurança cibernética, o gerador GEESE, apresentado, inicialmente, em (Lopes et al., 2015), foi estendido para uma construção 100% fiel às mensagens reais de forma que os ataques pudessem ser realizados. Para isso, as inclusões da codificação ASN.1 e da interface gráfica foram essenciais.

O GEESE 2.0 é uma ferramenta que gera e envia pacotes GOOSE pela rede obedecendo a janela de retransmissão escolhida e todo o comportamento e campos do protocolo. A nova versão proposta modifica a codificação implementada, de forma que IEDs de mercado pudessem receber os pacotes de forma transparente e atuar na rede elétrica como se a mensagem viesse de outros IEDs na rede, permitindo que os testes de segurança fossem realizados. Além disso, a nova versão conta com uma interface gráfica para facilitar a escolha dos parâmetros, o conteúdo das mensagens e a geração de pacotes.

[2] Wireshark é um famoso analisador de protocolo de rede que permite a análise de dados em tempo real da rede. Detalhes em: www.wireshark.org

[3] Um data set é um conjunto de atributos GOOSE que são agrupados dentro do mesmo pacote para envio

4.1 Modelo da rede

Os componentes da rede são, basicamente, os IEDs, capazes de monitorar e atuar na rede, o sistema supervisório e os *switches*, utilizados para interconexão entre IEDs e entre IEDs e o sistema supervisório.

É esperado que a norma IEC 61850 esteja implementada, o que implica a possibilidade de utilização dos protocolos GOOSE, MMS e *Sampled Values* (SV). Embora o GEESE 2.0 só atue nas mensagens GOOSE, ele supõe o funcionamento normal da subestação. Outros protocolos, como aqueles utilizados para recuperação de falhas, podem estar em uso e não irão interferir no funcionamento do GEESE 2.0. O sistema GEESE 2.0 deve ser executado em uma máquina a parte, a qual deve estar conectada em algum dos switches da subestação.

4.2 Modelo do ataque

As redes IEC 61850 são vulneráveis a vários tipos de ataque, mas a extensão completa dos ataques, assim como o seu impacto, ainda precisa ser estudada com ferramentas como o GEESE 2.0. Muitas das vulnerabilidades advêm da ausência de mecanismos de controle de acesso e de criptografia e precisam ser superadas por meio de métodos com baixo atraso. Apesar de pouco implementada, a segurança cibernética é um assunto muito discutido na área de automação de subestações. Segundo (Liu et al., 2012), em 2011, a empresa McAfee publicou um trabalho afirmando que tentativas de ataques cibernéticos estavam sendo realizadas contra empresas de energia elétrica, petróleo, óleo e gás. Segundo Liu et al. os ataques foram realizados com sucesso a partir de vários países que tiveram sua segurança violada e informações confidencias foram acessadas. Ressalta-se que esses tipos de ataques podem resultar em outros tipos de consequências que não sejam apenas violação de informações, mas também alteração de configuração em subestações e ataques como o descrito a seguir.

Os ataques já conhecidos contra subestações podem ser direcionados contra a própria rede de comunicação ou contra o sistema de potência. Quando direcionados contra o sistema de potência, o objetivo é a interrupção do serviço e/ou a destruição de equipamentos. Assim, o atacante utilizará as mensagens GOOSE para causar um funcionamento incorreto dos equipamentos, seja pela adulteração de valores ou pelo envio de comandos indevidos. O atacante pode, ainda, se aproveitando de vulnerabilidades do IED, realizar ataques de negação de serviço. Os ataques contra a rede de comunicação utilizando as mensagens do própria IEC 61850, em geral, estão associados a sobrecarga dos enlaces, seja pela criação de um grande número de mensagens falsas ou pela geração de eventos falsos na rede. Em geral, os ataques à rede de comunicação trazem impactos diretos ao funcionamento do controle e da proteção da rede, causando impactos negativos ao funcionamento da rede elétrica.

O GEESE 2.0 permite gerar ataques de todas essas naturezas, uma vez que dá liberdade para a troca de todos os campos de um quadro GOOSE, especificando o tempo de envio das mensagens. Com isso, o GEESE 2.0 permite que seja realizado um ataque *spoofing*, de forma a falsificar pacotes inserindo tráfego legítimo na rede com campos modificados.

