Universidade Federal da Paraíba

Centro de Informática

Programa de Pós-Graduação em Informática

Implementação e Mitigação de Ataques Cibernéticos em Sistemas SCADA

Camilla Emilly Jácome Ferreira de Figueiredo

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Informática da Universidade Federal da Paraíba como parte dos requisitos necessários para obtenção do grau de Mestre em Informática.

Área de Concentração: Ciência da Computação

Linha de Pesquisa: Sinais, Sistemas Digitais e Gráficos

Prof. Dr. Iguatemi Eduardo da Fonseca

(Orientador)

João Pessoa, Paraíba, Brasil

Catalogação na publicação
Seção de Catalogação e Classificação

F475i Figueiredo, Camilla Emilly Jácome Ferreira de.
Implementação e mitigação de ataques cibernéticos em sistemas SCADA / Camilla Emilly Jácome Ferreira de Figueiredo. - João Pessoa, 2021.
110 f. : il.

Orientação: Iguatemi Eduardo da Fonseca.
Dissertação (Mestrado) - UFPB/CI.

1. Arquitetura de Redes. 2. Smart Grids. 3. SCADA. 4. Modbus. 5. Scapy. 6. Segurança digital. 7. Ataque Cibernético. I. Fonseca, Iguatemi Eduardo da. II. Título.

UFPB/BC CDU 004.72(043)

Elaborado por ANNA REGINA DA SILVA RIBEIRO - CRB-15/024

Resumo

Em meio à realidade em que vivemos, na qual a tecnologia vem fazendo-se cada vez mais presente na sociedade, a *smart grid* surgiu a fim de ofertar inúmeros benefícios para a indústria e facilitar a distribuição de energia em grande escala. Entretanto, estas redes inteligentes - juntamente com seu Sistema de Supervisão e Aquisição de Dados (SCADA - *Supervisory Control and Data Acquisition*) - possuem numerosas fragilidades, encontrando-se expostas a diversos ciberataques que podem vir a causar insupríveis prejuízos. À vista disso, inserido no contexto de segurança de redes em sistemas ciber-físicos, o presente trabalho investiga vulnerabilidades nas comunicações entre os dispositivos presentes no SCADA, e através da execução de ataques (que caso bem-sucedidos, podem ter quaisquer fins, desde danos financeiros à letais) ambiciona penetrá-lo e comprometer os serviços fornecidos por uma *smart grid* e sucessivamente propor mitigações a fim de tornar esses sistemas mais seguros.

Para tanto, visando a obtenção de uma análise qualitativa, utilizou-se a pesquisa bibliográfica exploratória bem como a pesquisa prática experimental como metodologia, apresentando um mapeamento sistemático na área em questão e a implementação dos seguintes ataques cibernéticos: Homem no Meio (MitM - *Man-in-the-Middle*), *TCP Syn Flood*, Ataque de ARP e Ataque Reflexão, sendo o último não explorado em trabalhos anteriores. Resultante disso e mediante os estudos realizados e a efetividade dos ataques aqui trabalhados, reitera-se as vulnerabilidades do sistema exploradas em cenários reais e a importância de tais contribuições e contramedidas.

Palavras-chave: Smart Grids, SCADA, Modbus, Scapy, Segurança, Ataques Cibernéticos.

Abstract

In the midst of the reality in which we live, in which technology becomes increasingly present in society, the smart grid has emerged to offer numerous benefits to the industry and facilitate the distribution of energy on a large scale. However, these smart grids - along with their Supervisory Control and Data Acquisition Systems (SCADA) - have numerous weaknesses, being exposed to various cyber attacks that can cause unbearable losses. Given this, inserted in the context of network security in cyber-physical systems, this present work investigates vulnerabilities in the communications between the devices present in SCADA and, through the execution of attacks (which, if successful, can have any purpose, from financial to lethal damage), aims to penetrate and compromise the services provided by a smart grid and successively propose mitigations to make this system more secure.

For this purpose, aiming at obtaining a qualitative analysis, exploratory bibliographic research was used as well as practical experimental research as a methodology, presenting a systematic mapping in the area in question and the implementation of the following cyber attacks: Man-in-the-Middle, TCP Syn Flood, ARP Attack and Reflection Attack, the latter being absent in previous works. As a result of this and through the studies carried out and the effectiveness of the attacks worked on here, the system's vulnerabilities are explored in real scenarios and the importance of such contributions and countermeasures are reiterated.

Keywords: Smart Grids, SCADA, Modbus, Scapy, Security, Cyber Attacks.

Agradecimentos

Não foi fácil começar a produzir essa dissertação no ano de 2020. Em meio a uma pandemia e tantas aflições e angústias que esta infortuna situação nos trouxe, me faz que primeiramente eu deixe registrado minhas sinceras condolências a todos aqueles que perderam um ente querido. Todavia, apesar das adversidades, me sinto grata ao escrever estas palavras. Não apenas por ter conseguido finalizar este trabalho, apesar de todas as dificuldades enfrentadas, mas principalmente por aqueles que estiveram comigo (mesmo que não fisicamente) durante esta jornada.

Meus sinceros agradecimentos são para todos aqueles que me ajudaram a trilhar este caminho, estiveram tão prontamente ao meu lado e, mesmo que indiretamente, forneceram afeição, auxílio, força, um ombro amigo, e até mesmo palavras duras quando necessário. Esses foram essenciais na minha jornada acadêmica e são minha vida.

Agradeço à minha família, meus pais, em especial minha mãe, por sempre ter me dado apoio e incentivado a prosseguir com meus estudos e lutar pelos meus sonhos. Aos meus queridos amigos, a quem tenho muita estima e graditão, pela amizade incondicional, nomeadamente Michael, Pablo e João Rafael, e minhas grandes amigas Amanda e Ingrid. A Alexandre, que tem todo meu afeto, por ser o melhor inesperado que me aconteceu em 2020 e meu companheiro em todos os momentos. É uma dádiva ter todos vocês em minha vida.

Ao meu orientador, o Prof. Dr. Iguatemi E. Fonseca, pelos ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação acadêmica, conduzindo meu trabalho durante o mestrado e sempre compartilhando seu conhecimento para a realização deste e meu crescimento profissional e pessoal.

Sou grata por todos vocês.

Conteúdo

Lista de Siglas

SCADA: *Supervisory Control and Data Acquisition*, em inglês; ou Sistemas de Supervisão e Aquisição de Dados, em português

RTU: *Remote Terminal Unit, em inglês*; ou Unidade Terminal Remota, em português

TCP: *Transmission Control Protocol*, em inglês; ou Protocolo de Controle de Transmissão, em português

UDP: *User Datagram Protocol*, em inglês; ou Protocolo de Datagrama de Usuário, em português

ARP: *Address Resolution Protocol*, em inglês; ou Protocolo de Resolução de Endereços, em português

MITM: *Man-in-the-Middle*, em inglês; ou Homem no Meio, em português

DoS: *Denial of Service*, em inglês, ou Negação de Serviço, em português

DDoS: *Distributed Denial of Service*, em inglês; ou Ataque de Negação de Serviço Distribuído, em português

IP: *Internet Protocol*, em inglês; ou Protocolo da Internet, em português;

MAC: *Media Address Control*, em inglês; ou Endereço de Controle de Acesso à Mídia, em português

LAN: *Local Area Network*, em inglês; ou Rede de Área Local, em português

NIST: *National Institute of Standards and Technology*, em inglês; ou Instituto Nacional de Padrão e Tecnologia, em português

AMI: *Advanced Metering Infrastructure*, em inglês; ou Infraestrutura Avançada de Medição, em português

DER: *Distributed Energy Resources*, em inglês; ou Recursos Energéticos Distribuídos, em português

DA: *Distribution Automation*, em inglês; ou Automação de Distribuição, em português

SAS: *Substation Automation Systems*, em inglês; ou Sistema de Automação de Subestações, em português

IDS: *Intrusion Detection System*, em inglês; ou Sistema de Detecção de Intrusão, em português

MDMS: *Meter Data Management System*, em inglês; ou Sistema de Gerenciamento de Dados do Medidor, em português

EMS: *Energy Management System*, em inglês; ou Sistema de Gerenciamento de Energia, em português

MTU: *Master Terminal Unit*, em inglês; ou Unidade Terminal Principal, em português

HMI: *Human Machine Interface*, em inglês; ou Interface Homem Máquina, em português

RTU: *Remote Terminal Unit*, em inglês; ou Unidade Terminal Remota, em português

DNP3: *Distributed Network Protocol 3*, em inglês; ou Protocolo de Rede Distribuída 3, em português

IED: *Intelligent Electronic Devices*, em inglês; ou Dispositivo Eletrônico Inteligente, em português

IRT: *Isochronous Real-Time*, em inglês; ou Tempo Real Isócrono, em português

USB: *Universal Serial Bus*, em inglês; ou Barramento Serial Universal, em português

CIP: *Common Industrial Protocol*, em inglês; ou Protocolo Industrial Comum, em português

IoT: *Internet of Things*, em inglês; ou Internet das Coisas, em português

ICS: *Industrial Control Systems*, em inglês; ou Sistemas de Controle Industrial, em português

FIPS: *Federal Information Processing Standards*, em inglês; ou Informações Federais Padrões de Processamento, em português

IACS: *Industrial Automation and Control Systems*, em inglês; ou Segurança de Sistemas de Controle e Automação Industrial, em português

SAL: *Security Assurance Levels*, em inglês; ou Níveis de Garantia de Segurança, em português

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Diante do crescimento da população mundial, houve como consequência o aumento proporcional dos problemas energéticos, principalmente os de distribuição de energia elétrica em grande escala. Com base nessas adversidades enfrentadas, fez-se necessário que uma proposta de solução fosse arquitetada para tornar a geração de energia mais distribuída e acessível. Para tal, a fim de melhorar a eficiência e a confidencialidade do setor elétrico, um investimento significativo foi feito por meio da indústria e dos governos (principalmente o Norte-Americano), objetivando construir um sistema de energia mais inteligente, conectado e automatizado. Assim, mediante a tais premissas, surgiram as *smart grids*, as quais atendem como sistemas de distribuição e transmissão de energia que utilizam-se da tecnologia da informação e comunicação como suporte. De forma mais econômica e sustentável, é através destas redes inteligentes que realiza-se o controle, monitoramento e manutenção do setor elétrico, adquirindo um maior controle do fluxo de energia [Sun et al. 2018].

Incorporado a *smart grid*, o encargo de efetuar as coletas, supervisão e administração dos dados compete ao Sistemas de Supervisão e Aquisição de Dados (SCADA - *Supervisory Control and Data Acquisition*). Os dados obtidos geralmente referem-se a valores de medidas e *status* dos diversos componentes da rede, tornando o sistema uma parte fundamental do setor elétrico, também mediante a sua capacidade de cobrir grandes áreas e executar comunicações em tempo real. O SCADA é amplamente utilizado para supervisionar e monitorar continuamente infraestruturas críticas, como redes de distribuição de água, usinas de geração e distribuição de eletricidade, refinarias de petróleo, usinas nucleares e sistemas de transporte público [Tesfahun et al. 16].

Em contrapartida das amplas aplicabilidades e proveitos, as *smart grids* apresentam grandes riscos. Qualquer interrupção na geração de energia é capaz de

interferir na estabilidade da rede e consequentemente vir a causar impactos socioeconômicos em larga escala. Além destes informes, como dados significativos são trocados entre os sistemas, o furto ou alteração destes pode ainda violar a privacidade do consumidor dos serviços.

Diante destas vulnerabilidades, as *smart grids* tornaram-se alvo de atacantes, obtendo a atenção e interesse do governo, da indústria e de pesquisadores do mundo inteiro [El Mrabet et al. 2018]. Com a migração para as grandes redes, esses sistemas que anteriormente eram isolados, encontram-se expostos a inúmeros ataques cibernéticos conhecidos, e conforme esses e outros diversos problemas relacionados à segurança das *smart grids* (portanto também no SCADA e seus componentes), muitos esforços vêm sendo feitos visando ofertar uma maior proteção para esses sistemas. Para tal, o controle de acesso, a autenticação e a detecção de intrusões atuam como os mecanismos de segurança mais utilizados, todavia, à vista de que o SCADA opera integralmente durante a semana e 24 horas por dia, torna-se pouco viável a realização de pesquisas e experimentos em ambientes reais [Tesfahun et al. 2016].

Perante a este cenário exposto, a proposta de pesquisa desta dissertação consiste em estudar os problemas de segurança relacionados aos sistemas SCADA, explorando suas vulnerabilidades através da implementação de diferentes ataques cibernéticos e uma proposta de mitigação, considerando as fraquezas inerentes ao sistema e seus protocolos. Tais implementações servem como reforços as pesquisas realizadas e como base para a proposta de novas contramedidas de defesa para proteger o sistema contra esses nocivos ataques. No âmbito pesquisado neste trabalho (das redes industriais que fazem uso do sistema SCADA), os protocolos DNP3, Profinet, EtherNet/IP e Modbus são os mais comumente empregados. O último, existente em duas variantes (Modbus RTU e Modbus TCP/IP) e possuinte de diversas fragilidades, será utilizado neste trabalho através dos experimentos realizados na versão onde o pacote do protocolo é incorporado no segmento TCP, explorando suas vulnerabilidades através dos ataques implementados.

1.1 Objetivos

1.1.1 Objetivo Geral

Este trabalho tem como objetivo estudar e explorar as fraquezas presentes nos sistemas SCADA e seus protocolos de comunicação, bem como propor contramedidas para mitigar estas vulnerabilidades. Para alcançar tal propósito, mediante a linguagem *Python* em conjunto com a ferramenta *Scapy*, foram implementados e testados quatro ataques cibernéticos, a saber: i) Homem no Meio (*MitM - Man-in-the-Middle*); ii) *TCP Syn Flood*; iii) Ataque de reflexão; iv) Ataque ARP. Os dois primeiros são discutidos em outros trabalhos por meio de diferentes abordagens de reprodução [Tesfahun et al. 2016] [Ahmad et al. 2019]. O terceiro citado é uma contribuição deste estudo, e sua relevância se deve à falta de implementação deste ataque em outros trabalhos no contexto de sistemas SCADA. Para o último ataque implementado, é apresentada uma proposta de solução que utiliza algoritmos de *hash* para identificar e autenticar nós na rede SCADA, aplicando algoritmos HMAC e Diffie-Hellman para tornar o processo de estabelecimento de vizinhança mais seguro.

1.1.2 Objetivos Específicos

Para alcançar o objetivo geral proposto, os seguintes objetivos específicos foram buscados:

- Entender conceitos dos sistemas SCADA, sua arquitetura e protocolos de comunicação;
- Estudar problemas relacionados à segurança no qual esses sistemas estão sujeitos e realizar uma coleta dos artigos existentes na área através de um estudo de mapeamento sistemático, para assim analisar os resultados obtidos;
- Realizar experimentos de implementações de ataques a fim de explorar as vulnerabilidades presentes no SCADA;
- Analisar os resultados e efetividade dos ataques trabalhados;
- Propor contramedidas contra os ataques analisados.

1.2 Estrutura da Dissertação

O restante deste documento encontra-se organizado da seguinte forma:

Capítulo 2: Apresenta a fundamentação teórica necessária para o trabalho em questão. Sendo exposto os conceitos sobre *smart grids*, sistemas SCADA (arquitetura e protocolos de comunicação) e uma seção acerca da segurança cibernética com menção aos principais ataques aos quais o sistema está exposto e os principais métodos de defesa utilizados.

Capítulo 3: É demonstrado o resultado de um estudo de mapeamento sistemático acerca da segurança em sistemas SCADA, trazendo discussões e análises sobre estes trabalhos relacionados.

Capítulo 4: Compreende a apresentação e implementação dos ataques cibernéticos abordados e de uma proposta de mitigação para o ataque ARP. Tais implementações foram realizadas a fim explorar as vulnerabilidades inerentes ao sistema SCADA por meio dos ataques, e com isso, o capítulo exibe os resultados obtidos, os impactos que podem gerar no sistema, e qual proteção a contramedida proposta oferece para esses ambientes.

Capítulo 5: Apresenta as considerações finais e pretensões de trabalhos futuros.

Capítulo 2

Fundamentação Teórica

Neste capítulo é abordado os principais conceitos referentes às *smart grids* e aos sistemas SCADA, demonstrando o funcionamento, arquitetura, principais protocolos, problemas relacionados à segurança e mecanismos de defesa existentes na literatura. Como objetivo, visa auxiliar no entendimento da proposta de dissertação assim como os resultados obtidos presentes nos capítulos seguintes.

2.1 - Smart Grids

Entende-se por *smart grid*, um sistema baseado em comunicação e tecnologia da informação adequado para a geração, fornecimento e consumo de energia. Trata-se de redes inteligentes que são incorporadas às usinas a fim de recolher e administrar dados, e com base nestas informações coletadas, controlá-las com eficácia. Para tal, as *smart grids* utilizam-se do fluxo bidirecional de informações, com intuito de formar um sistema automatizado, amplamente distribuído e que disponibiliza de novas funcionalidades. Estas aplicabilidades indicadas são: controle, competência operacional, melhora no desempenho ambiental, integração de tecnologias renováveis e o aumento da resiliência [Sun et al. 2018]. A última indica a capacidade da rede de resistir a eventos inesperados com um rápido tempo de recuperação, e à vista disso, esta resiliência tornou-se um recurso inegociável no contexto atual, especialmente quando as interrupções de energia podem afetar potencialmente a economia. Para prover tamanhas atribuições, as *smart grids* prometem fornecer flexibilidade e confidencialidade, permitindo assim o provimento adicional de energia, facilitando a integração de novos recursos à rede e habilitando recursos corretivos caso ocorram falhas [El Mrabet et al. 2018].

2.1.1 Comunicação de Sistemas

No âmbito das subestações convencionais, a comunicação é analógica e realizada por intermédio de um cabo de cobre individual conectado entre cada par de dispositivos. Por outro lado, as *smart grids* (que utilizam-se da comunicação digital) permitem a interconectividade entre vários dispositivos, também trazendo uma melhoria na eficiência da troca de dados, uma vez que esta configuração permite que vários sinais sejam transmitidos simultaneamente na mesma linha. Em adição, oferece a vantagem de que os custos de engenharia e comunicação podem ser reduzidos e facilitados através da utilização de protocolos de comunicação como Ethernet e IP (*Internet Protocol*), entre outros. Uma vez conectados a uma rede local (LAN - *Local Area Network*), os dispositivos de *gateway* (RTUs e roteadores) podem agregar os dados internos em uma subestação e encaminhá-los para os destinos como centros de controle. A Figura 1 mostra as diferenças de configuração entre redes de comunicação de subestação tradicionais e digitais.

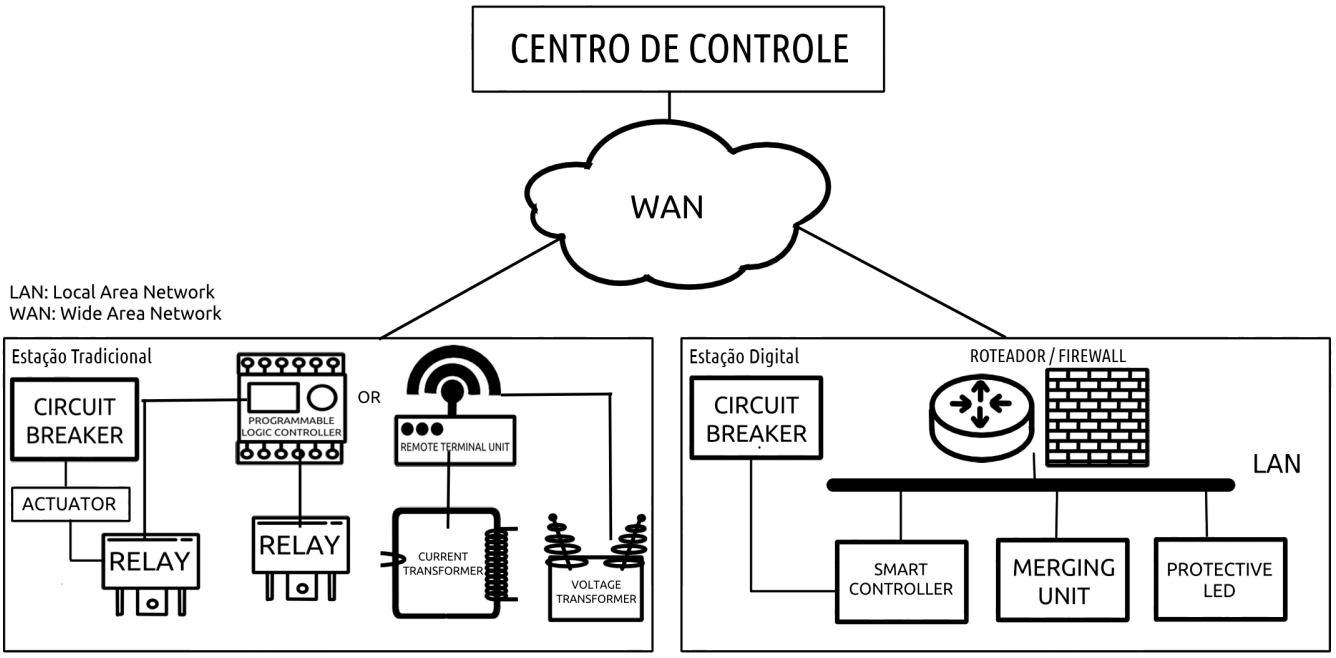

Figura 1: Comparação Entre a Subestação Tradicional e Digital (Imagem Autoral Baseada em [Sun Et Al. 2018]).

2.1.2 Modelo Conceitual das Smart Grids

Segundo o Instituto Nacional de Padrão e Tecnologia dos Estados Unidos (NIST - *National Institute of Standards and Technology*), uma *smart grid* é composta por sete

domínios lógicos, sendo estes: geração, transmissão e distribuição de energia, cliente, mercado, provedor de serviços e operações em massa. Em cada um dos citados inclui operadores (que atuam como programas, dispositivos e sistemas) e aplicações (que tratam-se de tarefas executadas por um ou mais operadores em cada domínio) [El Mrabet et al. 2018]. A Figura 2 exibe o modelo conceitual de rede inteligente e a interação de operadores de diferentes domínios por meio de um canal seguro.

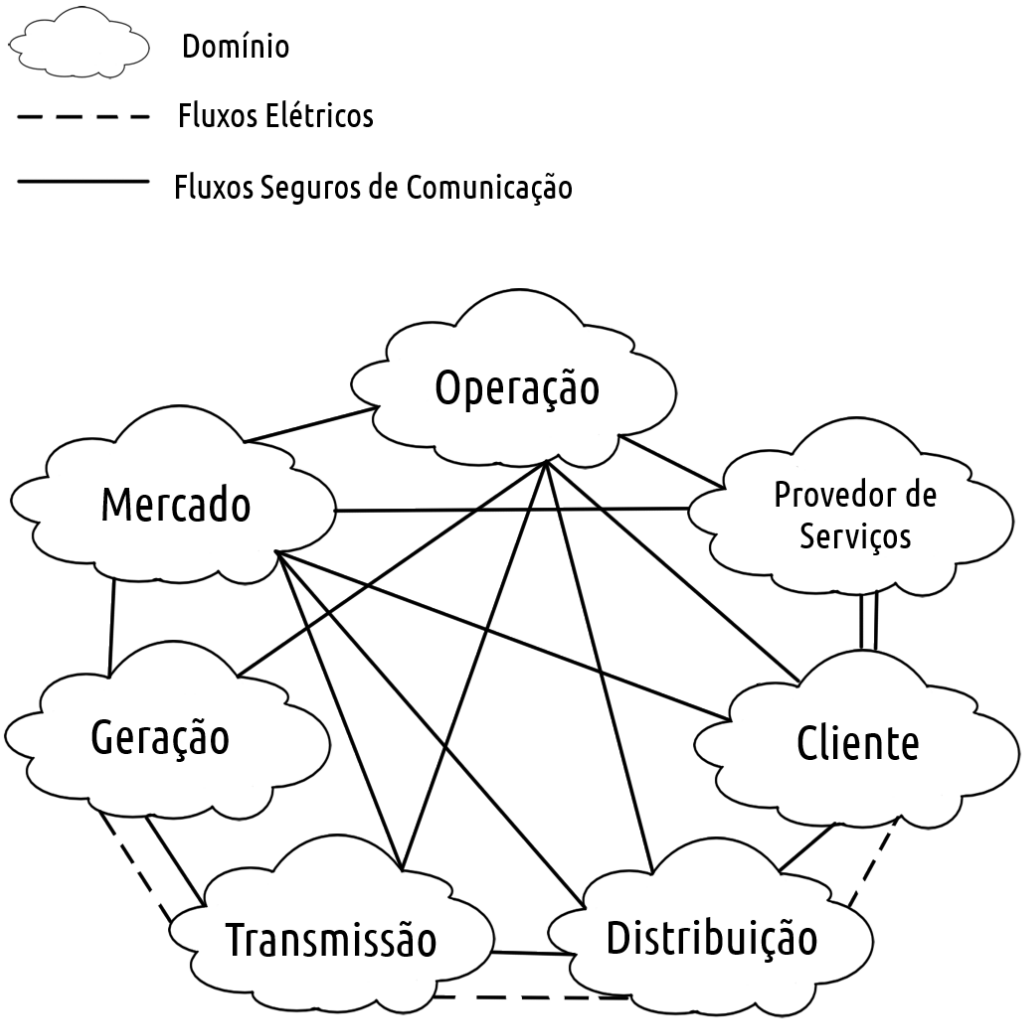

Figura 2: Modelo Conceitual de Smart Grids Baseado no NIST (Imagem Autoral Baseada em [El Mrabet et al. 2018])

Quando refere-se ao domínio do cliente, o operador principal é o usuário final. Em geral, existem três tipos de clientes: residencial, comercial e industrial. Estes, além de consumir eletricidade, também podem gerar, armazenar e gerenciar o uso de energia. É responsabilidade do domínio do provedor prestar serviços para eles (também como

para as concessionárias de energia elétrica) e fazer gerências como a do uso de energia e cobranças das contas dos clientes. Para tanto, interagem com o domínio da operação e desenvolvem serviços inteligentes como a permissão da interação do cliente com o mercado e a geração de energia em casa. Os demais domínios são discutidos em detalhes em [El Mrabet et al. 2018].

Além disso, as *smart grids* são compostas por diversos elementos como Infraestrutura Avançada de Medição (*Advanced Metering Infrastructure* (AMI), Recursos Energéticos Distribuídos (DER - *Distributed Energy Resources*), Automação de Distribuição (DA- *Distribution Automation*) e Sistema de Automação de Subestações (SAS- *Substation Automation System*). Estes possuem a finalidade de tornar a rede mais ampla, diversa e automatizada, contando com a capacidade de obter e trocar informações com uma maior precisão, tornando-se dessa forma capaz de detectar falhas e auto reparar-se sem a necessidade de intervenção humana. Tais características fazem com que a rede seja mais resistente a desastres naturais ou mudanças na topologia [Sun et al. 2018].

2.1.3 Aplicações nas Smart Grids

Em sua formação, a *smart grid* contém variadas aplicações distribuídas e heterogêneas, entre estas destacam-se: a AMI, a automação da subestação e sistema de supervisão e controle (SCADA), contextualizado na próxima seção. A AMI pertence ao cliente e aos domínios de distribuição e é responsável por coletar, medir e analisar o uso de energia, água e gás, permitindo comunicação bidirecional do usuário para a concessionária. A mesma é composta por três componentes: medidor inteligente, cabeçalho AMI e rede de comunicação. O primeiro é constituído de microprocessadores e uma memória local que é responsável por monitorar e coletar o uso de energia dos e pela transmissão de dados em tempo real para a matriz da AMI. Além disso, esta aplicação possui um servidor chamado *headend* que consiste em um Sistema de Gerenciamento de Dados do Medidor (MDMS - *Meter Data Management System*). A comunicação entre estes medidores inteligentes, os eletrodomésticos e o *headend* da AMI é definida através de protocolos de comunicação como Z-Wave e Zigbee [El Mrabet et al. 2018].

Pertencente aos domínios de geração, transmissão e distribuição, a subestação é um elemento-chave na rede elétrica. É responsável por executar várias funções, incluindo receber energia da instalação de geração, regular a distribuição e limitação da energia [El Mrabet et al. 2018]. A comunicação entre a subestação de automação e os outros dispositivos de transmissão e distribuição pode ser definida pela norma IEC 61850.

2.2 SCADA

Em uma *smart grid*, o sistema SCADA é uma ferramenta primordialmente utilizada para coletar medições e dados de *status* e enviar comandos de controle para dispositivos de comutação. Como visto, são sistemas amplamente distribuídos utilizados para supervisionar e monitorar continuamente infraestruturas críticas, e com base nestes dados coletados, um Sistema de Gerenciamento de Energia (EMS - Energy Management System) fornece ferramentas analíticas para que os operadores da rede possam visualizar e determinar remotamente o estado do sistema, e com isso tomarem as ações apropriadas [Sun et al. 2018].

Para tal, visando reduzir custos e aumentar a eficiência, a tecnologia SCADA migrou de sistemas isolados (monolíticos) para arquiteturas em rede que se comunicam com a rede corporativa e a Internet. Com isso, permitiu a substituição de protocolos proprietários por protocolos SCADA abertos e também a interoperabilidade (capacidade de um sistema de comunicar-se de forma transparente com outro) entre diferentes fornecedores de equipamentos. No entanto, essa melhoria foi implementada na maioria dos sistemas SCADA existentes, sem levar em consideração seu impacto na segurança cibernética. As violações de segurança dos sistemas SCADA podem atrapalhar e danificar a operação de infraestruturas críticas, contaminar o meio ambiente ecológico, causar enormes perdas econômicas (os processos gerenciados são críticos para a defesa e a economia de qualquer país) e em piores casos, pode levar até mesmo a perdas de vidas humanas [Tesfahun et al. 2016].

