UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LUIZA DOS SANTOS EITELVEIN

# Implementação e Avaliação de um Mecanismo de Detecção de Ameaças em uma Ferramenta Smart Grid

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação

Orientador: Prof. Dr. Alberto Egon Schaeffer-Filho

Porto Alegre
2015

## RESUMO

Resumo em português.



**Palavras-chave:** Smart grid.

**Implementation and Evaluation of a Threat Detection Mechanism in a Smart Grid Tool**

## ABSTRACT

Abstract in English.

**Keywords:** Smart Grid.

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| SCI | Sistema de Controle Industrial |
| CLP | Controlador Lógico Programável |
| TIC | Tecnologia da Informação e Comunicação |
| HMI | Interface Homem-Máquina |
| DEI | Dispositivos Eletrônicos Inteligente |
| UTR | Unidade Terminal Remota |
| SCADA | Supervisory Control and Data Acquisition |
| ENISA | European Network and Information Security Agency |
| NIST | National Institute of Standards and Technology |
| OCC | One-Class Classification |
| AM | Aprendizado de Máquina |
| SDI | Sistema de Detecção de Intrusão |
| OCSVM | One-Class Support Vector Machine |
| SVM | Support Vector Machine |

**SUMÁRIO**

# 1 INTRODUÇÃO

## 1.1 Motivação

## 1.2 Objetivos

## 1.3 Contribuição

## 1.4 Estrutura do Trabalho

# 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, será estabelecida a fundamentação teórica dos tópicos abordados neste trabalho, afim de fornecer o entendimento dos conceitos e tecnologias que serão utilizados e apresentar o estado da arte em que se encontram. A seção 2.1 introduz os smart grids, seu propósito, sua arquitetura e as ameaças que os afetam. Na seção 2.2, são abordados os mecanismos de segurança utilizados em smart grids. Finalmente, a seção 2.3 apresenta as ferramentas existentes para simulação de ambientes smart grid e sistemas SCADA.

## 2.1 Smart Grids

Smart Grids combinam redes de energia elétrica com estruturas de comunicação, baseadas em Tecnologia de Informação e Comunicação (TIC), que provêm um meio de troca de dados entre os componentes envolvidos no processo de produção, distribuição e consumo de energia. Como suas principais características, podem ser mencionados o fluxo bidirecional de energia elétrica entre produtores e consumidores e a incorporação de uma infraestrutura de comunicação, também bidirecional, que provê uma maior capacidade de automação à rede (YAN et al., 2013). Através de recursos e técnicas como monitoramento em tempo real, automação e controle de dispositivos, autoavaliação e autorecuperação, integração com de fontes de energia alternativas e mecanismos de segurança física e cibernética, Smart Grids imbuem a rede elétrica com maior confiabilidade, eficiência e segurança (LI et al., 2012). No restante desta sessão, são apresentados: as motivações para o uso de smart grids, em 2.1.1, sua arquitetura, em 2.1.2, e as ameaças às quais são suscetíveis, em 2.1.3.

### 2.1.1 Motivação

A infraestrutura de comunicação dos Smart Grids incorpora uma grande diversidade de benefícios ao sistema de produção, distribuição e consumo de energia. Dados coletados pela IMA podem ser utilizados para melhorar a eficiência e o desempenho da distribuição de energia, identificando picos de consumo e pontos de desperdício na rede, além de fornecer aos usuários informações detalhadas sobre seu consumo de energia, levando-os a um consumo mais eficiente. Uma maior automação da rede de distribuição leva à diminuição dos custos operacionais, pois seu funcionamento torna-se mais independente da mão de obra envolvida,

que, por sua vez, pode executar suas tarefas com mais eficiência. A capacidade de comunicação entre diversas entidades e o fluxo bidirecional de energia possibilitam uma utilização cada vez maior de recursos de energia distribuídos, incentivando o surgimento de fontes de geração de energia renovável, como solar e eólica. Entidades consumidoras podem também ser produtoras de energia, permitindo que microprodutores forneçam energia à rede simultaneamente a grandes produtores (YAN et al., 2013).