4.3 Estrutura e Implementação do GEESE 2.0

O programa foi implementado em *Python*, utilizando o framework de interface gráfica Tkinter e outro framework de envio de pacotes chamado Scapy. O GEESE 2.0 é dividido em várias seções que devem ser preenchidas a fim de construir o pacote. Para ilustrar uma das funcionalidades, a aba Packet, ilustrada na Figura 3 é uma aba onde o usuário preenche as informações do IED que será simulado, com o seu MAC de Destino Multicast e MAC de origem, o ID da VLAN, o ID da mensagem e outros campos que fazem parte do pacote GOOSE [4].

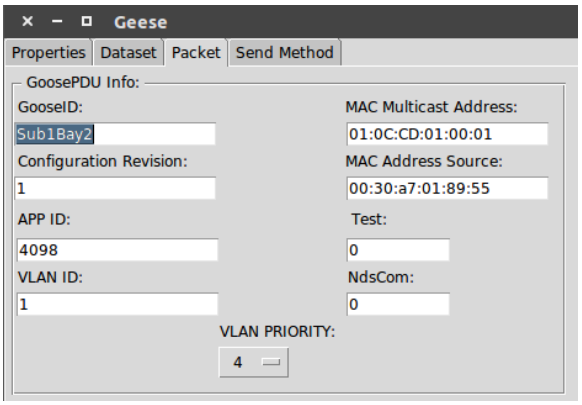

Figura 3: Ferramenta GEESE 2.0.

5 Experimentos e Testes de Vulnerabilidade

De forma geral os IEDs de proteção recebem leituras de corrente e tensão nas linhas identificando os diferentes tipos de faltas [5]. Através de mudanças na resistência do centro de carga C1, são reproduzidas as condições de sobrecarga e curto-circuito no sistema elétrico que resultam na atuação dos

[4] Para a visualização completa da ferramenta e de suas funcionalidades o GEESE 2.0 está disponibilizado no site http://www.midiacom.uff.br/midiacom/index.php/pt-BR/downloads/ferramentas/

[5] Defeitos e situações de risco na rede elétrica são chamados de falta.

IEDs. Foram utilizados equipamentos como fontes, chaves e contatoras para representar os principais equipamentos de uma subestação, permitindo observar a dinâmica no comportamento de equipamentos dos IEDs e seus disjuntores quando os eventos propostos são simulados. Para simular o comportamento de um centro de cargas, utilizou-se um bloco de cargas resistivas 6x500 ohms. Através de seis chaves é possível adicionar ou remover uma a uma as resistências de 500 ohms em paralelo. Acrescentando gradualmente as resistências, reproduz-se um cenário de aumento de carga até causar uma sobrecarga no sistema. Para simular um curto-circuito utilizou-se um conjunto de lâmpadas de 127V conectadas em paralelo. Ao acionar todo o conjunto por uma chave-faca, a corrente elétrica se eleva rapidamente e, devido aos ajustes dos IEDs, esta elevação é interpretada como curto-circuito. Para simular a falha do disjuntor foi posto um *jump* de modo a impedir que o circuito sob falta seja aberto, simulando uma falha no disjuntor. A atuação esperada é que os disjuntores estejam sempre fechados e que em uma condição de falta, como o evento de curto-circuito, o disjuntor abra para isolar a falta. No cenário implementado, caso o disjuntor 52-2 esteja em falha e não atue, o IED B envia uma mensagem GOOSE para que o IED A abra o disjuntor 52-1 e isole a falta mantendo o sistema protegido.

5.1 Resultados do ataque realizado com o GEESE 2.0

Os IEDs utilizados no experimento incorporam um sistema de Falha de Disjuntor com funções abrangentes, onde as correntes podem ser monitoradas. Nesse teste, o GEESE 2.0 envia mensagens GOOSE copiando a mensagem que o IED B enviaria para o IED A em caso de falha do disjuntor que, por consequência, envia um sinal de *trip* (que serve para abrir o disjuntor) para o disjuntor 52-1. No IED A, foi configurada a Função 50 para proteção de sobrecorrente instantânea de fase no ajuste de 10 A (amperes) e a Função 51 para proteção de sobrecorrente temporizada de fase no ajuste de 1,2 A. É possível observar na oscilografia da Figura 4 que a corrente não excedeu os valores ajustados. Isso significa que não haveria motivo para ocorrer um sinal de *trip*. Contudo, ao observar a Figura 4, comprova-se a efetividade do ataque no IED A que, por receber um sinal de falha de disjuntor indevido, da trip sem evento elétrico que justifique a atuação da proteção. A Figura 5 mostra a oscilografia pós-falta indicando que o disjuntor foi aberto interrompendo a passagem de corrente sem acionamento das funções de proteção 50 e 51.

