UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Jerusa Carneiro Gonçalves

# Modelagem do Ataque Grayhole ao Protocolo de Comunicação GOOSE usando o Framework ERENO

**Uberlândia, Brasil**

**2023**

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Jerusa Carneiro Gonçalves

# Modelagem do Ataque Grayhole ao Protocolo de Comunicação GOOSE usando o Framework ERENO

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Silvio Ereno Quincozes

Coorientador: Prof. Dr. Juliano Fontoura Kazienko

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Sistemas de Informação

Uberlândia, Brasil

2023

# Resumo

A crescente necessidade de reforçar a segurança cibernética na infraestrutura crítica, especificamente em subestações elétricas que se comunicam através do protocolo Generic Object Oriented Substation Event (GOOSE), requer técnicas efetivas de detecção e prevenção de ameaças. Esse protocolo é definido pelo padrão IEC-61850 e protege dispositivos físicos notificando eventos como faltas elétricas. Entretanto, a sua adoção abre brechas para a exploração de vulnerabilidades através de ataques cujas assinaturas precisam ser mapeadas. Destaca-se uma lacuna na literatura referente à falta de assinaturas do ataque *Grayhole*. Neste artigo, é proposta a modelagem e implementação de tal ataque ao protocolo GOOSE. Ademais, tal modelagem é incorporada ao ERENO, um framework para geração de datasets de intrusões. A eficácia do dataset resultante é validada através de cinco algoritmos de aprendizado de máquina, com destaque para o algoritmo J48 que obteve 90,68% de F1-Score.

**Palavras-chave**: Subestações Elétricas Digitais, GOOSE, IEC-61850, Grayhole, ERENO.

# Abstract

The growing need to enhance cybersecurity in critical infrastructure, specifically in electric substations that communicate via the Generic Object Oriented Substation Event (GOOSE) protocol, calls for effective threat detection and prevention techniques. This protocol, defined by the IEC-61850 standard, protects physical devices by notifying events such as electrical faults. However, its adoption opens gaps for the exploitation of vulnerabilities through attacks whose signatures need to be mapped. In particular, the literature lacks *Grayhole* attack signatures. This work proposes the modeling and implementation of such attack targeted to the GOOSE protocol. Furthermore, such modeling is incorporated into ERENO, a framework for generating intrusion datasets. The effectiveness of the resulting dataset is validated through five machine learning algorithms, with the J48 algorithm standing out, achieving a 90.68% F1-Score.

# Lista de abreviaturas e siglas

| | |
|---|---|
| DoS | Negação de Serviço, do inglês, Denial of Service |
| ERENO | Efficacious Reproduces Engine for Network Operations |
| GOOSE | Eventos de Subestação de Objetos Orientados Genéricos, do inglês, Generic Oriented Object Substation Events |
| IED | Dispositivos Eletrônicos Inteligentes, do inglês, Intelligent Electronic Device |
| IDS | Sistema de Detecção e Intrusão, do inglês, Intelligent Electronic System |
| MMS | Especificação De Mensagem De Fabricação, do inglês, Manufacturing Message Specification |
| SV | Sistema de Valores Amostrados, do inglês, Sampled Values |
| SCL | Linguagem de Configuração da Subestação, do inglês, Substation Configuration Language |
| SCD | Descrição de Configuração de Subestação, do inglês, Substation Configuration Description |
| SDN | Rede Definida por Software, do inglês, Software Defined Network |
| GNU | Licença Pública Geral, do inglês, General Public License |
| KNN | K-vizinhos mais próximos, do inglês, K-Nearest Neighbors |

# Sumário

# 1 Introdução

No contexto das subestações elétricas digitais e dos Dispositivos Eletrônicos Inteligentes (*Intelligent Electronic Devices* - IEDs), a comunicação efetiva e segura tornou-se cada vez mais crítica. A utilização de protocolos de comunicação, que determinam o tipo de mensagem e sua estrutura, tornou-se fundamental. Dentre os diversos protocolos existentes, o protocolo *Generic Object Oriented Substation Event* (GOOSE), definido pelo padrão IEC-61850, emergiu como um dos mais proeminentes para a comunicação entre IEDs (QUINCOZES, 2022) (WANG et al., 2022).

O protocolo GOOSE é amplamente utilizado no setor de subestações elétricas digitais, funcionando como um meio para notificar a ocorrência de eventos entre dispositivos de uma mesma subestação, ou entre diferentes subestações. Um exemplo de aplicação deste protocolo consiste nas funções de proteção de dispositivos físicos através da notificação de eventos de faltas elétricas que exigem a atuação dos sistemas de proteção para abrir disjuntores de energia e isolar trechos de linhas de transmissão (USTUN; FAROOQ; HUSSAIN, 2019). Essas notificações são realizadas por meio das mensagens GOOSE, que são transmitidas entre os IEDs e usadas para enviar o *status* dos equipamentos da subestação, comandos ou qualquer outro sinal digital. Essas mensagens, do tipo *multicast*, permitem o envio simultâneo para múltiplos dispositivos. Ademais, este protocolo possui a característica de retransmissão de mensagens para evitar a perda de dados em aplicações críticas (KUSH et al., 2014).

Ao passo que a norma IEC-61850 propõe protocolos que facilitam a comunicação entre IEDs, a adoção dos mesmos possibilita a exploração de novas vulnerabilidades nas subestações elétricas digitais. Segundo Rajkumar et al. (2020), o padrão IEC-61850 apresenta diversas vulnerabilidades de segurança cibernética. Muitos desses problemas se devem aos requisitos rígidos de tempo das aplicações onde tal padrão é comumente adotado. O protocolo GOOSE, por exemplo, não implementa nenhum mecanismo de criptografia devido aos requisitos de tempo

real impostos pelo sistema de proteção para comunicar o disparo de sinais. Além disso, as falhas e vulnerabilidades de segurança cibernética estão crescendo cada vez mais. Relatórios recentes (MCLENNAN; GROUP; GROUP, 2022) reafirmam as pesquisas feitas no setor de que o número de ataques cibernéticos vem aumentando a cada ano. Consequentemente, os ataques cibernéticos às subestações podem causar diversos cenários desastrosos, como apagões ou dano à equipamentos, por exemplo. Assim, é fundamental fortalecer a segurança cibernética da subestação para aumentar a resiliência da rede (HONG; LIU, 2019).

Em contraste com os sistemas de informações tradicionais, onde as propriedades de *Confidencialidade* e *Integridade* são consideradas prioritárias, nos sistemas industriais de infraestrutura crítica, a *Disponibilidade* é fundamental (HAHN; SUN; LIU, 2016). Nesse contexto, uma das principais ameaças consistem nos ataques de negação de serviço, do inglês, *Denial of Service* (DoS). Dentre os ataques desta categoria, destaca-se o ataque de descarte seletivo de mensagens, conhecido como *Grayhole* (PAL; SIKDAR; CHOW, 2018). Portanto, o uso de Sistemas de Detecção de Intrusões, do inglês, *Intrusion Detection Systems* (IDSs) se torna fundamental para a proteção das redes onde são transmitidas mensagens baseadas nesse padrão. No entanto, a obtenção de dados realistas e representativos para o treinamento de IDSs é um desafio (QUINCOZES, 2022).

Em direção a solução desse desafio, a ferramenta *Efficacious Reproduces Engine for Network Operations* (ERENO) (QUINCOZES, 2022) foi concebida. Ela possibilita a modelagem e simulação de ataques cibernéticos em redes de subestações elétricas. Trabalhos existentes baseados na ferramenta ERENO modelam ataques de retransmissão, injeção de mensagens, DoS e mascaramento (QUINCOZES, 2022). Contudo, existem diversas categorias de ataques que ainda não foram exploradas e, consequentemente, não existem dados disponíveis publicamente para o treinamento de IDSs.

## 1.1 Motivação

Segundo Rajkumar et al. (2020), o padrão IEC-61850 apresenta diversas vulnerabilidades de segurança cibernética. Um exemplo disso é o protocolo GO-

OSE, que não possui implementações ao sistema de proteção. Isso desperta preocupação pela possibilidade de que potenciais atacantes cibernéticos possam aproveitar dessas lacunas na segurança com objetivos muitas vezes maliciosos e ferir a propriedade de "Disponibilidade" que é considerada fundamental para os sistemas industriais (HAHN; SUN; LIU, 2016).

Além disso, as falhas e vulnerabilidades de segurança cibernética estão crescendo cada vez mais. Relatórios como o publicado pelo Fórum Econômico Mundial McLennan, Group e Group (2022) reafirmam as pesquisas feitas no setor de que o número de ataques cibernéticos vem aumentando a cada ano.