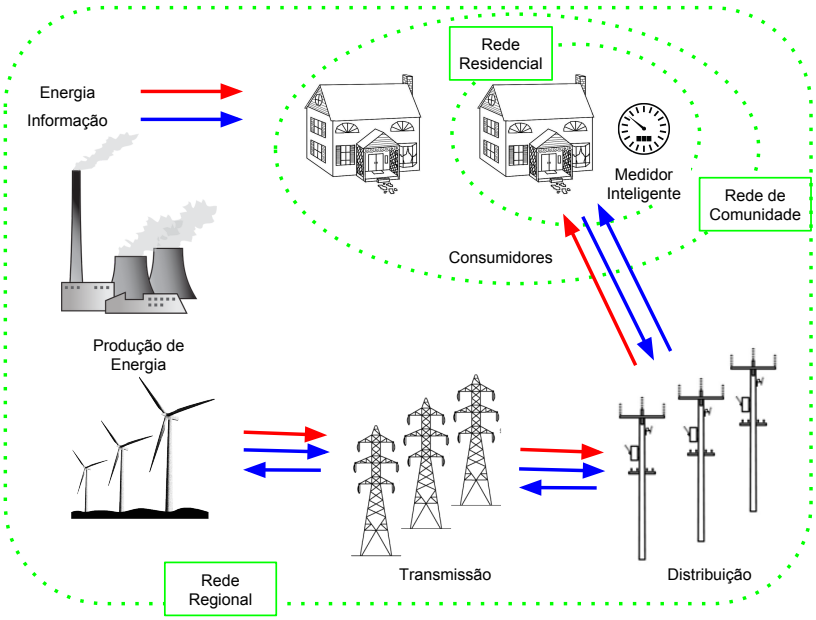
A capacidade de autoavaliação e autoajuste em redes elétricas e outras infraestruturas críticas, como sistemas de transporte e financeiros, é de imensa importância. Devido à modernização das tecnologias utilizadas, essas infraestruturas têm seus sistemas cada vez mais interconectados, aumentando o risco de falhas em cascata de grandes proporções. A demanda crescente por uma distribuição de energia mais eficiente e confiável traz a necessidade de aperfeiçoar métodos e ferramentas que forneçam às redes elétricas a capacidade de se autoregular e sofrer o menor impacto possível na ocorrência de sobrecarga, mal funcionamento ou ataques maliciosos (AMIN; WOLLENBERG, 2005).

### 2.1.2 Arquitetura

A produção de energia em um smart grid está distribuída em diversas fontes, que incluem usinas fixas e móveis e microprodutores. A energia elétrica é transportada das usinas de geração até as subestações de transmissão através de cabos de alta tensão, e então é transmitida, assim como a energia de outras fontes diversas, até as subestações de distribuição através de linhas de tensão variada. A partir das subestações de distribuição, finalmente, a energia é distribuída para consumo (BOU-HARB et al., 2013).

Cada consumidor de um smart grid, em conjunto com um medidor inteligente e disjuntores de controle forma uma rede residencial. Redes residenciais, Dispositivos Eletrônicos Inteligentes (DEIs) e Unidades Terminais Remotas (UTRs) são agrupados em redes de comunidades que, por sua vez, são conectadas a produtores de energia e outros elementos do smart grid em uma área geográfica por uma rede regional (LI et al., 2012). Controle e monitoramento da rede em cada região são realizados por centros de controle regionais que implementam sistemas de Controle de Supervisão e Aquisição de Dados – *Supervisory Control and Data Acquisition (SCADA)*. Sensores inteligentes instalados ao longo de toda a extensão da rede coletam, em tempo real, informações detalhadas sobre o consumo de energia e os transmitem para centrais de dados, formando uma Infraestrutura de Monitoramento Avançada (IMA) (YAN et al., 2013). A Figura 2.1 ilustra a arquitetura genérica da infraestrutura de um smart grid.

Figura 2.1 – Arquitetura de um smart grid




Fonte: Autor

### 2.1.3 Ameaças

A introdução de uma estrutura de comunicação autônoma e amplamente distribuída que ampara todo o funcionamento da rede elétrica expõe todo o sistema à possibilidade de ataques cibernéticos. A infraestrutura de comunicação, por ser desenvolvida sobre TIC, é inerentemente vulnerável a diversos tipos de ataque, que podem ser utilizados para manipular dados ou obstruir o funcionamento do sistema (CHEN; CHENG; CHEN, 2012). Medidores inteligentes também são potencialmente inseguros, estando vulneráveis a ataques de negação de serviço, roubo de informações de usuários e manipulação de dados (ASHFORD, 2011).

A evolução dos ataques cibernéticos e o risco que representam para infraestruturas críticas podem ser observados em fenômenos como o Stuxnet, um *malware* desenvolvido para atacar controladores de sistemas industriais. O Stuxnet insere código ilegítimo na execução do controlador, que passa a ser executado em detrimento do código original, sem ser detectado, podendo levar à interrupção do serviço e danificar componentes do sistema atingido (LANGNER, 2011).

Uma taxonomia dos tipos de ataques cibernéticos em estruturas de comunicação de smart grids é apresentada em (LI et al., 2012). Os autores descrevem quatro tipos de ataques, como apresentados na Tabela 2.1: ataques a dispositivos, ataques de dados, ataques de privacidade e ataques de disponibilidade de rede.

