Implementação de Ataques em Ambiente Simulado para Estudo de Segurança Cibernética em Sistemas Elétricos

Johnatan A. de Oliveira[1], **Anderson F. Pereira dos Santos**[2], **Ronaldo M. Salles**[12]

[1]Programa de Pós-Graduação em Engenharia de Defesa
Instituto Militar de Engenharia (IME) - Rio de Janeiro, RJ - Brasil

[2]Programa de Pós-graduação em Sistemas e Computação
Instituto Militar de Engenharia (IME) - Rio de Janeiro, RJ - Brasil

{alves.johnatan,anderson,salles}@ime.eb.br

Abstract. *The insertion of digital communications in electrical power systems made these critical infrastructures susceptible to cyber attacks. Network protocols of these systems, defined by the IEC 61850 standard, have known vulnerabilities and ways to mitigate them are currently studied. Therefore, this article presents a laboratory simulation of an electrical system modeled in Real-Time Digital Simulator (RTDS) using a real IED in hardware-in-the-loop with the implementation of cyber attacks . The experiments carried out will serve as a basis for the study of intrusion detection in these environments.*

Resumo. *A inserção das comunicações digitais nos sistemas elétricos de potência tornou essas infraestruturas críticas susceptíveis aos ataques cibernéticos. Protocolos de rede desses sistemas, definidos pelo padrão IEC 61850, possuem vulnerabilidades conhecidas e formas de mitigá-las são estudadas atualmente. Nesse sentido, este artigo apresenta uma simulação em laboratório de um sistema elétrico modelado no Real-Time Digital Simulator (RTDS) utilizando um IED real em hardware-in-the-loop com a implementação de ataques cibernéticos. Os experimentos realizados servirão de base no estudo de detecção de intrusão nesses ambientes.*

1. Introdução

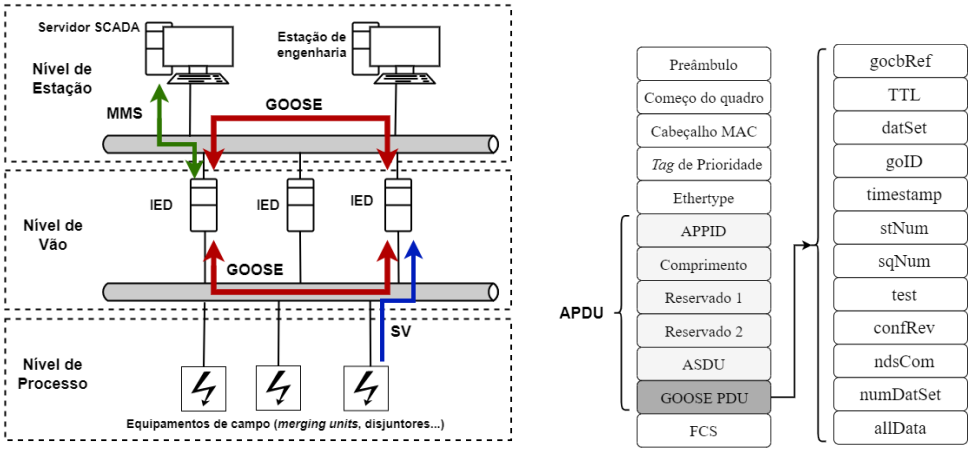
Os sistemas elétricos de potência são exemplos de infraestruturas críticas de extrema relevância na sociedade. A inovação tecnológica computacional e de comunicação fez com que parte dos processos de tais sistemas passassem do meio analógico para o meio digital. Ao facilitar a implementação de projetos, simplificar a comunicação e trazer interoperabilidade, a digitalização das comunicações dos sistemas elétricos acabou por trazer também uma maior exposição destes aos ataques cibernéticos [Quincozes et al. 2021].

Essa maior vulnerabilidade dos sistemas elétricos ficou evidente com a verificação de ataques reais, como por exemplo o que ocorreu na Ucrânia em 2015, que afetou o fornecimento de eletricidade a mais de 225.000 consumidores [M. Lee et al. 2016]. Uma forma de proteção cibernética que pode ser aplicada em infraestruturas críticas como os sistemas elétricos são os sistemas de detecção de intrusão (IDS), porém, um obstáculo à pesquisa desse tipo de solução é a limitação ao acesso de informações acerca do tráfego de rede de tais sistemas [Quincozes et al. 2022].