A variável interna do IED B que indica falha de disjuntor foi associada a uma mensagem GOOSE, com isso, em caso de tentativa de abertura

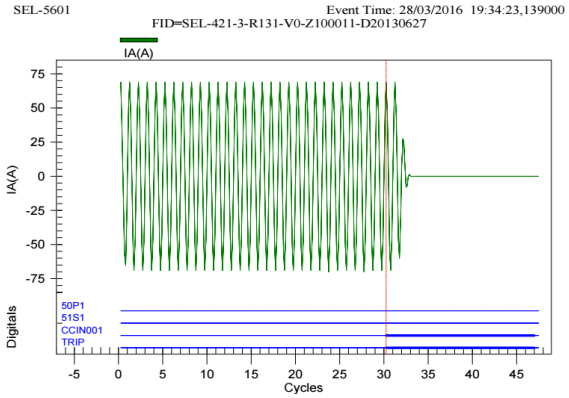

Figura 4: Oscilografia do IED A (IED-421) antes do sinal de *trip*.

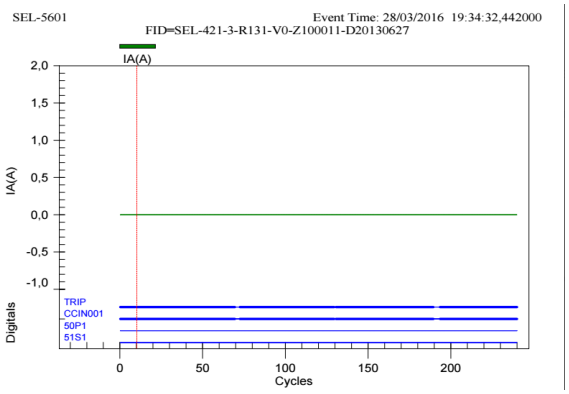

Figura 5: Oscilografia do IED A (IED-421) depois do sinal de *trip*.

do disjuntor sem sucesso, uma mensagem GOOSE é enviada para o IED A de forma que ele abra o disjuntor 52-1 e isole a falta. A CCIN001 é a variável no IED A que recebe essa mensagem GOOSE do IED B. A barra em azul escuro representa que essa variável recebeu a mensagem de falha de disjuntor e, portanto, enviou um sinal de *trip* para o disjuntor 52-1. Nas oscilografias das Figuras 4 e 5 é possível verificar que o sinal de *trip* foi acionado mesmo sem ocorrência de sobrecorrente.

O ataque ocorre devido à mensagem GOOSE gerada pelo GEESE 2.0 ser uma cópia da mensagem gerada pelo IED B com apenas duas diferenças: o valor do atributo de falha de disjuntor e o campo *State Number* que indica a mudança de estado (evento). O primeiro é modificado no campo *allData*, no qual o valor booleano, anteriormente em *False*, é alterado para *True*. O segundo valor modificado é no campo *stNum* que é incrementado. Assim, o IED A que só processa uma nova informação na ocorrência de um novo evento, recebe o valor do campo incrementado, entende que ocorreu um novo evento e atua. Cabe observar que nenhuma atitude foi tomada para evitar o envio das GOOSEs originais do IED B e, mesmo assim, o ataque foi efetivo, já que as mensagens reais são geradas em um evento considerado antigo após o ataque.

Por meio deste estudo de caso, foi possível mostrar como o GEESE 2.0 pode ser usado para identificar diferentes tipos de vulnerabilidades em subestações de energia elétrica apontado a necessidade da inclusão de segurança de redes nos projetos de subestação.

6 Conclusões e Trabalhos Futuros

Este trabalho confirma o quão importante a segurança é para indústria de energia elétrica, visto que o ataque apresentado poderia gerar grandes prejuízos à companhia elétrica. Este artigo detalhou o formato da mensagem GOOSE que é crucial para proteção dos IEDs e também foi para a criação do gerador de pacotes GEESE 2.0.