#### *2.1.3.1 Ataques a dispositivos*

Ataques a dispositivos têm como finalidade obter controle sobre um elemento do smart grid e utilizá-lo para um objetivo malicioso. De modo geral, servem a dois propósitos: fornecer os meios para um ataque de dados ou de disponibilidade ou, caso o dispositivo afetado possua funções de controle críticas, causar danos físicos ao sistema.

#### *2.1.3.2 Ataques de dados*

Ataques de dados configuram a tentativa de manipular os dados presentes na rede. Os dados manipulados podem ser informações de usuários ou sinais dos dispositivos de controle do smart grid. Seus usos variam de alterar dados de um usuário, para reduzir o valor da energia consumida, a eliminar sinais enviados por dispositivos de controle, para impedir o monitoramento e diagnóstico dos elementos da rede, o que pode levar à interrupção do funcionamento do sistema.

#### *2.1.3.3 Ataques de privacidade*

Ataques de privacidade têm o objetivo de obter informações privativas dos usuários. No caso dos smart grids, essas informações são os dados sobre o consumo de energia elétrica dos usuários, transmitidos pela rede de comunicação. Essas informações podem ser utilizadas para mapear dados privativos sobre a rotina dos usuários, que podem ser utilizados para fins maliciosos.

#### *2.1.3.4 Ataques de disponibilidade*

Ataques de disponibilidade de rede, ou ataques de negação de serviço, causam lentidão no tráfego de dados do smart grid através da sobrecarga da rede de comunicação e recursos computacionais. A velocidade da troca de dados é crítica para o funcionamento de um smart grid, e lentidão ou indisponibilidade do tráfego da rede podem causar prejuízos sérios aos seus usuários.

Tabela 2.1 – Taxonomia dos tipos de ataques cibernéticos em smart grids

| Nome | Descrição |
|---|---|
| Ataques a dispositivos | Têm como objetivo comprometer (controlar) um dispositivo da rede. Frequentemente, é o passo inicial de um ataque sofisticado. |
| Ataques de dados | Tentam inserir, alterar ou deletar dados no tráfego da rede para induzir o smart grid a tomar decisões erradas. |
| Ataques de privacidade | Têm como objetivo obter/inferir informações privadas do usuário analizando dados sobre a utilização de energia elétrica. |
| Ataques de disponibilidade de rede | Visam esgotar ou sobrecarregar os recursos de comunicação e computacionais do smart grid para causar atraso ou falha de comunicação. |

Fonte: (LI et al., 2012)

## 2.2 Mecanismos de Segurança

Garantir confiabilidade e segurança é um grande desafio no desenvolvimento dos smart grids. O desacoplamento das funcionalidades de controle e comunicação dos dispositivos elétricos e a modularização dos subsistemas leva a uma inevitável perda de confiabilidade. Componentes passam a ser originários de diferentes fabricantes, introduzindo margem à incompatibilidades e falhas de comunicação. A agregação de fontes de energia distribuída, incluindo usinas de geração instáveis, levarão a fluxos de energia reversos e variações de voltagem. Ataques maliciosos podem ser direcionados tanto à rede elétrica física quanto à rede de comunicação (LI et al., 2012). Apesar da existência de uma vasta gama de tecnologias de segurança voltadas à TIC, essas medidas de segurança não são capazes de resguardar o sistema contra ataques desenvolvidos para atingir sistemas SCADA, medidores inteligentes e outros componentes do smart grid (CARCANO et al., 2011). A seguir, são apresentados alguns mecanismos de segurança comumente utilizados em smart grids. Em 2.2.1, são introduzidas as normas de segurança documentadas para smart grids, e 2.2.2 aborda mecanismos de detecção de intrusão.

### 2.2.1 Normas de Segurança

A maior parte dos esforços para promover o desenvolvimento de smart grids mais seguros se concentra em normas e padrões de segurança. O conjunto de diretrizes de segurança NISTIR 7628 (NIST, 2014), desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos - National Institute of Standards and Technology (NIST), apresenta um pa-

norama geral de orientações, métodos e regulamentações para prover segurança cibernética a sistemas de controle industriais e automação. Entretanto, fatores como a complexidade do smart grid, sua ampla distribuição geográfica e sua larga escala fazem com que as práticas descritas pelas normas de segurança, como o uso de criptografia e autenticação nas interfaces de comunicação entre subsistemas, não sejam o bastante para garantir que o sistema estará seguro contra usuários maliciosos. Em (CHAN; ZHOU, 2013), os autores encontraram vulnerabilidades ao aplicarem o NISTIR 7628 a uma infraestrutura de carregamento de um veículo elétrico, demonstrando que os padrões de segurança descritos não são suficientes para garantir a segurança de um smart grid.