## 1.2 Justificativa

Enquanto a norma IEC-61850 propõe protocolos que facilitam a comunicação entre IEDs, a implementação desses protocolos abrem novas oportunidades para a exploração de vulnerabilidades em subestações elétricas digitais. Nesse cenário, a utilização de IDSs se torna crucial para garantir a segurança das redes que utilizam esse padrão de comunicação. No entanto, a obtenção de dados realistas e representativos para o treinamento dos IDSs tem sido um desafio frequente abordado na literatura. (QUINCOZES et al., 2021).

Os riscos da segurança da informação nas redes de controle de energia de acordo com a norma IEC-61850 estão sendo consideradas atualmente, principalmente pelo fato da troca das mensagens GOOSE não contemplarem confidencialidade, o que possibilita o acesso de informações por invadores através de *sniffers* de rede (ELGARGOURI; ELMUSRATI, 2017). Consequentemente, os ataques cibernéticos às subestações podem causar diversos cenários desastrosos, como apagões ou dano à equipamentos, por exemplo. Assim, é fundamental fortalecer a segurança cibernética da subestação para aumentar a resiliência da rede (HONG; LIU, 2019)

A ferramenta *Efficacious Reproduces Engine for Network Operations*, conhecida como ERENO (QUINCOZES, 2022) foi concebida para possibilitar a modelagem e simulação de ataques cibernéticos em redes de subestações elétricas. Trabalhos existentes baseados na ferramenta ERENO modelam ataques de re-

transmissão, injeção de mensagens, DoS e mascaramento (QUINCOZES, 2022). Contudo, existem diversas categorias de ataques que ainda não foram exploradas e modelados em ferramentas como o ERENO. Consequentemente, há uma escassez de dados disponíveis para o treinamento de IDSs. Um dos ataques significativos que não foi modelado é o *Grayhole*, que é um ataque relavante devido à sua capacidade de comprometer a disponibilidade, sendo uma propriedade fundamental nos sistemas industriais que operam em tempo real (PAL; SIKDAR; CHOW, 2018). Até onde o conhecimento se estende, não encontramos qualquer trabalho na literatura sobre o assunto que realize a modelagem, implementação e avaliação de tal ataque no âmbito do protocolo GOOSE.

## 1.3 Objetivo

### 1.3.1 Objetivo Geral

Este trabalho tem como objetivo principal preencher uma importante lacuna na literatura atual que coniste na ausência de assinaturas de ataques do tipo *Grayhole* direcionados ao protocolo GOOSE. Com isso, pretende-se efetuar a modelagem de tal ataque e implementá-la no *framework* ERENO (QUINCOZES, 2022). Assim, gerar assinaturas para o treinamento e avaliação da performance de IDSs baseados em algoritmos de aprendizado de máquina.

### 1.3.2 Objetivos Específicos

- Revisar a literatura sobre ataques ao protocolo GOOSE em subestações elétricas digitais;
- Estudar sobre ataques DoS em protocolos tradicionais;
- Modelagem e implementação do ataque do tipo *Grayhole* ao protocolo GOOSE, preenchendo uma lacuna existente na literatura;
- Incorporação da modelagem proposta ao framework ERENO (QUINCOZES, 2022), aumentando sua aplicabilidade e eficiência;

- Validação da eficácia do *dataset* resultante por meio de algoritmos de aprendizado de máquina, a saber: *J48*, *K-Nearest Neighbors*, *REPTree* e *Random Forest*.

## 1.4 Organização

O restante desta monografia está organizado como segue. No Capítulo 2, nós aprensatamos a fundamentação teórica da norma IEC-61850 e o funcionamneto do protocolo GOOSE. No Capítulo 3, nós apresentamos a nova modelagem de ataque ao protocolo GOOSE *Grayhole*, além de apresentar os matériais e metódos que serão utilizados no desenvolvimento do ataque proposto. No Capítulo 4, nós apresentamos os resultados obtidos na detecção de ataques tipo *Grayhole*. No Capítulo 5, nós apresentamos os desafios futuros sobre ataques que ainda não foram catalogados. No capítulo 6, nós apressentamos nossa conclusão e contribuições adicionando mais um ataque implementado.

# 2 Referencial Teórico

Nesse capítulo iremos introduzir alguns temas, como o protocolo GOOSE, que viabiliza a comunicação entre os IEDs. Além disso, a ferramenta ERENO, que permite a modelagem e simulação de ataques cibernéticos em redes industriais.

## 2.1 Conceitos Fundamentais

Para o desenvolvimento deste trabalho, é essencial entender alguns tópicos tais como o funcionamento do protocolo GOOSE que possibilita a troca de mensagens entre os IEDs, a ferramenta ERENO que possibilitar a modelagem e simulação de ataques cibernéticos em redes de subestações elétricas.

### 2.1.1 Protocolo GOOSE

A norma IEC-61850 Commission (2003) possui os seguintes objetivos: 1) interoperabilidade; 2) estabilidade a longo termo; 3) configuração simplificada através do *Substation Configuration Language* (SCL) e comandos remotos. Além disso, a norma fornece um abrangente modelo de dados que garante a compatibilidade entre diversos fabricantes de IEDS (MACKIEWICZ, 2006). Além do formato dos dados e aspectos de interoperabilidade, o padrão IEC-61850 detalha as possíveis topologias físicas (*e.g.,* topologia de rede em anel, redundância, *Local Area Networks* - LANs), protocolos de rede (*Sampled Values* - SV, *Manufacturing Message Specification* - MMS e GOOSE) e modelagem de objetos (COMMISSION, 2003; O'RAW; LAVERTY; MORROW, 2017).

É importante destacar que a norma IEC-61850 define outros protocolos, porém, nesse trabalho, focaremos no protocolo GOOSE, pois é um dos mais propensos a ataques. Para adquirir uma descrição mais detalhada sobre a norma, consulte (AFTAB et al., 2020).

O protocolo GOOSE permite a troca de mensagens entre os IEDs para relatar eventos nas subestações, como mudanças de *status*, alarmes e comandos

de controle. Diversos componentes enviam esses eventos por meio de mensagens GOOSE, que englobam alarmes de temperatura, estado do disjuntor, intertravamento da chave seccionadora, entre outros. Esses dados são adicionados em um campo denominado GOOSE *datSet* e posteriormente transmitidos, utilizando o conceito de publicação/assinatura, para um grupo de IEDs assinantes. Cada IED pode se inscrever em um tópico específico relacionado ao seu domínio, como controle, proteção ou medição, por exemplo. Na Figura 1 é apresentada a estrutura de um quadro *ethernet* GOOSE. Dentro do campo *datSet* podem conter valores booleanos que indicam, por exemplo, se um disjuntor deve ser aberto para isolar uma linha de transmissão durante uma falta elétrica ou fechado para reestabelecer e transmissão de energia, conforme ilustrado pelos valores "Fechar" e "Abrir" nas mensagens enviadas na Figura 2.

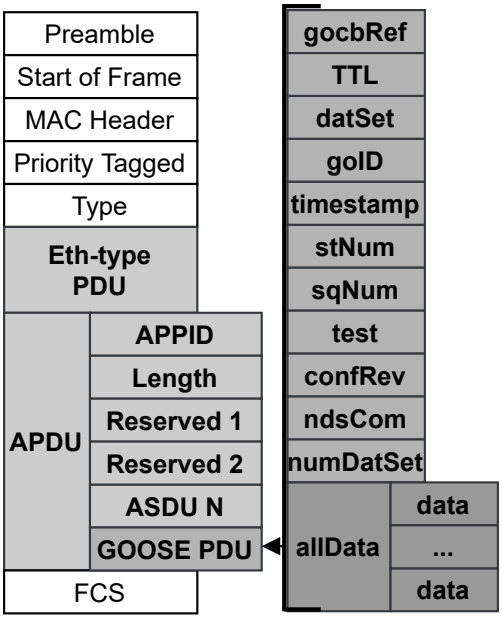



Figura 1 – Estrutura de um quadro *ethernet* GOOSE. Fonte: Quincozes (2022)

Quando as situações estão estáveis, não ocorrem novos eventos, portanto, não são detectadas alterações nos valores do conjunto de dados GOOSE. As mensagens GOOSE são enviadas em intervalos regulares de tempo, representados por $T_0$, e o número de sequência, *SqNum*, é incrementado. No início de um evento, o campo *SqNum* é definido como zero, o número de *status*, *StNum*, é incrementado e uma nova mensagem é enviada imediatamente. A mensagem é retransmitida em

intervalos crescentes, começando com o menor intervalo de retransmissão, ($T_1$), que é utilizado como separador para as três primeiras mensagens e repetido duas vezes, e a cada retransmissão o intervalo é sucessivamente aumentado ($T_2$, $T_3$, etc.), até alcançar o intervalo estável original, ($T_0$).