2.2.1 Arquitetura do Sistema

O sistema SCADA possui uma arquitetura constituída por dispositivos e componentes diversificados. Dentre estes, distingue-se a Unidade Terminal Principal (MTU - *Master Terminal Unit*), uma unidade de controle centralizada, responsável por todo o fluxo de informações e controles no sistema. Com o auxílio da EMS, o acesso a esta unidade é realizado através da Interface Homem Máquina (HMI - *Human Machine Interface*), local em que é possível visualizar dados, configurar parâmetros e executar comandos, possibilitando o administrador da rede determinar ações e envios destes comandos de controle aos demais dispositivos. Ainda é atribuído à MTU a supervisão e controle de processos físicos, dispositivos (sensores e atuadores) e da Unidade Terminal Remota (RTU - *Remote Terminal Unit*), cuja a função é coletar dados dos dispositivos em campo (como sensores) e retornar à MTU por meio de protocolos de comunicação [Tesfahun et al. 2016]. Na Figura 3 é representada uma arquitetura SCADA característica.

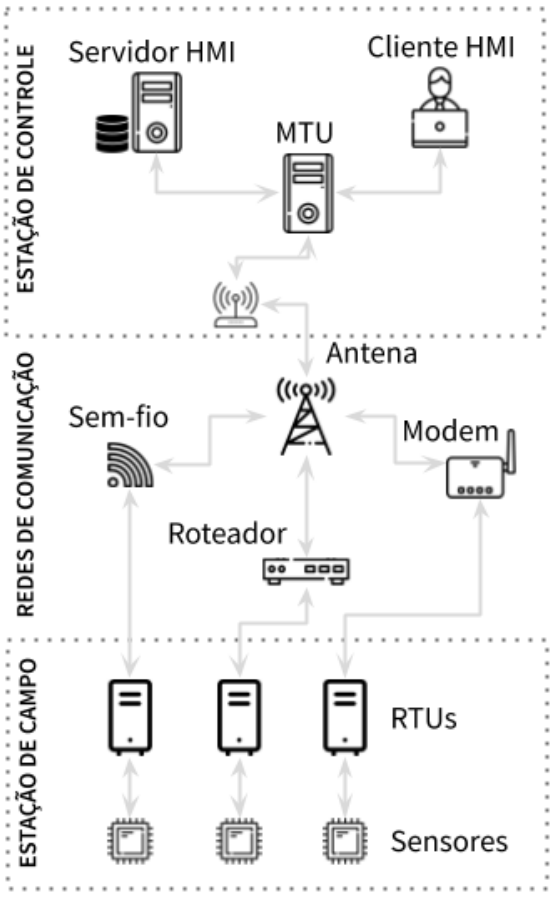

Figura 3: Arquitetura Típica dos Sistemas SCADA (Imagem Autoral)

2.2.2 Protocolos de Comunicação

O fluxo de informação entre os dispositivos do sistema ocorre a partir de protocolos de interconexão de rede, que projetados com este fim, garantem eficiência, confidencialidade e precisão nas operações. Realizadas em tempo real, prover tais operações teve influência direta no projeto dos protocolos, pois a priorização da velocidade e agilidade em detrimento de outras funcionalidades refletiram diretamente na negligência para com a segurança presente nestes, e como consequência, houve a retirada de algumas funcionalidades de proteção.

Como já mencionado, na história do SCADA, os sistemas (entre as décadas de 60 a 80) eram isolados e utilizavam protocolos proprietários de *hardware*, *software* e comunicação. Por esta razão, naquele contexto, tornavam-se menos propícios a ataques em comparação com os mais modernos, que trazem desafios à segurança por apresentarem interoperabilidade, conectividade e compatibilidade. Além disso, como o ciclo de vida dos equipamentos SCADA podem chegar a até 20 anos, não é incomum que nos dias de hoje nas usinas alguns dispositivos mais antigos (e sem medidas de segurança adequadas) coexistam com os mais modernos, comunicando-se entre si através de conversores [Yang et al. 2012].

Atualmente, existem diferentes protocolos propícios para os sistemas SCADA. Em [Irmak et al. 2018] os autores apresentam uma porcentagem das taxas de uso dos principais protocolos de comunicação utilizados. Para tal, uma busca foi realizada através do mecanismo de pesquisa Shodan, cujo resultado é apresentado na Figura 4. De acordo com esta informação, foi visto que enquanto o protocolo Modbus TCP possui cerca de 50% de uso, os protocolos EtherNetIP, Profinet e DNP3 têm taxas de uso de 30%, 15% e 5% respectivamente.

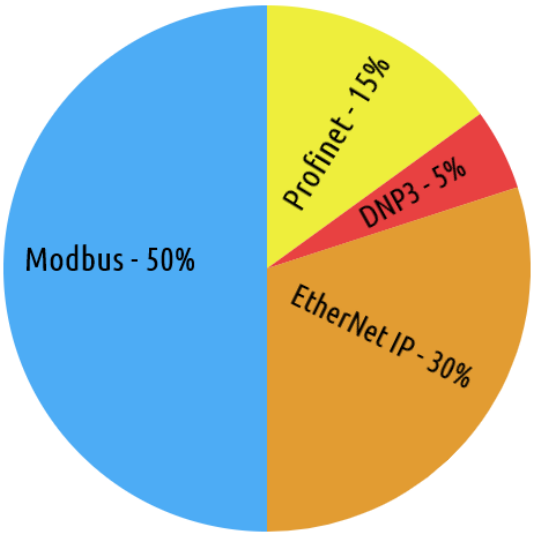

Figura 4: Taxas de Uso de Protocolos de Comunicação SCADA (Imagem Adaptada de [Irmak et al. 2018]

A seguir estão citados e sucintamente explicados os principais protocolos utilizados nos sistemas SCADA.

2.2.2.1 Modbus

O protocolo Modbus é fundamentado no conceito de supervisor/operário, no qual apenas um nó supervisor está conectado a um ou vários nós operários (tendo como número máximo 247). Sua comunicação é sempre iniciada pelo supervisor e os operários respondem apenas quando solicitados. Isto é, os nós operários nunca transmitem dados sem receber uma solicitação do nó supervisor, como também nunca há transmissões entre si [Modbus 2012].

Além destas características, no Modbus não existem requisitos para diagnósticos relacionados ao estado do nó operário. Caso o supervisor solicite um dado com informações desconhecidas ao operário, ele enviará como resposta uma exceção. Contudo, se a variável do processo estiver incorreta ou o dispositivo apresentar problemas de funcionamento, não há suporte no protocolo para que o operário comunique isto, uma vez que foi projetado sem mecanismo algum de segurança. Por consequência, as mensagens podem ser interceptadas, reproduzidas ou até mesmo falsificadas, gerando um enorme prejuízo nas operações de controle ou supervisão [Drias et al. 2015].

Na Figura 5 é possível observar a comunicação dos dispositivos através do protocolo Modbus que utiliza o conceito de supervisor/operário.

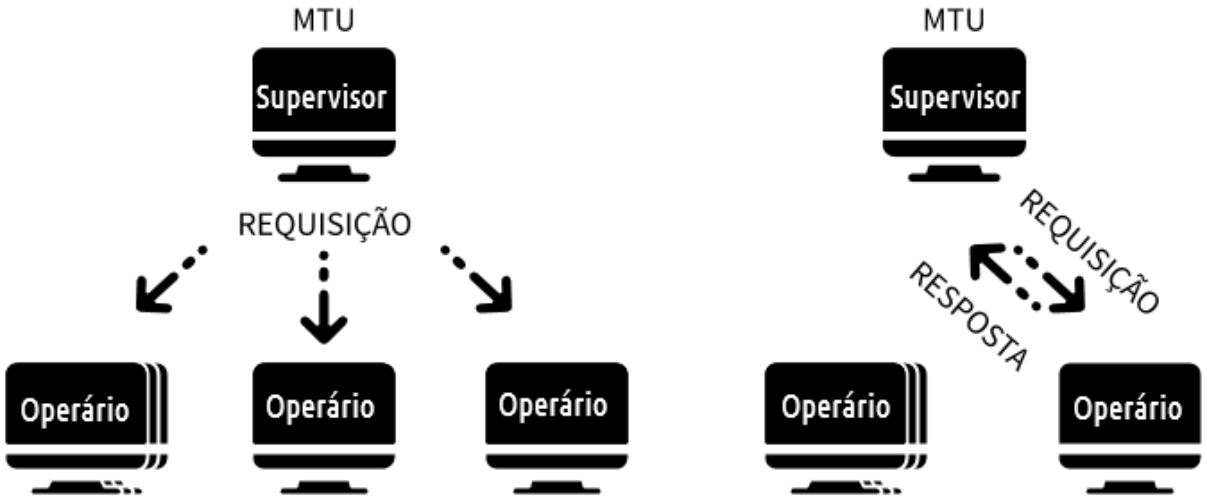

Figura 5: Troca de Mensagens Supervisor/Operário (Imagem Autoral)

2.2.2.2 DNP3

O Protocolo de Rede Distribuída (DNP3 - *Distributed Network Protocol 3*) iniciou-se como um projeto para alcançar a interoperabilidade entre os computadores, RTUs e IEDs das subestações. Baseado no conceito supervisor/operário, é utilizado para a troca de dados entre dispositivos do sistema de controle e, a fim facilitar tais comunicações, o DNP3 foi estendido para trabalhar sobre IP (encapsulado em pacotes TCP ou UDP) como a maioria dos protocolos atuais. Resultante disso, é estruturado em duas camadas e oferece vantagens como: multiplexação, fragmentação de dados e verificação de prioridades e erros. Por esta razão, passou a ser amplamente utilizado em indústrias de água, transporte, petróleo e gás [DNP ORG] [Drias et al. 2015].

2.2.2.3 Profinet

O Profinet é um protocolo cuja tecnologia é baseada em Ethernet, a fim de prover a comunicação de dados em tempo real em sistemas de controle industrial. Na época em que foi concebido, esses sistemas eram basicamente separados da rede de computadores

tradicionais, e por esta razão, o design deste protocolo não considera totalmente a segurança da informação, principalmente tratando-se do contexto atual. Apesar disso, o Profinet é um dos padrões líderes do mercado e é suportado por muitos fornecedores de produtos. Sua comunicação é dividida em três níveis: i) o TCP/IP para dados não críticos, ii) comunicação em tempo real para aplicações com até 10 ms de ciclo e iii) Tempo Real Isócrono (IRT - *Isochronous Real-Time*) para aplicações com menos de 1 ms de ciclo [Feng et al. 2016] [Profibus].

2.2.2.4 EtherNet/IP

O Protocolo Industrial Ethernet (EtherNet/IP - *EtherNet Industrial Protocol*) fornece ferramentas para implantar a tecnologia Ethernet padrão nas diferentes variedades de dispositivos do setor elétrico (não apenas os conectados por controladores), oferecendo várias opções de topologia de rede como estrela, linear ou em anel. Pode ser usado operando sobre TCP ou UDP (com mesmo número de porta reservada - 44818), sendo composto por duas partes: i) o Encapsulamento EtherNet/IP e ii) o Protocolo Industrial Comum (CIP - *Common Industrial Protoco*l). O primeiro contém dados que descrevem as conexões, sessões e métodos de comunicação e o segundo as informações sobre objetos, instâncias, atributos e valores, sendo amplamente usado como uma arquitetura de comunicação unificada no setor de fabricação [Wong et al. 2017][Odva Org].

2.3 Segurança Cibernética

Como componente principal dos sistemas de controle, o SCADA é o principal alvo dos invasores. Os ataques exploram as diversas fragilidades no sistema, sejam elas de *hardware*, *software* ou nos protocolos de comunicação. Com trocas de mensagens em larga escala acontecendo simultaneamente, o risco de um ataque cibernético explorando os protocolos de comunicação é alto. Constatando essas fragilidades, alguns ataques em grandes proporções sucederam-se ao longo dos anos. Em julho de 2010, uma arma cibernética atingiu uma instalação nuclear iraniana, introduzida através de um *pendrive* (dispositivo de memória USB). O *worm* denominado Stuxnet obteve controle do sistema SCADA responsável por controlar as centrífugas de enriquecimento de urânio, estabelecendo com que girassem 40% mais rápido e, como resultado, provocando rachaduras e problemas de funcionamento. O *software* malicioso também era incumbido

de capturar dados sensíveis e enviá-los diretamente aos invasores [Tesfahun et al. 2016] [Drias el al. 2015].

Posteriormente, em dezembro de 2015, na Ucrânia, houve uma queda de energia decorrente de um ataque cibernético, cuja interrupção afetou mais de 225.000 pessoas. A princípio, o ataque iniciou-se através de um *malware* para o reconhecimento e monitoramento da rede elétrica, visando o planejamento das etapas do ataque. No dia em que o ataque ocorreu, o sistema SCADA foi invadido e usado pelos atacantes para abrir remotamente vários disjuntores, ocasionando o corte direto na energia de milhares de cidadãos. Agravando a situação, o sistema telefônico e a rede de comunicação foram comprometidos por um ataque de negação de serviço (DoS - *Denial of Service*), impossibilitando que os clientes pudessem informar sobre o ocorrido. Esta ação, foi uma dentre as medidas danosas cometidas pelos atacantes a fim de dificultar as providências de restauração do sistema [Huang et al. 2018].

2.3.1 Requisitos de Segurança

Uma vez que o SCADA é usado para controlar infraestruturas críticas, a segurança torna-se um problema real que os usuários e fornecedores estão enfrentando. Para tal, antes de definir quaisquer mecanismos ou contramedidas, é essencial entender os objetivos e requisitos de segurança para garantir que esta ocorra, juntamente com a confidencialidade das operações de controle. O NIST definiu em um guia para os sistemas de controle industrial, três critérios necessários para manter a segurança [Guia NIST] [Drias et al. 2015]:

I. **Confidencialidade:** O critério de confidencialidade exige que as informações proprietárias e a privacidade pessoal sejam protegidas contra acesso ou divulgação por entidades, indivíduos ou processos não autorizados, visto que caso esta divulgação ocorra, a confidencialidade do sistema é perdida. No âmbito das *smart grids*, informações como controle de um medidor, uso da medição e dados de cobrança devem ser confidenciais e protegidas, pois, caso contrário, estas informações podem ser manipuladas, modificadas ou usadas para outros fins maliciosos [El Mrabet et al. 2018].

- **Vulnerabilidades:** esse tipo de insegurança inerente aos protocolos, oferece ao invasor a oportunidade de acessar informações particulares e roubar ilegalmente grandes quantidades de dados [Huang et al. 2018].

II. **Integridade:** Significa a proteção para que não haja uma alteração, modificação ou destruição não autorizada de dados de maneira não detectada, sendo necessário que, para evitar tais situações, o sistema possua a capacidade de detectar esta manipulação por entidades não autorizadas. Para tal, tanto o não repúdio quanto a autenticidade das informações são necessários para manter a integridade. O primeiro significa que indivíduos, entidade ou organização são incapazes de executar uma ação específica e depois a negarem, e a segunda concerne aos dados serem originários de uma fonte legítima [Drias et al. 2015] [El Mrabet et al. 2018].
   - **Vulnerabilidade:** para corromper a integridade do sistema, pacotes contendo dados falsos ou dados incompletos podem ser enviados para ou a partir do sistema através de protocolos vulneráveis [Huang et al. 2018].

III. **Disponibilidade:** O acesso em tempo real aos ativos de dados é primordial para controlar as operações do sistema. Portanto, a disponibilidade é definida como garantia de acesso oportuno e confiável e uso dessas informações. Ativos indisponíveis ou operações de controle interrompidas conduzem a danos econômicos e humanos e, por esta razão, a disponibilidade é considerada como o critério de segurança mais importante das *smart grids*.
   - **Vulnerabilidade:** o invasor pode comprometer a disponibilidade do sistema a partir ataques de exaustão de recursos, e também pode afetar outros dispositivos através da modificação de parâmetros(o que também afeta a integridade), o que em ambos os casos, acaba resultando na perda do controle do dispositivo e/ou na falha de operação adequada [Huang et al. 2018].

O [Guia NIST] também definiu uma tabela que resume as definições de impacto potencial para cada um dos objetivos de segurança, conforme representado na Tabela 1 a seguir.

	Impacto Potencial		
Objetivo de Segurança	**Baixo**	**Médio**	**Alto**
Confidencialidade : Preservar as restrições autorizadas ao acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias.	Espera-se que a divulgação não autorizada de informações tenha um efeito adverso **limitado** nas operações organizacionais, ativos organizacionais ou indivíduos.	Espera-se que a divulgação não autorizada de informações tenha um efeito adverso **sério** nas operações organizacionais, ativos organizacionais ou indivíduos.	Espera-se que a divulgação não autorizada de informações tenha um efeito adverso **grave ou catastrófico** nas operações organizacionais, ativos organizacionais ou indivíduos.
Integridade: Proteção contra modificação ou destruição indevida de informações e inclui a garantia do não-repúdio e da autenticidade das informações.	Espera-se que a modificação ou destruição não autorizada de informações tenha um efeito adverso **limitado** nas operações organizacionais, ativos organizacionais ou indivíduos.	Espera-se que a modificação ou destruição não autorizada de informações tenha um efeito adverso **sério** nas operações organizacionais, ativos organizacionais ou indivíduos.	Espera-se que a modificação ou destruição não autorizada de informações tenha um efeito adverso **grave ou catastrófico** nas operações organizacionais, ativos organizacionais ou indivíduos.
Disponibilidade: Garantir o acesso oportuno e confiável e o uso da informação.	Espera-se que a interrupção do acesso ou uso da informação ou de um sistema de informação tenha um efeito adverso **limitado** nas operações organizacionais, ativos organizacionais ou indivíduos.	Espera-se que a interrupção do acesso ou uso da informação ou de um sistema de informação tenha um efeito adverso **sério** nas operações organizacionais, ativos organizacionais ou indivíduos.	Espera-se que a interrupção do acesso ou uso da informação ou de um sistema de informação tenha um efeito adverso **grave ou catastrófico** nas operações organizacionais, ativos organizacionais ou indivíduos.

Tabela 1: Definições De Impacto Potencial Para Objetivos De Segurança [Guia NIST]

2.3.2 Ataques Cibernéticos

Muitos ataques cibernéticos em *smart grids* já sucederam-se em todo o mundo e, mesmo atualmente, continuam a ocorrer. A seguir estão citados os principais ataques relacionados a qual o sistema está sujeito, sendo alguns utilizados para os experimentos realizados neste trabalho.

- **Homem no Meio:** O ataque do homem no meio acontece quando um atacante está inserido entre dois dispositivos legítimos, "escutando" a comunicação, com a possibilidade de interceptar, alterar e modificar os dados transmitidos. O invasor está conectado aos dois dispositivos e retransmite o tráfego entre eles. Esses dispositivos legítimos parecem comunicar-se diretamente quando na verdade estão comunicando-se através do terceiro dispositivo atacante [El Mrabet et al. 2018]. Na Figura 6 é exibida uma ilustração do ataque.

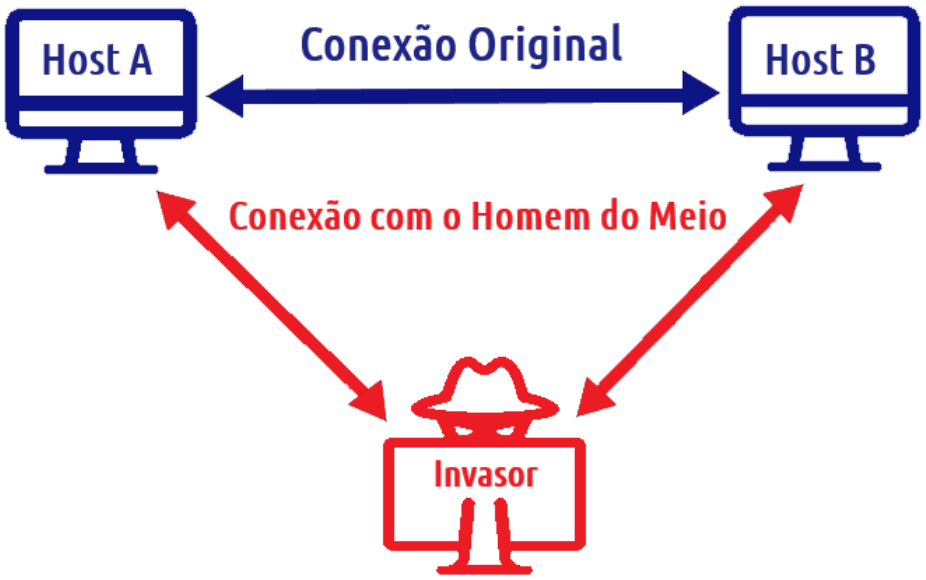

Figura 6: Ataque do Homem no Meio (Imagem Autoral)

- **Ataque no ARP:** O Protocolo de Resolução de Endereço (ARP - *Address Resolution Protocol*) fornece a resolução dinâmica de endereços físicos. Este processo consiste em obter um endereço Endereço de Controle de Acesso à

Mídia (MAC - *Media Address Control*) de uma interface a partir de seu endereço IP. Todavia, ele assume que todos os nós de uma rede são confiáveis, sendo essa suposição não válida para vários cenários, como por exemplo, uma rede sem fio, na qual existe a possibilidade um invasor entrar no enlace com uma autenticação mínima ou até inexistente. Por conta dessa vulnerabilidade, o protocolo torna-se alvo para muitos ataques, entre eles o do Homem no Meio, onde o atacante ambiciona passar-se por outro host e estabelece vizinhança com a vítima, que associa o IP buscado com o MAC do atacante.

- ***Replay*:** Neste ataque, em razão das informações do tráfego industrial serem transmitidas em texto plano, um invasor pode capturar pacotes, registrar parte das informações válidas e retorná-lo ao servidor do sistema, comprometendo assim a integridade da comunicação.

- **Exaustão de Recursos:** Também conhecidos como ataques de negação de serviço (DoS - *Denial of Service*), seu principal objetivo é afetar a disponibilidade do sistema incapacitando os dispositivos. Para isso, existem alguns ataques conhecidos na literatura, dentre esses destacam-se:

    - **TCP Syn Flood:** O invasor inunda o sistema de destino com solicitações de conexão sem responder aos *replays* (mensagens de respostas), forçando o sistema a travar. O protocolo Modbus / TCP é vulnerável a esses ataques, pois opera sobre TCP [El Mrabet et al. 2018].

    - **Reflexão:** O atacante envia uma mensagem com o endereço IP falsificado da vítima do ataque para hosts que atuarão como reflectores. Estes, por sua vez, enviam numerosas respostas ao endereço IP da vítima, sendo a carga útil dessas respostas muito superior à da solicitação. Dessa forma, quando a quantidade de tráfego de resposta for lançada, a vítima ficará submersa na inundação do ataque [Chang Liu et al. 2015]. No contexto dos sistemas SCADA, o supervisor atua como a vítima e os operários como reflectores. Na Figura 7 é possível ver a ilustração do ataque.

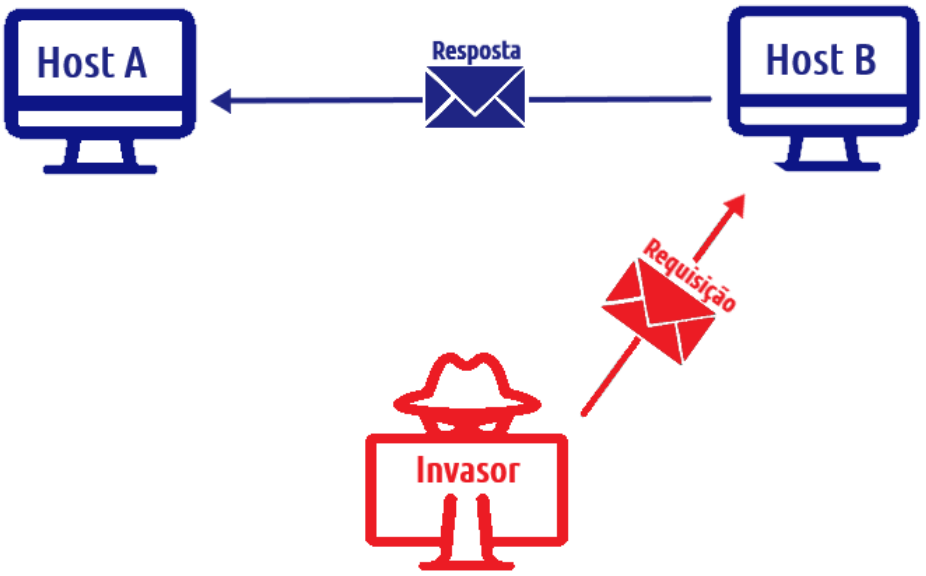

Figura 7: Ataque de Reflexão (Imagem Autoral)

- ***Malware*:** O SCADA é vulnerável a ser infectado por diversos *softwares* maliciosos (como vírus e *worms*) que possuem efeitos nocivos ao sistema. Dentre as diversas consequências, tem-se a diminuição da comunicação entre subestações e centros de controle [Yang et al. 2012]. Com o propósito de infectar um dispositivo ou sistema específico na *smart grid*, atacantes utilizam-se de *malwares* como o vírus. O *worm*, por sua vez, opera como um programa auto-replicante que espalha-se através da rede, copiando-se para infectar outros dispositivos e sistemas [El Mrabet et al. 2018].

- **Escaneamento:** O ataque é empregado a fim de descobrir quais os dispositivos e hosts estão ativos na rede. Em geral, podem ser classificados em quatro tipos diferentes de varreduras, sendo estas: dos endereços IPs, das portas (para determinar quais estão abertas), dos serviços em execução e das vulnerabilidades existentes, visando identificar os pontos fracos e deficiências do sistema e explorá-las posteriormente [El Mrabet et al. 2018].
- **Ataque de Injeção:** Esse ataque tem como alvo as vulnerabilidades que afetam a integridade do sistema, tencionando corrompê-la e com isso, provocando grande perturbação. A partir deste, o invasor envia dados e comandos inválidos

que modificam ou excluem parcialmente os dados no sistema [Huang et al. 2018].

2.3.3 Tipos de Atacantes

Segundo McAfee, Inc[1]., empresa norte-americana de *software* de segurança, também conhecida como Grupo de Segurança da Intel, os *hackers* (similarmente chamados de atacantes, ciberatacantes, invasores na rede, entre outras terminologias) podem ser divididos em alguns tipos, sendo estes:

- **Chapéu Branco (*White Hat*):** São especialistas em segurança computacional que se concentram em fazer testes de penetração e outras metodologias de modo a garantir que os sistemas de informação de empresas são realmente seguros. Esses profissionais de segurança fazem isso invadindo a rede do contratante, determinando o nível de segurança e apontando melhorias, usando um arsenal em constante evolução para enfrentar os *hackers* maliciosos.
- **Chapéu Preto (*Black Hat*):** Comumente chamados de *hackers* ou *crackers*, os termos costumam a ser usados especificamente para criminosos que invadem redes ou computadores, ou ainda que criam vírus de computador. Atacantes desse tipo continuam a agir mais rapidamente do que os do tipo *White Hat*, pois encontram o caminho que oferece menor resistência (seja erro humano ou negligência) ou criam um novo tipo de ataque. A motivação desse tipo costuma ser vantagens monetárias.
- **Chapéu Cinza (*Grey Hat*):** Esses são *hackers* que não usam suas habilidades para benefício próprio, mas não operam de forma totalmente legal. Por exemplo, um *hacker* que invada o sistema de uma empresa para revelar uma vulnerabilidade e poste a descoberta na internet pode, em última instância, está fazendo algo positivo para os clientes daquela empresa, mas, por outro lado, comprometeram um sistema sem permissão. Podem ser interessados na área que estão estudando e testando suas técnicas ou scripts sem prejudicar ninguém, todavia se este mesmo *hacker* solicitar dinheiro da empresa para não revelar a

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

vulnerabilidade, nesse caso o limite seria transposto e ele estaria agindo como um hacker do tipo *Black Hat*, operando totalmente para ganho próprio.

- ***Script Kiddies*:** Termo pejorativo indicando *hackers* que usam programas baixados da internet para atacar redes, alterar sites para se tornarem conhecidos. São considerados “amadores”.

- ***Hacktivistas*:** Agem por ideologias religiosas ou políticas e almejam fazer parte de mudanças sociais. Também podem agir pelo sentimento de vingança contra empresas ou movimentos.

- ***Spy Hackers* (Espiões):** Governos ou empresas podem contratar *hackers* para que se infiltrem em sistemas concorrentes e roubem segredos comerciais. Esses *hackers* podem tentar ataques externos ou podem agir como infiltrados, como por exemplo funcionários dentro de uma empresa. Seu propósito é atingir os objetivos do cliente e obter benefícios monetários.

- **Ciberterroristas:** Terroristas digitais, geralmente são motivados por crenças religiosas ou políticas, e tentam criar medo e caos ao interromper o funcionamento de serviços cruciais de infraestrutura, contando com uma ampla variedade de habilidades e objetivos. Em última instância, a motivação de ciberterroristas é espalhar medo, terror e violência, tornando-os o tipo de atacante mais perigoso.

2.3.4 Métodos de Defesa

Como mencionado previamente, em sua concepção, os sistemas SCADA foram criados para serem isolados das redes de comunicação externas, sendo o suficiente para garantir a sua segurança na época em questão. Todavia, o mero isolamento físico não é mais o bastante, visto que com a migração para as grandes redes o sistema foi exposto a diversas vulnerabilidades, e para tal, é necessário que haja diferentes métodos para garantir sua proteção. Devido a isso, muitas pesquisas vêm sendo realizadas a fim de desenvolver mecanismos mais eficientes que possam prover a segurança necessária para SCADA, e por conseguinte, para as *smart grids* como um todo. A seguir, estão retratados alguns dos principais métodos de defesa presentes na literatura.