Sendo assim, para a obtenção de dados próximos a de sistemas reais, esse trabalho buscou realizar ataques cibernéticos específicos da comunicação IEC 61850 em um sistema elétrico simulado. O cenário escolhido foi um sistema de proteção de linhas de transmissão modelado no *Real-Time Digital Simulator* (RTDS)[1] e utilizou-se a técnica *hardware-in-the-loop* (HIL) com um *Intelligent Electronic Device* (IED) comercial utilizado em sistemas reais. Os dados obtidos de tráfego de rede servirão de base na aplicação de aprendizado de máquina na detecção de intrusão.

2. IEC 61850 e suas vulnerabilidades cibernéticas

O conjunto de normas 61850 da *International Electrotechnical Comission* (IEC) definem os protocolos da comunicação digital nas subestações elétricas. O protocolo *Sample Value* (SV), em nível de processo, realiza a comunicação de medidas de corrente e tensão a partir das *merging units* (MU). O protocolo *Generic Object Oriented Substation Event* (GOOSE), no nível de vão, é utilizado na comunicação entre os IEDs para execução de funções de controle e proteção. Por fim, o protocolo *Manufacturing Message Specification* (MMS) é utilizado na comunicação entre sistemas supervisórios (SCADA) e estações de engenharia e os IEDs no nível de estação. Essa dinâmica está ilustrada pela Figura 1(a).



(a) Arquitetura de uma subestação digital, baseado em [Quincozes et al. 2021].

(b) Quadro do pacote GOOSE, baseado em [IEC61850 2011].

Figura 1. Comunicação no padrão IEC 61850.

Algumas das vulnerabilidades dos protocolos GOOSE e SV se dão pelo fato de que estes são definidos apenas até a camada de enlace e trafegam sem criptografia, devido aos requisitos de baixa latência para resposta aos fenômenos elétricos. A Figura 1(b) mostra o quadro Ethernet GOOSE, sendo importante ressaltar o papel do campo *stnum*, que indica a sequência dos eventos de proteção, e o campo *sqnum*, que indica a sequência de pacotes desde o último evento. Em sua revisão bibliográfica, [Quincozes et al. 2021] expõe os ataques que exploram as vulnerabilidades do protocolo GOOSE: ataques de retransmissão, de injeção de mensagens, de mascaramento e de envenenamento.

O ataque de retransmissão consiste no reenvio de mensagens GOOSE na rede [Hong et al. 2014]. O ataque de injeção de mensagem é realizado através de injeção de

[1]https://www.rtds.com/

pacotes GOOSE com parâmetros modificados [Hoyos et al. 2012]. Já o ataque de mascaramento é semelhante ao ataque de injeção de mensagem, porém mais complexo. Neste ataque, os parâmetros de sequenciamento da mensagem GOOSE maliciosa são definidos de forma que guardem relação com as mensagens originais em tempo real, isso com o objetivo de dissimular o comportamento legítimo dos pacotes falsos [Ustun et al. 2019]. Os ataques até então mencionados tomam proveito da falta de garantia de autenticidade e integridade do protocolo GOOSE. Nesse sentido, implementações de assinatura digital e de *hash* para endereçar essas vulnerabilidades se mostraram como caminhos para detecção desses ataques, necessitando-se da avaliação das latências acrescentadas frente aos requisitos da norma 61850 da IEC [Ustun et al. 2019]. Por fim, o ataque de envenenamento tem como objetivo a degradação da comunicação dos IEDs e pode ser realizado através da inundação de pacotes GOOSE causando a negação de serviço [Kush et al. 2014].