A Figura 2 ilustra esse processo, onde os parâmetros *StNum* e *SqNum* foram abreviados para `St.` e `Seq.`, respectivamente. Em cenários reais de subestações, o intervalo $T_1$ representa o parâmetro *minTime* definido no arquivo SCD, enquanto o intervalo $T_0$ é definido pelo parâmetro *maxTime* (COMMISSION, 2003). Embora os valores exatos dos incrementos não sejam definidos pela norma, os IEDs tipicamente implementam cálculos tais como o da Progressão Aritmética (PA) ou Progressão Geométrica (PG) para defini-los (HOYOS; DEHUS; BROWN, 2012).

Dadas essas características típicas, um IDS pode analisar várias propriedades para distinguir entre atividades legítimas e maliciosas. O registro de tempo do GOOSE pode revelar mensagens atrasadas que podem ser indicativas de um ataque DoS, pois em circunstâncias normais, o intervalo de tempo entre duas mensagens recebidas não deve exceder $T_0$. O *SqNum* e o *StNum* são elementos importantes, pois podem indicar a possibilidade de injeção de mensagens falsas ou ataques de repetição de mensagens, caso esses campos sejam alterados (HOYOS; DEHUS; BROWN, 2012; HONG; LIU; GOVINDARASU, 2014; USTUN; FAROOQ; HUSSAIN, 2019; QUINCOZES, 2022). Da mesma forma, os valores do *datSet* podem ser correlacionados com o *StNum* para identificar alterações indesejadas.

### 2.1.2 Framework ERENO

O *framework* ERENO, publicado em Quincozes (2022), é um framework de código aberto para gerar conjuntos de dados IEC-61850 com *features* (atributos) representativas para detectar diferentes tipos de intrusões. Ele é capaz de gerar *features* representativos para serem processados por algoritmos de aprendizado de máquina, combinando extração e seleção de *features*. Além disso, ERENO apresenta uma nova taxonomia dos aspectos de IDSs baseados em IEC-61850. Em resumo, ERENO é uma ferramenta que permite a geração de conjuntos de dados realistas para testar e avaliar a eficácia de sistemas de detecção de intrusão em subestações elétricas. A ferramenta ERENO possui modelos de ataques que foram

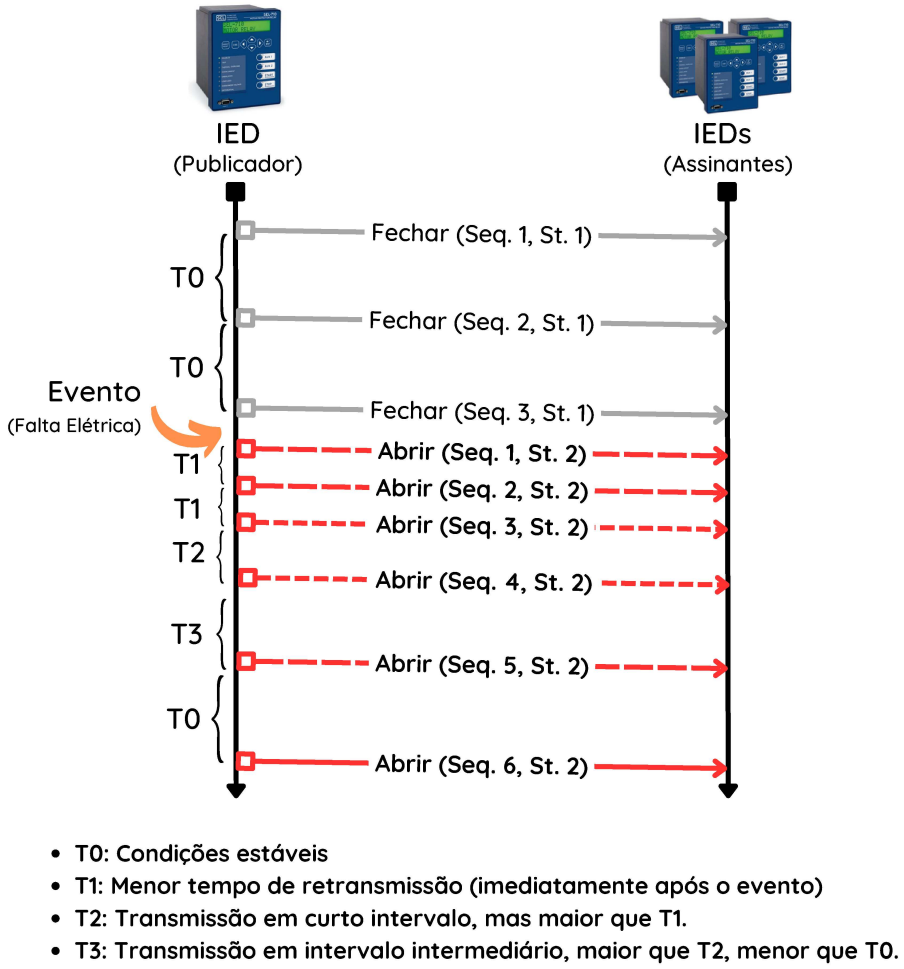



Figura 2 – Intervalos de transmissão de mensagens GOOSE.

propostos originalmente na tese de doutorado (QUINCOZES, 2022) que introduz a própria ferramenta. Tais ataques são listados na Seção 2.2, pois representam estudos relacionados ao presente trabalho.

Um dos aspectos relevantes acerca do ERENO para este trabalho consiste nas *features* que são geradas e introduzidas no *dataset* resultante da modelagem de seus ataques. Ao passo que o ERENO permite a geração de dados correspondentes aos protocolos GOOSE e SV, neste trabalho concentraremos apenas nas *features* do protocolo GOOSE, uma vez que o contexto do ataque estudado refere-se a tal protocolo. O ERENO propõe um conjunto de 28 *features* para o protocolo GOOSE, que são divididas em três categorias: (i) *features* de tempo, (ii) *features*

de conteúdo e (iii) *features* de tráfego, conforme segue:

- As *features* de tempo incluem informações sobre o intervalo de tempo entre as mensagens GOOSE, a duração da mensagem GOOSE e a hora do dia em que a mensagem foi enviada.
- As features de conteúdo incluem informações sobre o tipo de mensagem GOOSE, o número de sequência da mensagem, o tamanho da mensagem e o valor dos campos da mensagem.
- As *features* de tráfego incluem informações sobre o número de mensagens GOOSE enviadas, o número de mensagens GOOSE recebidas, o número de mensagens GOOSE enviadas por segundo e o número de mensagens GOOSE recebidas por segundo.

Essas *features* foram selecionadas com base em uma revisão da literatura e em experimentos preliminares para avaliar sua relevância para a detecção de intrusões em subestações elétricas.

## 2.2 Trabalhos Relacionados

Atualmente, na literatura existem alguns ataques que já foram modelados através de ferramentas de geração de *datasets*, como, por exemplo, pelo *framework* ERENO (QUINCOZES, 2022). Nesta seção serão discutidos os ataques ao protocolo GOOSE que já foram modelados e catalogados através de *datasets* publicamente disponíveis.

Em Hoyos, Dehus e Brown (2012), o protocolo GOOSE é explorado e potenciais ataques são modelados. Dentre as ameaças analisadas, a fabricação de mensagens GOOSE, ou *Message Injection*, é estudada. Ao executar um ataque de de *Message Injection*, o atacante cria e envia mensagens maliciosas, tais como a injeção de comandos pela rede. Nesse modelo, os invasores podem fazer alterações aleatórias (*i.e.,* ignorar sua conformidade com a norma IEC-61850) ou alterações com reconhecimento de padrões (*i.e.,* cumprir com a norma IEC-61850).

O trabalho de Hong, Liu e Govindarasu (2014) propõe o estudo de um IDS baseado em alguns ataques, incluindo ataques de retransmissão de mensagens, do inglês, *Replay Attacks*. Esse tipo de ataque consiste na captura e retransmissão de mensagens após algum período de tempo escolhido pelo atacante. Uma das principais características desse ataque consiste em não modificar o conteúdo original da mensagem. No entanto, esse ataque tem como principal limitação a sua facilidade de detecção, visto que o *SqNum* será idêntico ao de uma mensagem previamente transmitida na rede.

No estudo de Abdul et al. (2014), diversos ataques são explorados no contexto de subestações elétricas. No contexto do protocolo GOOSE, os autores discutem os *Replay Attacks* e a possibilidade de *malwares* automatizados executarem modificações nas mensagens antes de retransmiti-las na rede, constituindo assim o *Modification Attack*. Todavia, a simples modificação de uma mensagem evita apenas a repetição de mensagens previamente enviadas, não sendo essa uma abordagem suficientemente eficaz para enganar os mecanismos de descartes dos IEDs baseados nos valores dos campos *StNum* e *SqNum* das mensagens GOOSE.