2.3.4.1 Criptografia

Algoritmos criptográficos nas *smart grids* podem ser empregados para diferentes fins, como: garantir a integridade e a confidencialidade dos dados (em repouso e em trânsito), na autenticação da origem das mensagens e para o não repúdio às ações executadas no sistema de controle. Entretanto, o uso de contramedidas de criptografia em um ambiente industrial pode custar muito caro em termos de consumo de recursos, também acarretando em dificuldades para o armazenamento de chaves, distribuição e renovação da criptografia incorporada nos componentes do sistema de controle, entre outros. A vista disso, muitas pesquisas foram e são realizadas nesse campo para propor um sistema de gerenciamento de chaves para as diferentes técnicas criptográficas. Para tanto, os designers de sistemas criptográficos para estes ambientes precisam trabalhar para contornar estes obstáculos através de diferentes adaptações e novas metodologias [Drias el al. 2015].

2.3.4.2 Firewall

Entende-se por *firewall* um mecanismo que controla o tráfego da rede e determina através de regras específicas quais são as comunicações internas e externas autorizadas. Em particular, essa política de segurança pode ser classificada em duas categorias:

I. **Política negativa:** rejeita todas as comunicações internas ou externas e a utiliza de regras específicas para determinar as conexões autorizadas.

II. **Política positiva:** permite todas as comunicações e, usando regras de controle, define quais conexões serão descartadas.

Além disso, os sistemas de *firewall* podem ser classificados por sua funcionalidade ou por seu posicionamento. Para o primeiro caso, quatro categorias podem ser definidas, são estas: i) *Firewall* de filtragem de pacotes, ii) *Firewall* de inspeção com estado, iii) *Gateway* no nível do aplicativo e vi) *Gateway* no nível do circuito. No segundo caso, ocorre de acordo com os processos de gerenciamento de segurança e avaliação de risco, podendo haver várias combinações de arquitetura. É importante ressaltar que um *firewall* não pode fornecer serviços de proteção contra ataques que o contornam, como por exemplo, usuários internos mal intencionados ou acidentes não intencionais. À vista

disso, como em muitas usinas estes mecanismos são a única forma de proteção do sistema, caso um pacote malicioso consiga passar pelo *firewall*, pode gerar danos na rede e consequentemente em todo o sistema [Radoglou-Grammatikis et al. 2018].

2.3.4.3 Sistema de Detecção de Intrusão

Um Sistema de Detecção de Intrusão (IDS - *Intrusion Detection System*) é um mecanismo que monitora uma rede a fim de detectar tráfegos maliciosos que possam violar suas regras de segurança. Em geral, os IDS podem ser categorizados em dois tipos: i) os baseados em assinaturas e ii) os baseados em anomalias. O primeiro tipo, combina o conteúdo dos pacotes com padrões predefinidos (chamados assinaturas) associados ao tráfego malicioso, enquanto o segundo detecta invasões ao identificar comportamentos que desviam-se do normal [Nivethan et al. 2016].

Os mesmos IDS também são adotados para os sistemas SCADA e como resultado, podem ser realmente eficientes em detectar alguns tipos de ataques devido a muitos desses sistemas serem implantados em redes Ethernet e utilizarem protocolos de controle de processo capazes de transportar mensagens TCP/IP. A principal fraqueza na aplicação dessa abordagem é que esta falha em capturar ataques específicos ao protocolo de controle e ao próprio sistema SCADA. Contudo é possível adaptá-la, para assim tornar o IDS eficaz na detecção de ataques específicos do SCADA, sendo necessário que sua funcionalidade seja estendida à inspeção e análise de cargas de mensagens próprias para o sistema [Nivethan et al. 2016].

2.3.5 Padrões e Diretrizes de Segurança

Além dos métodos de defesa retratados na subsubseção anterior, também existem padrões e diretrizes de seguranças criados como guia de proteção para o setor elétrico. Estes padrões funcionam como manuais de boas práticas, orientando o que deve ser implementado, e contendo etapas como definição de requisitos, soluções de segurança para proteção de rede, bem como sistemas de gerenciamento de chaves para o projeto de autenticação, autorização e gestão dos requisitos de segurança do sistema. A seguir, estão retratados os principais padrões e diretrizes de segurança para as *smart grids*.

2.3.5.1 Guia de Orientações do NIST

Conforme mencionado, o NIST dispõe de um guia [Guia NIST] para os Sistemas de Controle Industrial (ICS - *Industrial Control Systems*), que trata-se de um projeto de segurança para esses tipos de sistemas que fornece arquiteturas e topologias típicas de ICS, discutindo as principais ameaças e vulnerabilidades desses sistemas. O objetivo deste projeto era a aplicação de Informações Federais Padrões de Processamento dos Estados Unidos (FIPS - *Federal Information Processing Standards*) [FIPS][Guia NIST] para sistemas de controle industrial como parte dos sistemas federais, e foi introduzido através da publicação do NIST 800-82 [Stoufler et al. 2014]. O FIPS exige os seguintes controles de segurança para sistemas federais: controle de acesso, conscientização e treinamento, auditoria e responsabilidade, avaliação de segurança, gerenciamento de configuração, identificação e autenticação, bem como resposta a incidentes. O documento também fornece contramedidas de segurança para mitigar o risco associado às vulnerabilidades e ameaças do ICS. Ainda no guia, os autores propõem um processo completo para aplicar a segurança no ICS, começando por políticas de segurança e conscientização das pessoas e, em seguida, conduzindo uma avaliação de risco para o ICS. Por abranger todas essas questões, o NIST 800-82 é a diretriz mais detalhada e específica para proteger sistemas de controle industrial para proprietários de segurança. A única limitação na especificação é a falta de diretrizes de design para provedores e fornecedores de ICS.

Em fevereiro de 2014, o NIST publicou uma estrutura de segurança intitulada *NIST Cyber Security Framework* [ANSI/ISA-62443-3-3], que provê um processo completo para implementar a segurança cibernética de um ponto de vista organizacional e técnico. Identificar, proteger, detectar, responder e recuperar são as cinco funções que a estrutura propõe para garantir a segurança cibernética de uma infraestrutura crítica. As cinco funções referem-se a diferentes padrões, como IEC62443, ISO27001 [Drias et al. 2015].

2.3.5.2 IEC 62443

O IEC 62443 formalmente denominado ISA99 Segurança de Sistemas de Controle e Automação Industrial (IACS - *Industrial Automation and Control Systems*), tem como objetivo criar documentos de orientação sobre como aplicar a segurança de TI em

sistemas de controle industrial, incluindo *hardware* e sistemas de *software*, como SCADA, DCS, PLC, HMI, sensores e dispositivos em rede. O padrão é dividido em quatro categorias principais de requisitos: requisitos gerais, requisitos de políticas e procedimentos, requisitos de sistema e requisitos de componentes. O IEC 62443 também refere-se a primeira norma que detalha os requisitos do ponto de vista do sistema, introduzindo na IEC 62443.3.x (que é adotada pela maioria dos fornecedores de ICS), Níveis de Garantia de Segurança (SAL - *Security Assurance Levels*) para sistemas de controle industrial e também para controles de segurança específicos a serem implementados em cada SAL. Os níveis de garantia de segurança são avaliados para cada zona funcional usando sete requisitos funcionais, sendo estes: identificação e controle de autenticação, controle de uso, integridade de dados, confidencialidade de dados, fluxo de dados restrito, resposta oportuna ao evento, disponibilidade de recursos [Drias et al. 2015].

2.3.5.2 IEC 62351

O IEC 62351 é um padrão desenvolvido pela IEC para segurança nas operações de controle do sistema de potência, e possui 11 partes que cobrem todos os aspectos de segurança na comunicação de concessionárias de energia. As partes 1 e 2 são especificações técnicas que discutem questões de segurança em sistemas de controle de energia, enquanto as partes 4, 5, 6 são publicadas como especificações técnicas sobre como implementar segurança em protocolos de comunicação de controle de energia, como MMS e IEC61850 sobre TCP / IP. Além do padrão de segurança para protocolos de comunicação, as partes 7 a 11 abordam um escopo maior para cobrir segurança de ponta a ponta, envolvendo políticas de segurança, mecanismos de controle de acesso, gerenciamento de chaves, log de auditoria e outras questões críticas de proteção de infraestrutura [Line et al. 2011].

2.3.6 Cenários de Ataque

De acordo com o que foi visto sobre a segurança cibernética das *smart grids* e sistemas SCADA, a Tabela 2 a seguir relaciona os requisitos de segurança apresentados na subsubseção 2.3.1, com os ataques cibernéticos expostos na subsubseção 2.3.2 e os tipos de atacantes apresentados na subsubseção 2.3.3, juntamente com a descrição do cenário

necessário para viabilizar que invasores realizem os ataques mencionados, quais os impactos gerados (baixo, médio ou alto), indicando quais contramedidas podem ser implementadas para prevenir tais ataques, conforme a seção 2.3.4 de métodos de defesa.

Ataque	Cenário de Ataque	Tipo do Atacante	Requisito de Segurança Afetado	Impacto	Contramedidas
Homem no Meio	Para realizar este ataque, o invasor precisa estar dentro da mesma rede que os hosts vítimas, seja fisicamente ou obtendo o acesso remoto.	***Black Hat*:** Para o caso de um atacante externo que consiga passar por todos os mecanismos de defesa e infiltrar-se na rede interna. ***Spy hackers*:** Para o caso de ser um funcionário ou infiltrado que tenha acesso físico a rede interna.	Integridade e confidencialidade	A interceptação, alteração e modificação de dados sensíveis tem impacto **médio a alto**, pois além de violar a privacidade dos consumidores dos serviços, a alteração dos dados pode prejudicar o funcionamento da rede e trazer prejuízos imensuráveis**.**	Autenticação dos hosts, *firewall* para evitar que o invasor consiga acesso a rede, criptografia para proteger os dados e IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
Ataque ARP	Para realizar este ataque, o invasor tem que estar dentro da mesma rede que os hosts vítimas, seja fisicamente ou obtendo o acesso remoto.	***Black Hat*:** Para o caso de um atacante externo que consiga passar por todos os mecanismos de defesa e infiltrar-se na rede interna. ***Spy hacker*:** Para o caso de ser um funcionário ou infiltrado que tenha acesso a rede interna.	Integridade e confidencialidade.	Uma vez que um host estabelece vizinhança com o atacante, possibilita o envio de dados imprecisos, gerando impacto **alto** e prejuízos imensuráveis**.**	Autenticação dos hosts, *firewall* para evitar que o invasor consiga acesso a rede, criptografia para proteger os dados e IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
Replay	Para realizar este ataque, o invasor tem que estar	***Black Hat*:** Para o caso de um atacante externo	Integridade	A interceptação dos dados sensíveis	Autenticação dos hosts, *firewall* para evitar que o

	dentro da mesma rede que os hosts vítimas, seja fisicamente ou obtendo o acesso remoto.	que consiga passar por todos os mecanismos de defesa e infiltrar-se na rede interna. ***Spy hacker*****:** Para o caso de ser um funcionário ou infiltrado que tenha acesso físico a rede interna.		tem impacto **baixo** pois apesar de violar a privacidade dos consumidores dos serviços não altera o funcionamento da rede.	invasor consiga acesso a rede, criptografia para proteger os dados e IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
DoS	Para realizar este ataque, os invasores, geralmente de forma remota, efetuam inúmeras solicitações a um sistema intencionando gerar uma alta demanda e interromper seu funcionamento.	Dependendo da dificuldade do sistema alvo, podem tratar-se de: ***Black Hat***, ***Script Kiddies*** e ***CiberTerroristas***.	Disponibilidade.	Pela troca de dados ocorrer em tempo real, sendo a disponibilidade o critério de segurança mais importante das *smart grids*, o impacto do ataque é **alto**.	IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
TCP *Syn Flood*	Para realizar este ataque, o invasor tem que estar dentro da mesma rede que os hosts vítimas, seja fisicamente ou obtendo o acesso remoto. Desta forma, através de solicitações TCP, gera sobrecarga direta na camada de transporte e indireta na camada de aplicação.	***Black Hat*****:** Para o caso de um atacante externo que consiga passar por todos os mecanismos de defesa e infiltrar-se na rede interna. ***Spy hacker*****:** Para o caso de ser um funcionário ou infiltrado que tenha acesso a rede interna.	Disponibilidade.	Pela troca de dados ocorrer em tempo real, sendo a disponibilidade o critério de segurança mais importante das *smart grids*, o impacto do ataque é **alto**.	IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
Reflexão	Para realizar este ataque, o invasor precisa estar dentro da mesma rede que os hosts vítimas e reflectores, seja	***Black Hat*****:** Para o caso de um atacante externo que consiga passar por todos os mecanismos	Integridade e disponibilidade.	Pela troca de dados ocorrer em tempo real, sendo a disponibilidade o critério de	Autenticação dos hosts, *firewall* para evitar que o invasor consiga acesso a rede, criptografia para

	fisicamente ou obtendo o acesso remoto.	de defesa e infiltrar-se na rede interna. ***Spy hacker*:** Para o caso de ser um funcionário ou infiltrado que tenha acesso a rede interna.		segurança mais importante das *smart grids*, o impacto do ataque é **alto**.	proteger os dados e IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
Malware	O *malware* precisa ser baixado ou instalado, seja acidentalmente ou intencionalmente.	***Black Hat***: Para o caso de um novo *malware* criado ou um atacante que consegue infectar uma rede altamente protegida. Dependendo do alvo e da intenção/impacto gerado podem ser **Ciberterroristas**. ***Script Kiddies***: Para o caso do atacante que utiliza *malwares* conhecidos para atacar redes ou sites desprotegidos. ***Spy hacker*:** Para o caso de ser um funcionário ou infiltrado que tenha acesso a rede interna e introduza o *malware* no sistema.	Dependendo do tipo do *malware* pode afetar a integridade, confidencialidade e disponibilidade do sistema.	Conforme o que o *malware* afeta no sistema, pode ter impacto de **médio a alto**. *Malwares* como o Stuxnet podem causar grandes danos e prejuízos, como o ocorrido no Irã em 2010.	Antivírus, manter os *softwares* atualizados e treinamento de funcionários para que evitem acessar links e e-mails suspeitos.
Escaneamento	Para realizar este ataque, o invasor precisa estar dentro da mesma rede que hosts vítimas,seja fisicamente ou obtendo o acesso	***Black Hat*:** Para o caso de um atacante externo que consiga passar por todos os mecanismos de defesa e	Confidencialidade.	A interceptação dos dados sensíveis tem impacto **baixo** pois apesar de violar a privacidade dos	Autenticação dos hosts, *firewall* para evitar que o invasor consiga acesso a rede, criptografia para proteger os dados

	remoto.	infiltrar-se na rede interna. ***Spy hacker*****:** Para o caso de ser funcionário ou infiltrado que tenha acesso físico a rede interna.		consumidores dos serviços não altera o funcionamento da rede.	e IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.
Ataque de Injeção	Para realizar este ataque, o invasor precisa estar dentro da mesma rede que hosts vítimas, seja fisicamente ou obtendo o acesso remoto.	***Black Hat*****:** Para o caso de um atacante externo que consiga passar por todos os mecanismos de defesa e infiltrar-se na rede interna. ***Spy hacker*****:** Para o caso de ser funcionário ou infiltrado que tenha acesso físico a rede interna.	Integridade.	O envio de dados e comandos inválidos tem impacto **alto**, pois prejudica o funcionamento da rede e trazendo prejuízos imensuráveis**.**	Autenticação dos hosts, *firewall* e criptografia para evitar que o invasor consiga acesso a rede e IDS para conter os tráfegos maliciosos que violem as regras de segurança do sistema.

Tabela 2: Relação entre Ataques X Cenário de Ataque X Tipo de Atacante X Requisito de Segurança Afetado X Impacto X Contramedidas

Capítulo 3

Trabalhos Relacionados

Mediante a importância do setor elétrico e aos recentes ataques que sucederam-se, a preocupação com questões de segurança expandiu-se e diversas pesquisas estão sendo desenvolvidas. Estas, buscam encontrar vulnerabilidades, avaliar o impacto dos ataques (anteriormente já conhecidos e os possíveis novos descobertos) e desta forma, desenvolver métodos de defesa eficientes para a proteção dos sistemas SCADA.

Em [Tesfahun et al. 2016], é proposto um *testbed* de segurança em SCADA, denominado CORE (*Common Open Research Emulator*), cujo os autores descrevem como sendo um ambiente virtual facilmente escalável e reconfigurável, que pode ser usado para desenvolver e avaliar soluções de segurança específicas para o SCADA. Utilizando a ferramenta, é demonstrado o resultado da implementação de ataques, sendo estes Ataque de Negação de Serviço Distribuída (DDoS - *Distributed Denial of Service)* e Ataque de Injeção de Dados Falsos (*False Data Injection Attack*), constatando como os invasores podem interromper a operação normal dos sistemas SCADA.

Seguindo a mesma linha de pesquisa, em [Ahmad et al. 2019], os autores explicam a construção de um simulador de código aberto para realização de testes de segurança em SCADA, desenvolvido através do simulador de eventos Omnet ++. Como estudo de caso, foram analisados os ataques *DDoS* e TCP *Syn Flood* , em uma simulação de um sistema de distribuição de energia, e como tais ataques podem causar danos e prejuízos à indústria elétrica.

Na literatura, muitos trabalhos apontam para tais problemas relativos à segurança desses sistemas e, muitas pesquisas foram e estão sendo feitas, visando tornar estes ambientes mais seguros. Trabalhos como [Sun Et Al. 2018], [El Mrabet et al. 2018], [Huang et al. 2018], [Drias et al. 2015] e [Ericsson 2010], fazem um levantamento da área e apontam vários problemas de segurança referentes ao setor

elétrico. De igual modo, estudos como [Radoglou-Grammatikis et al. 2018], [Feng et al. 2016], [Wong et al. 2017] e [Nivethan el al. 2016] indicam mecanismos de defesa que possam prover segurança para o SCADA, e por conseguinte, para as *smart grids* como um todo.

A seguir, este capítulo exibe um mapeamento sistemático acerca da segurança em sistemas SCADA, que foi realizado a partir das coletas dos trabalhos relacionados, e através destas, apresenta uma análise dos resultados obtidos.

3.1 Mapeamento Sistemático Sobre Segurança em SCADA

Ainda que estudos descrevam os esforços de pesquisa aplicados à segurança do SCADA, durante a pesquisa, não foram encontrados registros de que algum destes sejam voltados para a coleta e classificação sistemática dos trabalhos anteriores realizados na área, sendo estes tipos de estudos capazes de auxiliar na identificação de temas de pesquisa bem explorados e também lacunas que possam representar novas oportunidades de pesquisa. Este trabalho, juntamente com os demais colaboradores desta pesquisa, coletou essas informações sobre segurança em SCADA em artigos anteriormente publicados, para a realização de um estudo de mapeamento sistemático. Segundo [Trigueiro 2011], um estudo de mapeamento é um tipo de estudo secundário que permite ao pesquisador ter um resultado consistente acerca de publicações em uma determinada área. Esse tipo de estudo pode prover um resumo visual (como um mapa), e fornecer uma visão geral de uma área de pesquisa, identificando a quantidade, os tipos de busca e os resultados disponíveis

3.1.1 Protocolos de Pesquisa

O primeiro passo no mapeamento é a definição de um protocolo de pesquisa, que serve para auxiliar na condução do estudo. De acordo com [Petersen et al. 2008], este pode ser organizado nas seguintes etapas :

1. Estabelecer questões da pesquisa;
2. Coleta de estudos primários;
3. Selecionar os artigos coletados;
4. Palavras-chave de resumos;
5. Extração dos dados e mapeamento.

3.1.2 Questões de Pesquisa

O principal objetivo desse estudo de mapeamento sistemático é entender como as publicações estão relacionadas à segurança dos sistemas SCADA. Para alcançar esse objetivo, foram construídas as seguintes Questões de Pesquisa:

- Quais são os principais locais de publicação? Conferência, Workshop ou Revista?
- Quais são as instituições e pesquisadores mais influentes sobre o assunto?
- Quantas publicações foram realizadas ao longo dos anos sobre o assunto?
- É possível classificar as pesquisas seguindo uma taxonomia? Caso positivo qual?

3.1.3 Estratégia de Pesquisa

Para este estudo, foram utilizadas como ferramentas de pesquisa o *IEEE Xplore*, a *ACM Digital Library* e o *ScienceDirect*. O acesso irrestrito aos mecanismos de busca acima, fornecido pela UFPB através do portal Capes, motivou a escolha por essas ferramentas. Foi importante a calibração durante a seleção da *string* de busca para que os resultados fossem os mais precisos possíveis dentro do assunto em questão (segurança em SCADA). A seguinte *string* de pesquisa foi utilizada:

"SCADA AND Smart Grid AND Cyber Security"

Como resultado dessa busca, 135 artigos foram encontrados no IEEE, 27 através ACM e 401 pela Science Direct, totalizando em 563 artigos que foram incluídos na fase inicial do mapeamento.

3.1.4 Critérios de Exclusão

Após a coleta dos artigos e mediante os resultados obtidos pela string de busca aplicada nas ferramentas escolhidas, para cada um dos estudo, foi aplicado um conjunto de critérios de exclusão, sendo estes:

1. Trabalhos com conteúdo irrelevante em relação à área de pesquisa;
2. Trabalhos duplicados entre as diferentes ferramentas de pesquisa. O primeiro encontrado é incluído, as duplicações foram descartadas;
3. Estudos incompletos;
4. Trabalhos não escritos em inglês;
5. Trabalhos que não são estudos primários.

3.1.5 Tipos de Pesquisa

De acordo com [Petersen et al. 2008], são os seguintes protocolos de pesquisa para classificar os trabalhos:

- **Pesquisa de avaliação:** é a investigação de um problema prático ou implementação de uma técnica prática. Inclui também trabalhos como pesquisa, estudos de caso, etc;
- **Proposta de solução:** Um artigo que propõe uma nova técnica de solução ou ao menos uma melhoria significativa de uma técnica existente;
- **Pesquisa de validação:** Trabalhos que investigam as propriedades de uma proposta de solução. Experimentos em métodos de pesquisas, simulação, análise matemática, etc;
- **Artigo filosófico:** Artigos que tratam de uma nova solução conceitual ou teoria;
- **Artigo de experiência pessoal:** Artigos que contém uma lista de lições aprendidas pelo autor através de suas experiências.

3.1.6 Taxonomia da Classificação

A classificação dos tipos de pesquisa foi relacionada com outras facetas. No estudo, foi construída a relação com os seguintes itens:

- **Tipo de ataque:** Estudos relacionados que lidam com Falsificação (*spoofing*, injeção de dados falsos, *replay*, sequestro ...), Reconhecimento (varredura, análise de tráfego, *man-in-the-middle* ...), Exaustão de recursos (*DoS*, consumo de recursos ...), Fragmentação, Malware (*worms*, vírus, *spywares* ...) ou não especificado.

- **Tipo de vulnerabilidade:** Qual vulnerabilidade foi explorada no estudo, podendo ser de *hardware*, *software* e/ou de comunicação.

- **Mecanismos de segurança:** Estudos que utilizam de criptografia, sistemas de prevenção (sistemas de detecção de invasão, sistemas de prevenção de intrusos, *firewall*, ...), sistemas de configuração (novas abordagens ou protocolos) ou não especificados.

- **Objetivo do estudo:** Relacionar os estudos com foco em ataque, defesa ou vulnerabilidade.

- **Princípios de segurança afetados:** Se os estudos relacionados lidam com Confidencialidade, Integridade e/ou Disponibilidade.

3.1.7 Executando o Mapeamento Sistemático

Para sua execução, o processo de mapeamento foi dividido em dois estágios, sendo estes:

- **Estágio 1:** Análise do título e do resumo de todos os artigos para compará-los com os critérios de exclusão;

- **Estágio 2:** Leitura mais aprofundada dos artigos selecionados para coletar dados e classificá-los de acordo com o tipo de pesquisa.

A Figura 8 demonstra o processo de mapeamento de acordo com o número de artigos analisados em cada etapa.

Figura 8: Etapas do Mapeamento (Imagem autoral)

Na primeira coluna da Figura 8 encontram-se as etapas, onde são respectivamente: os estudos coletados, o estágio 1 e o estágio 2. Em seguida, a segunda coluna apresenta a descrição de cada estágio, no qual os estudos coletados representam os estudos relevantes identificados pelas ferramentas de busca, o estágio 1 indica os estudos excluídos baseados nos critérios de exclusão e o estágio 2 a coleta de dados e classificação dos estudos incluídos. A terceira coluna contém o número de artigos referente a cada estágio, onde há 563 artigos no estágio da coleta de estudos e 259 artigos para o estágio 1 e para o estágio 2. Nota-se que mais da metade dos trabalhos indexados foram excluídos por algum dos critérios de exclusão. Conjectura-se que muitos dos estudos excluídos apresentam o título, resumo e palavras-chave que não representam claramente o assunto em questão abordado pelo artigo.

3.1.8 Resultados Obtidos

A partir dos estudos que foram incluídos neste mapeamento e os dados obtidos resultantes da classificação dos 259 artigos (que estão dispostos em um período de tempo entre 2005 e 2020), foi possível responder às questões de pesquisa definidas anteriormente. Os resultados estão dispostos a seguir.

3.1.8.1 Locais com mais Publicações

Através da coleta de dados dos artigos analisados, extraiu-se as cinco principais conferências que receberam mais trabalhos incluídos no mapeamento, sendo tais resultados apresentados na Tabela 3 e explicados a seguir. Estima-se que as conferências listadas são mais predispostas nos tópicos relacionados à segurança da *smart grid*. É provável que grandes avanços da segurança dos sistemas SCADA e seus protocolos sejam discutidos nesses eventos, indicando que os pesquisadores e a indústria devem observar de perto os estudos apresentados nessas conferências.

Local	Nº de artigos
Renewable and Sustainable Energy Reviews	13
IEEE Transactions on Smart Grid	10
Computers & Security, International Journal of Critical Infrastructure Protection, International Journal of Electrical Power & Energy Systems	8
Electric Power Systems Research	7
The Electricity Journal	6

Tabela 3: Principais Locais de Publicações

Renewable and Sustainable Energy Reviews: trata-se de uma revista científica que publica artigos com foco em energias renováveis, é lançada 12 vezes por ano e publicada pela Elsevier [Journals Elsevier].

IEEE Transactions on Smart Grid: buscando disseminar resultados de pesquisas sobre *smart grid*, a revista publica pesquisas originais sobre teorias e desenvolvimentos acerca deste tema [IEEE Xplore].

Computers & Security: publicada pela Elsevier, é uma das revistas mais respeitadas relacionada à segurança em tecnologia da informação [Journals Elsevier].

International Journal of Critical Infrastructure Protection: lançada em 2008, é uma revista publicada pela Elsevier, com o objetivo de lançar artigos em todas as áreas de proteção de infraestrutura crítica [Journals Elsevier].

International Journal of Electrical Power & Energy Systems: concerne a uma revista com foco na produção, transmissão, distribuição e utilização de energia [Journals Elsevier].

Electric Power Systems Research: trata-se de uma revista com foco em publicar artigos originais e expor resultados na área de produção, transmissão, distribuição de energia [Journals Elsevier].

The Electricity Journal: Referência na área de diversidade de combustíveis e otimização de performance do setor elétrico, a revista tem como objetivo reunir os pensadores mais influentes do mundo inteiro [Journals Elsevier].

3.1.8.2 Artigos mais Citados

Além dos meios de publicações, também é importante entender quais artigos foram os mais citados por outros estudos e quais são as suas contribuições. A Tabela 4 apresenta os cinco artigos que receberam o maior número de citações em outros estudos.

Título	Autores	Nº de Citações
Cyber–Physical System Security for the Electric Power Grid	S. Sridhar; A. Hahn; M. Govindarasu	406
Cyber Security and Privacy Issues in Smart Grids	J. Liu; Y. Xiao; S. Li; W. Liang; C. L. P. Chen	232
Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure	G. N. Ericsson	223
Vulnerability Assessment of AC State	G. Hug; J. A.	

Estimation With Respect to False Data Injection Cyber-Attacks	Giampapa	194
On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures	J. Kim; L. Tong	121

Tabela 4: Artigos Mais Citados do IEEE e ACM

Os artigos presentes na Tabela 4 provém do acervo do IEEE e da ACM. Os oriundos ScienceDirect não estão presentes nesta contagem, pela justificativa que a mesma não fornece o número de citações que cada artigo possui, desta forma, não sendo possível incluí-los. Para maior entendimento do que cada um dos artigos mais citados abordam, tem-se um breve resumo a seguir.

É apresentada uma abordagem em camadas em *"Cyber–Physical System Security for the Electric Power Grid"* [Sridhar et al. 2012], para avaliar os riscos com base na segurança dos aplicativos de energia física e da infraestrutura cibernética de suporte. Os autores também discutem questões de segurança para mitigar ataques cibernéticos.

Em *"Cyber Security and Privacy Issues in Smart Grids"* [Liu et al. 2012] é apresentada uma visão geral sobre questões relevantes acerca da segurança cibernética e privacidade em *smart grids.* O trabalho discute vários campos de pesquisa em potencial com base nas literaturas atuais da sua época de publicação.

Em *"Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure",* [Ericsson 2010] trata de questões de segurança cibernética como importantes soluções para *smart grid* e destaca pontos de acesso em uma subestação. Além disso, a modelagem do domínio de segurança da informação também é discutida no trabalho.

Novas técnicas analíticas para executar a análise de vulnerabilidade da estimativa de estado são propostas pelos autores em *"Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks*" [Hug et al. 2012]. Estas, servem para quando o sistema está sujeito a um ciberataque oculto de injeção de dados falsos no sistema SCADA, em uma rede elétrica. É apresentado um algoritmo baseado na teoria dos grafos, que permite determinar quantos e quais sinais de medição

um invasor na rede atacará.