3. Simulação de Comunicação em uma Subestação Elétrica

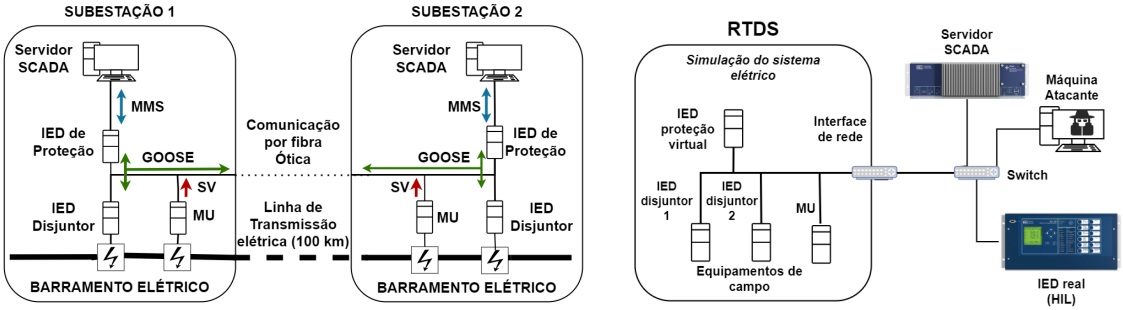
O estudo de comunicações em sistemas elétricos possui, como uma adversidade, a dificuldade de se obter dados reais. O uso da infraestrutura real para testes acadêmicos pode afetar o fornecimento regular dos serviços desses sistemas. Um esforço para transpor esse problema foi a criação de um gerador de *datasets* de tráfego de pacotes GOOSE e SV por [Quincozes et al. 2022], com o objetivo de auxiliar na pesquisa na área de detecção de intrusão em subestações elétricas. Outra forma de endereçar esse problema é o uso de simulações com ferramentas como o PSCAD[2] ou o RTDS, sendo esta última utilizada neste trabalho. O RTDS é um computador de alto desempenho com capacidade de simular diversos tipos de sistemas elétricos, além de poder ser empregado em conjunto com IEDs reais em *hardware-in-the-loop*, ou seja, o computador da simulação troca informações e sinais em tempo-real com o equipamento. Essa característica do RTDS aprimora o grau de realismo das simulações, permitindo a análise dos impactos de ataques cibernéticos no sistema modelado e no funcionamento de equipamentos reais. Por exemplo, a inundação de pacotes no ataque de negação de serviço afeta o tráfego de rede, podendo influenciar no tempo e na priorização de envio de mensagens na rede pelos IEDs e *switches*, cujo impacto pode ser analisado pelos dados de tráfego advindos da simulação em HIL.

Na literatura, pode-se verificar a utilização do RTDS ou ferramentas semelhantes no estudo de segurança cibernética. [Rajkumar et al. 2020] utilizou o RTDS em HIL com IEDs reais na análise do impacto de um ataque cibernético de injeção de mensagem em um sistema elétrico com corte de carga e geração de energia. No seu experimento, foram utilizados a biblioteca Scapy, em linguagem *python*, para a realização dos ataques. [Rajkumar et al. 2020] mostrou que ataques de injeção de mensagem podem causar falhas cascateadas em um sistema elétrico de potência e gerar um *blackout*. Especificamente em sistemas de proteção de linhas de transmissão, [Jahromi et al. 2020] utilizou a OPAL-RT, ferramenta semelhante ao RTDS, em conjunto com o simulador de rede Riverbed Modeler que permitem a simulação da comunicação GOOSE em tempo real. Foram utilizados o programa *wireshark*[3] para monitoramento dos pacotes falsos e o simulador Riverbed Modeler para a realização dos ataques. [Jahromi et al. 2020] verificou que o ataque de negação de serviço e o ataque de injeção de mensagem falsa prejudicaram a comunicação de diferentes esquemas de proteção de linhas de transmissão.

[2]https://www.pscad.com/

[3]https://www.wireshark.org/

Este artigo buscou englobar os ataques de retransmissão, mascaramento e de negação de serviço em um sistema de proteção de linha de transmissão modelado no RTDS, sendo o ataque de negação de serviço realizado com a inundação de pacotes GOOSE. O sistema modelado foi o de proteção de distância de linhas de transmissão, onde IEDs em subestações no começo e no final da linha comunicam entre si e com os IEDs disjuntores para executar funções de proteção e controle, como visto na Figura 2(a). Foram utilizados na simulação o RTDS, um IED SEL-421, o SEL RTAC 3555, como sistema supervisório (SCADA), e uma máquina convencional para a realização dos ataques, processador Intel I7-8550U 1.8 GHz e memória RAM 12 GB DDR4. A configuração da simulação pode ser verificada na Figura 2(b). A implementação dos ataques em protocolo GOOSE, cujos códigos encontram-se publicamente disponíveis[4], foi realizada com o auxílio da biblioteca *libiec61850*[5], em linguagem C, visando o aumento da eficiência do ataque e consequentemente o grau de similaridade com a situação real.