Em Kush et al. (2014), os autores estudam abordagens de ataques de envenenamento GOOSE, os quais têm por finalidade invalidar mensagens legítimas transmitidas após a execução do ataque (causando negação de serviço). Para tanto, os autores exploram vulnerabilidades no mecanismo de descarte de mensagens antigas do IEDs, que se baseiam nos valores de *StNum* e *SqNum*. Uma das variantes estudadas consiste no *High-Status Number Attack*, onde as mensagens GOOSE são interceptadas de modo que o atacante descubra o atual número do *StNum*. Em seguida, o atacante envia mensagens maliciosas com um *StNum* modificado, sendo este maior que o *StNum* atual. O efeito esperado no equipamento do assinante é que mensagens GOOSE legítimas sejam descartadas devido ao seu *StNum* aparentemente desatualizado. Outra variante é o *High-Rate Flooding Attack*, na qual o invasor inunda o canal multicast enviando várias mensagens GOOSE falsas em um curto intervalo (entre duas mensagens legítimas). Desse modo, cada mensagem falsa incrementa o valor de *StNum* em uma unidade e a próxima mensagem legítima é descartada pelo IED que a recebe. Em ambas as variações, as mensagens descartadas podem gerar alertas se um IDS estiver monitorando o descarte

de mensagens. Em geral, ataques de envenenamento visam impedir o processamento das mensagens legítimas mas, são detectáveis por mecanismos existentes na literatura (BOHARA et al., 2020).

Em Ustun, Farooq e Hussain (2019) é proposto o ataque *Masquerade*. Esse ataque consiste em uma especialização dos ataques de injeção que aumenta significativamente a dificuldade de detecção por parte de um IDS, pois o mesmo exige que os invasores aprendam com o conteúdo das mensagens GOOSE anteriores e imitem o comportamento legítimo ao enviar novas mensagens falsas. Isso envolve a modificação inteligente (não aleatória) de campos de mensagem como *StNum* e *SqNum* e a injeção de eventos de mudança de estado maliciosos falsos para causar a mesma mudança de comportamento de uma mensagem legítima. Uma característica importante dos ataques *Masquerade* consiste na reprodução do mecanismo de retransmissão usado pelos IEDs legítimos (vide Figura 2).

Todos os ataques supracitados já foram implementados (vide Figura 3) através do *framework* ERENO e avaliados em Quincozes (2022). No entanto, ainda não existem implementações de ataques considerando as particularidades e desafios específicos do protocolo GOOSE. Portanto, iremos explorar um novo ataque, ainda não catalogado, a fim de preencher essa lacuna de conhecimento e identificar possíveis vulnerabilidades que possam afetar a segurança e a confiabilidade das comunicações.

| Ataques | Descrição | Propriedades de Segurança Prejudicadas | Referências |
|---|---|---|---|
| Message Injection | Cria e envia mensagens maliciosas. | Integridade | Hoyos, Dehus e Brown (2012) |
| Replay Attacks | Captura e retransmissão de mensagens. | Freshness | Hong, Liu e Govindarasu (2014) |
| Modification Attack | Modifica as mensagens antes de retransmiti-las. | Integridade | Abdul et al. (2014) |
| High-Status Number Attack | Envia mensagens maliciosas com um StNum modificado. | Integridade e Disponibilidade | Kush et al. (2014) |
| High-Rate Flooding Attack | Inunda o canal multicast enviando várias mensagens falsas. | Integridade e Disponibilidade | Kush et al. (2014) |
| Masquerade | Envia novas mensagens falsas imitando o comportamento legítimo. | Integridade | Ustun, Farooq e Hussain (2019) |

Figura 3 – Ataques que já foram modelados.

# 3 Desenvolvimento

Neste Capítulo serão abordadas as etapas de modelagem e implementação do ataque *Grayhole* no *framework* ERENO. Neste trabalho é proposto um novo ataque ao protocolo GOOSE, no contexto de subestações elétricas digitais. Tal ataque representa uma variação do ataque DoS. Na Seção 3.1, é apresentada a modelagem do ataque GOOSE *Grayhole*. Em seguida, na Seção 3.2, o cenário de experimentação é abordado, o qual é usado como base para os experimentos e resultados gerados e discutidos no capítulo seguinte. Por fim, na Seção 3.3, são abordados os detalhes de implementação desse ataque no *framework* ERENO.

## 3.1 Modelagem do Ataque Grayhole

Os ataques *Grayhole* são uma forma de ataque direcionado às redes e computadores que se caracteriza pelo descarte seletivo de pacotes de dados. Em particular, o ataque *Grayhole* consiste em uma categoria específica de ataques que se enquadra na classificação de ataques DoS. Neste trabalho, propõem-se a modelagem desses ataques visando o descarte seletivo de mensagens transmitidas através do protocolo GOOSE, no contexto da automação de subestações de energia. A Figura 4 ilustra a modelagem do ataque *Grayhole* em uma comunicação entre IEDs através do paradigma de publicação e assinatura.

A modelagem de ataques *Grayhole* em um cenário de subestação GOOSE foi concebida, neste trabalho, considerando um descarte seletivo randômico de 20% das mensagens enviadas por um IED. Então, o atacante, neste cenário hipotético modelado, não tem conhecimento prévio sobre a relevância ou o conteúdo das mensagens que está descartando. Como resultado, as mensagens descartadas podem variar de simples notificações de *status* até comandos críticos de controle e operação. Essa porcentagem foi escolhida, através de uma análise empírica, assumindo-se que os efeitos de um ataque *Grayhole* no protocolo GOOSE podem ser significativos com um descarte de 20% das mensagens, podendo-se gerar falhas na comunica-

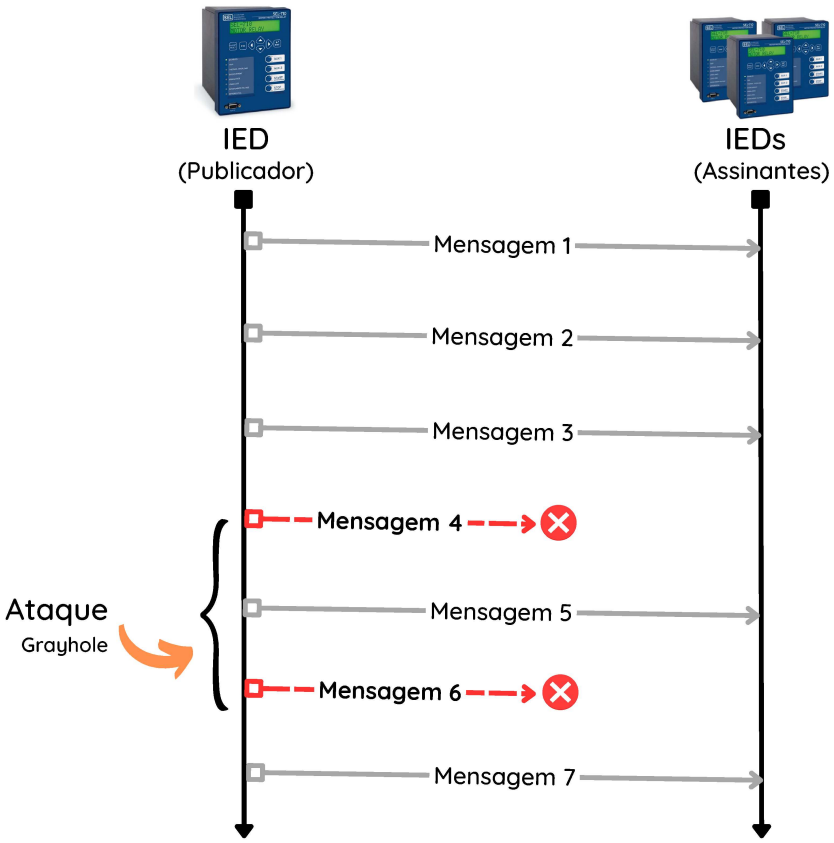


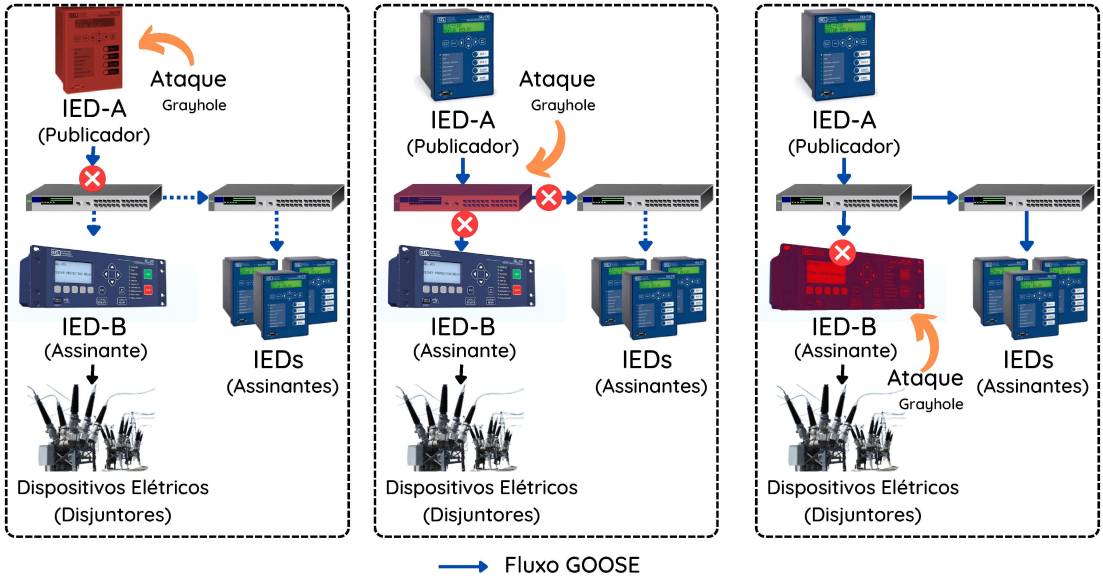

Figura 4 – Modelagem do ataque Grayohole.