Em *"On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures"* [Kim et al. 2013], é proposto métodos de ataques testados em sistemas IEEE 14-bus e IEEE 118-bus e, logo após, é demonstrado seus efeitos. Também são consideradas contramedidas para evitar tais ataques.

3.1.8.3 Autores com mais Publicações

O conhecimento dos pesquisadores mais influentes e das instituições que eles representam ajuda a entender onde estão as maiores contribuições relacionadas à segurança em SCADA, sendo provável esperar que novas pesquisas e possíveis soluções para problemas existentes sejam desenvolvidas por estes. A Tabela 5 lista os pesquisadores com mais publicações dentre os estudos analisados.

Autores	**Nº de Publicações**
Cristina Alcaraz	7
Javier Lopez, M. Govindarasu	6
H. T. Mouftah	5
Béla Genge, C. Liu, K. McLaughlin, M. M. Hasan, S. Sezer, Y. Yang	4

Tabela 5: Autores Mais Citados

A Sra. Cristina Alcaraz é Ph.D. em Ciências da Computação pela Universidade de Málaga, na Espanha, onde atua como professora assistente no Departamento de Ciências da Computação. Seus principais interesses de pesquisa estão relacionados à proteção de infraestrutura crítica e, mais especificamente, à segurança de sistemas SCADA, sistemas ciber-físicos e sistemas de redes inteligentes e Internet industrial das coisas.

O Sr. Javier Lopez é Ph.D. é professor da Universidade de Málaga na Espanha. Ocupa o os cargos de Co-editor-chefe da *International Journal of Information Security* (IJIS), de membro sênior da ACM e IEEE, e também de membro do conselho editorial de veículos de publicações importantes como a Elsevier, John Wiley & Sons, Springer,

IOS Press, IET, IEEE, Inderscience Publishers e Emerald.

O Sr. Manimaran Govindarasu recebeu o Ph.D. em Ciência da Computação e Engenharia pelo Indian Institute of Technology (IIT), Chennai. Atualmente é professor de Engenharia de Computação no Departamento de Engenharia Elétrica e de Computação da Iowa State University, Estados Unidos. Seus interesses estão nas áreas de segurança de sistemas ciber-físico para *smart grids*, segurança cibernética, sistemas e redes em tempo real e Internet das Coisas (IoT - *Internet of Things*). Atuou como co-editor convidado das principais publicações do IEEE e é o presidente fundador da Força-Tarefa de Segurança Cibernética no Comitê de AMPS da *IEEE Power & Energy Society*.

O Sr. Hussein T. Mouftah é professor e pesquisador na Escola de Engenharia Elétrica e Ciência da Computação da Universidade de Ottawa, Canadá. É autor ou co-autor de 9 livros, 63 capítulos de livros, mais de 1300 artigos técnicos, 12 patentes e 142 relatórios industriais.

O Sr. Béla Genge é Ph.D. em segurança de redes pela Universidade Técnica de Cluj-Napoca na Romênia e pós doutor no Instituto de Proteção e Segurança do Cidadão, na Itália. Atualmente, é bolsista Marie Curie, professor associado e chefe do Departamento de Ciência da Computação da Universidade de Medicina, Farmácia, Ciências e Tecnologia de Târgu Mureş (UMFST), Romênia. Ele é autor de vários artigos em revistas especializadas e seus interesses de pesquisa incluem segurança e resiliência de sistemas de controle em rede e segurança na Internet Industrial das Coisas.

O Sr. Chen-Ching Liu é professor destacado da Boeing em Engenharia Elétrica e diretor do Centro de Inovação de Sistemas de Energia (ESIC) da *Washington State University*, Pullman, Estados Unidos. Também é professor visitante na Escola de Engenharia Mecânica e de Materiais da University College Dublin na Irlanda e atuou como Presidente do Conselho ISAP e Presidente do Conselho de Administração.

O Sr. Kieran Mclaughlin é atualmente o líder de pesquisa em segurança de rede de Sistemas de Controle Industrial (ICS - *Industrial Control Systems*) para SCADA, *smart grid* e infraestruturas críticas. Seus interesses incluem tecnologias para detecção e prevenção de intrusões usando o protocolo ICS / SCADA, técnicas de análise comportamental e com estado e análise de vulnerabilidade e comportamento do ataque

ICS.

O Sr. Md. Mahmud Hasan é Ph.D. em Engenharia Elétrica e de Computadores pela Universidade de Ottawa no Canadá. Sua experiência industrial inclui operação e manutenção de equipamentos de telecomunicações de vários fornecedores. Seus interesses atuais de pesquisa incluem otimização de rede, análise de dados, alocação de recursos e aprimoramento de cibersegurança em operações de redes inteligentes.

O Sr. Sakir Sezer é Ph.D. pela *Queen's University Belfast* no Reino Unido e é o Diretor e Chefe da Pesquisa de Rede e Cibersegurança do Centro de Tecnologias de Informação Segura (CSIT) da *Queen's University Belfast*. Ele é uma autoridade de renome mundial em processamento de rede de alto desempenho e tecnologias de segurança da Internet e suas pesquisas lideram grandes avanços. Ele é membro de vários comitês executivos e de pesquisa.

O Sr. Yi Yang é formado em engenharia elétrica pela Universidade de Ciência e Tecnologia Huazhong, Wuhan na China e Ph.D. em engenharia elétrica e eletrônica pela *Queen's University Belfast* no Reino Unido. Seus interesses atuais de pesquisa incluem segurança cibernética em *smart grids* e já atuou como presidente da sessão e como membro do comitê do programa técnico em inúmeras conferências e simpósios internacionais.

3.1.8.4 Quantidade de Artigos Publicados ao Longo dos Anos

A Figura 9 apresenta um gráfico com a quantidade de publicações entre os anos de 2005 a 2020. Observa-se através do ano do artigo mais antigo incluído no estudo (2005), o quão recente é esse campo de pesquisa. A partir da mesma figura, também é possível verificar um crescimento considerável começando no começo dessa década e estendendo-se até os dias atuais. Conjectura-se que seja devido aos ataques recentes aos sistemas SCADA como o que ocorreu no Irã em 2010 e na Ucrânia em 2015, além do crescimento da relevância do assunto em questão.

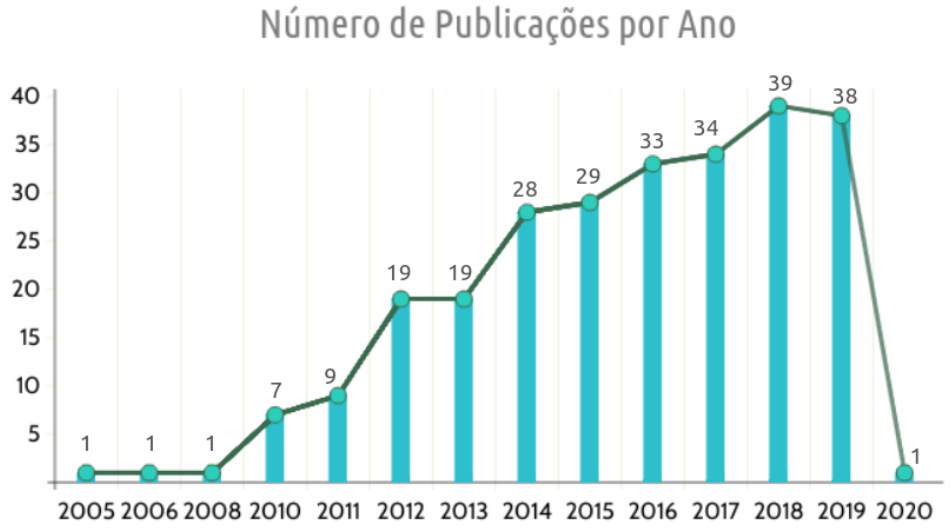

Figura 9: Quantidade de Publicações por Ano (Imagem autoral)

Para o presente estudo, os artigos foram coletados entre o final de agosto e começo de setembro de 2019. Apesar dos 4 meses restantes para o final deste ano, 2019 possui quase mesma quantidade de artigos publicados do que no ano anterior. Provavelmente o estudo datado com ano 2020 trata-se de um artigo de revista que só irá ser publicado no ano de 2020.

3.1.8.5 Fundamentos da Segurança

Com uma análise mais aprofundada dos estudos, foi possível analisar as relações entre as várias sub-áreas de segurança em SCADA. Uma dessas áreas de conhecimento trata-se dos princípios segurança da informação, que foi construída sob três conceitos fundamentais: Confidencialidade, Integridade e Disponibilidade, conforme presente na Figura 10 a seguir.

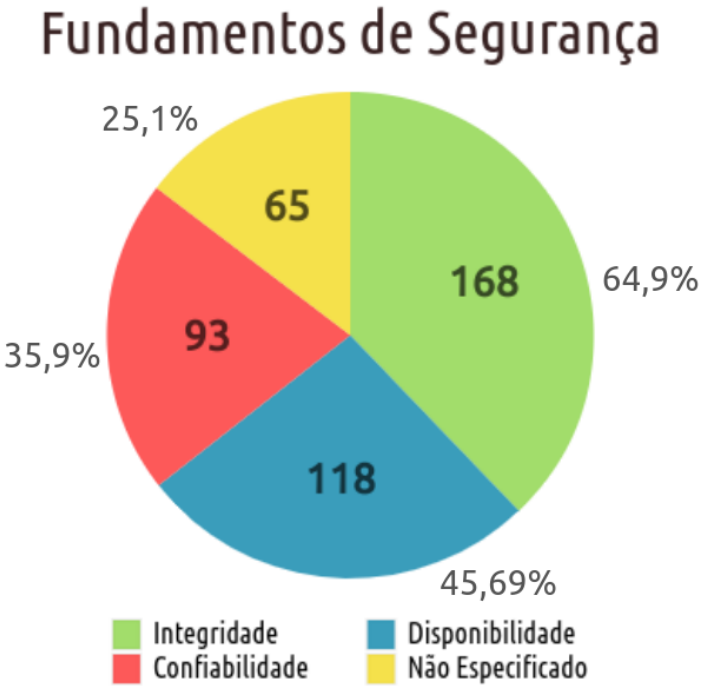

Figura 10: Fundamentos da Segurança Abordados nos Artigos (Imagem autoral)

Com base na Figura 10, é possível observar uma quantidade maior de menções a disponibilidade e integridade em relação às outras alternativas. Isso é decorrente de que a confidencialidade dos dados não é algo crítico para os sistemas SCADA, apesar da importância desta para a *smart grid* no domínio do cliente (onde é preciso preservar as informações pessoais). Em contrapartida, para o SCADA, a disponibilidade dos dispositivos é imprescindível, pois este executa suas funções e envia os dados em tempo real. A integridade dos dados transmitidos também é de suma relevância, visto que estes são responsáveis por determinar as medidas de controle. Conjectura-se que a maior menção a integridade também deve-se a integração da *smart grid* com a Internet, pois com dados sendo transmitidos através da rede, torna-a mais vulnerável do que antes quando os dispositivos estavam fisicamente protegidos e a rede era apenas interna. Caso estes dados sejam modificados por um atacante, este pode induzir comandos de controle equivocados e gerar danos ao sistema.

3.1.8.6 Objetivos do Estudo

Dentre os artigos avaliados, foi realizada uma classificação de acordo com seu objetivo, sendo estes: um método de defesa, o impacto causado por um ataque e vulnerabilidades no sistema. A Figura 11 exibe os resultados obtidos na pesquisa mediante a esta classificação.

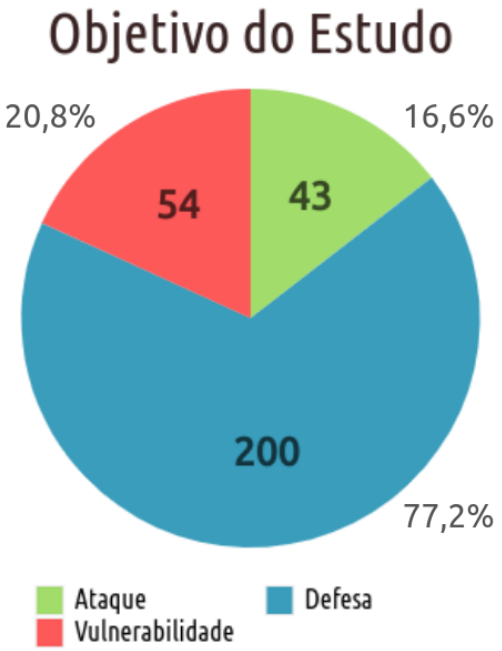

Figura 11: Dados da Classificação de Acordo com o Objetivo de Estudo do Artigo (Imagem autoral)

Como observado, a maior parte dos artigos analisados focaram em algum método de defesa. Isso demonstra a preocupação atual em tornar o sistema SCADA mais seguro, a fim de evitar que futuros ataques possam continuar a causar perdas significativas. Em seguida, os estudos sobre vulnerabilidades foram os segundos mais enfatizados nos trabalhos. Este, ajuda a compreender quais os problemas (sejam nos protocolos, *softwares* ou dispositivos utilizados) mais comumente enfrentados, podendo também servir de base para novos métodos serem desenvolvidos ou para melhoria dos já existentes. Por último, é demonstrado que estudos que possuem ataques como objetivo foram os menos presentes dentre os artigos analisados. Apesar deste resultado, é importante afirmar que o estudo de ataques são essenciais para o entendimento e para

o desenvolvimento de técnicas de defesa. Ademais, também podem auxiliar a lidar com a recuperação da rede em cenários de pós ataque.

3.1.8.7 Vulnerabilidades Exploradas

Mediante o conhecimento das vulnerabilidades comumente mais exploradas nos estudos, é possível compreender quais partes do sistema SCADA (*software*, *hardware* ou protocolos de comunicação) necessitam de uma maior proteção. Na Figura 12 é demonstrado quais destes tiveram suas vulnerabilidades mais expostas nos artigos analisados.

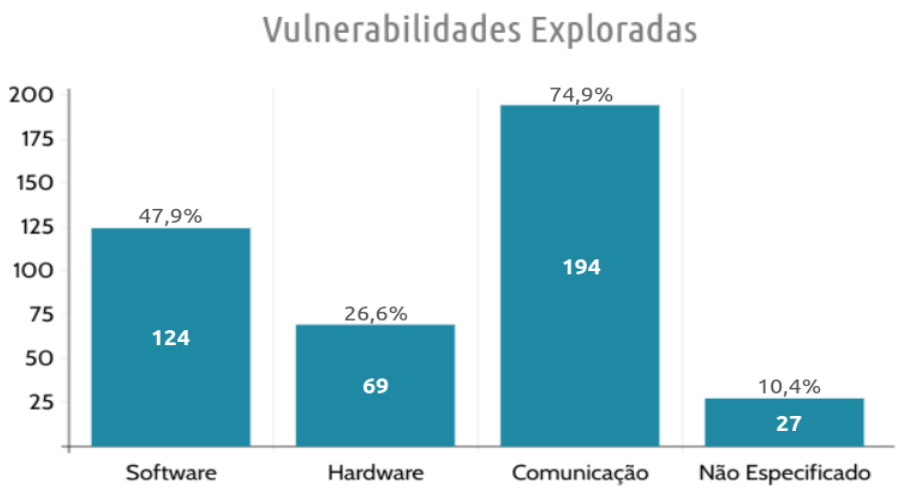

Figura 12: Vulnerabilidades mais Exploradas (Imagem autoral)

Como observado, a maior parte dos estudos exploram falhas nas comunicações dos sistemas SCADA. Atualmente, com o uso intensivo da Internet para a comunicação nas *smart grids* sem que haja uma maior preocupação com a segurança, é possível que várias fraquezas nos protocolos de comunicação sejam exploradas. Através de análises mais detalhadas nestes estudos, foi observado que as vulnerabilidades mais investigadas eram relativas aos protocolos Modbus e DNP3.

Seguindo como o segundo mais debatido, o *software* do sistema SCADA também possui diversas vulnerabilidades que são analisadas nos estudos classificados. Apesar do *hardware* ser suscetível a ataques (como por exemplo sabotagem de um

funcionário insatisfeito), corre um risco menor que o *software* e protocolos de comunicação por estar mais protegido, devido ao isolamento geográfico das usinas.

3.1.8.8 Relação entre Tipo de Pesquisa, Tipo de Ataque e Método de Defesa

A partir dos dados coletados na classificação, foi possível construir um gráfico que relaciona os tipos de pesquisa definidos com os principais tipos de ataques e métodos de defesa discutidos na literatura. A Figura 13 mostra a relação entre esses três parâmetros em um gráfico bolha.

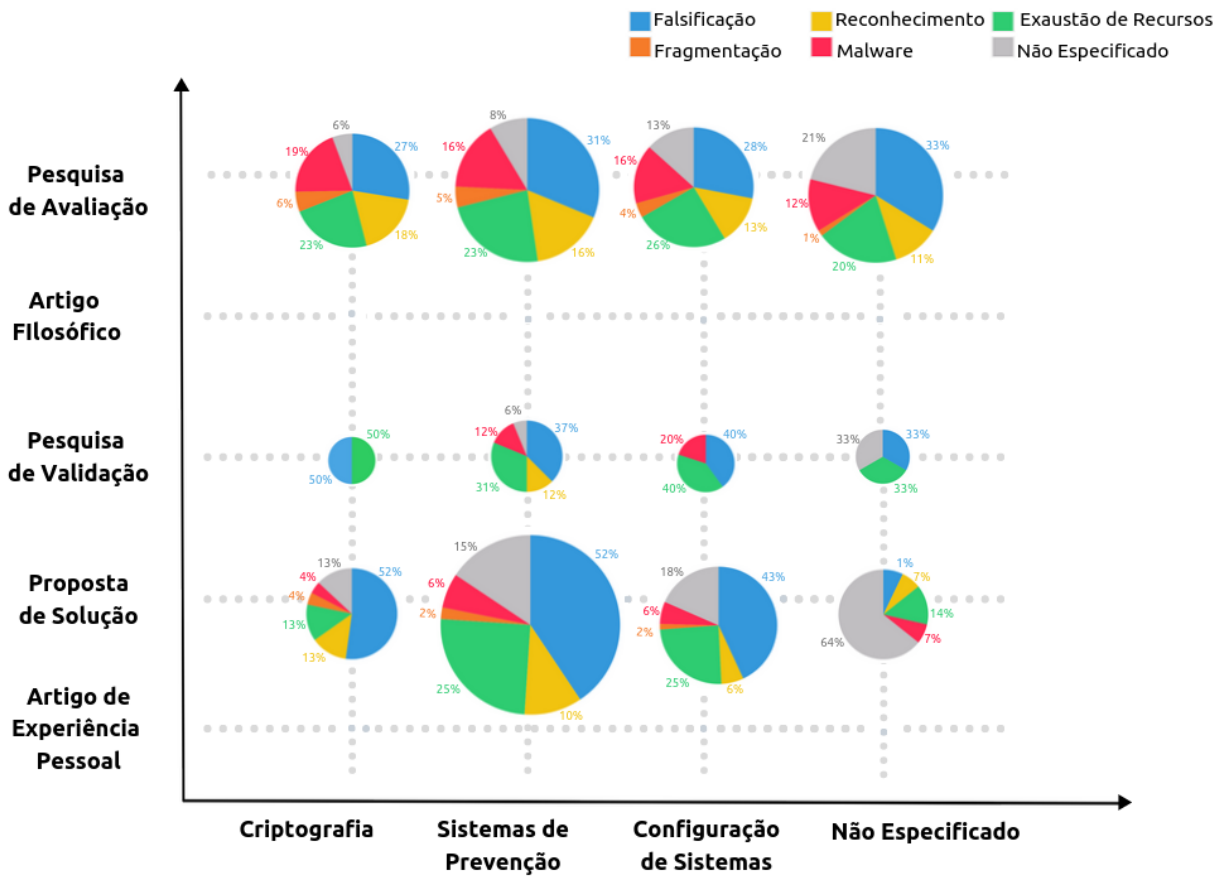

Figura 13: Gráfico Bolha Tipo de Pesquisa X Método de Defesa X Tipo de Ataque (Imagem autoral)

É possível observar que existem subáreas bem desenvolvidas, como Propostas de Solução com Sistemas de Prevenção. Porém, nota-se também que existem lacunas pouco exploradas pelos pesquisadores, como Pesquisa de Validação, e a ausência de trabalhos classificados como Artigo de Experiência Pessoal ou Artigo Filosófico. Conjectura-se que a maioria dos estudos é de Propostas de Solução e Pesquisa de Avaliação, devido a necessidade da busca por novas formas de proteger o SCADA.

É exposto na parte dos ataques um grande número de pesquisas relacionadas a ataques de falsificação. Estudos mais aprofundados nestes artigos apontaram que muitos tratam-se de ataques de injeção, conhecido como *False Data Injection*, que modifica os dados que o SCADA recebe para estimar o estado da rede, podendo assim levar ao sistema realizar os comandos de controle de forma equivocada. É possível também perceber que todos os tipos de métodos de defesa foram utilizados para tais ataques, seja estes criptografia, métodos de prevenção (como IDS e afins) e também diferentes configurações para que desta forma a rede torne-se mais resistente.

Os ataques de exaustão de recursos (como ataques de negação de serviço) e *malwares* também foram bastante mencionados nos estudos. O último teve o *worm* Stuxnet atuando como um dos mais citados. Os tidos como de reconhecimento aparecem muito no contexto de ataques coordenados, onde estes podem obter informações sobre a rede e através destas auxiliar atacantes a realizar ataques mais efetivos.

Além das informações anteriormente citadas, é importante salientar que pelo fato do SCADA realizar trocas de informações em tempo real, o uso de técnicas de criptografia pode ser pouco viável, devido que uma vez aplicadas, são capazes de atrasar a comunicação do sistema. Constatando isso, o gráfico da Figura 13 mostra que este método não foi muito empregado pelos pesquisadores. De igual modo, também no mesmo gráfico é notório que ataques de fragmentação não tiveram muitas menções nos estudos, dado que este ataque pode não ser tão efetivo para estes sistemas.

Capítulo 4

Resultados e Discussão

Este capítulo contém a apresentação dos ataques implementados, sendo estes *TCP Syn Flood*, Ataque ARP, Homem no Meio e Ataque de Reflexão, assim como os respectivos resultados decorrentes da implementação de tais ataques, apresentando posteriormente uma proposta de mitigação para o Ataque ARP e os resultados obtidos.

4.1 Cenário Experimental e Métricas

Para o presente estudo, os experimentos foram desenvolvidos a partir de nós virtuais, dispostos pelo software de virtualização *VMWare Workstation*, conectados entre si por meio do adaptador da rede configurado no modo *bridge*. Nesta condição, estão conectados diretamente pela rede física. Posto que tais dispositivos estão operantes, para implementar o Modbus / TCP, a pesquisa utilizou a linguagem de programação *Python* em conjunto com o *Scapy* para a implementação manual do protocolo. Este último é uma ferramenta de manipulação de pacotes capaz de forjar ou decodificar mensagens de um grande número de protocolos, com a possibilidade de enviá-los na rede e capturá-los, como também corresponder solicitações e respostas, além de outras funcionalidades [Especificação Scapy].

Correlacionado aos experimentos, foram definidas algumas métricas em conformidade com o estudo, sendo estas: integridade, confidencialidade e disponibilidade do sistema. Adicionalmente, também foi examinado o consumo da largura de banda da rede utilizado a ferramenta de monitoramento de rede *Bmon* (*Bandwidth* Monitor), que opera como um monitor de largura de banda e estimador de taxa confiável e eficaz em tempo real.

Na Figura 14 pode-se observar o cenário utilizado para a realização dos testes.

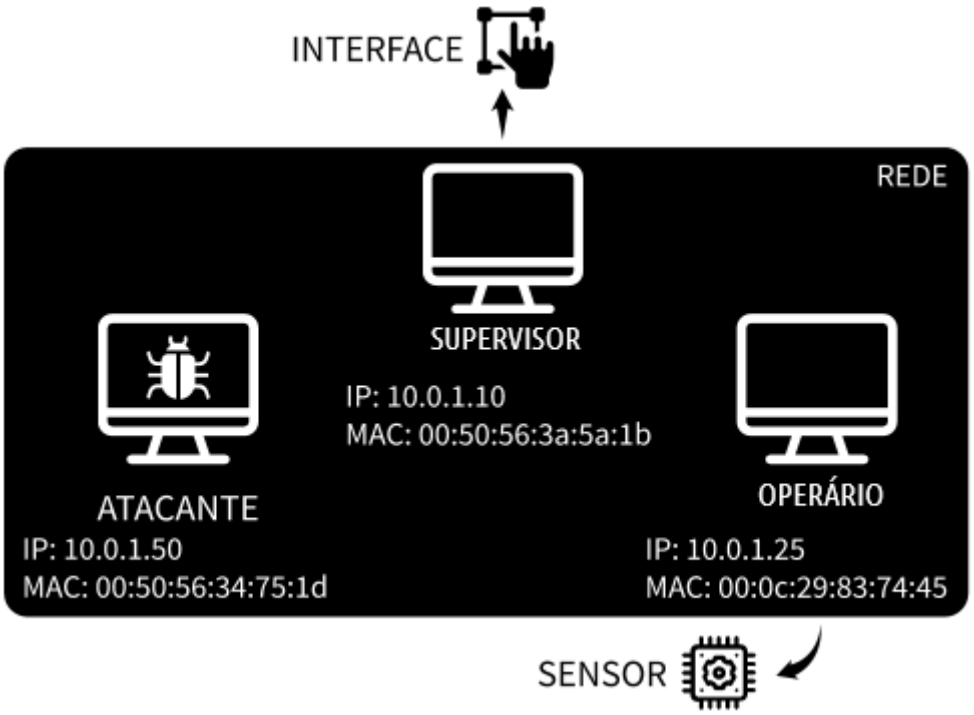

Figura 14: Cenário dos Experimentos (Imagem autoral)

Como constatado na Figura 14, o cenário construído é composto pelos seguintes dispositivos: máquinas RTU e MTU, HMI, sensores e uma máquina atacante. O primeiro destes atua como dispositivo operário, enquanto o segundo desempenha função de nó supervisor. Tendo esse princípio, e visto que a comunicação só pode ser iniciada pelo supervisor, para o RTU apenas é lícito operar mediante solicitação da MTU, recebendo comandos e enviando mensagens de respostas de volta ao supervisor. Conformemente, o atacante refere-se a um invasor na rede cujo o propósito é acometer o funcionamento do sistema seja na integridade, disponibilidade ou confidencialidade. Para o caso destes experimentos, o objetivo do invasor é afetar a disponibilidade da rede mediante dos ataques de reflexão e *TCP Syn Flood*. Complementarmente, o nó malicioso operou ainda como um homem no meio, executando o ataque homônimo que corrompe a integridade da mensagem e a confidencialidade e integridade do sistema. O mesmo dano ao sistema ocorre na implementação do Ataque ARP.

Conforme mencionado na Tabela 2 presente subsubseção 2.3.6, para a realização destes ataques, o invasor precisa estar na mesma rede que os hosts vítimas, não sendo do escopo dos experimentos realizados demonstrar como os atacantes passam pelos mecanismos de defesa (caso existente, como *firewalls* e IDS) e infiltram-se na rede. No

cenário dos experimentos realizados neste documento, verifica para os casos de que o invasor já está ingresso na rede, seja porque conseguiu passar pela defesa do sistema ou devido a ter obtido acesso de algum modo (como um funcionário mal intencionado ou um *spy hacker*), e desta forma então, consegue explorar as vulnerabilidades presentes no sistema e seus protocolos de comunicação.

4.2 Ataques Implementados

Foram escolhidos quatro ataques para serem implementados, sendo estes o TCP *Syn Flood*, ataque no ARP, do Homem no Meio e ataque de Reflexão. A escolha destes foi dada em virtude ao cenário definido (onde o atacante encontra-se dentro da rede), e também devido ao impacto desses ataques, de acordo com a Tabela 2, onde foram avaliados com alto impacto.

4.2.1 TCP Syn Flood

Conforme apresentado na fundamentação teórica, a realização do *TCP Syn Flood* ocorre quando o invasor inunda o sistema destino com solicitações de conexão, ambicionando interromper o sistema. Para a implementação deste, o *script* foi reproduzido no nó invasor, e quando executado, tem a função de inundar a vítima com pacotes Modbus na porta 502 (reservada unicamente ao protocolo). A cada nova mensagem remetida, o atacante substitui seu próprio endereço IP por um novo, gerado aleatoriamente, e envia inúmeras e sucessivas mensagens Modbus / TCP para a vítima em questão. Após inundar o alvo, cumpre em possivelmente consumir toda a largura de banda disponível e interrompe sua comunicação com os demais dispositivos da rede. Quanto mais abundante o número de mensagens oriundas do invasor na rede, maior o consumo da mesma.

A Figura 15 a abaixo apresenta a ilustração deste ataque.

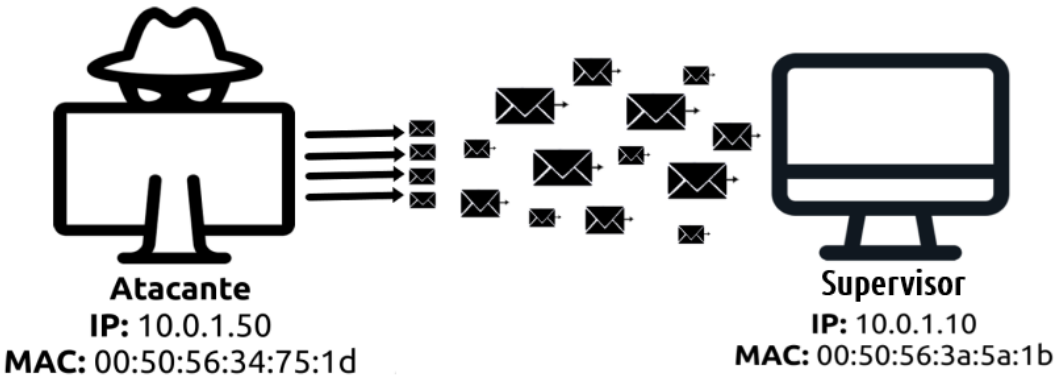

Figura 15: Ilustração do Ataque de TCP Syn Flood (Imagem Autoral)

4.2.2 Ataque no ARP

Neste ataque, o invasor objetiva passar-se por outro host da rede visando estabelecer vizinhança com o alvo pretendido. Na implementação realizada neste trabalho, a vítima trata-se do supervisor, no qual o atacante ambiciona estabelecer vizinhança fingindo ser um nó operário. Caso bem sucedido, possibilita o envio de dados imprecisos todas as vezes que o supervisor solicita a aquele host, uma vez que este acredita estar comunicando-se com o operário.

