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

SUMÁRIO

1 INTRODUÇÃO

1.1 Motivação

1.2 Objetivos

1.3 Contribuição

1.4 Estrutura do Trabalho

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Smart Grids

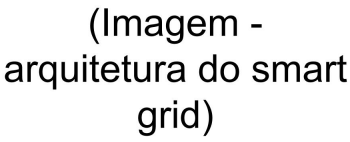
Smart Grids combinam redes de energia elétrica com estruturas de comunicação, baseadas em Tecnologia de Informação e Comunicação (TIC), que provêm um meio de troca de dados entre os componentes envolvidos no processo de produção, distribuição e consumo de energia. Como suas principais características, 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).

2.1.1 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

2.1.2 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 mínimo impacto possível na ocorrência de sobrecarga, mal funcionamento ou ataques maliciosos (AMIN; WOLLENBERG, 2005).

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 a 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 Detecção

2.3 Ferramentas de Simulação

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 topologias. 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 loop 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 trocar mensagens JSON. A API alto nível é a implementação API baixo nível em uma linguagem de programação, cuja versão atual tem disponíveis as linguagens Python e Java, e encapsulamento da comunicação em uma classe abstrata.

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 fluxo 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 3, 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 scheduler 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 2 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 pro-

tocolos 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 dispositivos 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 BACnet Device Simulator 2.0

O BACnet Device Simulator 2.0 (BACNET. . . ,) permite testar a funcionalidade de uma rede BACnet através da criação de dispositivos e objetos. O protocolo BACnet foi desenvolvido comunicação de sistemas de construção automatizada e controle, permitindo a troca de informação entre dispositivos de construção automática.

A ferramenta age como um simulador global que executa todas as instâncias de todos

os dispositivos internos do sistema e permite a criação de novas redes, acessar e salvar redes previamente definidas. É possível criar dispositivos presentes na rede e os objetos associados a esses dispositivos, manipular as propriedades e os valores associados às propriedades dos objetos, a fim de modelar a rede simulada.

Embora permita a definição e troca de dados entre componentes, o BACnet Device Simulator 2.0 se restringe a dispositivos e objetos de redes BACnet, não havendo a possibilidade de definir outros componentes de comunicação e da estrutura do smart grid.

2.3.6 Comparação entre ferramentas de simulação

Tabela 2.2 – Comparação entre ferramentas de simulação

	VirtuaPlant	*Mosaik*	*SCADASim*	*Modbus PLC Simulator*	*BACnet Device Simulator 2.0*
Simulação da infraestrutura CIT	N/D	Através do simulador de rede	Através do componente SSGate	N/D	Apenas da estrutura de rede BACnet
Simulação de consumo e geração de energia	N/D	Modelado pelo simulador pypower	N/D	N/D	N/D
Elementos modeláveis	Leitura e escrita no CLP	TIC e consumo e geração de energia	TIC e componentes SCADA	Tráfego de dados entre componentes e CLP	Tráfego de dados entre componentes da rede BACnet
Protocolos de rede	Modbus	API para integração com simuladores de rede	Modbus e DNP3	Modbus	BACnet
Modelagem de troca de pacotes de rede e informações de energia	N/D	Através do simulador de rede	Através do componente SSGate	N/D	N/D
Definição de novas topologias	N/D	Definição de componentes e topologias	Definição de componentes e topologias	N/D	N/D
Criação e simulação de ataques	Inclui ataques para o componente CLP	Possível desenvolver ataques para os os simuladores	Inclui biblioteca de ataques a estruturas SCADA	Possível desenvolver ataques para o componente CLP	N/D

Fonte: O Autor

3 MODELAGEM E DESENVOLVIMENTO

3.1 Integração dos Simuladores Mosaik e ns-3

3.2 Mecanismos de Detecção

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. Accessed: 2015-08-25. Available from Internet: <http://www.computerweekly.com/news/1280097292/Smart-meter-and-smart-grids-security-risk-or-opportunity>.

BACNET Device Simulator 2.0. Accessed: 2015-08-11. Available from Internet: <http://www.scadaengine.com/software6.html>.

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. Accessed: 2015-08-11. Available from Internet: <http://www.plcsimulator.org/>.

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.

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. Accessed: 2015-08-11. Available from Internet: <https://mosaik.offis.de/>.

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. Accessed: 2015-08-11. Available from Internet: <http://wroot.org/projects/virtuaplant/>.

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.