(a) Representação simplificada de um sistema real de proteção de linha de transmissão.

(b) Configuração da simulação realizada em laboratório.

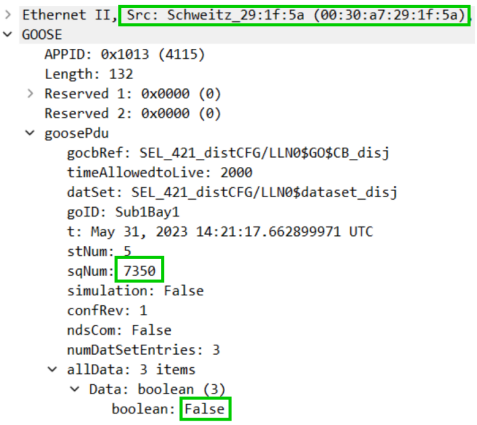
Figura 2. Simulação do sistema elétrico.

4. Resultados

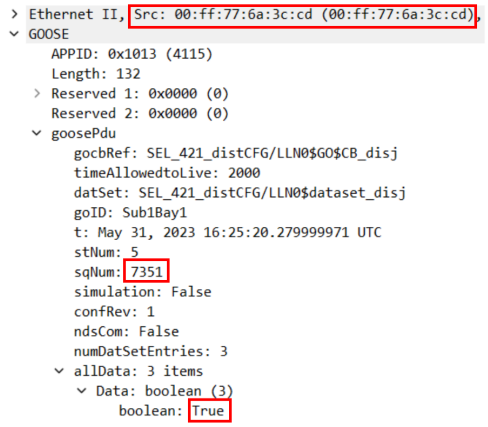
O ataque de retransmissão, considerado o mais simples, foi realizado ao reenviar pacotes de comando de *trip*, que realiza a abertura do IED disjuntor simulado no RTDS. O IED virtual recebeu as mensagens geradas, realizando novamente o comando de abertura de disjuntor. No ataque de mascaramento, o pacote original do IED real possuía o valor de *stnum* de 5 e *sqnum* 7350 e o valor de *false* no campo de dado para o comando de *trip*. O pacote falso e injetado na rede teve o seu valor de *sqnum* incrementado para 7351 e o valor do comando de *trip* modificado para *true*, o que ocasionou a abertura do disjuntor e consequente interrupção na transmissão de energia na linha de transmissão simulada. As capturas de tela relativas ao ataque de mascaramento estão apresentadas na Figura 3, podendo ser verificado a diferença do endereço MAC da fonte do pacote.

O ataque de negação de serviço foi realizado pela injeção consecutiva de 500.000 (quinhentos mil) pacotes GOOSE na rede pela máquina atacante com o objetivo de obstruir a comunicação GOOSE dos IEDs legítimos na rede, o que pode ser visualizado na captura de tela do programa *wireshark* na Figura 4(a). Além disso, pode-se verificar na Figura 4(b) que o tráfego médio antes do ataque de negação de serviço era de 5 pacotes

[4]https://github.com/comp-ime-eb-br/seg-ciber-sistemas-eletricos
[5]https://libiec61850.com/



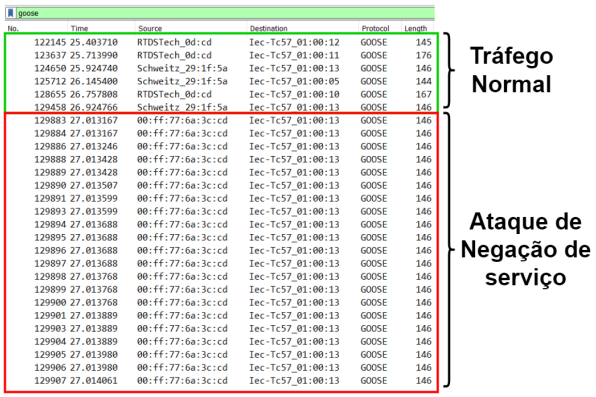
(a) Pacote GOOSE original do IED real.