Para tal, no *script* executado no host invasor, foi feito o uso da função *sniff*, cuja finalidade é capturar pacotes, permitindo realizar tais capturas através de filtros para deter apenas determinados tipos de pacotes. Deste modo, a função foi utilizada com filtragem das mensagens do tipo ARP, correspondente ao Protocolo de Resolução de Endereços - utilizado para conversão de endereços da camada de rede em endereços da camada de enlace. Mediante a esta função, o invasor “escuta” a rede a espera de mensagens ARP de solicitação, e quando captura um pacote correspondente, responde com uma nova mensagem ARP *Reply* contendo como origem o endereço IP do operário e seu próprio endereço de Controle de Acesso à Mídia (MAC - *Media Access Control*). Obtendo êxito, a tabela de endereços do supervisor vai associar o IP do operário ao MAC do atacante, e consequentemente, toda vez que este solicitar algo ao operário por meio de uma mensagem, ficará sujeita a ações maliciosas por parte do invasor, pois é este que responderá.

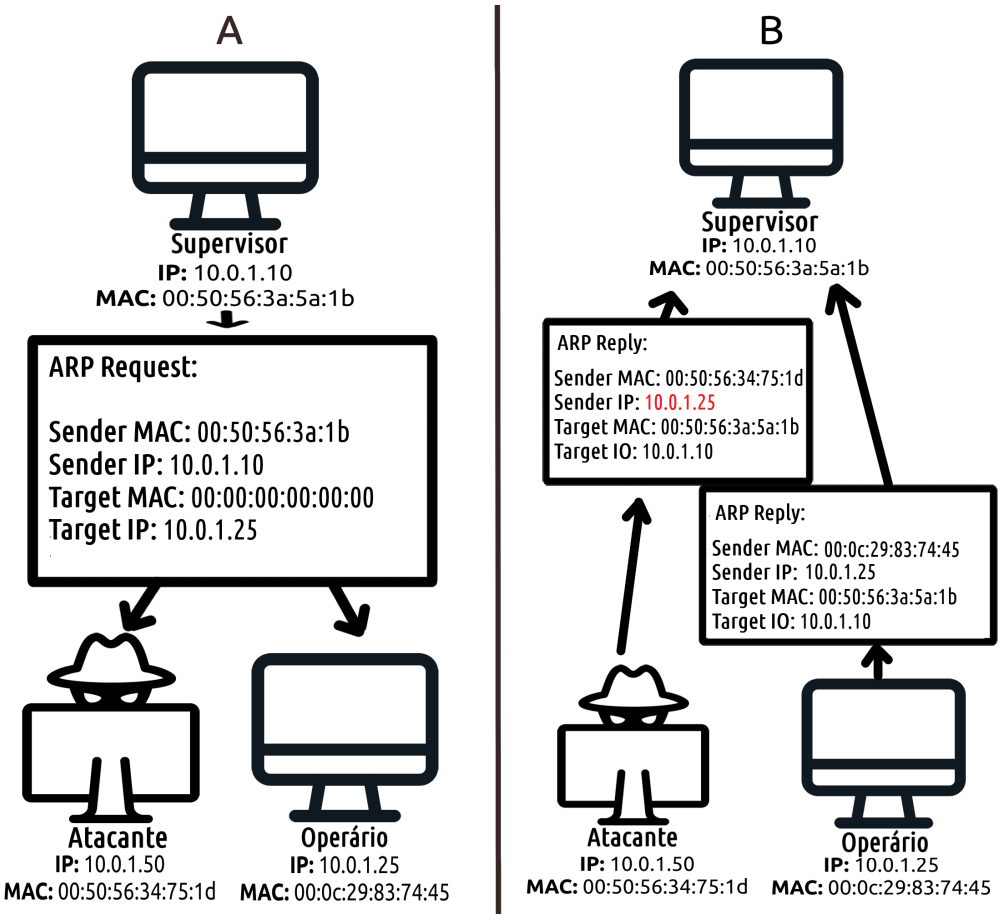

Figura 16: Ilustração Ataque no ARP (Imagem Autoral)

Na Figura 16 é possível observar a ilustração deste ataque, adequado com o cenário dos experimentos, onde o supervisor deseja estabelecer vizinhança com o operário. Para isso ocorrer, na parte A, o supervisor envia um ARP *Request* em *broadcast* (para todos os nós da rede), a fim de descobrir o endereço físico do host procurado. Neste tipo de mensagem, o campo *Target* IP corresponde ao endereço IP a ser resolvido e o campo *Sender* MAC ao endereço MAC da origem, evitando assim que o destino refaça o mesmo processo de resolução de endereço antes de responder.

Na parte B, após todos os nós da rede receberem a solicitação (incluindo o invasor), apenas o host que verifica seu próprio endereço IP contido no campo *Target* deveria responder informando seu endereço MAC em unicast (diretamente) para o supervisor. Todavia, o atacante também responde a essa solicitação conforme foi descrito acima, com um ARP *Reply* contendo como *Sender IP* o endereço IP do operário e seu próprio endereço MAC no campo *Sender* MAC.

É importante ressaltar que a vizinhança é estabelecida com a primeira mensagem recebida, sendo as demais ignoradas pela origem. Mediante a isto, no *script* deste experimento, o atacante envia sucessivas mensagens, a fim de obter maior chances de sucesso.

4.2.3 Homem no Meio

Na ocorrência deste ataque, o *script* efetuado pelo invasor desempenha o homem no meio, interceptando mensagens de comando e controle entre o MTU e o RTU. No cenário realizado neste experimento, o atacante deseja se passar como supervisor e forjar solicitações para o operário, sendo necessário que o ataque ARP seja previamente realizado para que a vítima tenha vizinhança estabelecida com o atacante. Inicialmente, utiliza-se da função *sniff* do *Scapy* para filtrar as mensagens destinadas à porta 502 (correspondente ao protocolo Modbus, como mencionado). Após a captura das mensagens anteriores, o atacante apodera-se de dados como IP de origem e de destino, entre outras informações expostas em texto plano, e, mediante a estas, envia uma nova mensagem Modbus /TCP contendo o endereço do supervisor(origem) e o do operário (destino) com qualquer conteúdo que desejar. Todavia, para conservar o disfarce, o atacante mantém o seu MAC, alterando apenas o endereço IP para o do supervisor, intencionando passar-se por ele e assim possibilitando a solicitação e envios de comando a fim de obter de informações e prejudicar o sistema, uma vez que a vítima acredita estar comunicando-se com o supervisor, comprometendo assim a integridade e confidencialidade do sistema. A Figura 17 contém a ilustração deste ataque, de acordo com o cenário dos experimentos, onde é possível visualizar o processo descrito do ataque.

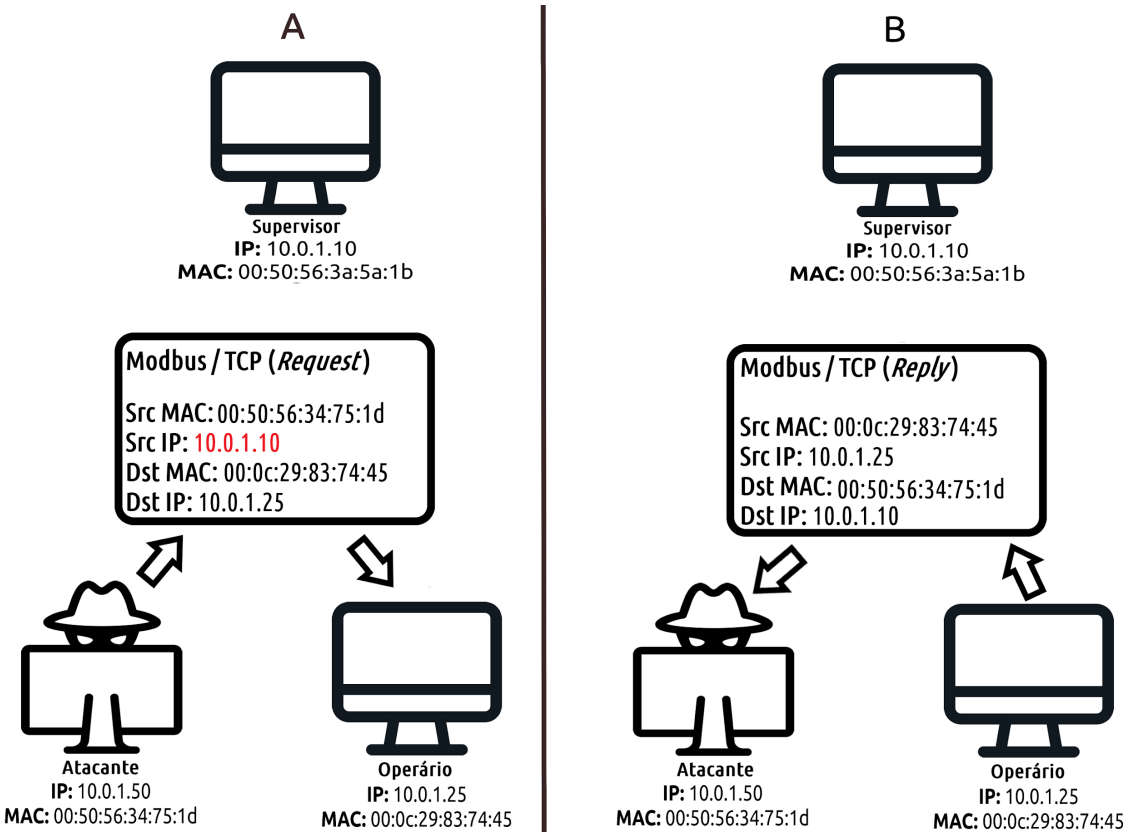

Figura 17: Ilustração Ataque do Homem no Meio (Imagem Autoral)

4.2.4 Ataque de Reflexão

A implementação desse ataque ocorre similarmente ao Homem no Meio, conforme emprega-se a função *sniff* com intuito de filtrar na rede mensagens destinadas também à porta 502. Com base nas capturas filtradas, o invasor obtém não apenas endereços *IPs* contidos no pacote, mas apropria-se ainda do MAC de origem e de destino. Subsequentemente, o atacante envia um pacote Modbus /TCP para o *host* operário, e diferente do ataque do homem no meio (que adultera apenas os campos que contém endereços IPs), é posto no campo *source* do pacote o *MAC* de origem do supervisor oriundo da captura. O intuito é que o operário destine a resposta desta mensagem ao MTU (nó supervisor). Caso seja bem-sucedido, múltiplas mensagens provindas do atacante com destino ao operário serão lançadas para que este replique ao supervisor, ocorrendo uma inundação em ambos que prejudicará (ou até esgotar) os recursos de disponibilidade da rede, além de acometer a integridade e confidencialidade do sistema.

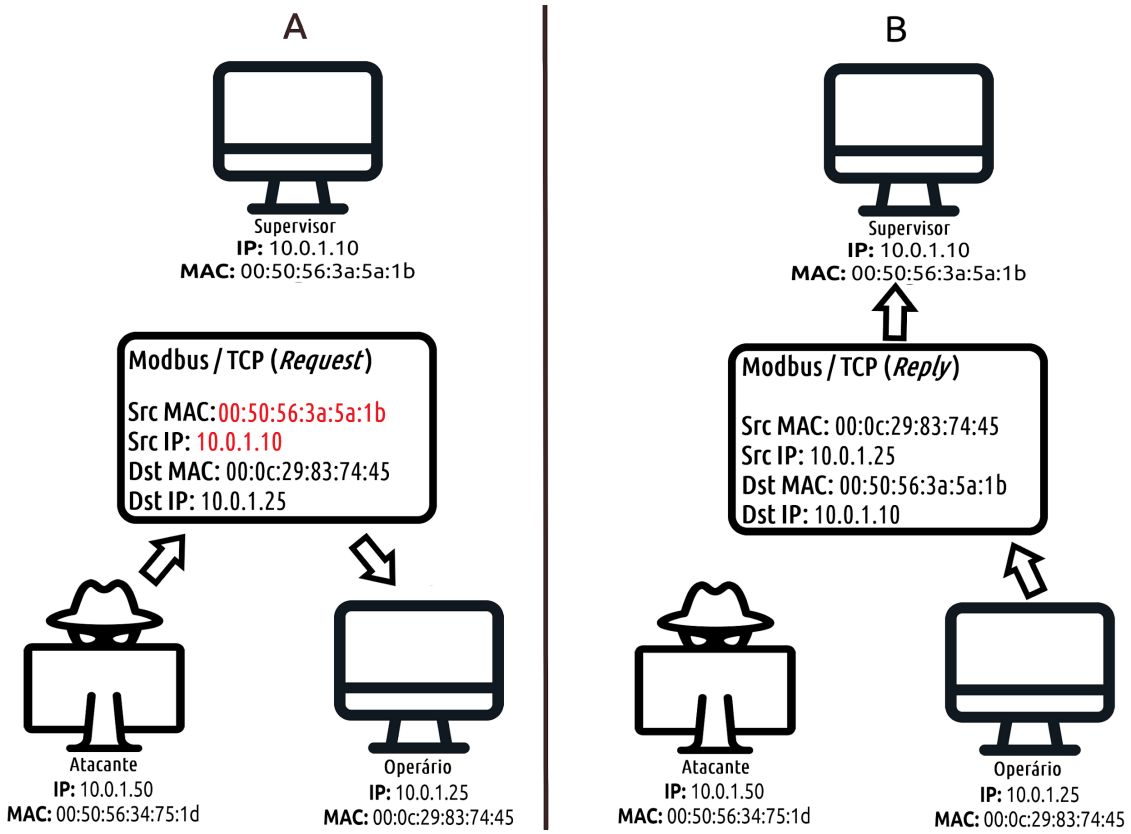

Figura 18: Ilustração Ataque de Reflexão (Imagem Autoral)

Na Figura 18 observa-se uma ilustração deste ataque, em conformidade com o cenário da implementação. A parte A corresponde ao envio por parte do atacante de uma mensagem de solicitação Modbus / TCP para o host operário, contendo o endereço IP e MAC de origem correspondente ao do supervisor. Na parte B, conforme mencionado, o nó operário responde esta requisição ao supervisor, uma vez que a acredita que a mensagem foi oriunda deste.

4.3 Resultados das Implementações

Tendo em vista que os ataques implementados foram avaliados como de alto impacto na Tabela 2, a seguir é apresentado através dos resultados das implementações o porquê desse impacto gerado, e como esses ataques exploram as vulnerabilidades do sistema e interferem no funcionamento da rede.

4.3.1 TCP Syn Flood

A Figura 19 exibe uma captura de tela de um pacote capturado pelo programa *Wireshark* no dispositivo supervisor, onde é possível observar as inúmeras mensagens modbus provenientes do atacante, demonstrando que a cada nova mensagem enviada, este substitui seu próprio endereço IP por um novo, gerado aleatoriamente.

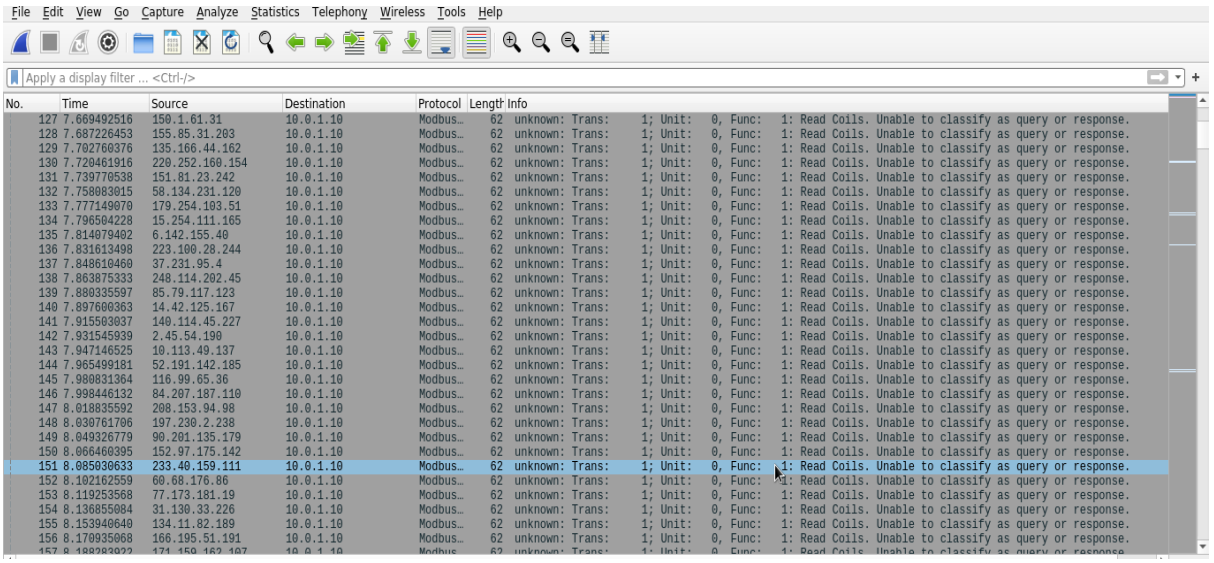

Figura 19: Captura mensagens TCP Syn Flood (Imagem Autoral)

Como resultado deste ataque, a Figura 20 apresenta um gráfico gerado pelo *Bmon*, que demonstra a taxa de dados recebida em *bytes* pelo tempo em segundos. Neste caso, o monitoramento foi verificado na MTU (supervisor), com o tráfego da rede regular e sem intermédio de ataques.

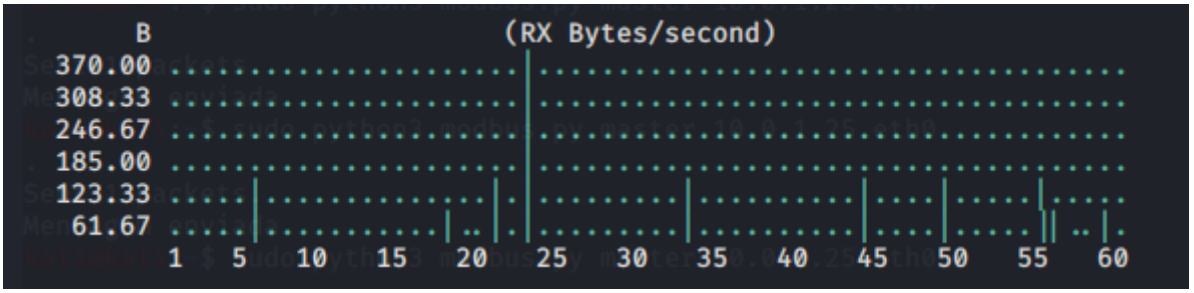

Figura 20: Gráfico do Tráfego de Rede Normal (Imagem Autoral)

Em contrapartida, a Figura 21 exibe o gráfico resultado do monitoramento do tráfego da rede também efetuado na MTU mas, nesta ocorrência, com a interferência do ataque *TCP Syn Flood*, onde nota-se uma ampliação significativa do consumo da rede. É importante acentuar que a Figura 20 indica a unidade em *bytes*, distinguindo-se da Figura 21 cuja unidade é *quilobytes* - equivalente a 1024 *bytes* -, evidenciando a diferença entre os dois gráficos e o êxito do ataque em ocupar a largura de banda da rede, que conforme visto, afeta a disponibilidade do sistema, gerando alto impacto.

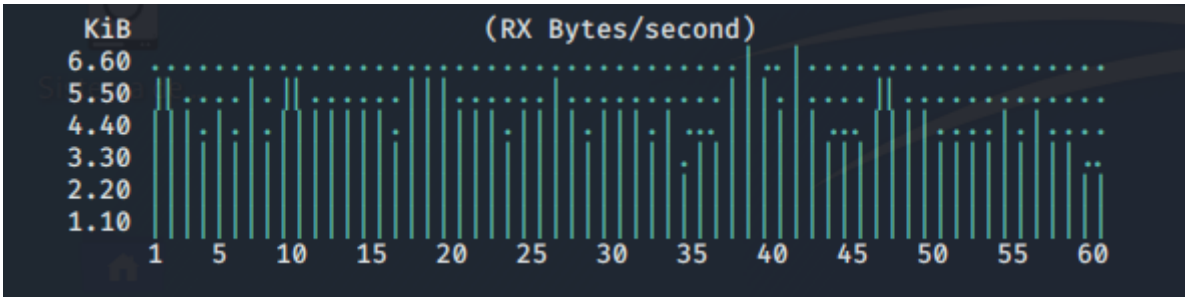

Figura 21: Gráfico do Tráfego de Rede com Ataque TCP Syn Flood.(Imagem Autoral)

4.3.2 Ataque no ARP

Tendo em vista o que foi abordado, o ARP trata-se de um protocolo que opera a fim de obter um endereço MAC de uma interface a partir de seu endereço IP. Para tal, conforme foi elucidado, no primeiro passo do estabelecimento de vizinhança, um host manda uma mensagem ARP *Request* e em conformidade com o cenário proposto, na Figura 22 vemos a captura deste pacote de solicitação enviado pelo nó supervisor para o operário.

```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VMware_3a:5a:1b (00:50:56:3a:5a:1b)
    Sender IP address: 10.0.1.10
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.1.25
```

Figura 22: Captura ARP Request (Imagem Autoral)

Após o recebimento desta e com finalidade de atender a requisição, é possível observar na Figura 23 a seguir que como esperado, o host operário (sem a interferência de nenhum ataque), respondeu à requisição de estabelecimento com um ARP *reply* contendo suas informações íntegras, para assim prosseguir a comunicação com o supervisor.

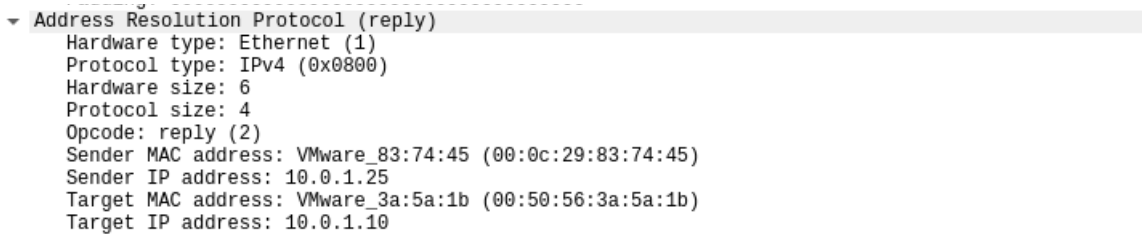

Figura 23: Captura ARP Reply (Imagem Autoral)

Todavia, quando esta mesma solicitação ocorre quando o *script* está sendo executado na rede a partir do host invasor, existem duas possibilidades iminentes. A primeira trata-se da mensagem de resposta do atacante chegar ao nó supervisor após o pacote verdadeiro enviado pelo operário contendo o *reply*, e caso esta ocorra, a mensagem falsa enviada pelo atacante é ignorada pelo solicitante. Na Figura 24, podemos ver que para esta circunstância, o Wireshark identificou a mensagem do invasor como duplicada, uma vez que a mensagem deste não foi a primeira a chegar.

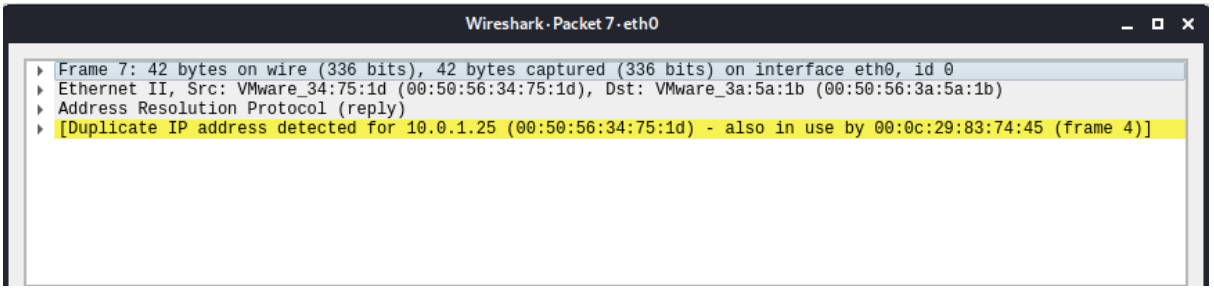

Figura 24: Captura ARP Duplicado (Imagem Autoral)

A segunda possibilidade, corresponde ao êxito do atacante, dado que sua resposta chegou primeiro ao host solicitante (o nó supervisor). Como é possível observar na Figura 25, este enviou um *reply* adulterado, contendo o endereço IP do operário no campo *Sender IP Address* (IP de Origem), e preencheu o campo *Sender MAC Address* (MAC de Origem) com o seu próprio endereço físico, desta forma

intencionando caracterizar-se como um nó operário. Por conseguinte, a tabela ARP do dispositivo supervisor irá associar o IP do operário com o MAC do atacante, recebendo respostas deste a cada solicitação. Na Figura 26 constata-se através do comando “arp -a” (que exibe as ligações entre os endereços físicos e os endereços lógicos relacionados à máquina), o sucesso do atacante em estabelecer vizinhança com a vítima, o que afeta a integridade do sistema e o deixa desprotegido para outros ataques e envios de dados imprecisos.

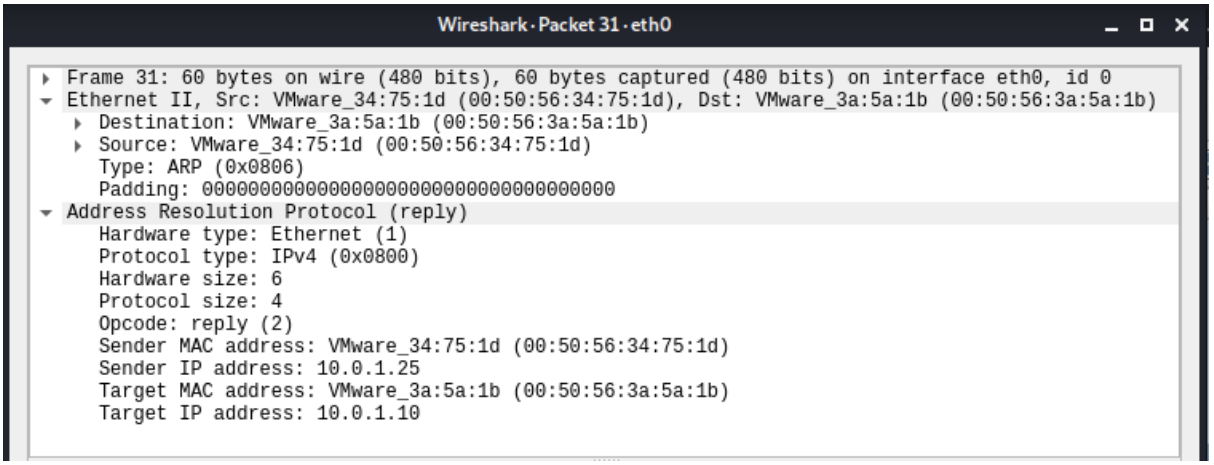

Figura 25: Captura ARP Reply do Atacante (Imagem Autoral)

Figura 26: Tabela ARP do Supervisor (Imagem Autoral)

4.3.3 Homem no Meio

A Figura 27 exibe uma captura de tela de um pacote capturado na MTU referente a mensagem Modbus enviada pelo Homem no Meio. É possível observar no quadro Internet Protocol Version 4, que o campo source (endereço de origem) apresenta o IP do operário e o campo destination (endereço de destino) compreende ao IP do supervisor. De igual modo, constata-se que no quadro *Ethernet II,* como destino, está contido o MAC dispositivo invasor e no *source* o MAC do operário. Isto ocorre pois conforme foi

exposto previamente, o atacante deseja disfarçar-se como supervisor e forjar solicitações para o operário.

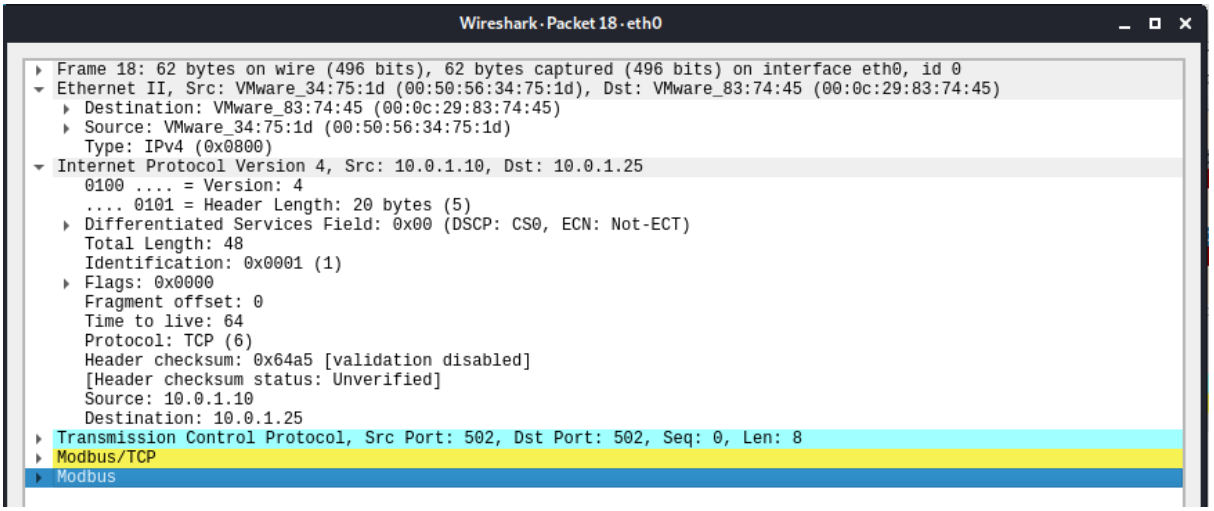

Figura 27: Captura do Pacote Modbus Enviado pelo Homem no Meio (Imagem Autoral)

Decorrente da mensagem recebida na Figura 27, o host operário envia uma mensagem de resposta direcionada ao remetente, representada a partir da Figura 28. É possível observar que a origem compreende ao IP do operário e o destino ao IP do supervisor. Também nota-se que o endereço MAC de destino (no campo *Src* no quadro *Ethernet II*) refere ao MAC dispositivo invasor, testificando desta forma, o êxito do ataque e a viabilidade de realizá-lo nos sistemas SCADA. Uma vez que esse ataque é bem sucedido, possibilita a interceptação, alteração e modificação de dados sensíveis, gerando um dano de alto impacto no sistema.