### 2.2.2 Mecanismos de Detecção de Intrusão

Sistemas de Detecção de Intrusão (SDI) são aptos a detectar ataques lançados através de dispositivos internos do sistema que tenham sido comprometidos, reconhecendo o comportamento padrão de um sistema e identificando ataques a partir da premissa de que as ações de um atacante diferem do funcionamento convencional do sistema (LI et al., 2012). Todavia, SDIs tradicionalmente desenvolvidos para TIC falham em suprir os requisitos de segurança de sistemas SCADA, e mecanismos voltados para satisfazer as necessidades desses sistemas ainda não estão suficientemente amadurecidos. Em (COUTINHO et al., 2009), os autores apresentam uma técnica de detecção de anomalias para centros de controle de infraestruturas críticas, utilizando o Algoritmo de Classificação de Conjuntos Irregulares, capaz de identificar dados corrompidos introduzidos em um sistema de energia elétrica de seis barramentos. Uma abordagem à detecção de intrusão em sistemas SCADA baseada em Análise de Estado Crítico e Proximidade de Estados é analisada em (CARCANO et al., 2011). (TSANG; KWONG, 2005) introduz um SDI multi agente, baseado no Modelo de Clusterização da Colônia de Formigas, para detecção descentralizada de anomalias em redes distribuídas.

#### *2.2.2.1 Classificação de Tráfego com algoritmos de Aprendizado de Máquina*

Algoritmos de Aprendizado de Máquina têm sido utilizados para a classificação de tráfego internet por por possuírem diversas características vantajosas para a tarefa. Enquanto técnicas de classificação de tráfego tradicionais dependem da inspeção do conteúdo de pacotes, mecanismos baseados em AM classificam os dados através de atributos que podem ser observados externamente, como tamanho dos pacotes e tempo entre a chegada de pacotes, criando padrões

estatísticos. Há benefícios consideráveis nessa abordagem: o campo de dados do pacote deixa de ser obrigatoriamente visível (os dados podem estar criptografados, por exemplo), e o classificador não precisa conhecer a sintaxe dos dados nos pacotes de cada aplicação (NGUYEN; ARMITAGE, 2008).

Primeiramente, a tarefa de classificação utilizando AM requer que atributos sejam definidos. Atributos são características dos fluxos de pacotes, como tamanho máximo e mínimo de pacote e tempo médio entre chegada de pacotes, que serão utilizados para selecionar instâncias de dados de tráfego. É necessário, então, treinar o algoritmo classificador, associando conjuntos de atributos com classes de tráfego definidas. Através da etapa de treinamento, o algoritmo gera o conjunto de regras que será utilizado para determinar a qual classe pertence uma determinada entrada. Finalmente, utilizando o conjunto de regras geradas no treinamento, o classificador pode receber dados de tráfego desconhecidos e identificar a que classe pertencem (NGUYEN; ARMITAGE, 2008).

## 2.3 Ferramentas de Simulação

Inserir texto aqui.

### 2.3.1 VirtuaPlant

VirtuaPlant (SEIDL, 2015) é um simulador de Sistemas de Controle Industriais (SCI). Possui uma interface gráfica chamada World View que simula o efeito das ações do sistema de controle sobre um recurso virtual utilizando protocolo Modbus. O recurso é representado por uma fábrica que enche garrafas.

O Controlador Lógico Programável (CLP) é implementado sobre a biblioteca pymodbus, que roda em uma thread separada no componente World View e compartilha seu contexto, que contém registradores, entradas e valores, com as funções do World View para simular recursos sendo conectados ao controlador.

A Interface Homem-Máquina (HMI) utiliza GTK3 e executa o cliente pymodbus em uma thread separada, que conecta com o servidor através de TCP/IP, obtendo leituras constantes dos valores do servidor, isto é, do CLP.

A ferramenta VirtuaPlant fornece uma variedade de scripts de ataque ao CLP. Entretanto, não permite a definição de novos dispositivos, não sendo possível a definição de novas topolo-

gias. Também não possibilita a modelagem de elementos da infraestrutura de comunicação, já que a simulação engloba apenas a leitura e escrita dos valores do controlador PLC.

### 2.3.2 Mosaik

O Mosaik (MOSAIK, 2015) permite usar diversos simuladores existentes em um contexto comum para realizar uma simulação coordenada de um cenário, que representa um conjunto de componentes de smart grid. Oferece uma API para os simuladores se comunicarem com ele e possui handlers para cada tipo de processo dos simuladores.

