UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

SEGURANÇA CIBERNÉTICA E REDES DE COMUNICAÇÃO EM SISTEMAS SCADA NO CONTEXTO DE SMART GRID

TRABALHO DE CONCLUSÃO DE CURSO

Pedro Wessel

Santa Maria, RS, Brasil
2015

STRC/UFSM, RS WESSEL, Pedro Tecnólogo 2015

SEGURANÇA CIBERNÉTICA E REDES DE COMUNICAÇÃO EM SISTEMAS SCADA NO CONTEXTO DE SMART GRID

Pedro Wessel

Trabalho apresentado ao Curso de Graduação em Tecnologia em Redes de Computadores, Área de concentração em Segurança da Informação, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores.

Orientador: Prof. Me. Tiago Antonio Rizzetti

Coorientador: Prof. Me. Renato Preigschadt de Azevedo

Santa Maria, RS, Brasil

2015

Universidade Federal de Santa Maria
Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em Redes de Computadores

A Comissão Examinadora, abaixo assinada, aprova a Monografia

SEGURANÇA CIBENÉTICA E REDES DE COMUNICAÇÃO EM SISTEMAS SCADA NO CONTEXTO DE SMART GRID

elaborada por
Pedro Wessel

como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA

Tiago Antonio Rizzetti, Me.
(Presidente/Orientador)

Alfredo Del Fabro Neto, Tecg. (UFSM)

Murilo Cervi, Dr. (UFSM)

Santa Maria, 03 de julho de 2015

Dedico este trabalho a minha namorada **Ane Weber** pelo apoio e carinho oferecidos em todos momentos, pessoa de grande importância em minha formação.

AGRADECIMENTOS

Agradeço a minha mãe Otilia Maria Wessel, que acreditou nos meus propósitos e soube compreender minha ausência em muitos momentos.

A minha namorada Ane Weber, pelo amor, carinho e compreensão. Essa conquista não seria possível sem o teu apoio.

Ao meu orientador Prof. Me. Tiago Antonio Rizzetti, pela oportunidade, pelos ensinamentos, amizade e paciência. Pela orientação que se iniciou no 2° semestre.

Ao meu coorientador Prof. Me. Renato Preigschadt de Azevedo, pelo aceite do convite de coorientação, pelas dicas, técnicas e orientações.

Ao Prof. Dr. Murilo Cervi, pelos ensinamentos, pelo auxilio, pelas oportunidades, pela amizade.

Um agradecimento especial a toda família, Roque Weber, Ilca Maria Weber, Augusto Weber, Márcia Hammerschmitt, Marli Gerhardt, Tamily Joana Gerhardt, Juliano Gerhardt, que de alguma forma fizeram parte dessa conquista.

A todos professores do curso de Redes de Computadores, os meus agradecimentos pelos ensinamentos e conversas que foram muito importantes para o meu crescimento pessoal e profissional.

Agradeço aos amigos da bolsa, pelo compartilhamento dos conhecimentos, pelas ajudas, pelos momentos de estudo, pelas risadas, pelas ótimas lembranças que certamente ficarão em minha memória.

A todos que direta ou indiretamente colaboraram na concretização deste trabalho.

Muito obrigado a todos!

“Posso ainda não ter
chegado onde eu queria,
mas estou mais
perto do que ontem.”

(Autor Desconhecido)

RESUMO

Monografia
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

SEGURANÇA CIBENÉTICA E REDES DE COMUNICAÇÃO EM SISTEMAS SCADA NO CONTEXTO DE SMART GRID

AUTOR: PEDRO WESSEL
ORIENTADOR: TIAGO ANTONIO RIZZETTI
Data e Local da Defesa: Santa Maria, 03 de julho de 2015