ção entre os IEDs, ocasionando possíveis interrupções na transmissão de energia, bem como outros potenciais problemas na subestação. Isso pode resultar em perda de controle operacional, aumento do tempo de inatividade e potencialmente uma paralisação total das operações da subestação.

Destaca-se que, na revisão da literatura, encontrou-se modelagens deste ataque para fins de geração de *datasets* para a detecção de intrusões apenas em outros contextos, tais como em redes de sensores sem fio, conforme publicado por Almomani, Al-Kasasbeh e Al-Akhras (2016). Portanto, é importante observar que o objetivo deste trabalho não é aferir a eficácia do protocolo GOOSE em si, mas, sim, criar, um *dataset* para avaliar a capacidade da identificação desses ataques em subestações que utilizam o protocolo GOOSE por meio de IDSs baseados em aprendizado de máquina.

## 3.2 Cenário de Ataque Grayhole

Com base na definição fornecida em Pal, Sikdar e Chow (2018), o ataque *Grayhole* possui um modelo em que o invasor obtém controle sobre um ou mais dispositivos na rede e, posteriormente, escolhe descartar seletivamente os pacotes que os atravessam, em vez de encaminhá-los, visando causar o máximo de danos e descartar a maior quantidade possível de pacotes sem ser detectado. Dessa forma, observa-se que os cenários de ataques *Grayhole* ao protocolo GOOSE podem seguir três abordagens diferentes, conforme ilustrado na Figura 5 e discutido a seguir.




(a) Origem comprometida. (b) *Switch* comprometido. (c) Destino comprometido.

Figura 5 – Modelagem do ataque Grayohole dividida em subfiguras.

- Comprometimento do IED publicador, de modo a permitir o descarte seletivo das mensagens GOOSE antes mesmo do seu envio (descarte na fonte), conforme ilustrado na Figura 5a;
- Comprometimento de um dispositivo intermediário, tal como um *switch* de rede que, por sua vez, passa a descartar determinadas mensagens GOOSE, conforme ilustrado na Figura 5b;

- Comprometimento do(s) IED(s) assinante(s), de modo a permitir o descarte seletivo das mensagens GOOSE antes de serem processadas pelo receptor (descarte no destino), conforme ilustrado na Figura 5c.

A partir da definição apresentada para o ataque *Grayhole*, foi modelada uma variação para as redes de subestações elétricas baseadas no padrão IEC–61850 (COMMISSION, 2003). Em contraste às redes de sensores sem fio, onde o *Grayhole* pode ser executado por nós sensores (QUINCOZES; KAZIENKO; QUINCOZES, 2023), em subestações elétricas, o método utilizado para causar o ataque de *Grayhole* deve seguir uma das alternativas apresentadas anteriormente para permitir que o atacante efetue a estratégia proposta neste trabalho.

Esse método pode explorar, por exemplo, uma vulnerabilidade na comunicação *multicast* do protocolo GOOSE que permite a exclusão da vítima (*i.e.,* dispositivo assinante) do inventário de assinantes no grupo *multicast* relacionado ao evento ao qual pretende-se evitar deliberadamente a chegada da mensagem. Ou então, em subestações que usam Redes Definidas por Software, do inglês, *Software Defined Network* (SDN), regras de descarte de fluxos ou mensagens podem ser configuradas no *switch* (SOARES et al., 2021a; VIEIRA et al., 2021; SOARES et al., 2021b). Assim, não será possível o recebimento de mensagens transmitidas pelos dispositivos publicadores que forem vítimas do ataque. Dessa forma, o atacante assume o controle das mensagens do publicador e descarta deliberadamente as mensagens GOOSE, sem enviá-las aos dispositivos assinantes. Como resultado, nenhum dispositivo que tenha assinado o publicador receberá os pacotes de dados esperados (QUINCOZES; KAZIENKO; QUINCOZES, 2023).

## 3.3 Implementação do Ataque Grayhole

A implementação do ataque *Grayhole* proposto neste trabalho é ilustrada no pseudocódigo do Algoritmo 1. Esse pseudocódigo apresenta quatro funções: `grayholeAtaque()`, `obterMensagens()`, `selecionarMensagensDescartadas()` e `enviarMensagensDescartadas()`, as quais são descritas a seguir.

A função `grayholeAtaque()` é a função principal responsável por reali-

**Algorithm 1** Lógica do *Grayhole* implementada no ERENO *framework*.

```
1: function GRAYHOLEATAQUE
2:     mensagens ← obterMensagens()
3:     mensagensDescartadas ← selecionarMensagensDescartadas(mensagens)
4:     enviarMensagensDescartadas(mensagensDescartadas)
5: function OBTERMENSAGENS
6:     mensagens ← []
7:     while houverMensagens() do
8:         mensagem ← receberMensagem()
9:         mensagens ← mensagens ∪ mensagem
10:    return mensagens
11: function SELECIONARMENSAGENSDESCARTADAS(mensagens)
12:    mensagensDescartadas ← []
13:    for mensagem in mensagens do
14:        if aleatorio() < 0.2 then                ▷ 20% de chance de descarte
15:            mensagensDescartadas ← mensagensDescartadas ∪ mensagem
16:    return mensagensDescartadas
17: function ENVIARMENSAGENSDESCARTADAS(mensagensDescartadas)
18:    for mensagem not in mensagensDescartadas do
19:        destino ← selecionarDestino()
20:        enviarMensagem(mensagem, destino)
```

zar o ataque *Grayhole*. Ela chama as outras funções para obter as mensagens (`obterMensagens()`), selecionar as mensagens a serem descartadas de maneira aleatória com uma taxa de descarte de 20%(`selecionarMensagensDescartadas()`), e enviar as mensagens que não foram sorteadas para o descarte para o destino original (`enviarMensagem()`).

O algoritmo supracitado foi implementado como proposta deste, sendo uma proposta original do mesmo, e posteriormente integrado ao ERENO (QUINCOZES, 2022). Conforme mencionado no Capítulo 2.1.2, o ERENO é um *framework* extensível de código aberto que pode ser usado para gerar um conjunto de dados (*dataset*) que reproduz o comportamento de protocolos como o GOOSE, baseado na norma IEC-61850. Tal *framework* contém *features* (*i.e.,* atributos) que foram extraídas dos protocolos de comunicação GOOSE. A Figura 6 ilustra a metodologia adotada neste trabalho ao implementar um novo modelo de ataque, estendendo

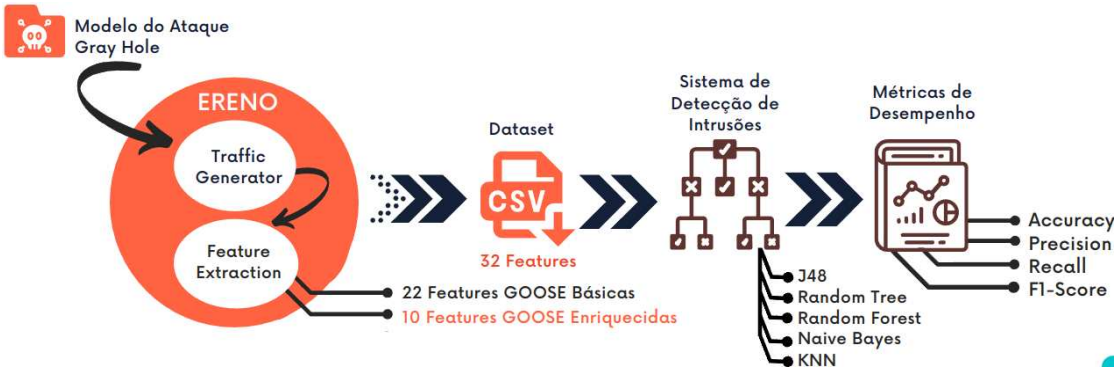



Figura 6 – Processo de modelagem no *framework* Ereno e detecção de ataques *Grayhole*. Fonte: Adaptado de Quincozes (2022)

o ERENO.