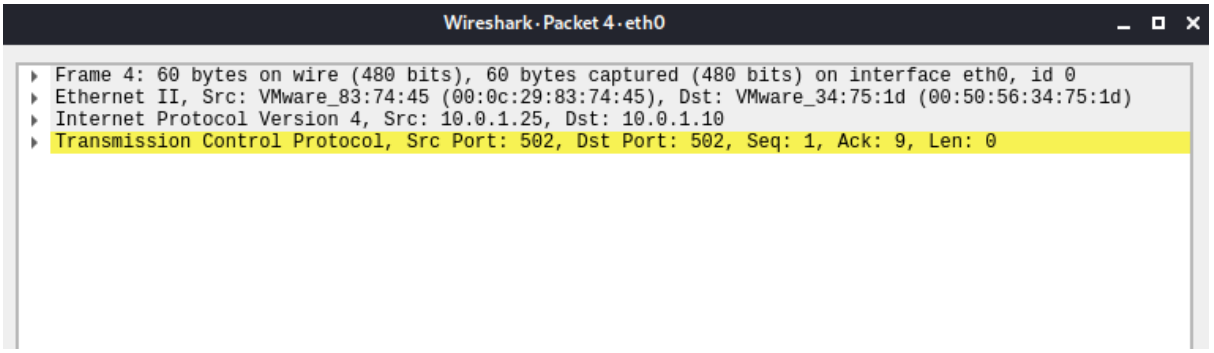

Figura 28: Captura pacote Modbus Enviado em resposta ao Homem no Meio (Imagem Autoral)

4.3.4 Ataque de Reflexão

Conforme como foi conceituado, neste ataque, um invasor na rede envia uma mensagem com o endereço IP falsificado da vítima do ataque para os hosts vítimas que que atuarão como reflectores. Como demonstração dos resultados, na captura de tela presente na Figura 29 é observado que o campo *source* (no quadro *Internet Protocol Version 4*) exibe o IP do supervisor no campo *destination* o *IP* do operário. Observa-se também que no quadro *Ethernet II* o campo *source* contém o *MAC* do supervisor o *destination* apresenta o *MAC* do operário. Isto significa que o host invasor enviou este pacote contendo as informações referentes ao supervisor.

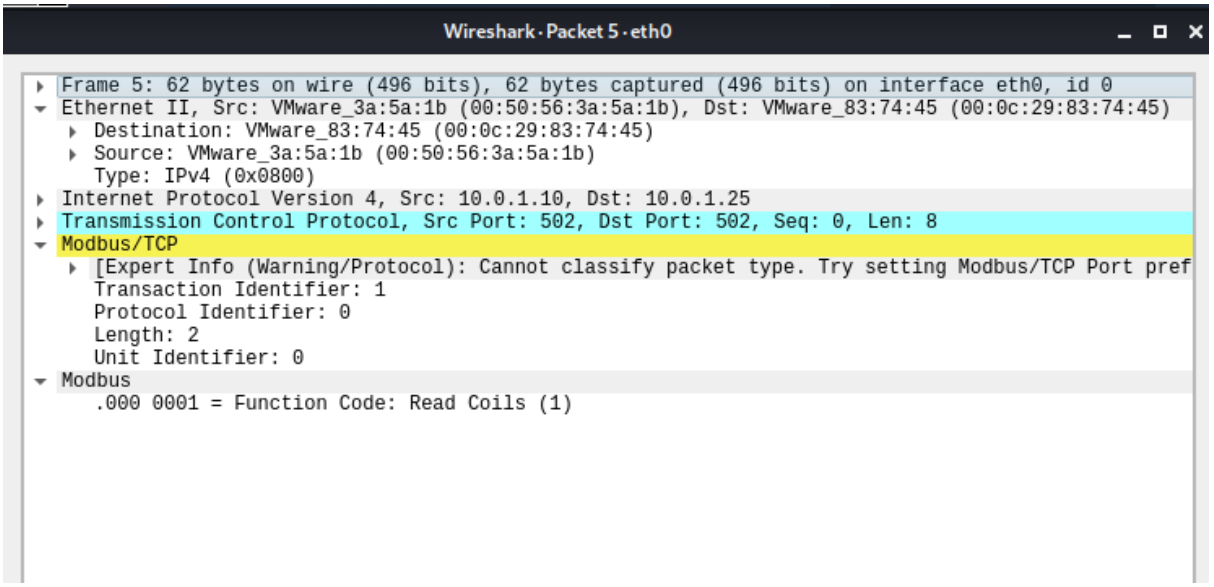

Figura 29: Captura do Pacote Modbus do Ataque de Reflexão (Imagem Autoral)

Mediante a esta mensagem recebida, é esperado que o host responda a esta solicitação sem quaisquer suspeitas. Comprovando esta suposição, a Figura 30 a seguir comprova que o host operário efetivamente compreendeu a mensagem como oriunda do supervisor, o respondendo e não ao invasor. Desta forma, infere o sucesso do ataque neste cenário, que como visto, compreendia a apenas um host operário. Para ter maior competência em consumir os recursos na rede, o atacante pode enviar esta mesma mensagem para inúmeros hosts, onde eventualmente reteria grande parte ou até mesmo esgotar seus recursos. Caso isto ocorra, afeta a integridade e disponibilidade do sistema,

impedindo a comunicação e causando um dano de alto impacto no funcionamento da rede.

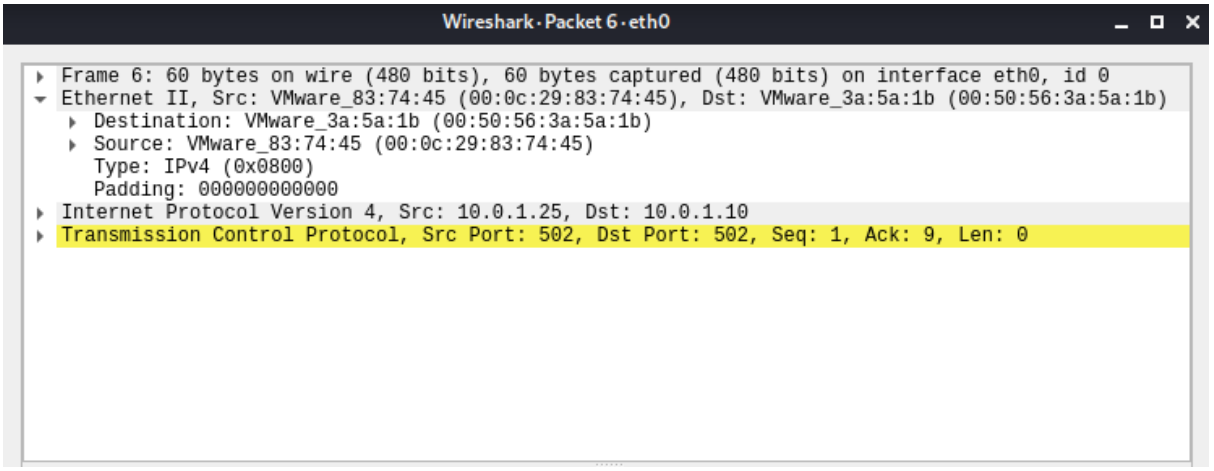

Figura 30: Captura do Pacote Modbus de Resposta ao Ataque de Reflexão (Imagem Autoral)

4.4 Propostas de Soluções

À medida que a Tabela 2 também informa contramedidas já existentes que podem servir para mitigar os ataques e, tendo em vista que não seria viável abordar soluções para todos os ataques implementados no tempo do mestrado, foi elaborada uma proposta apenas para o Ataque ARP. Sendo o estabelecimento de vizinhança o primeiro passo que é dado com a entrada de um novo host na rede, tornar esse passo inicial mais seguro pode vir a ser contramedida também para outros ataques, como por exemplo o do Homem no Meio. Na subsubseção a seguir é apresentada essa proposta de solução, juntamente com seu funcionamento, resultados e aplicabilidade em sistemas SCADA.

4.4.1 Proposta para Mitigação do Ataque no ARP

Devido às vulnerabilidades relacionadas ao ARP apresentadas na subsubseção 4.2.2, a proposta apresenta um mecanismo de defesa diferente dos adotados na literatura para tornar o processo de estabelecimento de vizinhança mais seguro e, por conseguinte, dificultar e mitigar possíveis ataques. Com a utilização do algoritmo de Código de Autenticação com Base em *Hash* (HMAC - *Hash-based Message Authentication Code*), em conjunto com o Diffie-Hellman, propõe-se que o endereço IP contido no campo

Target IP da mensagem de ARP *Request* seja disfarçado através de uma função de *hash*, seguido de outras funções desenvolvidas. Como mencionado, o campo *Target* IP corresponde ao endereço IP a ser resolvido. Ao mascarar o IP contido neste campo, conjectura-se que caso a mensagem de ARP *Request* seja interceptada por um atacante, o mesmo não poderia passar-se pelo host procurado (como demonstrado nas sub-subseções 4.2.2 e 4.3.2), em decorrência que o IP ali contido não trata-se do verdadeiro, mas de um disfarce.

No cenário onde a proposta é aplicada, inicialmente ocorre o processo de troca de chaves utilizando o Diffie-Hellman (enviadas no campo *Padding* de um pacote Ethernet), para que todos os hosts da rede tenham um segredo compartilhado entre si e possuam um canal seguro. Quando é necessário que um host estabeleça vizinhança com outro, e para isto solicite o endereço MAC correspondente a um determinado endereço IP, este envia uma mensagem ARP *Request* em *broadcast* para todos os nós da rede. Todavia, nesta abordagem, o IP contido no campo *Target* IP não irá em texto plano, pois será gerado um novo IP disfarce para substituí-lo. Para tal, é utilizado o HMAC juntamente à chave (de tamanho 1024 bits) já estabelecida anteriormente entre os hosts, para realizar uma função de *hash* no IP, gerando uma saída de 128 bits totalmente diferente do IP inicial. Em seguida, para adicionar mais uma camada de proteção e deixar esta saída gerada semelhante a um endereço IPv4 usual, é aplicada uma nova função, que divide esta saída em 4 grupos de 32 bits, escolhendo um entre estes e aplicando uma função para transformá-lo em um endereço IPv4.

Após o envio do ARP *Request*, os demais hosts da rede aplicam a mesma abordagem em seu próprio endereço IP, e comparam com o contido no *Target* IP do pacote recebido. Desta forma, apenas o host verdadeiro irá autenticar e enviará o ARP *Reply* correto, dado que o atacante certamente enviará um ARP *Reply* passando-se pelo IP disfarce. Uma vez que o invasor não teria conhecimento prévio de qual seria o endereço procurado inicialmente, a prova real que o ARP *Reply* é proveniente do host verdadeiro sucede-se quando este responde com o seu próprio endereço IP no campo *Sender* IP.

A seguir a proposta é ilustrada através da Figura 31 e Figura 32. Neste cenário, o host A deseja estabelecer vizinhança com o host B, e não possui adjacência com os demais hosts apresentados.

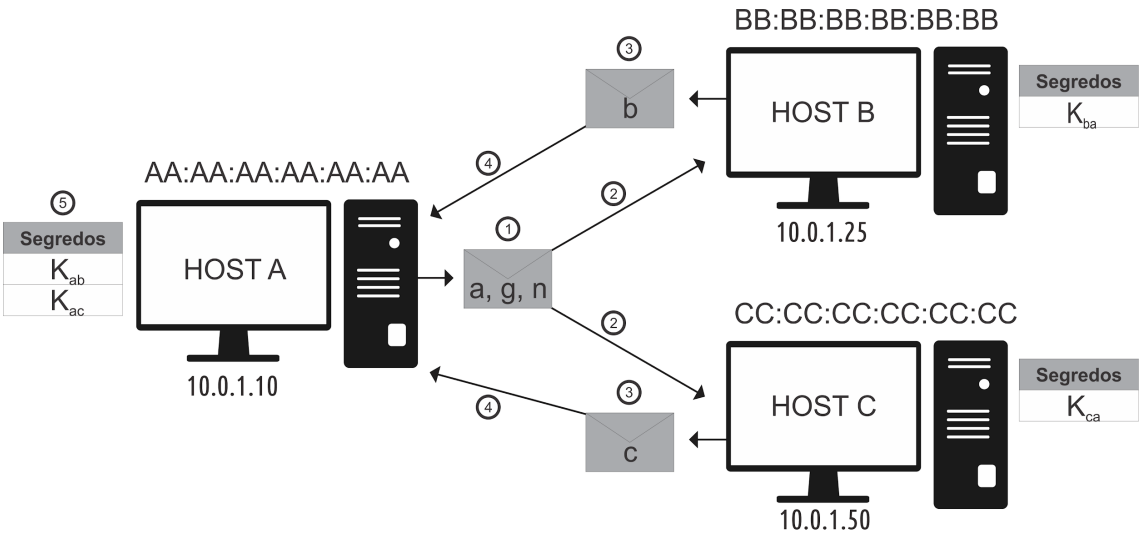

Figura 31: Troca de Chaves Diffie-Hellman (Imagem Autoral)

Seguindo os passos apontados na Figura 31:

1. O host A gera o cálculo *a* usando Diffie-Hellman.
2. O host A divulga em broadcast sua chave pública gerada pelas variáveis a, g e n.
3. Os hosts B e C recebem a mensagem de A e geram as variáveis *b* e *c*, além dos segredos K_{ab} e K_{ac}.
4. Os hosts B e C, ao receberem a mensagem, enviam para o host A seus cálculos *b* e *c* .
5. O host A recebe os cálculos *b* e *c* e gera os segredos K_{ab} e K_{ac} respectivamente.

Após a troca de segredos entre os hosts da rede, o host A envia um ARP *Request* direcionado ao endereço IP do host B. Este cenário pode ser visto na Figura 32.

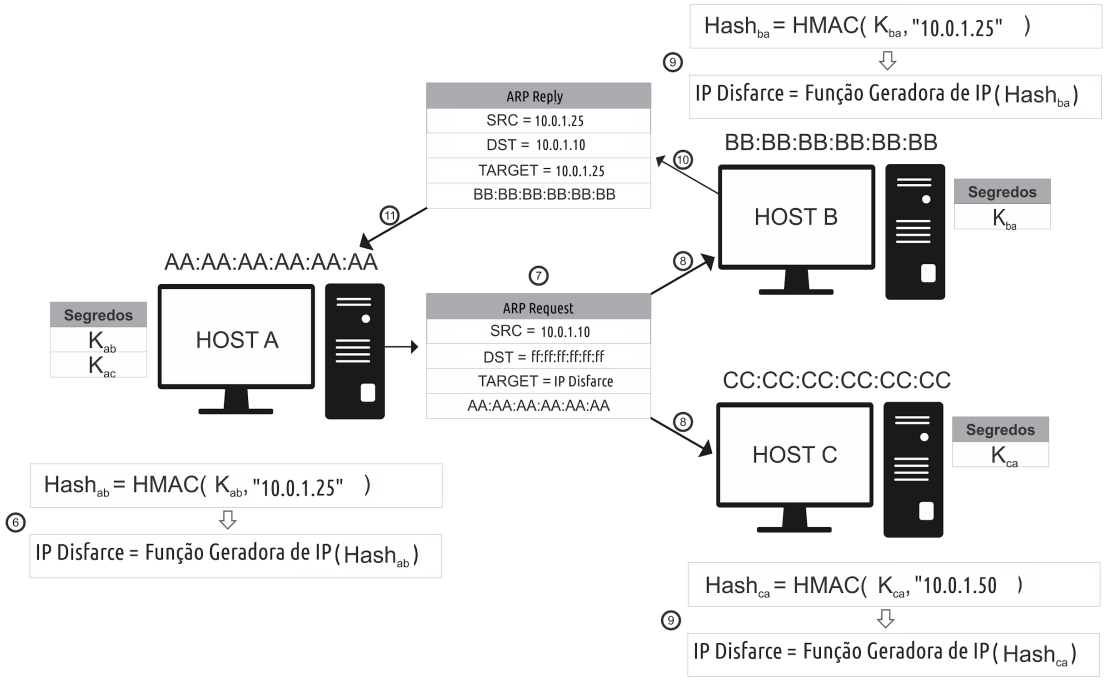

Figura 32: Processo de Estabelecimento de Vizinhança com a Proposta (Imagem Autoral)

Seguindo os passos apontados na Figura 32:

6. O host A calcula o *hash* do IP do host B usando a chave K_{ab} , assim gerando o IP disfarce com o $Hash_{ab}$ através da função geradora de IP.

7. O host A envia um ARP *Request*, contendo o IP disfarce no *Target*.

8. Os hosts B e C recebem o ARP *Request*.

9. Os hosts B e C fazem o mesmo processo do passo 6, [com o seu próprio endereço IP, utilizando a chave K_{*a} (sendo '*' correspondente à letra que o host representa, ex: K_{ba}, K_{ca}) e comparam com *Target* do pacote recebido.

10. O host B, sendo o único a ter correspondência, envia um ARP *Reply* ao host A contendo seu endereço IP como origem e informando seu MAC.

11. O host A recebe o ARP *Reply*, confere o endereço de origem, e caso correto, faz a associação na tabela ARP e assim prossegue com a comunicação.

4.4.1.1 Resultados Obtidos

Seguindo um exemplo real, a Tabela 6 apresenta valores reais obtidos através de um dos experimentos realizados.

Chave Pública A (k_a) (1024 bits)	14736811896592631964836074774869135679576219016315693844411395272795217146754408600324174233454750328576696806289875839707483054680931159656819735103685112181872249643587327227914973890061137136618173558369877636648422589155421312987804933867566784900290448635477724434389670072283874618187557240423574026111 8
Chave Pública B (k_b) (1024 bits)	25959713933826566013455001200547803115049029090102597124689162740985326091321095521673057418012690255206908796128030460804220563259997379998394021842396160156173947604555092082160396447011204557014643485105531880624291476042322359311806907864357661179861076153193787881598788122996871327955542280632797773362
Chave comum entre A e B (k_{ab}) (1024 bits)	13198370863424735338969083510287146591874932307370367814342843751549249214500741113571111259710361738122251744960671788200910957979334892962163085016625593260050685093981971329309964458056454269547851277633856385388019935430118747152202640015181989110010928899499550626449260337392979584066124982376982638378 0
Hash Criado HMAC(“10.0.1.25”, k_{ab}) (128 bits)	25a1:00b8:b2b4:e51a:7695:7c9f:e3db:2ae0
Convertendo *Hash* em Números	631308472.2998199578.1989508255.3822791392
Grupo A (32 bits)	631308472
Grupo B (32 bits)	2998199578
Grupo C (32 bits)	1989508255
Grupo D (32 bits)	3822791392

Convertendo grupo A em IPv4 - IP disfarce	37.161.0.184

Tabela 6: Exemplo de Valores Obtidos com a Proposta

De acordo com o exemplo apresentado na Tabela 6, a Figura 33 retrata a captura do ARP *Request,* onde o IP disfarce gerado está contido no campo *Target IP Address.*

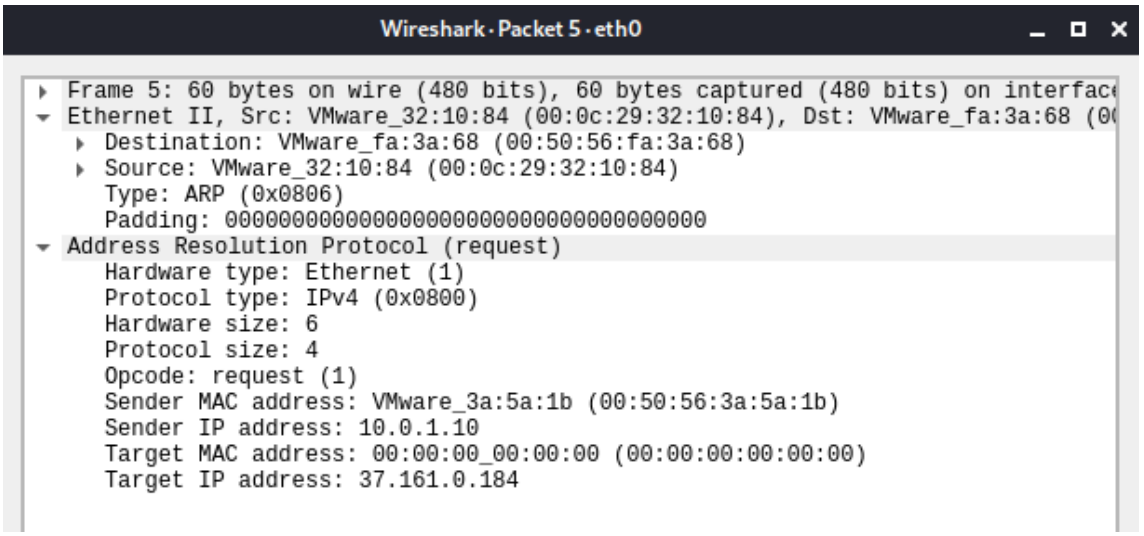

Figura 33: Arp Request Proposta

Ao tentar realizar a ataque demonstrado na subsubseção 4.2.2, o invasor não obtém o mesmo resultado apresentado na subsubseção 4.3.2. Em razão do IP ir disfarçado, o atacante envia o ARP *Reply* passando-se pelo IP incorreto, como apresentado na Figura 34, não tendo êxito na realização do ataque.

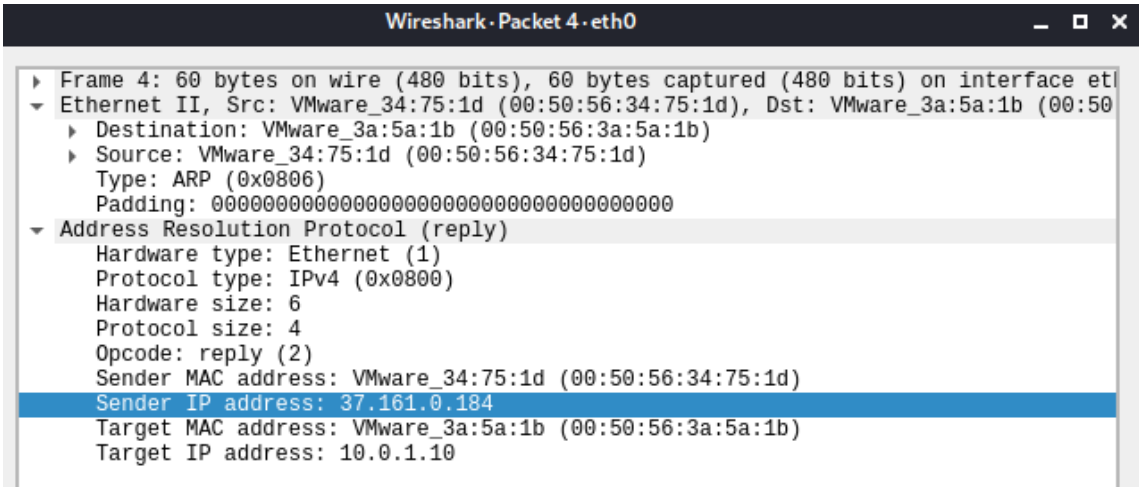

Figura 34: Arp Reply Atacante Após Proposta

Para o caso do atacante capturar os pacotes onde foram feitas as trocas de chave ou realizar o processo do Homem no Meio, ainda seria necessário que ele conhecesse quais passos foram aplicados até a geração daquele endereço IP:

I. A função de hash aplicada com a chave no endereço IP procurado;
II. A conversão do resultado em um número inteiro;
III. A divisão desse número em grupos;
IV. Qual destes grupos foi escolhido para a geração do IP disfarce.

Portanto, para o cenário em que o invasor na rede que não estivesse ciente do método aplicado, o ataque torna-se inviável. Na circunstância que o invasor tem esse conhecimento, ainda teria que descobrir os passos III e IV, podendo o último ser aplicado com outras diversas estratégias de cálculo para a geração do IP disfarce. Como citado, a vizinhança é estabelecida com a primeira mensagem recebida, o que daria tempo hábil de vantagem para o host alvo do ARP *Request* responder com o ARP *Reply* correto (contendo seu endereço IP e MAC) com maior velocidade do que um atacante demoraria para solucionar qual o IP alvo verdadeiro.

Tendo em vista que a proposta apresentada confere um maior nível de segurança no processo de estabelecimento de vizinhança, é necessário também averiguar o quanto esse ganho de segurança afeta e consome os recursos computacionais. A fim de obter dados de consumo das máquinas utilizadas, foi utilizada a ferramenta Collectl [Especificação Collecl], que coleta e armazena dados de desempenho de computadores e equipamentos de rede. O processo de ARP normal e do ARP com a proposta foram realizados 30 vezes, e a cada execução ocorrida foi recolhido dados de CPU, memória e rede através desta ferramenta. A média dos resultados é apresentada na Tabela 7 a seguir:

	Servidor		Rede			
	CPU (%)	Memória Livre (MB)	KBIn (kB)	PktIn (Pacote)	KBOut (kB)	PktOut (Pacote)
ARP	35,7	176,8	0,04	4,2	0	1,8
Proposta	38,5	131,4	0,6	6,2	0,06	2,6

Tabela 7: Uso de Recursos Computacionais

Como observado na Tabela 7, é possível notar algumas diferenças referentes aos consumos dos recursos citados, entre o ARP funcionando de forma habitual e a proposta apresentada. Iniciando pelo uso da CPU, observa-se que a proposta consome em média 2,8% a mais, seguido pela memória, onde a proposta apresenta um consumo adicional de em média 45 megabytes. Em termos de rede, verifica-se que a maior diferença encontra-se nos pacotes de entrada e de saída, onde a proposta exibe um número um pouco maior. Esta diferença é dada devido à troca de chaves Diffie-Hellman no começo do processo. Essa troca de chaves e os cálculos realizados também explicam o maior consumo de CPU e memória.

4.4.1.2 Aplicação em Sistemas Scada

Apesar da proposta apresentada poder ser aplicada em diversas redes que fazem o uso do protocolo ARP, é especialmente adequada para o ambiente industrial. Por gerar um par de chaves entre todos os hosts da rede, em uma rede de grande porte, onde um grande número de hosts podem ingressar ao mesmo tempo, essa geração de chaves entre eles pode ocasionar uma sobrecarga. Para o caso dos sistemas SCADA, em particular os que fazem o uso de protocolos como o Modbus, um nó supervisor está conectado ao número máximo de 247 nós operários [Especificação Modbus]. Posto isto, não é provável que um grande número de hosts ingresse na rede no mesmo intervalo de tempo, visto que isso só ocorre quando é adicionado um novo dispositivo (ou troca de um já existente) ou os nós são reiniciados por alguma razão.

Como foi visto, o uso de criptografia em um ambiente industrial pode custar muito caro em termos de consumo de recursos computacionais, e por esta razão torna-se difícil a implementação desta técnica como contramedida nesses cenários [Drias el al. 2015]. Levando em consideração que um sistema SCADA funciona com troca de dados em tempo real, o uso de criptografia simétrica é mais adequada para ser implantada [Kang et al. 2009], sendo a proposta uma boa alternativa por utilizar o Diffie-Hellman. O seu funcionamento é bem mais rápido do que um método assimétrico se comparado com um do mesmo nível, e conforme o apresentado, o consumo adicional dos recursos não é expressivo o suficiente para prejudicar o funcionamento da rede e dos equipamentos, principalmente quando comparado à maior garantia de segurança ofertada.

Para a implementação desse método em cenários industriais, sabendo que é comum a coexistência de equipamentos antigos com os mais modernos, seria necessário apenas uma atualização nos *firmwares* dos equipamentos que são conectados à rede, para que assim o processo de ARP seja realizado conforme a proposta, não sendo necessária a troca dos dispositivos ou maiores complexidades em termos de *hardware*.

Capítulo 5

Considerações Finais

A *smart grid* oferta inúmeros benefícios para a indústria, e decorrentemente, para sociedade, sendo assim essencial garantir a proteção de seu sistema e componentes vitais. Todavia, de acordo com as vulnerabilidades dissertadas e dos experimentos realizados neste trabalho, é notório o quão os sistemas SCADA estão expostos a diversos problemas de cibersegurança e como isso pode vir a acarretar diversos prejuízos.

Na literatura, muitos trabalhos apontam para problemas relativos à segurança desses sistemas, e conforme o que foi apresentado no mapeamento sistemático presente no capítulo 3, muitas pesquisas foram e estão sendo feitas a fim de tornar estes ambientes mais seguros. A partir dos resultados obtidos por esta classificação (algo que ainda não havia sido feito anteriormente nesta área), o estudo pode vir a contribuir como introdução a novos entusiastas e também auxiliar aos pesquisadores e estudiosos a enxergar quais áreas carecem de mais esforços e quais já estão mais avançadas, entre outras contribuições.