A interface gráfica desenvolvida se mostrou essencial para facilitar a utilização da ferramenta, simplificando a modificação do pacote GOOSE. Assim como sua versão anterior, o GEESE 2.0 é um software livre, flexível e de fácil uso com grande grau de importância para pesquisas em redes IEC 61850.

Esse trabalho propôs a comprovação da vulnerabilidade a que as subestações digitalizadas estão sujeitas e uma primeira versão da ferramenta gráfica do GEESE. Como trabalhos futuros, pode-se destacar a melhoria na serialização de ataques na rede elétrica, facilitando o desenvolvimento de novos padrões de teste. Além disso, espera-se disponibilizar na ferramenta os padrões de ataque já bem conhecidos, para que o GEESE 2.0 possa ser usado como um *checklist* de vulnerabilidades no sistema de comunicação de subestações.

A contribuição principal desse artigo está na disponibilização de uma ferramenta que pode ser usada e aperfeiçoada ciclicamente para testar os esquemas de segurança atuais e as novas propostas dentro de redes de subestações, garantindo que as inovações disponibilizadas por *smart grids* não sejam inviabilizadas devido à existência de vulnerabilidades na comunicação.

7 Agradecimentos

Os autores gostariam de agradecer ao CNPq, CAPES e FAPERJ pelo apoio financeiro ao projeto. Além disso, um agradecimento especial a empresa SEL (*Schweitzer Engineering Laboratories*) pelos equipamentos doados e apoio ao laboratório.

Referências

61850, I. (2002–2013). *IEC 61850: Communication Networks and Systems for Power Utility Automation*, International Electrotechnical Commission.

ASN1 (2002–2015). *OSI networking and system aspects - Abstract Syntax Notation One: Specification of basic notation*, ITU.

Emmerich, P., Gallenmüller, S., Raumer, D., Wohlfart, F. and Carle, G. (2015). Moongen: A scriptable high-speed packet generator, *IMC*, ACM, NY, USA, pp. 275–287.

Hoyos, J., Dehus, M. and Brown, T. X. (2012). Exploiting the goose protocol: A practical attack on cyber-infrastructure, *IEEE Globecom Workshops*, pp. 1508–1513.

Kriger, C., Behardien, S. and Modiya, J. C. R. (2013). A detailed analysis of the goose message structure in an iec 61850 standard-based substation automation system, Vol. 8, pp. 708–721.

Kush, N., Ahmed, E., Branagan, M. and Foo, E. (2014). Poisoned goose: Exploiting the goose protocol, *AISC*, Australian Computer Society, Inc., Darlinghurst, Australia, pp. 17–22.

Liu, C. C., Stefanov, A., Hong, J. and Panciatici, P. (2012). Intruders in the grid, *IEEE Power and Energy Magazine* **10**(1): 58–66.

Lopes, Y., Frazão, R. H., Molano, D. A., dos Santos, M. A., Calhau, F. G. a., Bastos, C. A. M., Martins, J. S. B. and Fernandes, N. C. (2012). Smart Grid e IEC 61850: Novos Desafios em Redes e Telecomunicações para o Sistema Elétrico, *Minicursos do XXX SBrT*, 1 edn, pp. 1–44.

Lopes, Y., Muchaluat-Saade, D. C., Fernandes, N. C. and Fortes, M. Z. (2015). Geese: A traffic generator for performance and security evaluation of IEC 61850 networks, *IEEE 24th ISIE*, pp. 687–692.

Nivethan, J., Papa, M. and Hawrylak, P. (2014). Modeling and simulation of electric power substation employing an iec 61850 network, *CISR*, ACM, NY, USA, pp. 89–92.

Nivethan, J., Papa, M. and Hawrylak, P. J. (2013). Estimating link availability and timing delays in ethernet-based networks, *CSI-IRW '13*, ACM, NY, USA, pp. 1–4.

Rodofile, N. R., Radke, K. and Foo, E. (2016). Dnp3 network scanning and reconnaissance for critical infrastructure, *ACSW '16*, ACM, NY, USA, pp. 39:1–39:10.

Wang, X., Li, Z., Xu, J., Reiter, M. K., Kil, C. and Choi, J. Y. (2006). Packet vaccine: Black-box exploit detection and signature generation, *13th ACM CCS*, NY, USA, pp. 37–46.

Zeng, H., Kazemian, P., Varghese, G. and McKeown, N. (2014). Automatic test packet generation, *ACM Trans. Netw.* **22**(2): 554–566.