Os componentes do lado direito da figura, na cor marrom, representam a etapa de avaliação dos algoritmos de detecção de intrusões (na Seção 3.4) e extração de resultados de métricas de desempenho (abordado no Capítulo 4).

Já na parte esquerda da figura, estão ilustrados os processos de modelagem do ataque *Grayhole* e de extração de *features*. Essas *features* são usadas para treinar algoritmos de aprendizado de máquina, por exemplo, tendo como propósito a detecção dos diferentes tipos de ataques modelados no ERENO. Como prova de conceito, o *framework* ERENO (QUINCOZES, 2022) foi configurado para a geração de um *dataset* com 1.000 amostragens que representam correlações entre mensagens transmitidas usando os protocolos GOOSE e SV, incluindo amostras de comportamento normal e também ataques contra os IEDs. Cada amostra possui 32 *features* extraídas das mensagens GOOSE. O método para a detecção de ataques *Grayhole* ao protocolo GOOSE é apresentada na Seção 3.4.

## 3.4 Detecção de Ataques Grayhole

A detecção do ataque *Grayhole* desempenha um papel crucial na segurança de redes de subestações elétricas baseadas no protocolo GOOSE. Neste contexto, a identificação desse tipo de ataque pode ser realizada através de diferentes estratégias de detecção. No estudo de Attia et al. (2015), esse tipo de ataque é identificado

pela alteração no número de pacotes enviados. Consequentemente, a distribuição normal do número de pacotes enviados não é mais observada, diferenciando-se de situações normais. No entanto, para a detecção eficiente desses ataques, é necessário o uso de algoritmos capazes de processar e analisar grandes volumes de dados e aprender dinamicamente os padrões do atacante.

Dessa forma, a abordagem que será experimentada nesta monografia para a detecção de ataques *Grayhole* consiste na a utilização de algoritmos de mineração de dados. O WEKA (WITTEN; FRANK, 2002), uma coleção de algoritmos de mineração de dados de código aberto, desenvolvido em Java e licenciado sob a *General Public License* (GNU), é uma ferramenta amplamente utilizada para esse fim. Nesta monografia, será adotada a biblioteca WEKA para avaliar a capacidade de algoritmos classificadores em detectar o ataque *Grayhole*, verificando-se assim a qualidade e representatividade do *dataset* gerado através da modelagem proposta.

É necessário utilizar os algoritmos de mineração de dados para avaliar a importância de cada recurso, de modo a aprimorar o desempenho dos algoritmos de detecção. Além disso, essa abordagem favorece a implementação oportuna de contramedidas com o objetivo de identificar as técnicas mais eficientes para a seleção de atributos na detecção do ataque (QUINCOZES, 2022) (QUINCOZES; KAZIENKO; COPETTI, 2018).

Especificamente, serão utilizados algoritmos de árvore de decisão, como o *Random Forest*, *Random Tree* e *J48*, bem como outros algoritmos tradicionais como o *K-Nearest Neighbors* (*KNN*, ou "K-vizinhos mais próximos") e *Naive Bayes*. Dessa forma, a utilização dos algoritmos apontados pelo WEKA desempenhará um papel fundamental nesta monografia a fim de permitir a avaliação da modelagem proposta. Os resultados dos experimentos são apresentados no Capítulo 4.

# 4 Resultados

Este capítulo apresenta os resultados da detecção do ataque *Grayhole* que foi modelado e implementado nesta monografia. Para a presente avaliação, foram realizados validações cruzadas com número de dobras igual a cinco, *i.e.,* o conjunto de dados é divido aleatoriamente em cinco partes iguais que são usadas para testar o IDS separadamente. Ao final final das cinco rodadas, é calculada a média aritmética simples para obter o resultado.

O gráfico da Figura 7 apresenta os resultados de diferentes algoritmos de classificação, *J48*, *Naive Bayes*, *Random Forest*, *Random Tree* e KNN. A seguir serão discutidas os principais achados e destacados pontos relevantes referente à escolha do melhor algoritmo, a partir da análise dos resultados obtidos, para a detecção de ataques do tipo *Grayhole*.

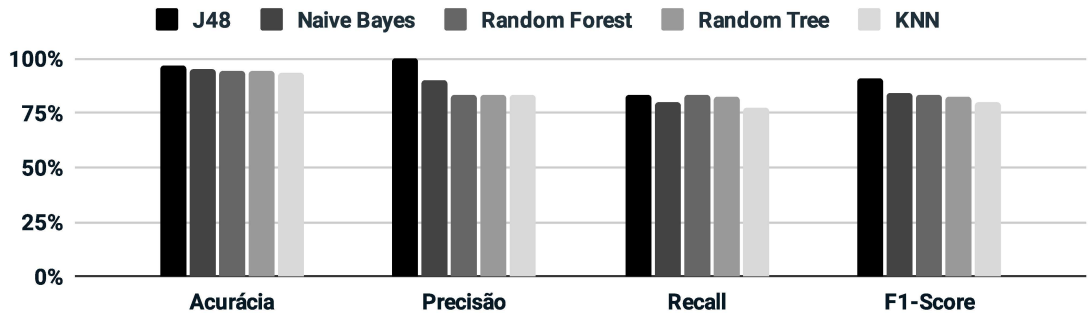



Figura 7 – Detecção do ataque *Grayhole* com uma taxa de descarte de 20%.

A acurácia mede a proporção de amostras classificadas corretamente em relação ao total de amostras. Observou-se que o algoritmo *J48* obteve a maior acurácia (97.11%), seguido por *Naive Bayes* (94.80%), *Random Forest* (94.23%), *Random Tree* (94.06%) e *KNN* (93.40%). Portanto, em termos de acurácia geral, *J48* se destacou.

A precisão mede a proporção de instâncias classificadas corretamente como positivas (*Grayhole*) em relação ao total de instâncias classificadas como positivas. Nesse aspecto, o algoritmo *J48* obteve 100% de precisão, o que significa que todas

as instâncias classificadas como positivas foram corretas (*i.e.,* sem apresentar falsos positivos). *KNN* (83.27%), *Random Forest* (82.87%) e *Random Tree* (82.92%) também apresentaram níveis razoáveis de precisão, enquanto *Naive Bayes* (89.81%) foi ligeiramente superior que os anteriores, ficando atrás apenas do J48. Tais resultados demonstram que mesmo os algoritmos mais simples, como o *Naive Bayes*, são capazes de processar corretamente as *features* geradas a partir da modelagem do ataque *Grayhole* apresentada neste trabalho.

O *recall* (ou recuperação) mede a proporção de instâncias positivas corretamente classificadas em relação ao total de instâncias positivas presentes. *Random Forest* obteve um *recall* de 83.55%, seguido por *J48* (82.96%), *Random Tree* (82.72%), *Naive Bayes* (80.20%) e *KNN* (77.47%). Isso indica que *Random Forest* tem um melhor desempenho em identificar amostras de ataque corretamente em relação aos demais classificadores.

O *F1-Score* é a média harmônica entre a precisão e o *recall*, fornecendo uma medida geral do desempenho do modelo. O algoritmo J48 obteve o maior *F1-Score* (90.68%), seguido por *Naive Bayes* (84.35%), *Random Forest* (83.17%), *Random Tree* (82.76%), e *KNN* (80.17%). Isso indica que J48 possui um equilíbrio entre precisão e *recall*, resultando em um desempenho geral melhor.

## 4.1 Tempo de Processamento

Além das métricas relacionadas ao desempenho na detecção que foram apresentadas, o tempo de execução é um fator relevante a ser considerado ao avaliar o desempenho dos algoritmos. Nos experimentos deste trabalho, observou-se uma variação significativa nos tempos de execução entre os diferentes algoritmos. A Figura 8 ilustra os tempos obtidos para o processamento das amostras produzidas pelos cinco algoritmos classificadores experimentados.

O algoritmo *J48* se destaca como o mais rápido, requerendo, em média, apenas 1,68 micro-segundos para concluir o processo de classificação de cada amostra. Em contraste, o algoritmo *KNN* apresenta o tempo mais longo, demandando, em média, 94,60 micro-segundos para cada classificação. Essa diferença considerável no tempo de execução pode ter implicações práticas em situações onde a rapidez é

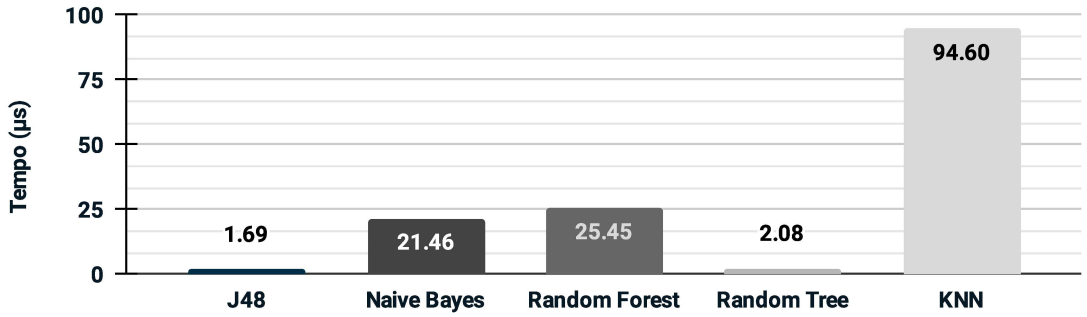



Figura 8 – Detecção do ataque *Grayhole* com uma taxa de descarte de 20%.

uma exigência, como em sistemas de tempo real ou aplicações sensíveis à latência.