A necessidade por energia, nas mais diversas atividades humanas, torna os sistemas elétricos de potência um serviço essencial, cuja disponibilidade afeta de forma intensa a sociedade. A integração das tecnologias da informação e o conjunto de aplicações utilizados para gerenciá-lo compõe um sistema de Redes Elétricas Inteligentes. Neste sistema, é imprescindível um canal bidirecional de dados, que ofereça segurança na comunicação, para que o sistema de energia possa realizar o monitoramento e gerenciamento através de softwares específicos para essa finalidade, como os sistemas SCADA (*Supervisory Control and Data Acquisition*). Essa comunicação converge para o uso de redes IP, o que traz ganhos em função da ampla utilização deste tipo de rede. Em função da criticidade dos sistemas de energia, prover um sistema de comunicação confiável e seguro são premissas fundamentais para seu correto funcionamento. Para isso, este trabalho tem por objetivo abordar as principais tecnologias utilizadas, ameaças e vulnerabilidades existentes em aplicações SCADA no contexto de Redes Elétricas Inteligentes. E também implementar uma proposta visando tornar as comunicações entre os sistemas SCADA e os IEDs (*Intelligent Electronic Devices*) segura, para evitar ataques de negação de serviço (DoS) além de atender aos critérios de autenticidade, integridade e confidencialidade.

Palavras-chave: Redes Elétricas Inteligentes, SCADA, IED, Segurança, Redes de Comunicação.

ABSTRACT

Monography
Superior Course of Tchnology in Computer Networks
Federal University of Santa Maria

Cyber security and communication network on SCADA systems in the context of Smart Grids

AUTHOR: PEDRO WESSEL
ADVISER: TIAGO ANTONIO RIZZETTI
Defense Place and Date: Santa Maria, July 03rd, 2015

The need for energy at the various human activities, makes the power system an essential service, and its whose the availability affects intensively the society. The integration of information technology and the applications set utilized to manage it comprises a Smart Grids System. In this system, is essential a two-way channel data that provides security in communication. Thus, the power system can perform monitoring and management through specific software for this purpose, such as Supervisory Control and Data Acquisition (SCADA) systems. This communication converges into the use of IP networks, which brings gains in function of the wide utilization of this type of network. In function on the criticality of power systems, provide a reliable and secure communication system are fundamental premises for your seemly correct. Therefore, this study aims to address the key technologies used, threats and vulnerabilities in SCADA applications in the context of Smart Grids. Also implement a proposal to make communications between SCADA systems and Intelligent Electronic Devices (IEDs) secure. Thus to avoid denial of service (DoS) attacks and meet the criteria of authenticity, integrity and confidentiality.

Key words: Smart Grid, SCADA, IED, Security, Communication Networks.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AMI	*Advanced Metering Infrastructure*
AMR	*Automatic Meter Reading*
CCM	Centro de Controle de Medição
DDoS	*Distributed Denial of Service*
DoS	*Denial of Service*
GOOSE	*Generic Object Oriented Substation Event*
HMI	*Human Machine Interface*
ID	Identificador
IEC	*International Electrotechnical Commission*
IED	*Intelligent Electronic Devices*
IP	Internet *Protocol*
MMS	*Manufacturing Message Specification*
MEPA	Mediador de Pacotes
P&D	Pesquisa e Desenvolvimento
PMU	*Phasor Measurement Units*
QoS	*Quality of Service*
RTU	*Remote Terminal Units*
SCADA	*Supervisory Control and Data Acquisition*
SECOM	*Security Communication Middleware*
SEP	Sistema Elétrico de Potência
SIN	Sistema Interligado Nacional
SV	*Sampled Value*
TI	Tecnologia da Informação
TIC	Tecnologias de Informação e Comunicação
TLS	*Transport Layer Security*
WAMPAC	*Wide Area Monitoring, Protection and Control*

SUMÁRIO

1 INTRODUÇÃO

A energia elétrica é um produto amplamente utilizado no mundo. No Brasil a maior parte dela é gerada em usinas hidrelétricas, usando o potencial energético da água (CGEE, 2012). Porém a energia elétrica também pode ser produzida em usinas nucleares, eólicas, termoelétricas, solares, entre outras. A sociedade possui uma dependência intrínseca quanto ao uso da energia elétrica, sendo, portanto, de fundamental importância para o desenvolvimento das sociedades atuais.

O avanço da industrialização nos países emergentes e do contínuo crescimento da população mundial implica um aumento do consumo de energia em todo o mundo. Em média o consumo de energia cresce aproximadamente 4,5% a.a. no Brasil e 2,5% a.a. no mundo, segundo dados do Ministério de Minas e Energia (2015). Em função deste crescimento da demanda e do esgotamento da capacidade de exploração hídrica de muitos países, faz-se necessário a busca por fontes alternativas com vistas a possibilitar o aumento da produção de energia de forma sustentável.