A ferramenta permite a modelagem de diferentes cenários envolvendo esses simuladores, possibilitando a criação de novos objetos e definição de novas topologias. A biblioteca SimPy é utilizada para a simulação coordenada de cenários, e a execução da simulação é feita executando passos em cada simulador ao longo do tempo. Cada simulador executa o seu próprio processo e laço de eventos, enquanto o Mosaik sincroniza esses processos e gerencia a troca de dados entre eles. Através da combinação com outros simuladores, é possível simular uma estrutura TIC.

O protocolo de comunicação entre o Mosaik e os simuladores é definido por uma API. Existem duas versões da API: alto nível e baixo nível. A API baixo nível utiliza sockets TCP para estabelecer a comunicação entre o mosaik e os simuladores através da troca de mensagens JSON. A API alto nível, atualmente disponível nas linguagens Python e Java, fornece o encapsulamento dessa comunicação em uma classe abstrata, onde as mensagens trocadas entre os simuladores e o mosaik são implementadas como métodos.

A criação de cenários de simulação é feita por uma API que permite iniciar simuladores e instanciar modelos a partir deles, criando um conjunto de entidades. É possível conectar as entidades entre si para estabelecer a troca de dados entre elas.

O gerenciador de simuladores é responsável por iniciar e gerenciar os processos dos simuladores e a comunicação entre eles. Permite iniciar novos processos de simuladores, conectar a processos que já estão em execução e, no caso de simuladores desenvolvidos em Python, também permite importar módulos de simuladores e executá-los durante a execução do processo.

### 2.3.3 SCADASim

A ferramenta SCADAsim (QUEIROZ; MAHMOOD; TARI, 2011) é um framework para construção de simulações SCADA. Possui um conjunto de módulos que representam os componentes SCADA, como RTUs, PLCs e MTUs, e implementa os protocolos Modbus TCP e DNP3. Permite a integração de componentes externos e componentes internos simultaneamente através do conceito de Gates, que são objetos que conectam um ambiente externo com o ambiente da simulação.

É baseado em 3 componentes principais: SSScheduler, SSGate e SSProxy. SSScheduler é um escalonador em tempo real que permite controlar e sincronizar mensagens recebidas. Gerencia uma lista de instâncias do componente SSGate, que são responsáveis por enviar e receber mensagens de um ambiente externo, garantindo a sincronização das mensagens entre dois ambientes. SSGate fornece conexão com o ambiente externo através de um protocolo, que é utilizado para se comunicar com os componentes SCADA externos. Atualmente os protocolos disponíveis são: ModbusGate, DNP3Gate e HTTPGate. SSProxy representa um dispositivo real ou aplicação externa que interage com os objetos simulados e com um SSGate, que direciona suas mensagens para componentes externos.

Os protocolos são gerenciados de dois modos. Os protocolos utilizados dentro do ambiente do simulador para comunicação entre componentes da simulação são chamados de protocolos simulados. Os protocolos utilizados para comunicação entre dispositivos e aplicações externas e os SSGates são chamados de protocolos originais. No ambiente interno da simulação, toda a comunicação entre os componentes utiliza versões simuladas dos protocolos SCADA. O framework possui uma biblioteca de protocolos SCADA originais e simulados, contendo: Modbus TCP, DNP3 TCP e HTTP.

O simulador SCADASim permite, através dos módulos integrados de componentes SCADA, criar componentes e definir topologias, além de possibilitar a integração com componentes reais através da API. Possui, também, uma biblioteca com alguns tipos de ataques comuns à estruturas SCADA, como worm e DDoS. Não suporta, todavia, a modelagem de elementos de geração de energia, presentes em um smart grid.

### 2.3.4 Modbus PLC Simulator

O Modbus PLC Simulator (BRAAM, 2009) é um simulador de CLP baseado na ferramenta Modbus Slaves. O Modbus Slaves é uma ferramenta que permite simular até 32 dispo-

sitivos simultaneamente. Os dados contidos nos dispositivos escravos (slaves) são acessíveis à aplicação mestre. Permite monitoramento de tráfego serial. Cada instância de escravo pode ser configurada para representar dados de um mesmo nodo ou de nodos diferentes.

A ferramenta suporta os protocolos Modbus TCP/IP, Modbus RTU (serial) e AB-DF1. Funciona criando uma thread de comunicação com interface para a API de comunicação e controla um bloco de RAM que funciona como a memória do CLP.

O Modbus PLC Simulator possibilita a simulação da troca de dados entre um dispositivo CLP, representado pela aplicação mestre, e outros dispositivos, não fornecendo suporte, entretanto, para os demais aspectos da comunicação TIC, como modelagem de topologias e de dispositivos da infraestrutura de rede.