Tais resultados estão de acordo com o que se espera, visto que o KNN é um algoritmo *Lazzy* (preguiçoso). Isso significa que ele não mantém um modelo simplificado (como a árvore de decisão que o J48 monta) e, portanto, precisa computar os K vizinhos mais próximos sempre que há uma nova instância a ser classificada (WITTEN; FRANK, 2002).

## 4.2 Discussão

O *dataset* gerado através da modelagem proposta mostrou-se útil para todos os classificadores experimentados, especialmente para o algoritmo classificador *J48*. Os resultados demonstraram que o *J48* obteve um desempenho geral destacado, com alta acurácia, precisão, *recall* e *F1-Score*. Além disso, o *J48* apresentou um maior número de verdadeiros positivos e um menor número de falsos negativos em comparação com os outros algoritmos.

Os resultados evidenciam a qualidade do *dataset* gerado através da modelagem proposta do ataque *Grayhole* no *framework* ERENO, que forneceu informações precisas e representativas para a detecção eficiente desse ataque por meio de diferentes classificadores.

# 5 Desafios Futuros

Neste trabalho, foram abordados os ataques *Grayhole* ao protocolo GOOSE e sua modelagem e implementação usando o framework ERENO. No entanto, existem desafios adicionais que podem ser explorados como continuação desta pesquisa. Um desafio importante na área de segurança cibernética em infraestruturas críticas é a detecção de outros ataques ainda não catalogados. Os ataques *Grayhole* abordados neste trabalho são apenas um exemplo de ameaça que pode ser enfrentada pelas subestações elétricas digitais. Existem outras variantes de ataques que podem explorar vulnerabilidades no protocolo GOOSE ou em sistemas de comunicação semelhantes. Neste capítulo, serão apresentados alguns desses desafios que representam os trabalhos futuros em relação ao estudo realizado.

Uma área de pesquisa promissora é a identificação e modelagem de ataques de *Reflection/Amplification DoS*. Esses ataques envolvem o uso de respostas de terceiros para amplificar o volume de tráfego direcionado à vítima, causando uma sobrecarga em seus recursos. No contexto do protocolo GOOSE, seria interessante investigar como ataques desse tipo podem ser realizados e como podem ser detectados e mitigados (GONDIM; ALBUQUERQUE; OROZCO, 2020).

Outro desafio futuro é a modelagem e detecção de ataques de injeção furtiva (*Stealthy Injection*). Enquanto os ataques *Grayhole* visam interromper a comunicação entre dispositivos, os ataques de injeção furtiva buscam modificar sutilmente as mensagens legítimas enquanto imitam padrões de comportamento legítimos. Esses ataques podem ser mais difíceis de detectar, pois os IDSs podem ter dificuldade em distinguir entre mensagens genuínas e mensagens modificadas de forma furtiva. Uma abordagem interessante para pesquisas futuras seria a modelagem de ataques de injeção furtiva invisíveis, *i.e.*, ataques que um IDS não consegue perceber que ocorreram. Isso poderia envolver o estudo de técnicas de ocultação e disfarce das alterações feitas nas mensagens, tornando-as indetectáveis aos sistemas de detecção existentes. Além disso, seria importante explorar métodos de detecção mais avançados que possam identificar esses ataques sutis (WRIGHT; WOLTHUSEN,

2018).

Os ataques *black hole* são uma categoria específica de ataques DoS que envolvem o bloqueio da entrega de mensagens para a vítima, descartando todo o tráfego da rede em vez de entregá-lo (ATTIA et al., 2015). Embora esse tipo de ataque seja relevante para redes de sensores sem fio, em subestações elétricas digitais baseadas no protocolo GOOSE, um desafio futuro seria explorar variações desses ataques adaptadas ao contexto específico das subestações. Uma possibilidade seria investigar ataques de *black hole* que exploram vulnerabilidades na comunicação *multicast* do protocolo GOOSE. Esses ataques poderiam envolver a exclusão de dispositivos assinantes do inventário de assinantes de um grupo *multicast* relacionado a eventos específicos, impedindo assim a entrega de mensagens aos dispositivos-alvo. Seria necessário explorar como esses ataques podem ser executados e desenvolver técnicas de detecção capazes de identificar a exclusão maliciosa de dispositivos do inventário de assinantes.

Esses desafios futuros representam oportunidades de pesquisa promissoras para aprimorar ainda mais a segurança cibernética em infraestruturas críticas, como subestações elétricas digitais. A investigação desses desafios pode levar a avanços significativos na detecção e prevenção de ataques, fortalecendo a resiliência das redes e garantindo a integridade e disponibilidade das operações.

# 6 Conclusão

A segurança no protocolo GOOSE é utilizada em subestações elétricas e é um protocolo que possui brechas que permitem a exploração de vulnerabilidades que não possuem assinaturas catalogadas. Por isso, é abordado o desenvolvimento de uma nova modelagem de ataque que ainda não foi catalogada no protocolo GOOSE. O ataque modelado inclui o *Grayhole* que foi implementado e simulado usando o framework ERENO, além de ser avaliado através de diversos algoritmos de aprendizado de máquina.

O método adotada visou modelar e implementar o ataque *Grayhole* usando o framework ERENO. Além disso, foi utilizado uma coleção de algoritmos de aprendizado de máquina, presentes no *software* WEKA, para fazer uma avaliação do ataque implementado. Na avaliação em questão, foram utilizados os algoritmos *J48*, *K-Nearest Neighbors* (KNN), *REP Tree* e *Random Forest* para testar a capacidade de detecção do ataque proposto.

Como trabalhos futuros, pretende-se explorar outros ataques que ainda não foram catalogados de forma a produzir-se assinaturas para o treinamento de IDSs, tais como os ataques *black hole*, *stealthy false data injection* e *reflection/amplification DoS*.

# Referências

ABDUL, R. M. T.; SALMAN, Y.; YUNUS, Y.; ROSLAN, I. A review of security attacks on IEC61850 substation automation system network. In: IEEE. **Proceedings of the 6th International Conference on Information Technology and Multimedia**. Malaysia: IEEE, 2014. p. 5–10. Disponível em: <https://doi.org/10.1109/ICIMU.2014.7066594>. Citado na página 16.

AFTAB, M. A.; HUSSAIN, S. S.; ALI, I.; USTUN, T. S. Iec 61850 based substation automation system: A survey. **International Journal of Electrical Power & Energy Systems**, Elsevier, v. 120, p. 106008, 2020. Disponível em: <https://doi.org/10.1016/j.ijepes.2020.106008>. Citado na página 11.

ALMOMANI, I.; AL-KASASBEH, B.; AL-AKHRAS, M. Wsn-ds: A dataset for intrusion detection systems in wireless sensor networks. **Journal of Sensors**, Hindawi, v. 2016, 2016. Disponível em: <https://doi.org/10.1155/2016/4731953>. Citado na página 19.

ATTIA, M.; SEDJELMACI, H.; SENOUCI, S. M.; AGLZIM, E.-H. A new intrusion detection approach against lethal attacks in the smart grid:temporal and spatial based detections. In: **2015 Global Information Infrastructure and Networking Symposium (GIIS)**. Guadalajara, Mexico: IEEE, 2015. p. 1–3. Disponível em: <https://doi.org/10.1109/GIIS.2015.7347186>. Citado 2 vezes nas páginas 23 e 29.

BOHARA, A.; ROS-GIRALT, J.; ELBEZ, G.; VALDES, A.; NAHRSTEDT, K.; SANDERS, W. H. Ed4gap: Efficient detection for goose-based poisoning attacks on iec 61850 substations. In: IEEE. **2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)**. Tempe, AZ, USA: IEEE, 2020. p. 1–7. Disponível em: <https://doi.org/10.1109/SmartGridComm47815.2020.9303015>. Citado na página 17.

COMMISSION, I. E. **Communication networks and systems in substations - ALL PARTS**. Bruselas: IET, 2003. Citado 3 vezes nas páginas 11, 13 e 21.

ELGARGOURI, A.; ELMUSRATI, M. Analysis of cyber-attacks on iec 61850 networks. In: **2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT)**. Moscow, Russia: IEEE, 2017. p. 1–4. Disponível em: <https://doi.org/10.1109/ICAICT.2017.8686894>. Citado na página 8.