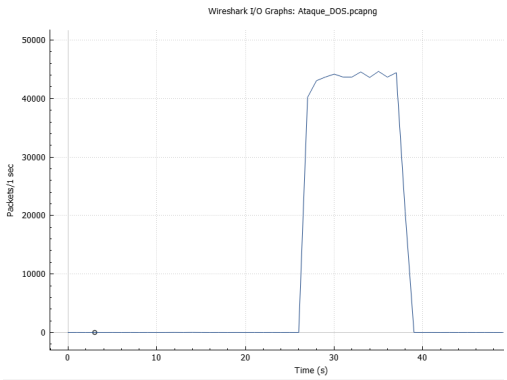
(b) Pacote GOOSE falso no ataque de mascaramento.

Figura 3. Ataque de mascaramento.

por segundo, alcançando a taxa cerca de 44.000 pacotes por segundo durante o ataque. A negação de serviço foi observada através do fato de que, durante a inundação dos pacotes GOOSE, a transmissão do comando de fechamento do disjuntor pelo IED SEL-421, a partir do acionamento manual do botão ou comando do servidor SCADA, ficou prejudicada. O não fechamento do disjuntor representa o impedimento do retorno à normalidade do sistema elétrico, evitando-se assim a transmissão de energia elétrica pela linha no caso de um desligamento causado por um ataque bem sucedido.



(a) Captura de tela no wireshark no início do ataque de negação de serviço.



(b) Quantidade de pacotes GOOSE por segundo durante o ataque de negação de serviço.

Figura 4. Ataque de negação de serviço.

5. Conclusão

A segurança cibernética de sistemas elétricos se tornou mais relevante devido à digitalização dessas infraestruturas. De forma a contribuir nessa área de pesquisa, este artigo apresentou a simulação de um sistema de proteção de linha de transmissão elétrica no RTDS em conjunto com um IED real utilizando a técnica *hardware-in-the-loop* para a análise de ataques cibernéticos na comunicação em protocolo GOOSE. Os ataques de retransmissão, mascaramento e de negação de serviço foram realizados na rede de

comunicação entre os IEDs, sendo descrito os seu impactos. Os dados de tráfego de rede dos experimentos serão utilizados em trabalhos futuros na detecção de intrusão na rede dos sistemas elétricos utilizando-se aprendizado de máquina no processo de detecção.

Registro que este trabalho foi possível graças ao Acordo de Parceria para Pesquisa, Desenvolvimento e Inovação, firmado entre o Exército Brasileiro, a ITAIPU Binacional e a Fundação Parque Tecnológico Itaipu-Brasil, que vem desenvolvendo em conjunto o Projeto Centro de Estudos Avançados em Proteção de Estruturas Estratégicas (Ceape²), que encerra a cooperação técnica, científica e financeira nas áreas de Segurança de Infraestruturas Críticas (IEC), Segurança da Informação e Cibernética e Sistemas Elétricos de potência.

Referências

Hong, J., Liu, C.-C., and Govindarasu, M. (2014). Detection of cyber intrusions using network-based multicast messages for substation automation. In *ISGT 2014*, pages 1–5.

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

IEC61850 (2011). *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*. International Electrotechnical Commission: Geneva, Switzerland.

Jahromi, A. A., Kemmeugne, A., Kundur, D., and Haddadi, A. (2020). Cyber-physical attacks targeting communication-assisted protection schemes. *IEEE Transactions on Power Systems*, 35(1):440–450.

Kush, N., Ahmed, E., Branagan, M., and Foo, E. (2014). Poisoned goose: Exploiting the goose protocol. In *Proceedings of the Twelfth Australasian Information Security Conference - Volume 149*, AISC '14, page 17–22.

M. Lee, R., J. Assante, M., and Conway, T. (2016). Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388:1–29.

Quincozes, S., Albuquerque, C., Passos, D., and Mossé, D. (2022). Ereno: An extensible tool for generating realistic iec-61850 intrusion detection datasets. In *Anais Estendidos do XXII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 1–8, Porto Alegre, RS, Brasil. SBC.

Quincozes, S. E., Albuquerque, C., Passos, D., and Mossé, D. (2021). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, 184:107679.

Rajkumar, V. S., Tealane, M., Ştefanov, A., and Palensky, P. (2020). Cyber attacks on protective relays in digital substations and impact analysis. In *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, pages 1–6.

Ustun, T. S., Farooq, S. M., and Hussain, S. M. S. (2019). A novel approach for mitigation of replay and masquerade attacks in smartgrids using iec 61850 standard. *IEEE Access*, 7:156044–156053.