### 2.3.5 Comparação entre ferramentas de simulação

Tu precisas de um texto aqui...

Explica que como o propósito desse trabalho é desenvolver e avaliar um mecanismo de detecção em uma ferramenta de simulação, tu estabeleceu uma série de critérios X, Y, Z para selecionar a ferramenta mais adequada as tuas necessidades, etc, etc, etc

Tabela 2.2 – Comparação entre ferramentas de simulação

| | *VirtuaPlant* | *Mosaik* | *SCADASim* | *Modbus PLC Simulator* |
|---|---|---|---|---|
| Simulação da infraestrutura TIC | N/D | API permite integração com simuladores de rede | Componente SSGate simula estrutura de comunicação | N/D |
| Simulação de consumo e geração de energia | N/D | Modelado pelo simulador Pypower | N/D | N/D |
| Elementos modeláveis | Leitura e escrita de valores do CLP | Infraestrutura TIC, consumo e geração de energia e componentes SCADA | Infraestrutura TIC e componentes SCADA | Apenas tráfego de dados entre componentes e CLP |
| Protocolos de rede | Modbus | API para integração com simuladores de rede | Modbus e DNP3 | Modbus |
| Modelagem de troca de pacotes de rede e informações de energia | N/D | Através dos simuladores de rede integrados | Modelagem realizada pelo componente SSGate | N/D |
| Definição de novas topologias | N/D | Permite definição de componentes e topologias | Permite definição de componentes e topologias | N/D |
| Criação e simulação de ataques | Inclui ataques que atingem os dados do CLP | Não inclui ataques, mas é possível desenvolvê-los para componentes SCADA e TIC | Inclui biblioteca de ataques a componentes da estrutura SCADA | Possível desenvolver ataques para o componente CLP |

Fonte: O Autor

# 3 MODELAGEM E DESENVOLVIMENTO

O problema proposto por esse trabalho consiste em implementar um mecanismo de detecção de intrusão e avaliá-lo utilizando uma ferramenta que simule a infraestrutura de um smart grid. Para isso, é necessário desenvolver um SDI e integrá-lo à ferramenta de simulação, de modo que o SDI possa receber, em tempo real, dados do ambiente smart grid e operar sobre eles.

Neste capítulo, serão apresentadas a modelagem e as ferramentas utilizadas para o desenvolvimento de uma solução para problema proposto. A Seção 3.1 contém mais informações sobre o framework ASTORIA, utilizado para configurar as simulações do ambiente smart grid. A Seção **??** descreve a modelagem do SDI proposto e as tecnologias utilizá-das para desenvolvê-lo.

## 3.1 Simulação da estrutura de smart grid com Framework ASTORIA

O Framework ASTORIA, descrito pelos autores em (WERMANN et al., ), permite modelar simulações de ambientes smart grid, definir e executar ataques nesses ambientes e avaliar seus resultados e o comportamento do sistema. O propósito da utilização do mosaik é agregar diversos simuladores em um contexto comum, para que sua execução sincronizada possa criar um ambiente de smart grid. Para isso, é necessário conectar as ferramentas que farão a simulação dos componentes dos smart grid.

A simulação da rede elétrica é realizada pelo PYPOWER, uma ferramenta nativamente integrada ao mosaik. Para realizar a simulação do componente de comunicação do smart grid, foi realizada a integração do mosaik com o simulador de redes ns-3. O restante desta seção descreve o framework ASTORIA, seu funcionamento e as simulações produzidas por ele. Em 3.1.1, é abordado o simulador de redes ns-3, utilizado para compor os elementos de comunicação da simulação. 3.1.2 fala sobre a integração entre as ferramentas que compõe o framework, os simuladores mosaik, ns-3 e PYPOWER. Por fim, 3.1.3 mostra a estrutura das simulações produzidas pelo framework.

### 3.1.1 ns-3

O ns-3 [nsnam] é um simulador de redes que funciona mantendo uma lista de eventos que devem ser executados, sequencialmente, em determinados tempos da simulação. Desenvolvido para fins de estudo e pesquisa, está disponível publicamente para uso, e sua estrutura suporta simulações tanto de redes baseadas em IP quanto de redes não baseadas em IP. Também permite a interação entre simulações e dispositivos reais, possibilitando o envio de pacotes gerados pelo simulador para dispositivos de uma rede real.

O ns-3 utiliza possui diversas classes que representam abstrações dos objetos reais de uma rede.