GONDIM, J. J.; ALBUQUERQUE, R. de O.; OROZCO, A. L. S. Mirror saturation in amplified reflection distributed denial of service: A case of study using snmp, ssdp, ntp and dns protocols. **Future Generation Computer Systems**, Elsevier, v. 108, p. 68–81, 2020. Disponível em: <https://doi.org/10.1016/j.future.2020.01.024>. Citado na página 28.

HAHN, A.; SUN, C.-C.; LIU, C.-C. Cybersecurity of scada within substations. In: _____. Nova Jersey, EUA: Smart Grid Handbook, 2016. Disponível em: <https://doi.org/10.1002/9781118755471.sgd055>. Citado 2 vezes nas páginas 7 e 8.

HONG, J.; LIU, C.; GOVINDARASU, M. Detection of Cyber Intrusions Using Network-Based Multicast Messages for Substation Automation. In: IEEE. **Innovative Smart Grid Technologies (ISGT)**. Washington, DC, USA, 2014. p. 1–5. Disponível em: <https://doi.org/10.1109/ISGT.2014.6816375>. Citado 2 vezes nas páginas 13 e 16.

HONG, J.; LIU, C.-C. Intelligent electronic devices with collaborative intrusion detection systems. **IEEE Transactions on Smart Grid**, v. 10, n. 1, p. 271–281, 2019. Disponível em: <https://doi.org/10.1109/TSG.2017.2737826>. Citado 2 vezes nas páginas 7 e 8.

HOYOS, J.; DEHUS, M.; BROWN, T. X. Exploiting the goose protocol: A practical attack on cyber-infrastructure. In: IEEE. **2012 IEEE Globecom Workshops**. Anaheim, CA, USA, 2012. p. 1508–1513. Disponível em: <https://doi.org/10.1109/GLOCOMW.2012.6477809>. Citado 2 vezes nas páginas 13 e 15.

KUSH, N.; BRANAGAN, M.; FOO, E.; AHMED, E. Poisoned goose: exploiting the goose protocol. In: AUSTRALIAN COMPUTER SOCIETY, INC. **Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014)**. Auckland, New Zealand: Australian Computer Society, Inc., 2014. v. 149, p. 17–22. Disponível em: <https://www.researchgate.net/publication/259933868_Poisoned_GOOSE_exploiting_the_GOOSE_protocol>. Citado 2 vezes nas páginas 6 e 16.

MACKIEWICZ, R. E. Overview of iec 61850 and benefits. In: IEEE. **2006 IEEE Power Engineering Society General Meeting**. Montreal, QC, Canada, 2006. p. 8–pp. Disponível em: <https://doi.org/10.1109/PSCE.2006.296392>. Citado na página 11.

MCLENNAN, M.; GROUP, S.; GROUP, Z. I. **The Global Risks Report 2022 17th Edition**. 2022. Link. Disponível em: <https://www.weforum.org/reports/

global-risks-report-2022/>. Acesso em: 10 fev. 2023. Citado 2 vezes nas páginas 7 e 8.

O'RAW, J.; LAVERTY, D. M.; MORROW, D. J. IEC 61850 substation configuration language as a basis for automated security and SDN configuration. In: IEEE. **Power & Energy Society General Meeting**. Chicago, IL, USA, 2017. p. 1–5. Disponível em: <https://doi.org/10.1109/PESGM.2017.8274265>. Citado na página 11.

PAL, S.; SIKDAR, B.; CHOW, J. H. An online mechanism for detection of gray-hole attacks on pmu data. **IEEE Transactions on Smart Grid**, v. 9, n. 4, p. 2498–2507, 2018. Disponível em: <https://doi.org/10.1109/TSG.2016.2614327>. Citado 3 vezes nas páginas 7, 9 e 20.

QUINCOZES, S.; KAZIENKO, J.; COPETTI, A. Avaliação de conjuntos de atributos para a detecção de ataques de personificação na internet das coisas. In: **Anais Estendidos do VIII Simpósio Brasileiro de Engenharia de Sistemas Computacionais**. Porto Alegre, RS, Brasil: SBC, 2018. ISSN 2763-9002. Disponível em: <https://sol.sbc.org.br/index.php/sbesc_estendido/article/view/11000>. Citado na página 24.

QUINCOZES, S. E. **ERENO: An Extensible Tool for Generating Realistic IEC–61850 Intrusion Detection Datasets**. Tese (Doutorado) — Fluminense Federal University, 2022. Disponível em: <https://doi.org/10.5753/sbseg_estendido.2022.224642>. Citado 12 vezes nas páginas 6, 7, 8, 9, 12, 13, 14, 15, 17, 22, 23 e 24.

QUINCOZES, S. E.; ALBUQUERQUE, C.; PASSOS, D.; MOSSÉ, D. A survey on intrusion detection and prevention systems in digital substations. **Computer Networks**, Elsevier, v. 184, p. 107679, 2021. Disponível em: <https://doi.org/10.1016/j.comnet.2020.107679>. Citado na página 8.

QUINCOZES, S. E.; KAZIENKO, J. F.; QUINCOZES, V. E. An extended evaluation on machine learning techniques for denial-of-service detection in wireless sensor networks. **Internet of Things**, v. 22, p. 100684, 2023. ISSN 2542-6605. Disponível em: <https://doi.org/10.1016/j.iot.2023.100684>. Citado na página 21.

RAJKUMAR, V. S.; TEALANE, M.; ŞTEFANOV, A.; PALENSKY, P. Cyber attacks on protective relays in digital substations and impact analysis. In: IEEE. **2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems**. Sydney, NSW, Australia, 2020. p. 1–6. Disponível em: <https://doi.org/10.1109/MSCPES49613.2020.9133698>. Citado 2 vezes nas páginas 6 e 7.

SOARES, A. A. Z.; SOARES, L. F.; MATTOS, D. P.; PINHEIRO, P. H.; QUINCOZES, S. E.; FERREIRA, V. C.; APOSTOLO, G. H.; CARRARA, G. R.; MORAES, I. M.; ALBUQUERQUE, C. et al. Enabling emulation and evaluation of iec 61850 networks with titan. **IEEE Access**, IEEE, v. 9, p. 49788–49805, 2021. Disponível em: <https://doi.org/10.1109/ACCESS.2021.3068366>. Citado na página 21.

SOARES, A. A. Z.; VIEIRA, J. L.; QUINCOZES, S. E.; FERREIRA, V. C.; UCHÔA, L. M.; LOPES, Y.; PASSOS, D.; FERNANDES, N. C.; MORAES, I. M.; MUCHALUAT-SAADE, D. et al. Sdn-based teleprotection and control power systems: A study of available controllers and their suitability. **International Journal of Network Management**, Wiley Online Library, v. 31, n. 3, p. e2112, 2021. Disponível em: <https://doi.org/10.1002/nem.2112>. Citado na página 21.

USTUN, T. S.; FAROOQ, S. M.; HUSSAIN, S. S. A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard. **IEEE Access**, IEEE, v. 7, p. 156044–156053, 2019. Disponível em: <https://doi.org/10.1109/ACCESS.2019.2948117>. Citado 3 vezes nas páginas 6, 13 e 17.

VIEIRA, J. L.; FERREIRA, V. C.; BASTOS, I. V.; QUINCOZES, S. E.; DELFINO, W. de O.; SANTOS, Y. d. R. dos; LOPES, Y.; PASSOS, D.; ALBUQUERQUE, C. V.; MORAES, I. M. et al. Thanos: Teleprotection holistic application for onos controller. In: IEEE. **2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)**. Bordeaux, France, 2021. p. 818–823. Disponível em: <https://ieeexplore.ieee.org/document/9463963>. Citado na página 21.

WANG, X.; FIDGE, C.; NOURBAKHSH, G.; FOO, E.; JADIDI, Z.; LI, C. Anomaly detection for insider attacks from untrusted intelligent electronic devices in substation automation systems. **IEEE Access**, IEEE, v. 10, p. 6629–6649, 2022. Disponível em: <https://doi.org/10.1109/ACCESS.2022.3142022>. Citado na página 6.

WITTEN, I. H.; FRANK, E. Data mining: practical machine learning tools and techniques with java implementations. **ACM Sigmod Record**, ACM New York, NY, USA, v. 31, n. 1, p. 76–77, 2002. Disponível em: <https://doi.org/10.1145/507338.507355>. Citado 2 vezes nas páginas 24 e 27.

WRIGHT, J. G.; WOLTHUSEN, S. D. Stealthy injection attacks against iec61850's goose messaging service. In: IEEE. **2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)**.

Sarajevo, Bosnia and Herzegovina, 2018. p. 1–6. Disponível em: <https://doi.org/10.1109/ISGTEurope.2018.8571518>. Citado na página 29.