Sucessivamente, mediante aos resultados obtidos através dos experimentos realizados e expostos no capítulo 4, infere-se que ataques que visam deliberadamente a sabotagem - como do homem no meio, o *TCP Syn Flood* e o ataque ARP e de Reflexão - permitem a influência e comprometimento de operações outrora seguras e confiáveis do SCADA. Tais resultados demonstram como os invasores podem prejudicar e/ou interromper o sistema, ocasionando insupríveis danos, e assim reforçando a necessidade de estudos e novas propostas de soluções, conforme a proposta apresentada para o ataque ARP, para tornar esses ambientes mais protegidos. Esconder o IP durante a descoberta de vizinhança, embora não resolva todos os problemas relacionados ao ARP,

aumenta o nível de segurança e torna o processo mais seguro, podendo assim mitigar os ataques conforme demonstrado nos experimentos.

5.1 Propostas de Trabalhos Futuros

Considerando a significativa importância da segurança em *smart grids*, é visado progredir os estudos nesta área em questão a fim de explorar demais fraquezas eminentes no SCADA e em seus protocolos de comunicação, bem como novas propostas de solução, buscando assim trazer maiores contribuições. A seguir, encontram-se os principais aspectos de propensão de estudos:

- Aprofundar o conhecimento dos conceitos dos sistemas SCADA, sua arquitetura e protocolos de comunicação;
- Realizar experimentos de implementações de ataques em diferentes cenários, como por exemplo, atacantes que encontram-se fora da rede e precisam passar pelos mecanismos de defesa para acessá-la. Desta forma, pode-se assim explorar as fraquezas presentes no sistema e seus protocolos, cuja a pretensão também é realizar esses experimentos com diferentes protocolos industriais além do Modbus;
- Propor novas contramedidas para mitigação dos ataques e soluções para tornar esses ambientes mais seguros e confiáveis, mantendo o desempenho que é necessário para o funcionamento adequado do setor elétrico e sistemas SCADA.

Bibliografia

[Sun et al. 2018] C. Sun, A. Hahn e C. Liu, “Cyber security of a power grid: State-of-the-art”, International Journal of Electrical Power & Energy Systems, v. 99, pp. 45-56, Julho 2018.

[Tesfahun et al. 16] A. Tesfahun e L. Bhaskari, “A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures”, Automatic Control and Computer Sciences, v. 50, pp 54-62, Abril 2016.

[El Mrabet et al. 2018] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi e H. E. Ghazi, “Cyber-security in smart grid: Survey and challenges”, Computers & Electrical Engineering, v. 67, pp. 469-482, Abril 2018.

[Ahmad et al. 2019] Z. Ahmad e M. H. Durad, "Development of SCADA Simulator using Omnet++," 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 676-680, 2019.

[Yang et al. 2012] Y. Yang et al., "Man-in-the-middle Attack Test-bed Investigating Cyber-security Vulnerabilities In Smart Grid Scada Systems", International Conference on Sustainable Power Generation and Supply (SUPERGEN), pp. 1-8, 2012.

[Irmak et al. 2018] E. Irmak e İ. Erkek, "An overview of cyber-attack vectors on SCADA systems," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-5, Maio 2018.

[Modbus 2012] MODBUS Protocol Specification, Disponível em: <http://www.modbus.org/specs.php>, Acesso em: 20 de Abril, 2020.

[Drias et al. 2015] Z. Drias, A. Serhrouchni e O. Vogel, "Analysis of cyber security for industrial control systems," International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), pp. 1-8, 2015.

[DNP ORG]Overview Of DNP3 Protocol, Disponível em: <https://www.dnp.org/About/Overview-of-DNP3-Protocol>, Acesso em: 05 de Junho, 2020.

[Feng et al. 2016] Z. Feng, S. Qin, X. Huo, P. Pei, Ye Liang e L. Wang, "Snort improvement on Profinet RT for Industrial Control System Intrusion Detection", 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 942-946, Maio 2016.

[Profibus] - Profinet Overview, Disponível em: <https://www.profibus.com/technology/profinet/overview/>, Acesso em: 05 de Junho, 2020.

[Wong et al. 2017] K. Wong, C. Dillabaugh, N. Seddigh e B. Nandy, "Enhancing Suricata intrusion detection system for cyber security in SCADA networks," 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-5, Junho 2017.

[Odva Org] EtherNet/IP™, Disponível em: <https://www.odva.org/technology-standards/key-technologies/ethernet-ip/>, Acesso em: 05 de Junho, 2020.

[Guia NIST] Standards for Security Categorization of Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 199, Fevereiro, 2004.

[FIPS] Minimum Security Requirements for Federal Information and Information Systems, National Institute for Standards and Technology, FIPS 200, Março, 2006. Framework for Improving Critical Infrastructure Cybersecurity, NIST, Fevereiro, 2014.

[Stoufler et al. 2014] Keith Stoufler, Susan Lightman e Marshal Abrams, ” Guide to industrial control systems Security", NIST special publication 800- 82, Maio, 2014.

[Line et al. 2011] M. B. Line, I. A. Tondel, e M. G. Jaatun, "Cyber security challenges in Smart Grids", Innovative Smart Grid Technologies (ISGT Europe), 2nd IEEE PES International Conference and Exhibition, pp. 1-8, 2011.

[ANSI/ISA-62443-3-3] ANSI/ISA-62443-3-3, “Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels, 2014.

[Huang et al. 2018] X. Huang, Z. Qin e H. Liu, "A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis", IEEE Access, v. 6, pp. 69023-69035, 2018.

[Chang Liu et al. 2015] C. Liu, G. Xiong, J. Liu e G. Gou, "Detect The Reflection Amplification Attack Based On Udp Protocol", 10th International Conference on Communications and Networking in China (ChinaCom), pp. 260-265, 2015.

[Radoglou-Grammatikis et al. 2018] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Liatifis, T. Apostolakos and S. Oikonomou, "An Overview of the Firewall Systems in the Smart Grid Paradigm," 2018 Global Information Infrastructure and Networking Symposium (GIIS), pp. 1-4, Fevereiro 2019.

[Nivethan el al. 2016] J. Nivethan e M. Papa, "Dynamic rule generation for SCADA intrusion detection," 2016 IEEE Symposium on Technologies for Homeland Security (HST) pp. 1-5, Setembro 2016.

[Trigueiro 2011] A. Trigueiro; S. Castelo Branco, “Um mapeamento sistemático de mecanismos para guiar estudos empíricos em engenharia de software.”, Dissertação (Mestrado), Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, 2011.

[Petersen et al. 2008] K. Petersen e R. Feldt, “Systematic mapping studies in software engineering”, 12th International Conference on Evaluation and Assessment in Software Engineering, pp. 68–77, 2008.

[Almeida et. al 2018] L. Almeida, P. Carvalho, C. Jacome, M. Monteiro e M. Cabral, “An In-Depth Analysis of the Last Twenty Years About IPv6 Security”, IEEE 10th Latin-American Conference on Communications (LATINCOM), pp. 1-6, 2018.

[Journals Elsevier] - Jornauls Elsevier, Disponíve em: <https://www.journals.elsevier.com/>, Acesso em: 20 nov. 2019.

[IEEE Xplore] - IEEE Xplore, Disponível em: <https://ieeexplore.ieee.org/>, Acesso em: 20 nov. 2019.

[Sridhar et al. 2012] S. Sridhar, A. Hahn e M. Govindarasu, “Cyber–Physical System Security for the Electric Power Grid”, Proceedings of the IEEE vol. 100, pp. 210-224. Outubro 2011.

[J. Liu et al. 2012] J. Liu, Y. Xiao, S. Li, W.Liang e C. L. Philip Chen, “Cyber Security and Privacy Issues in Smart Grids”, IEEE Communications Surveys & Tutorials vol.14, pp. 981 - 997, Janeiro 2012.

[Ericsson 2010] G. N. Ericsson, “Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure”, IEEE Transactions on Power Delivery, pp. 1501 - 1507, Abril 2010.

[Hug et al. 2012] G. Hug, J. A. Giampapa, “Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks”, IEEE Transactions on Smart Grid vol. 3, pp. 1362-1370, Setembro 2012.

[Kim et al. 2013] J. Kim e L. Tong, “On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures”, IEEE Journal on Selected Areas in Communications, vol. 31, pp. 1294-1305, Julho 2013.

[Especificação Scapy] Scapy’s documentation, Disponível em: <https://scapy.readthedocs.io/en/latest/>, Acesso em: 20 de Abril, 2020.

[Especificação Collectl] Collectl’s documentation, Disponível em <http://collectl.sourceforge.net>, Acesso em: 26 de Setembro, 2020.

[Stefanov et al. 2012] A. Stefanov e C. Liu, "Cyber-power system security in a smart grid environment," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1-3, Janeiro 2012.

[Sridhar et al. 2012] S. Sridhar, A. Hahn e M. Govindarasu, "Cyber attack-resilient control for smart grid," 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1-3, 2012.

[Alguliyev et al.] R. Alguliyev, Y. Imamverdiyev e L. Sukhostat. “Cyber-physical systems and their security issues”, Computers in Industry 100, pp. 212–223, 2018.

[Kang et al. 2009] D. Kang e H. Kim, “Development of test-bed and security devices for SCADA communication in electric power system”, 31st International Telecommunications Energy Conference, pp. 1–5, Outubro. 2009.

[Misyrlis et al. 2016] M. Misyrlis, R. Kannan, C. Chelmis e V. K. Prasanna, “Sparse Causal Temporal Modeling to Inform Power System Defense”, Procedia Computer

Science 95, pp. 450–456, Novembro 2016.

[Ruzhi Xu et al. 2017] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu e X. Du, “Achieving Efficient Detection against False Data Injection Attacks in Smart Grid”. IEEE Access PP, pp. 1– 1, Julho 2017.

[Sadi et al. 2015] M. A. H. Sadi, M. H. Ali, D. Dasgupta, R. K. Abercrombie e S. Kher,“Co-Simulation Platform for Characterizing Cyber Attacks in Cyber Physical Systems”, IEEE Symposium Series on Computational Intelligence, pp. 1244–1251, Dezembro 2015.

[Hong et al. 2011] S. Hong, T. N. Phuong e M. Lee, “Development of Smart Devices for Secure Communication in the SCADA System”, International Conference on Computational Science and Its Applications, pp. 176–180, Junho 2011.

[Hong et al. 2010] S. Hong e M. Lee, “Challenges and Direction toward Secure Communication in the SCADA System”, 8th Annual Communication Networks and Services Research Conference, pp. 381–386, Maio 2010.

[Darwish et al. 2015] I. Darwish, O. Igbe, O. Celebi, T. Saadawi e J. Soryal, “Smart Grid DNP3 Vulnerability Analysis and Experimentation”. IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 141–147, Novembro 2015.

[Darwish et al. 2015] I. Darwish, O. Igbe e T. Saadawi, “Experimental and theoretical modeling of DNP3 attacks in smart grids”, 36th IEEE Sarnoff Symposium, pp. 155–160, Setembro 2015.

[Anu et al] J. Anu, R. Agrawal, C. Seay e S. Bhattacharya “Smart Grid Security Risks”, 12th International Conference on Information Technology - New Generations, pp. 485–489, Abril 2015.

[Chen et al. 2015] B. Chen, N. Pattanaik, A. Goulart , K. L. Butler-purry e D. Kundur, “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed”, IEEE International Workshop Technical Committee on Communications Quality and Reliability, pp. 1–6, Maio 2015.

[Baalbaki et al 2013] B. A. Baalbaki, Y. Al-Nashif, S. Hariri e D. Kelly, “Autonomic Critical Infrastructure Protection (ACIP) system”, ACS International Conference on Computer Systems and Applications (AICCSA), pp. 1–4, Maio 2013.

[Singh et al 2015] P. Singh, S. Garg, V. Kumar e Z. Saquib, “A testbed for SCADA cyber security and intrusion detection”, 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), pp. 1–6, Agosto. 2015.

[Kwon et al. 2015] Y. Kwon, H. K. Kim, Y. H. Lim e J. I. Lim, “A behavior-based intrusion detection technique for smart grid infrastructure”, 2015 IEEE Eindhoven PowerTech, pp. 1–6, Junho 2015.

[Rege et al. 2014] A. Rege, F. Ferrese, S. Biswas e L. Bai, “Adversary dynamics and smart grid security: A multiagent system approach”, 7th International Symposium on Resilient Control Systems (ISRCS), pp. 1–7, Agosto 2014.

[Tanha et al. 2012] M. Tanha e F. Hashim, “An intrusion tolerant system for improving availability in smart grid control centers”, 18th IEEE International Conference on Networks (ICON), pp. 434–440, Dezembro. 2012.

[Y. Yang et al. 2013] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono e H. F. Wang, “Intrusion Detection System for IEC 60870-5-104 based SCADA networks”, 2013 IEEE Power Energy Society General Meeting , pp. 1–5, Julho 2013.

[Mavee et al. 2012] S. M. A. Mavee e E. M. Ehlers. “A Multiagent Immunologically-inspired Model for Critical Information Infrastructure Protection – An Immunologically-inspired Conceptual Model for Security on the Power Grid”, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1089–1096, Junho 2012.

[J. Fadul et al 2011] J. Fadul, K. Hopkinson, C. Sheffield, J. Moore e T. Andel,“Trust Management and Security in the Future Communication-Based ”Smart” Electric Power Grid”, 44th Hawaii International Conference on System Sciences, pp. 1–10, Janeiro 2011.

[Kumar et al. 2014] S. Kumar, M. K. Soni e D. K. Jain, “A secure wide area monitoring system network model using shared key cryptography”, 2015 International Conference on Soft Computing Techniques and Implementations (ICSCTI), pp. 66–715, Outubro 2015.

[J. Kim et al. 2013] J. Kim e L. Tong, “On phasor measurement unit placement against state and topology attacks”, 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 396–401, Outubro 2013.

[Myers et al. 2018] D. Myers, S. Suriadi, K. Radke e Ernest Foo, “Anomaly detection for industrial control systems using process mining”, Computers Security 78, pp. 103–125, 2018.

[Sicard et al. 2019] F. Sicard, E. Zamai e J. Flaus. “An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems”, Reliability Engineering System Safety 188, pp. 584–603, 2019.

[Wen et al. 2019] X. Wen, H. Wang, S. Aziz, H. Jiang e Jianchun Peng, “Interval State Estimation for Attack Detection Base on PQ decomposition”, Energy Procedia 158, Innovative Solutions for Energy Transitions, pp. 6607– 6612, 2019.

[Basumallik et al. 2019] S. Basumallik, R. Ma e S. Eftekharnejad, “Packet-data anomaly detection in PMU-based state estimator using convolutional neural network”, International Journal of Electrical Power Energy Systems 107, pp. 690–702, 2019.

[Priya et al. 2014] V. Priya e J. Bapat, “Bad data detection in smart grid for AC model”, 2014 Annual IEEE India Conference (INDICON), pp. 1–6, Dezembro 2014.

[Stefanov et al. 2012] A. Stefanov e C. Liu, “Cyber-power system security in a smart grid environment”, 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1–3, 2012.

[G. Andersson et al. 2012] G. Andersson et al, “Cyber-security of SCADA systems”, IEEE PES Innovative Smart Grid Technologies (ISGT), pp. 1–2, 2012.

[Genge el al. 2011] B. Genge e C. Siaterlis, “Developing cyberphysical experimental capabilities for the security analysis of the future Smart Grid”, 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp. 1–7, 2011.

[Hwett el al. 2014] R. Hewett, S. Rudrapattana e P. Kijsanayothin, “Smart Grid security: Deriving informed decisions from cyber attack game analysis”, IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 946–951, 2014.

[Safa et al. 2016] H.H. Safa, D.M. Souran, M. Ghasempour e A. Khazaee, “Cyber security of smart grid and SCADA systems, threats and risks”, IET Conference Proceedings, pp 1-4, Jan. 2016.

[Hawrtlak et al. 2012] P. J. Hawrylak et al, “Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid”, 5th International Symposium on Resilient Control Systems, pp. 161–164, 2012.

[Faisal et al. 2016] M. M. A. Faisal e M. A. I. Chowdhury, “Bio inspired cyber security architecture for smart grid”, International Conference on Innovations in Science, Engineering and Technology (ICISET), pp. 1–5, 2016.

[Boroomand et al. 2010] F. Boroomand et al, “Cyber security for Smart Grid: A human-automation interaction framework”, IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), pp. 1–6, 2010.

[Rizzetti et al. 2015] T. A. Rizzetti et al, “Cyber security and communications network on SCADA systems in the context of Smart Grids”, 50th International Universities Power Engineering Conference (UPEC), pp. 1–6, 2015.

[Akhtar et al. 2018] T. Akhtar, B. B. Gupta e S. Yamaguchi,“Malware propagation effects on SCADA system and smart power grid”, 2018 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–6, 2018.

[Akhtar et al. 2018] T. Akhtar e B. B. Gupta, “Towards a Framework for Analyzing Cyber Attacks Impact Against Smart Power Grid on SCADA System”, International Conference on Communication and Signal Processing (ICCSP), pp. 1087–1093, 2018.

[Nordbø 2013] P.E. Nordbø, “Cyber security in smart grid stations”, IET Conference

Proceedings, pp. 1-4, Janeiro 2013.

[Hu et al. 2015] R. Hu, W. Hu, e Z. Chen, “Research of smart grid cyber architecture and standards deployment with high adaptability for Security Monitoring”, International Conference on Sustainable Mobility Applications, Renewables and Technology (SMART), pp. 1–6, 2015.

[Tawde et al. 2015] R. Tawde, A. Nivangune e M. Sankhe, “Cyber security in smart grid SCADA automation systems”, International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1–5, 2015.

[Tornelli 2012] C. Tornelli, “Impact of DER integration on the cyber security of SCADA systems - the medium voltage regulation case study”, IET Conference Proceedings, pp. 214–214, Janeiro 2012.

[Hasan et al. 2016] M. M. Hasan and H. T. Mouftah, “Optimal Trust System Placement in Smart Grid SCADA Networks”, IEEE Access 4, pp. 2907– 2919, 2016.

[Igbe et al. 2017] O. Igbe, I. Darwish, e T. Saadawi, “Deterministic Dendritic Cell Algorithm Application to Smart Grid Cyber-Attack Detection”, IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 199–204, 2017.

[Hasan et al. 2019] M. M. Hasan e H. T. Mouftah, “Optimization of Trust Node Assignment for Securing Routes in Smart Grid SCADA Networks”, IEEE Systems Journal 13.2, pp. 1505–1513, 2019.

[Pandey et al. 2016] R. K. Pandey e M. Misra, “Cyber security threats — Smart grid infrastructure”, National Power Systems Conference (NPSC), pp. 1–6, 2016.

[Seewald 2012] M. G. Seewald, “Benefits of end-to-end IP for cyber and physical security”, PES T D 2012, pp. 1–6, 2012.

[Dcruz et al. 2018] H. J. Dcruz e B. Kaliaperumal, “Analysis of Cyber-Physical Security in Electric Smart Grid : Survey and challenges”, 6th International Renewable and Sustainable Energy Conference (IRSEC), pp. 1–6, 2018.

[Cameron et al. 2018] C. Cameron et al, “Using Self-Organizing Architectures to Mitigate the Impacts of Denial-ofService Attacks on Voltage Control Schemes”, IEEE Transactions on Smart Grid 10.3, pp. 3010–3019, 2019.

[Zhang et al 2015] Y. Zhang et al, “Power System Reliability Evaluation With SCADA Cybersecurity Considerations”, In: IEEE Transactions on Smart Grid 6.4, pp. 1707–1721, 2015.

[McMillin 2012] B. McMillin, “Privacy and confidentiality in Cyber-Physical Power Systems”, IEEE Power and Energy Society General Meeting, pp. 1–3, 2012.

[Alimi et al, 2018] O. A. Alimi e K. Ouahada, “Security Assessment of the Smart Grid: A Review focusing on the NAN Architecture”, 2018 IEEE 7th International Conference

on Adaptive Science Technology (ICAST), pp. 1–8, 2018.

[Choucri et al. 2017] N. Choucri e G. Agarwal, “Analytics for smart grid cybersecurity”, 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–3, 2017.

[Hasan et al. 2016] M. M. Hasan e H. T. Mouftah, “A study of resource-constrained cyber security planning for smart grid networks”, IEEE Electrical Power and Energy Conference (EPEC), pp. 1–6, 2016.

[Singh et al. 2018] V. K. Singh, H. Ebrahem e M. Govindarasu,“Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment”, North American Power Symposium (NAPS), pp. 1–6, 2018.

[Shitharth et al. 2016] S. Shitharth e D. P. Winston,“A novel IDS technique to detect DDoS and sniffers in smart grid”, World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), pp. 1–6, 2016.

[Rahman et al. 2016] M. A. Rahman, A. H. M. Jakaria e E. AlShaer, “Formal Analysis for Dependable Supervisory Control and Data Acquisition in Smart Grids”, 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 263–274, 2016.

[Yang et al. 2014] Y. Yang et al, “Multiattribute SCADA-Specific Intrusion Detection System for Power Networks”, IEEE Transactions on Power Delivery, pp. 1092–1102, Março 2014.

[Ding et al. 2017] Y. Ding e J. Liu, “Real-time false data injection attack detection in energy internet using online robust principal component analysis”, 2017 IEEE Conference on Energy Internet and Energy System Integration, pp. 1–6, 2017.

[Katzir et al. 2011] L. Katzir e I. Schwartzman, “Secure firmware updates for smart grid Devices”, 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp. 1–5, 2011.

[Antonini et al. 2014] A. Antonini et al, “Security challenges in building automation and SCADA”, International Carnahan Conference on Security Technology (ICCST), pp. 1–6, 2014.

[Radoglou-Grammatikis et al. 2019] P. I. Radoglou-Grammatikis e P. G. Sarigiannidis, “Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems”, IEEE Access 7, pp. 46595–46620, 2019.

[Czechowski et al. 2015] R. Czechowski, P. Wicher e B. Wiecha, “Cyber security in communication of SCADA systems using IEC 61850”, Modern Electric Power Systems (MEPS), pp. 1–7, 2015.

[Hahn et al. 2011] A. Hahn e M. Govindarasu, “Cyber Attack Exposure Evaluation Framework for the Smart Grid”, IEEE Transactions on Smart Grid 2.4, pp. 835–843,

2011.

[Chalamasetty et al. 2016] G. K. Chalamasetty, P. Mandal e Tzu-Liang Tseng, “Secure SCADA communication network for detecting and preventing cyber-attacks on power systems”, Clemson University Power Systems Conference (PSC), pp. 1–7, 2016.

[Pappa et al. 2017] A. C. Pappa, A. Ashok, e M. Govindarasu, “Moving target defense for securing smart grid communications: Architecture, implementation evaluation”, IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5, 2017.

[Stefanov et al. 2012] A. Stefanov e C. Liu, “ICT modeling for integrated simulation of cyber-physical power systems”, 3rd IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe), pp. 1–8, 2012.

[Weerathunga et al. 2016] P. E. Weerathunga e A. Cioraca, “The importance of testing Smart Grid IEDs against security vulnerabilities”, 2016 69th Annual Conference for Protective Relay Engineers (CPRE), pp. 1–21, 2016.

[Ghosh et al, 2018] S. Ghosh e M. H. Ali, “Impact of Crash Override and Tampering Communication Data Cyber-Attacks on the Power Quality of the Hybrid System”, IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), pp. 1–5, 2018.

[Sommestad et al. 2010] T. Sommestad, G. N. Ericsson e J. Nordlander, “SCADA system cyber security — A comparison of standards”, IEEE PES General Meeting, pp. 1–8, 2010.

[Sou et al. 2013] K. C. Sou, H. Sandberg e K. H. Johansson, “On the Exact Solution to a Smart Grid CyberSecurity Analysis Problem”, IEEE Transactions on Smart Grid 4.2, pp. 856–865, 2013.

[Hasan et al. 2016] M. M. Hasan e H. T. Mouftah, “Latencyaware segmentation and trust system placement in smart grid SCADA networks”, IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), pp. 37–42, 2016.

[Hadbah et al. 2017] A. Hadbah, A. Kalam e A. Zayegh, “Powerful IEDs, ethernet networks and their effects on IEC 61850-based electric power utilities security”, Australasian Universities Power Engineering Conference (AUPEC), pp. 1– 5, 2017.

[Lai et al. 2017] J. Lai et al, “An active security defense strategy for wind farm based on automated decision”, 2017 IEEE Power Energy Society General Meeting, pp. 1–5, 2017.

[Giani] A. Giani et al, “Smart Grid Data Integrity Attacks”, IEEE Transactions on Smart Grid 4.3, pp. 1244–1253, 2013.

[Senyondo et al. 2015] H. Senyondo et al, “PLCloud: Comprehensive power grid PLC

security monitoring with zero safety disruption", IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 809–816, 2015.

[Oyewumi et al.] I. A. Oyewumi et al., "ISAAC: The Idaho CPS Smart Grid Cybersecurity Testbed", IEEE Texas Power and Energy Conference (TPEC), pp. 1–6, 2019.

[Yoo et al. 2016] H. Yoo and T. Shon, "Grammarbased adaptive fuzzing: Evaluation on SCADA modbus protocol", 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 557–563, 2016.

[Erol-Kantarci et al. 2013] M. Erol-Kantarci e H. T. Mouftah, "Smart grid forensic science: applications, challenges, and open issues", IEEE Communications Magazine 51.1, pp. 68–74, 2013.

[Al Jahil et al. 2016] A. A. Al Jahil e D. Giarratano, "Improvement of cyber-security measures in National Grid SA substation process control", Saudi Arabia Smart Grid (SASG), pp. 1– 6, 2016.

[Karimipour et al. 2017] H. Karimipour e V. Dinavahi, "On false data injection attack against dynamic state estimation on smart power grids", IEEE International Conference on Smart Energy Grid Engineering (SEGE), pp. 388–393, 2017.

[Rob et al. 2014] R. Rob et al, "Addressing cyber security for the oil, gas and energy sector", 2014 North American Power Symposium (NAPS), pp. 1–8, 2014.

[Kumar et al. 2017] R. J. R. Kumar and B. Sikdar, "Efficient detection of false data injection attacks on AC state estimation in smart grids", 2017 IEEE Conference on Communications and Network Security (CNS), pp. 411–415, 2017.

[Pal et al. 2016] S. Pal, B. Sikdar, e J. Chow, "Detecting data integrity attacks on SCADA systems using limited PMUs", IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 545–550, 2016.

[Matsumoto et al. 2010] T. Matsumoto et al, "Information-theoretic approach to authentication codes for power system communications", IEEE PES T D 2010, pp. 1–7, 2010.

[Zhang et al. 2017] Y. Zhang, Y. Xiang e L. Wang, "Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems", IEEE Transactions on Smart Grid 8.5, pp. 2343–2357, 2017.

[Karimipour et al. 2018] H. Karimipour e V. Dinavahi, "Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack, IEEE Access 6, pp. 2984–2995, 2018.

[Sajid et al. 2016] A. Sajid, H. Abbas e K. Saleem, "CloudAssisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges", IEEE

Access 4, pp. 1375–1384, 2016.

[S. Wu et al. 2014] S. Wu, C. Liu e A. Stefanov, “Distributed specification-based firewalls for power grid substations”, IEEE PES Innovative Smart Grid Technologies, pp. 1–6, 2014.

[Silva et al. 2016] E. G. da Silva et al, “A One-Class NIDS for SDN-Based SCADA Systems”. IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Vol. 1, pp. 303–312, 2016.

[Wilson et al. 2018] D. Wilson et al, “Deep Learning-Aided CyberAttack Detection in Power Transmission Systems”, IEEE Power Energy Society General Meeting (PESGM), pp. 1–5, 2018.

[Chromik et al. 2016] J. J. Chromik, A. Remke e B. R. Haverkort, “What’s under the hood? Improving SCADA security with process awareness”, 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG), pp. 1–6, 2016.

[Kirsch et al. 2014] J. Kirsch et al., “Survivable SCADA Via Intrusion-Tolerant Replication”, IEEE Transactions on Smart Grid 5.1, pp. 60– 70.

[Hug et al. 2012] G. Hug e J. A. Giampapa, “Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks”, IEEE Transactions on Smart Grid 3.3, pp. 1362–1370, 2012.

[Mallouhi et al. 2011] M. Mallouhi et al.,“A testbed for analyzing security of SCADA control systems (TASSCS)”, ISGT 2011, pp. 1–7, 2011.

[Chen et al. 2018] B. Chen, Z. Lu e H. Zhou, “Reliability Assessment of Distribution Network Considering Cyber Attacks”, 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), pp. 1–6, 2018.

[Yan et al. 2013] J. Yan et al., “A PMU-based risk assessment framework for power control systems”, IEEE Power Energy Society General Meeting, pp. 1–5, 2013.

[Zhongxi et al. 2018] L. Zhongxi et al. “Detecting False Data by CUSUM Algorithm Synergy with UKF”, IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 669–674, 2018.

[Xiang et al. 2014] Y. Xiang, L. Wang e Y. Zhang, “Power system adequacy assessment with probabilistic cyber attacks against breakers”, IEEE PES General Meeting — Conference Exposition, pp. 1–5, 2014.

[Khurana 2011] H. Khurana, “Moving beyond defense-in-depth to strategic resilience for critical control systems”, IEEE Power and Energy Society General Meeting, pp. 1–3, 2011.

[Ten et al. 2018] C. Ten et al.,“Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems”, IEEE Transactions on Smart Grid 9.5, pp.

4405–4425, 2018.

[Y Yang et al. 2017] Y. Yang et al., “Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks”, IEEE Transactions on Power Delivery 32.2, pp. 1068–1078, 2017.