- Nó: Um nó, modelado pela classe Node, representa um dispositivo computacional, também referido como host ou terminal em um rede Internet.
- Aplicação: Uma aplicação é um programa de usuário que gera alguma atividade a ser simulada. Como o simulador não possui conceito de programas de sistema, existem apenas as aplicações que são executadas nos nós, representados pela classe Application.
- Canal de Comunicação: Canais de comunicação são objetos que conectam sub-redes e os nós, formando o meio de comunicação entre os elementos. São descritos pela classe Channel.
- Dispositivo de Rede: Um dispositivo de rede é acoplados a um nó para permitir que ele se comunique com outros nós através dos canais de comunicação. É modelado pela classe NetDevice e simula tanto os elementos de hardware quanto os de software de um dispositivo de rede real. É possível conectar um nó a diversos canais utilizando múltiplos dispositivos de rede.
- Assistentes de Topologia: Assistentes de Topologia são objetos que combinam diversas operações distintas que são necessárias para a execução da simulação, como a criação e interconexão de objetos, com o objetivo de oferecer um modelo simplificado para a simulação.

### 3.1.2 Integração entre as ferramentas

A simulação de um smart grid utilizando o ASTORIA acontece através da integração das funcionalidades de três ferramentas: PYPOWER, que realiza a simulação da rede de energia elétrica, ns-3, que simula a rede de comunicação da estrutura SCADA, e mosaik, que sincroniza

a execução das demais ferramentas.

O PYPOWER [pypower], é uma ferramenta que implementa as funcionalidades do MATPOWER [matpower] na linguagem Python e permite simular cenários de fluxo de energia elétrica, fornecendo os dados de produtores e consumidores de energia. O PYPOWER permite a simulação de uma estrutura de rede elétrica e gera dados de produção e consumo em tempo real. Esses dados são fornecidos, através do mosaik, para a rede de comunicação. Como o PYPOWER já é originalmente integrado ao mosaik, os dois já estão conectados e não há necessidade de implementar a troca de dados entre eles.

A integração do mosaik com o simulador ns-3, utilizado para compor o elemento de comunicação da simulação do smart grid, foi feita através da mosaik Sim API, que possibilita a sincronização com outros simuladores. A comunicação entre as ferramentas é realizada através de sockets TCP e mensagens JSON. As mensagens seguem o padrão requisição-resposta e são compostas por um cabeçalho, que carrega o número de bytes no corpo, e pelo corpo da mensagem, que contém o tipo, o identificador e o conteúdo da mensagem. As mensagens a seguir são utilizadas pelo mosaik para comunicação com os simuladores.

Chamadas enviadas pelo mosaik para os simuladores:

- *init()*: Inicialmente, quando a conexão é estabelecida, o mosaik chama o método init(), que passa parâmetros globais ao simulador, que responde com informações sobre ele.
- *create()*: As simulaçoes podem ser instanciadas pelo mosaik utilizando o método create(), que também retorna dados sobre os objetos criados.
- *setup_done()*: A fase de configuração é encerrada pela chamada do método setup_done(), que é seguido por múltiplas chamadas do método step().
- *step()*: Cada chamada de step() feita pelo mosaik permite que o simulador avance uma etapa de simulação no tempo e execute eventos agendados para aquele instante. A chamada é retornada com o próximo instante de tempo em que o simulador deve performar a próxima ação.
- *get_data()*: Mensagens get_data() podem ser enviadas para requisitar dados sobre alguma instancia.
- *stop()*: O envio da mensagem stop() pelo mosaik para cada simulador indica que ele deve ser encerrado.

As seguintes requisições assíncronas podem ser enviadas pelos simuladores, durante uma etapa da simulação, para o mosaik:

O ns-3 inicia a conexão com o mosaik através de um socket TCP e, por meio dessa

conexão, é realizado o envio das mensagens, através das quais o mosaik sincroniza a execução dos dois simuladores, PYPOWER e ns-3, e fornece os dados da rede elétrica para a rede de comunicação.

A execução do mosaik é baseada em passos. Após a fase de configuração, em que é feita a inicialização dos simuladores e a criação das instâncias de simulação, é enviada para o ns-3 uma mensagem a cada passo de execução, contendo os dados referentes à produção e ao consumo de energia, gerados pelo PYPOWER. Ao receber a mensagem contendo esses dados, o ns-3 executa a etapa atual da simulação, responde a mensagem com o instante em que a próxima etapa de simulação deve ser executada e entra em espera até receber a próxima mensagem.

### 3.1.3 Simulação do ambiente smart grid

A rede de energia elétrica é composta por nodos de geração, consumo e distribuição de energia. Os dados medidos nos componentes são gerados a partir de perfis de produção e consumo de energia presentes no simulador. A estrutura SCADA formada pela rede de comunicação é composta por sensores, RTUs e MTUs. Cada nodo de produção, distribuição e consumo presente na rede elétrica possui um nodo correspondente na rede de comunicação SCADA. Cada nodo de produção ou consumo está pareado com um sensor SCADA, enquanto os nodos de distribuição de energia estão pareados com as RTUs. As MTUs não possuem nenhum componente respectivo na rede elétrica, por serem um componente exclusivo da estrutura SCADA. A Figura **??** mostra a estrutura dos componentes na simulação do ambiente smart grid com o framework ASTORIA. Os dados recebidos por cada sensor SCADA contém informações sobre a produção e o consumo de energia da unidade associada a ele. As RTUs recebem os dados de todos os sensores conectados a elas, e então enviam todas as informações recolhidas para a MTU. A comunicação entre os componentes SCADA acontece através do protocolo modbus.

(inserir aqui imagem da estrutura dos componentes da simulação)

## 3.2 Mecanismo de Detecção de Intrusão

# 4 IMPLEMENTAÇÃO E ANÁLISE DE RESULTADOS

## 4.1 Implementação dos Mecanismos de Detecção

## 4.2 Execução dos Experimentos

## 4.3 Análise dos Resultados

# 5 CONCLUSÃO E TRABALHOS FUTUROS

## 5.1 Resumo de Contribuições

## 5.2 Trabalhos Futuros

## REFERÊNCIAS

AMIN, S.; WOLLENBERG, B. Toward a smart grid: power delivery for the 21st century. **Power and Energy Magazine, IEEE**, v. 3, n. 5, p. 34–41, Sep 2005.

ASHFORD, W. **Smart meter and smart grids: security risk or opportunity?** 2011. Available from Internet: <http://www.computerweekly.com/news/1280097292/Smart-meter-and-smart-grids-security-risk-or-opportunity>.

BOU-HARB, E. et al. Communication security for smart grid distribution networks. **Communications Magazine, IEEE**, v. 51, n. 1, p. 42–49, Jan 2013.

BRAAM, C. **Modbus PLC Simulator**. 2009. Available from Internet: <http://www.plcsimulator.org/>.

CARCANO, A. et al. A multidimensional critical state analysis for detecting intrusions in scada systems. **Industrial Informatics, IEEE Transactions**, v. 7, n. 2, p. 179–186, May 2011.

CHAN, A.; ZHOU, J. On smart grid cybersecurity standardization: Issues of designing with nistir 7628. **Communications Magazine, IEEE**, v. 51, n. 1, p. 58–65, Jan 2013.

CHEN, P.-Y.; CHENG, S.-M.; CHEN, K.-C. Smart attacks in smart grid communication networks. **Communications Magazine, IEEE**, v. 50, n. 8, p. 24–29, Aug 2012.

COUTINHO, M. et al. Anomaly detection in power system control center critical infrastructures using rough classification algorithm. **Digital Ecosystems and Technologies, 2009. DEST 09. 3rd IEEE International Conference**, p. 733–738, Jun 2009.

LANGNER, R. Stuxnet: Dissecting a cyberwarfare weapon. **Security and Privacy, IEEE**, v. 9, n. 3, p. 49–51, May 2011.

LI, X. et al. Securing smart grid: cyber attacks, countermeasures, and challenges. **Communications Magazine, IEEE**, v. 50, n. 8, p. 38–45, Aug 2012.

MOSAIK. 2015. Available from Internet: <https://mosaik.offis.de/>.

NGUYEN, T.; ARMITAGE, G. A survey of techniques for internet traffic classification using machine learning. **Communications Surveys and Tutorials, IEEE**, v. 10, n. 4, p. 56–76, Fourth Quarter 2008.

NIST. Nistir 7628 revision 1: Guidelines for smart grid cybersecurity. **NISTIR 7628 Rev. 1**, v. 1-3, Sep 2014.

QUEIROZ, C.; MAHMOOD, A.; TARI, Z. Scadasim - a framework for building scada simulations. **Smart Grid, IEEE Transactions**, v. 2, n. 4, p. 589–597, Sep 2011.

SEIDL, J. **VirtuaPlant**. 2015. Available from Internet: <http://wroot.org/projects/virtuaplant/>.

TSANG, C.-H.; KWONG, S. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. **Industrial Technology, 2005. ICIT 2005. IEEE International Conference**, p. 51–56, Dec 2005.

WERMANN, A. G. et al. Astoria: A framework for attack simulation and evaluation in smart grids.

YAN, Y. et al. A survey on smart grid communication infrastructures: Motivations, requirements and challenges. **Communications Surveys and Tutorials, IEEE**, v. 15, n. 1, p. 5–20, Feb 2013.