[Hasan et al. 2018] S. Hasan et al, “Vulnerability analysis of power systems based on cyber-attack and defense models”, 2018 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5, 2018.

[Stellios et al. 2018] I. Stellios et al, “A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services”, IEEE Communications Surveys Tutorials 20.4, pp. 3453–3495, 2018.

[Irita et al. 2017] T. Irita e T. Namerikawa, “Detection of replay attack on smart grid with code signal and bargaining game”, 2017 American Control Conference (ACC), pp. 2112–2117, 2017.

[Hendrickx et al. 2014] J. M. Hendrickx et al, “Efficient Computations of a Security Index for False Data Attacks in Power Networks”, IEEE Transactions on Automatic Control 59.12, pp. 3194–3208, 2014.

[Tuttle et al. 2019] M. Tuttle et al. “Algorithmic Approaches to Characterizing Power Flow Cyber-Attack Vulnerabilities”, IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5, 2019.

[Ismail et al. 2015] Z. Ismail et al, “A Game-Theoretical Model for Security Risk Management of Interdependent ICT and Electrical Infrastructures”, IEEE 16th International Symposium on High Assurance Systems Engineering, pp. 101– 109, 2015.

[James et al. 2013] J. James et al. “Cyber-physical situation awareness and decision support”, IEEE 2nd Network Science Workshop (NSW), pp. 114–117, 2013.

[J. Kim et al. 2013] J. Kim and L. Tong. “On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures”, IEEE Journal on Selected Areas in Communications 31.7, pp. 1294– 1305, 2013.

[Radoglou-Grammatikis et al. 2019] P. Radoglou-Grammatikis et al., “Attacking IEC-60870-5-104 SCADA Systems”, IEEE World Congress on Services (SERVICES). Vol. 2642-939X, pp. 41–46, 2019.

[Yuan et al. 2012] Y. Yuan, Z. Li e K. Ren, “Quantitative Analysis of Load Redistribution Attacks in Power Systems”, IEEE Transactions on Parallel and Distributed Systems 23.9, pp. 1731– 1738, 2012.

[Roberts et al. 2020] C. Roberts et al., “Learning Behavior of Distribution System Discrete Control Devices for Cyber-Physical Security”., IEEE Transactions on Smart Grid 11.1, pp. 749–761, 2020.

[Hewett et al. 2014] Rattikorn Hewett, Sudeeptha Rudrapattana e Phongphun Kijsanayothin, “CyberSecurity Analysis of Smart Grid SCADA Systems with Game Models”, Proceedings of the 9th Annual Cyber and Information Security Research Conference, pp. 109–112, 2014.

[Hahn et al. 2013] Adam Hahn e Manimaran Govindarasu, “Model-Based Intrustion Detection for the Smart Grid (MINDS)”, Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1-4, 2013.

[Korman et al. 2017] Matus Korman et al, “Analyzing the Effectiveness of Attack Countermeasures in a SCADA System”, Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grid, pp. 73–78, 2017.

[Wallace et al. 2014] N. Wallace, S. Ponomarev and T. Atkison, “A Dimensional Transformation Scheme for Power Grid Cyber Event Detection”, Proceedings of the 9th Annual Cyber and Information Security Research Conference, pp. 13–16, 2014.

[Hahn et al 2010] A. Hahn et al., “Development of the PowerCyber SCADA Security Testbed”, Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, pp. 1-4, 2010.

[Lin et al. 2013] H. Lin et al., “Adapting Bro into SCADA: Building a Specification-Based Intrusion Detection System for the DNP3 Protocol”, Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1-4, 2013.

[Majed et al. 2014] S. Majed, S. Ibrahim e Mohamed Shaaban, “Architecting and Development of the SecureCyber: A SCADA Security Platform Over Energy Smart Grid”, Proceedings of the 16th International Conference on Information Integration and Web-Based Applications Services, pp. 170–174, 2014.

[Alves et al. 2016] T. Alves, R. Das, e T. Morris, “Virtualization of Industrial Control System Testbeds for Cybersecurity”, Proceedings of the 2nd Annual Industrial Control System Security Workshop, pp. 10–14, 2016.

[Lin et al. 2013] H. Lin et al., “Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids”, Proceedings of the First ACM Workshop on Smart Energy Grid Security, pp. 29–34, 2013.

[Matuszak et al. 2013] W. J. Matuszak, L. DiPippo e Y. L. Sun, “CyberSAVe: Situational Awareness Visualization for Cyber Security of Smart Grid Systems”, pp. 25–32, 2013.

[Belqruch et al. 2019] A. Belqruch e A. Maach, “SCADA Security Using SSH Honeypot”, Proceedings of the 2nd International Conference on Networking, Information Systems Security, pp. 1-5, 2019.

[Ten et al. 2008] C. Ten, C. Liu e M, Govindarasu, “Cyber-Vulnerability of Power Grid

Monitoring and Control Systems", pp. 1-3, 2008.

[Hewett et al. 2013] R. Hewett e P. Kijsanayothin, "Securing System Controllers in Critical Infrastructures", Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1-4, 2013.

[Larkin et al. 2014] R. D. Larkin et al., "Evaluation of Security Solutions in the SCADA Environment", SIGMIS Database 45.1, pp. 38– 53, Março 2014.

[Konstantinou et al. 2016] C. Konstantinou e Michail Maniatakos, "A Case Study on Implementing False Data Injection Attacks Against Nonlinear State Estimation", Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pp. 81–92, 2016.

[Saranyan Senthivel et al] Saranyan Senthivel et al, "Denial of Engineering Operations Attacks in Industrial Control Systems", Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. CODASPY '18, Association for Computing Machinery, pp. 319–329, 2018.

[Yulia Cherdantseva et al] Yulia Cherdantseva et al, "A review of cyber security risk assessment methods for SCADA systems", Computers Security 56, pp. 1–27, 2015.

[W. Li et al] W. Li et al., "False sequential logic attack on SCADA system and its physical impact analysis", Computers Security 58, pp. 149–159, 2016.

[Genge et al. 2019] B. Genge, P. Haller e A. Duka, "Engineering security-aware control applications for data authentication in smart industrial cyber–physical systems", Future Generation Computer Systems 91, pp. 206–222, 2019.

[Stefanov et al. 2014] A. Stefanov e C. Liu, "Cyber-Physical System Security and Impact Analysis", IFAC Proceedings Volumes 47.3, 19th IFAC World Congress, pp. 11238– 11243. 2014.

[Kimani et al. 2019] K. Kimani, V. Oduol e K. Langat, "Cyber security challenges for IoTbased smart grid networks", International Journal of Critical Infrastructure Protection 25, pp. 36–49, 2019.

[Mohandes et al. 2018] B. Mohandes et al., "Advancing cyber–physical sustainability through integrated analysis of smart power systems: A case study on electric vehicles", International Journal of Critical Infrastructure Protection 23, pp. 33–48, 2018.

[Shitharth et al. 2015] S. Shitharth e D. Prince Winston,"A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network", Procedia Technology 21, SMART GRID TECHNOLOGIES, pp. 179–186, 2015.

[Ferrag et al. 2018] M. A. Ferrag et al., "A systematic review of data protection and privacy preservation schemes for smart grid communications", Sustainable Cities and

Society 38, pp. 806–835, 2018.

[Patel et al. 2017] A. Patel et al., “A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems”, Computers Security 64, pp. 92–109, 2017.

[Ding et al. 2018] D. Ding et al. “A survey on security control and attack detection for industrial cyber-physical systems”, Neurocomputing 275, pp. 1674–1683, 2018.

[Abdo et al. 2018] H. Abdo et al., “A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis”, Computers Security 72, pp. 175–195, 2018.

[Zang et al. 2019] T. Zang et al., “Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks”, Reliability Engineering System Safety 189, pp. 232–241, 2019.

[Subhankar Mishra et al] Subhankar Mishra et al, “Optimal packet scan against malicious attacks in smart grids”, Theoretical Computer Science 609, pp. 606-619, 2016

[Lucie Langer et al] Lucie Langer et al, “From old to new: Assessing cybersecurity risks for an evolving smart grid”, Computers Security 62, pp. 165–176, 2016.

[Rodofile et al. 2019] N. R. Rodofile, K, Radke e E. Foo, “Extending the cyber-attack landscape for SCADA-based critical infrastructure”, International Journal of Critical Infrastructure Protection 25, pp. 14–35, 2019.

[Nicholson et al. 2012] A. Nicholson et al., “SCADA security in the light of Cyber-Warfare”, Computers Security 31.4, pp. 418–436, 2012.

[Mahmoud et al. 2019] M. S. Mahmoud, M. M. Hamdan e U. A. Baroudi, “Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges”, Neurocomputing 338, pp. 101–115, 2019.

[Poudel et al. 2017] S. Poudel, Z. Ni e N. Malla, “Real-time cyber physical system testbed for power system security and control”, International Journal of Electrical Power Energy Systems 90 , pp. 124–133, 2017.

[T. Liu et al. 2015] T. Liu et al., “Abnormal traffic-indexed state estimation: A cyber–physical fusion approach for Smart Grid attack detection”, Future Generation Computer Systems 49, pp. 94–103, 2015.

[Adamsky et al. 2018] F. Adamsky et al., “Integrated protection of industrial control systems from cyber-attacks: the ATENA approach”, International Journal of Critical Infrastructure Protection 21, pp. 72–82, 2018.

[Pramod et al. 2019] T. C. Pramod et al., “Key pre-distribution scheme with join leave support for SCADA systems”, International Journal of Critical Infrastructure Protection

24, pp. 111–125, 2019.

[Maw et al. 2019] A. Maw, S. Adepu e A. Mathur, “ICS-BlockOpS: Blockchain for operational data security in industrial control system”, Pervasive and Mobile Computing 59, pp. 101048, 2019.

[Wang et al. 2019] D. Wang et al., “Detection of power grid disturbances and cyber-attacks based on machine learning”, Journal of Information Security and Applications 46, pp. 42–52, 2019.

[Xiang et al. 2018] Y. Xiang, L. Wang e Y. Zhang, “Adequacy evaluation of electric power grids considering substation cyber vulnerabilities”, International Journal of Electrical Power Energy Systems 96, pp. 368–379, 2018.

[Jolfaei et al. 2019] A. Jolfaei e K. Kant, “A lightweight integrity protection scheme for low latency smart grid applications”, Computers Security 86, pp. 471–483, 2019.

[Bretas et al. 2017] A. S. Bretas et al., “Smart grids cyberphysical security as a malicious data attack: An innovation approach”, Electric Power Systems Research 149, pp. 210–219, 2019.

[Dibaji et al. 2019] S. M. Dibaji et al., “A systems and control perspective of CPS security”, Annual Reviews in Control 47, pp. 394–411, 2019.

[Ficco et al. 2017] M. Ficco, M. Choraś e R. Kozik, “Simulation platform for cyber-security and vulnerability analysis of critical infrastructures”, Journal of Computational Science 22, pp. 179–186, 2017.

[Yoo et al. 2016] H. Yoo e T. Shon, “Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture”, Future Generation Computer Systems 61, pp. 128–136, 2016.

[Nguyen et al. 2016] V. H. Nguyen, Q. T. Tran e Y. Besanger, “SCADA as a service approach for interoperability of micro-grid platforms”, Sustainable Energy, Grids and Networks 8, pp. 26–36, 2016.

[Kumar et al. 2014] V. A. Kumar, K. K. Pandey e D. K. Punia, “Cyber security threats in the power sector: Need for a domain specific regulatory framework in India”, Energy Policy 65, pp. 126–133, 2014.

[Hammad et al. 2019] E. Hammad, M. Ezeme e Abdallah Farraj, “Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification”, International Journal of Electrical Power Energy Systems 104, pp. 817–826, 2019.

[Hawk et al. 2014] C. Hawk e A. Kaushiva, “Cybersecurity and the Smarter Grid”, The Electricity Journal 27.8, pp. 84–95, 2014.

[Jana et al. 2018] D. K. Jana e R. Ghosh, “Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security”, Journal of Information Security and Applications 40, pp. 173–182, 2018.

[Wang et al. 2019] H. Wang et al., “Deep learning aided interval state prediction for improving cyber security in energy internet”, Energy 174, pp. 1292–1304, 2019.

[Nazir et al. 2017] S. Nazir, S. Patel e D. Patel, “Assessing and augmenting SCADA cyber security: A survey of techniques”, Computers Security 70, pp. 436–454, 2017.

[Orojloo et al. 2017] H. Orojloo e M. A. Azgomi, “A game-theoretic approach to model and quantify the security of cyber-physical systems”, In: Computers in Industry 88, pp. 44–57, 2017.

[Igure et al. 2006] V. M. Igure, S. A. Laughter e R. D. Williams, Security issues in SCADA networks”. In: Computers Security 25.7, pp. 498–506, 2006.

[Ashok et al, 2014] A. Ashok, A. Hahn e M. Govindarasu, “Cyber-physical security of WideArea Monitoring, Protection and Control in a smart grid environment”, Journal of Advanced Research 5.4. Cyber Security, pp. 481–489, 2014.

[Maglaras et al. 2018] L. A. Maglaras et al. “Cyber security of critical infrastructures”, ICT Express 4.1, SI: CI Smart Grid Cyber Security, pp. 42–45, 2018.

[Ge et al. 2019] H. Ge et al., “A unified modeling of muti-sources cyber-attacks with uncertainties for CPS security control”, Journal of the Franklin Institute, pp. 1-25 , 2019.

[Chen et al. 2019] R. Chen et al., “A novel online detection method of data injection attack against dynamic state estimation in smart grid”, Neurocomputing 344, NEURAL LEARNING IN LIFE SYSTEM AND ENERGY SYSTEM, pp. 73–81, 2019.

[Parra et al. 2019] G. D. L. T. Parra, P.l Rad e K. R. Choo. “Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities”, Journal of Network and Computer Applications 135, pp. 32–46, 2019.

[Leszczyna 2018] R. Leszczyna, “Cybersecurity and privacy in standards for smart grids – A comprehensive survey”, Computer Standards Interfaces 56, pp. 62–73, 2018.

[Wang et al. 2019] X. Wang et al., “Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers”. In: International Journal of Electrical Power Energy Systems 110, pp. 208–222, 2019.

[Conti et al. 2016] S. Conti et al., “Impact of cyber-physical system vulnerability, telecontrol system availability and islanding on distribution network reliability”, Sustainable Energy, Grids and Networks 6, pp. 143–151, 2016.

[Tøndel et al. 2018] I. A. Tøndel et al., “Interdependencies and reliability in the combined ICT and power system: An overview of current research”, Applied

Computing and Informatics 14.1 (2018), pp. 17–27, 2018.

[Sahay et al. 2019] R. Sahay, W. Meng e C. D. Jensen, “The application of Software Defined Networking on securing computer networks: A survey”, Journal of Network and Computer Applications 131, pp. 89–108, 2019.

[Knijff 2014] R.M. van der Knijff. “Control systems/SCADA forensics, what’s the difference?”, Digital Investigation 11.3, Special Issue: Embedded Forensics, pp. 160–174, 2014.

[L. Yang et al. 2017] L. Yang, Y. Li e Z. Li, “Improved-ELM method for detecting false data attack in smart grid”, International Journal of Electrical Power Energy Systems 91, pp. 183–191, 2017.

[Chabukswar et al. 2011] R. Chabukswar, Y. Mo e B. Sinopoli, “Detecting Integrity Attacks on SCADA Systems”, IFAC Proceedings Volumes 44.1, 18th IFAC World Congress, pp. 11239– 11244. 2011.

[Zimba et al. 2018] A. Zimba, Z. Wang e H. Chen, “Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems”, ICT Express 4.1, SI: CI Smart Grid Cyber Security, pp. 14–18, 2018.

[Salunkhe et al. 2018] O. Salunkhe et al. “Cyber-Physical Production Testbed: Literature Review and Concept Development”, Procedia Manufacturing 25, Proceedings of the 8th Swedish Production Symposium (SPS 2018), pp. 2–9, 2018.

[Maglaras et al. 2016] L. A. Maglaras, J. Jiang, and T. J. Cruz. “Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems”, Journal of Information Security and Applications 30, pp. 15–26, 2016..

[Demir et al. 2019] K. Demir, F. Nayyer e N. Suri, “MPTCP-H: A DDoS attack resilient transport protocol to secure wide area measurement systems”, International Journal of Critical Infrastructure Protection 25, pp. 84–101, 2019.

[Timpson et al. 2018] D. Timpson e E. Moradian, “A Methodology to Enhance Industrial Control System Security”, Procedia Computer Science 126, Knowledge-Based and Intelligent Information Engineering Systems: Proceedings of the 22nd International Conference, pp. 2117–2126, 2018.

[Shi et al. 2018] L. Shi, Q. Dai e Y. Ni, “Cyber–physical interactions in power systems: A review of models, methods, and applications”, Electric Power Systems Research 163, pp. 396–412, 2018.

[Kolosok et al.] I. Kolosok e E. Korkina, “Development of a State Estimation Methodology to Improve the Quality of Control of the Boundary Areas of the Neighboring Smart Transmission Grids”, IFAC Workshop on Control of Transmission and Distribution Smart Grids CTDSG 2016, pp. 461–466, 2016.

[Xiang et al. 2017] Y. Xiang, L. Wang e N.Liu, “Coordinated attacks on electric power systems in a cyber-physical environment”, Electric Power Systems Research 149, pp. 156– 168, 2017.

[Almalawi et al. 2014] A. Almalawi et al., “An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems”, Computers Security 46, pp. 94–110, 2014.

[Pramod et al. 2015] T. C. Pramod e N. R. Sunitha, “Polynomial Based Scheme for Secure SCADA Operations”, Procedia Technology 21, SMART GRID TECHNOLOGIES, pp. 474–481, 2015.

[Onyeji et al, 2014] I. Onyeji, M. Bazilian e C. Bronk, “Cyber Security and Critical Energy Infrastructure”, The Electricity Journal 27.2, pp. 52–60, 2014.

[Rahman et al. 2019] M. A. Rahman, A. Datta e E. Al-Shaer, “Security design against stealthy attacks on power system state estimation: A formal approach”, Computers Security 84, pp. 301–317, 2019.

[Knowles et al. 2015] W. Knowles et al., “A survey of cyber security management in industrial control systems”, International Journal of Critical Infrastructure Protection 9, pp. 52–80, 2015.

[Ntalampiras 2016] S. Ntalampiras, “Automatic identification of integrity attacks in cyber-physical systems”, Expert Systems with Applications 58, pp. 164–173, 2016.

[J. Wang et al. 2017] J. Wang et al, “A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities”, Pervasive and Mobile Computing 39, pp. 52– 64, 2017.

[Perkins et al. 2015] C. Perkins e G. Muller, “Using Discrete Event Simulation to Model Attacker Interactions with Cyber and Physical Security Systems”, Procedia Computer Science 61 pp. 221–226, 2015.

[Marelli et al. 2018] D. Marelli, T. Sui e M. Fu, “Statistical Approach to Detection of Attacks for Stochastic Cyber-Physical Systems”, 9th IFAC Symposium on Robust Control Design ROCOND 2018, pp. 178–183, 2018.

[Xiong et al. 2019] W. Xiong e R. Lagerstrom, “Threat modeling – A systematic literature review”, Computers Security 84, pp. 53–69, 2019.

[Q. Li et al. 2018] Q. Li et al., “Data-driven attacks and data recovery with noise on state estimation of smart grid”, Journal of the Franklin Institute, pp. 1-21, 2018.

[Rubio et al. 2019] J. E. Rubio et al., “Current cyberdefense trends in industrial control systems”, Computers Security 87, p. 101561, 2019.

[Schlegel et al. 2017] R. Schlegel, S. Obermeier e J. Schneider, “A security evaluation of IEC 62351”, Journal of Information Security and Applications 34, pp. 197–204,

2017.

[Anwar et al. 2015] A. Anwar, A. N. Mahmood e Z. Tari. “Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid”, Information Systems 53, pp. 201–212, 2015 .

[Yaseen et al. 2017] A. A. Yaseen e M. Bayart, “CyberAttack Detection with Fault Accommodation Based on Intelligent Generalized Predictive Control”, IFAC-PapersOnLine 50.1, 20th IFAC World Congress, pp. 2601–2608, 2017.

[Shitharth 2017] S. Shitharth e P. D. Winston, “An enhanced optimization based algorithm for intrusion detection in SCADA network”, Computers Security 70, pp. 16–26, 2017.

[Coppolino et al. 2014] L. Coppolino, S. DAntonio e L. Romano, “Exposing vulnerabilities in electric power grids: An experimental approach”, International Journal of Critical Infrastructure Protection 7.1, pp. 51–60, 2014.

[Genge et al. 2015] B. Genge, I. Kiss e Piroska Haller, “A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures”, International Journal of Critical Infrastructure Protection 10, pp. 3–17, 2015.

[Gonzalez-Granadillo et al. 2018] G. Gonzalez-Granadillo et al. “Dynamic risk management response system to handle cyber threats”, Future Generation Computer Systems 83, pp. 535–552, 2018.

[Y. Li et al. 2014] Y. Li e Y. Wang, “State summation for detecting false data attack on smart grid”, International Journal of Electrical Power Energy Systems 57, pp. 156–163, 2014.

[Fei Hu et al. 2016] Fei Hu et al., “Robust Cyber–Physical Systems: Concept, models, and implementation”, Future Generation Computer Systems 56, pp. 449–475, 2016.

[Burmester et al. 2012] M. Burmester, E. Magkos e V. Chrissikopoulos, “Modeling security in cyber–physical systems”, International Journal of Critical Infrastructure Protection 5.3, pp. 118–126, 2012.

[Treytl et al. 2005] A. Treytl, P. Palensky e T. Sauter, “SECURITY CONSIDERATIONS FOR ENERGY AUTOMATION NETWORKS”, IFAC Proceedings Volumes 38.2, . 6th IFAC International Conference on Fieldbus Systems and their Applications, pp. 158–165, 2005.

[Lees et al. 2018] M. J. Lees, M. Crawford and C. Jansen, “Towards Industrial Cybersecurity Resilience of Multinational Corporations”, IFAC-PapersOnLine 51.30, 18th IFAC Conference on Technology, Culture and International Stability TECIS, pp. 756–761, 2018.

[Xiang et al. 2017] Y. Xiang e L. Wang, “A gametheoretic study of load redistribution attack and defense in power systems”, Electric Power Systems Research 151, pp.

12–25, 2017.

[Hong et al. 2017] J. B. Hong et al., “A survey on the usability and practical applications of Graphical Security Models”, Computer Science Review 26, pp. 1–16, 2017.

[Genge et al. 2014] B. Genge e C. Siaterlis, “Physical process resilience-aware network design for SCADA systems”, Computers Electrical Engineering 40.1, 40th-year commemorative issue, pp. 142–157, 2014.

[Mander et al. 2010] T. Mander, R. Cheung e F. Nabhani, “Power system DNP3 data object security using data sets”, Computers Security 29.4, pp. 487–500, 2010.

[Giani et al. 2014] A. Giani, R. Bent, and R. Pan. “Phasor measurement unit selection for unobservable electric power data integrity attack detection”, International Journal of Critical Infrastructure Protection 7.3, pp. 155– 164, 2014.

[Liu et al. 2017] X. Liu, Y. Mo e E. Garone. “Secure Dynamic State Estimation by Decomposing Kalman Filter”, IFAC-PapersOnLine 50.1, 20th IFAC World Congress, pp. 7351–7356, 2017.

[Khalil 2016] Y. F. Khalil, “A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures”, Process Safety and Environmental Protection 102, pp. 473–484, 2016.

[A. Lu et al. 2020] A. Lu e H. Yang, “False data injection attacks against state estimation in the presence of sensor failures”, Information Sciences 508, pp. 92–104, 2020.

[X. Liu et al, 2017] X. Liu e Z. Li, “False data attack models, impact analyses and defense strategies in the electricity grid”, The Electricity Journal 30.4, Special Issue: Contemporary Strategies for Microgrid Operation Control, pp. 35–42, 2017.

[Lai et al. 2019] K. Lai, M. Illindala e K. Subramaniam, “A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment”, Applied Energy 235, pp. 204– 218, 2019.

[Mohammadpourfard et al. 2017] M. Mohammadpourfard, A. Samie e A. R. Seifi, “A statistical unsupervised method against false data injection attacks: A visualization-based approach”, Expert Systems with Applications 84, pp. 242–261, 2017.

[Gonda et al. 2014] O. Gonda, “Understanding the threat to SCADA networks”,: Network Security, pp. 17–18, 2014.

[M. Ma et al. 2017] M. Ma et al., “Voltage Control in Distributed Generation under Measurement Falsification Attacks”. IFACPapersOnLine 50.1, 20th IFAC World Congress, pp. 8379–8384, 2017.

[Morris et al. 2011] T. Morris et al., “A control system testbed to validate critical infrastructure protection concepts”, International Journal of Critical Infrastructure Protection 4.2, pp. 88– 103, 2011.

[Martinez et al. 2019] C. V. Martinez e B. VogelHeuser, “A Host Intrusion Detection System architecture for embedded industrial devices”, Journal of the Franklin Institute, pp.1-27 2019.

[Islam et al. 2018] S. N. Islam, M. A. Mahmud e A. M. T. Oo, “Impact of optimal false data injection attacks on local energy trading in a residential microgrid”, ICT Express 4.1, SI: CI Smart Grid Cyber Security, pp. 30–34. 2018.

[Kriaa et al 2015] S. Kriaa et al., “A survey of approaches combining safety and security for industrial control systems”, Reliability Engineering System Safety 139, pp. 156–178, 2015.

[Genge et al. 2012] B. Genge et al., “A cyber-physical experimentation environment for the security analysis of networked industrial control systems”, Computers Electrical Engineering 38.5, Special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing, pp. 1146–1161, 2012.

[Meng et al. 2019] A. Meng et al., “Kalman Filtering Based Interval State Estimation For Attack Detection”, Energy Procedia 158, Innovative Solutions for Energy Transitions, pp. 6589–6594, 2019.

[Alcaraz et al. 2013] C. Alcaraz et al., “Security of industrial sensor network-based remote substations in the context of the Internet of Things”, Ad Hoc Networks 11.3, pp. 1091–1104, 2013.

[Anwar et al. 2017] A. Anwar, A. N. Mahmood e M. Pickering, “Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements”, Journal of Computer and System Sciences 83.1, pp. 58–72, 2017.

[Jang-Jaccard et al, 2014] J. Jang-Jaccard e S. Nepal, “A survey of emerging threats in cybersecurity”, Journal of Computer and System Sciences 80.5, Special Issue on Dependable and Secure Computing, pp. 973–993, 2014.

[Alcaraz et al. 2015] C. Alcaraz and S. Zeadally, “Critical infrastructure protection: Requirements and challenges for the 21st century”, International Journal of Critical Infrastructure Protection 8, pp. 53–66, 2015.

[Lopez et al. 2013] J. Lopez, C. Alcaraz e R. Roman, “Smart control of operational threats in control substations”, Computers Security 38, Cybercrime in the Digital Economy, pp. 14–27, 2013.

[Chabukswar et al. 2013] R. Chabukswar, Y. Mo e B. Sinopoli, “Secure Detection Using Binary Sensors”, IFAC Proceedings Volumes 46.27 , 4th IFAC Workshop on Distributed

Estimation and Control in Networked Systems, pp. 160–167, 2013.

[Jiang et al. 2013] W. Jiang et al. “Measurement-based research on cryptographic algorithms for embedded realtime systems”, Journal of Systems Architecture 59.10, Parte D , pp. 1394–1404, 2013.

[Domínguez et al. 2017] M. Domínguez et al., “Cybersecurity training in control systems using real equipment, IFAC-PapersOnLine 50.1. 20th IFAC World Congress, pp. 12179–12184, 2017.

[Xie et al. 2019] B. Xie et al., “A novel trust-based false data detection method for power systems under false data injection attacks”, Journal of the Franklin Institute, pp. 1-18, 2019.

[L. Silva et al. 2017] L. E. Silva e D. V. Coury, “A new methodology for real-time detection of attacks in IEC 61850-based systems”, Electric Power Systems Research 143, pp. 825–833, 2017.

[Reaves et al, 2012] B. Reaves e T. Morris, “Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems”, International Journal of Critical Infrastructure Protection 5.3 , pp. 154– 174, 2012.

[G. Li et al 2019] G. Li et al., “Detecting cyberattacks in industrial control systems using online learning algorithms”, Neurocomputing 364, pp. 338–348, 2019.

[Lopez et al, 2014] C. Alcaraz e J. Lopez. “Diagnosis mechanism for accurate monitoring in critical infrastructure protection”, Computer Standards Interfaces 36.3, pp. 501–512, 2014.

[Gonzalez-Granadillo et al. 2015] G. Gonzalez-Granadillo et al., “Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index”, Computers Electrical Engineering 47, pp. 13–34, 2015.

[Zio 2016] E. Zio, “Challenges in the vulnerability and risk analysis of critical infrastructures”. In: Reliability Engineering System Safety 152, pp. 137–150, 2016.

[Ntalampiras et al. 2015] S. Ntalampiras, Y. Soupionis e G. Giannopoulos, “A fault diagnosis system for interdependent critical infrastructures based on HMMs”, Reliability Engineering System Safety 138, pp. 73–81, 2015.

[Cazorla et al. 2015] L. Cazorla, C. Alcaraz e J. Lopez. “A three-stage analysis of IDS for critical infrastructures”, Computers Security 55, pp. 235–250, 2015.

[Masood et al. 2019] Z. Masood, R. Samar e M. A. Z. Raja, “Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure”, Computers Security 87, pp. 101565, 2019.

[S. Muller et al.] S. Muller et al., “A training-resistant anomaly detection system”,

Computers Security 76, pp. 1–11, 2018.

[Cazorla et al. 2015] L. Cazorla, C. Alcaraz e J. Lopez, “Awareness and reaction strategies for critical infrastructure protection”, Computers Electrical Engineering 47, pp. 299– 317, 2015.