Em função da racionalização da demanda e geração de energia, incluindo novas possibilidades de aplicações, surge a necessidade de evoluções tecnológicas. Nestas, é impreterível o uso de TIC (Tecnologias de Informação e Comunicação). O controle inteligente é necessário para neutralizar ou impedir a flutuação na geração de energia a partir de fontes renováveis. Além disso, são necessárias formas eficientes para o armazenamento de energia, distribuição e transporte para garantir a disponibilidade da energia quando necessário, como por exemplo, durante o horário de pico ou em áreas densamente industrializadas (GIEHL, 2013).

No Brasil, as Redes Elétricas Inteligentes estão em estágio inicial, sendo que vários projetos de P&D (Pesquisa e Desenvolvimento) estão em andamento (CGEE, 2012). Uma das inovações tecnológicas desta área pode ser percebida na proposta de automação da leitura do consumo de energia elétrica do consumidor e, na diferenciação de tarifa de acordo com os períodos do dia (CGEE, 2012).

As Redes Elétricas tradicionais estão evoluindo para Redes Elétricas Inteligentes, também denominadas Smart Grid, integrando a tradicional rede elétrica

com TIC. Essa integração permite melhorar a eficiência e a disponibilidade do sistema de energia, tanto para fornecedores quanto para clientes (ALOUL et al., 2012).

A eficiência e disponibilidade da energia elétrica se dá através do constante monitoramento, controle e gerenciamento das demandas dos clientes, fontes geradoras, transmissão e subestações de redes elétricas. Para realizar o gerenciamento, controle e monitoramento utiliza-se um sistema denominado como SCADA (Supervisory Control and Data Acquisition - Sistema de Supervisionamento, Controle e Aquisição de Dados) (BJÖRKMAN et al., 2010), em virtude da dificuldade em monitorar inúmeros dispositivos manualmente.

Os sistemas SCADA são utilizados por empresas e setores públicos, para monitorar e controlar infraestruturas críticas, como produção e distribuição de energia elétrica, distribuição de água, centrais nucleares, tráfego, entre outros (PIRES et al., 2004). Um sistema SCADA utilizado em Redes Elétricas Inteligentes pode ser considerado um alvo atraente de ataques cibernéticos, em função da criticidade da rede monitorada.

Uma tendência é a convergência das redes de comunicação para redes de protocolos abertos, amplamente baseadas no protocolo IP (*Internet Protocol*), visto que esse tipo de rede é utilizado para comunicação na Internet e, portanto, é amplamente suportado e testado. No sistema elétrico, alguns padrões abertos, que já consideram o uso de redes IP, são utilizados (ARAUJO, 2011). Sendo dois deles o IEC 61850 para automação de subestações de redes elétricas (IEC 61850-8-1) e, o IEC 62351 que estabelece normas de segurança da informação para operações de controle do sistema de potência (IEC TS 62351-3).

Estudos e pesquisas relacionados a segurança em redes IP são realizados frequentemente, em função das diversas vulnerabilidades que podem ser exploradas. Com uma relevância ainda maior do que na Internet, as vulnerabilidades de segurança são questões de extrema importância num ambiente SCADA (ALOUL et al., 2012), pois, em geral, é realizada uma troca considerável de informações entre o sistema SCADA e dispositivos, que muitas vezes estão espalhados geograficamente. Um ataque num sistema desse porte traria riscos, podendo deixar cidades sem energia elétrica, danificando equipamentos, colocando vidas em risco. Em casos extremos a rede de energia pode ser altamente danificada, causando demora na sua recuperação.

1.1 Objetivos

Essa subseção apresenta o objetivo geral e os objetivos específicos do trabalho.

1.1.1 Objetivo Geral

Verificar os mecanismos de proteção e o impacto das vulnerabilidades exploradas na comunicação de um sistema SCADA no contexto de Redes Elétricas Inteligentes. Essa análise se dará com a simulação de ataques através de técnicas já conhecidas nas redes públicas, baseadas em IPs.

1.1.2 Objetivos Específicos

O objetivo proposto será alcançado a partir da abordagem dos seguintes tópicos:

- Identificar as funcionalidades e protocolos utilizados em sistemas SCADA;
- Identificar as principais tecnologias utilizadas pelo sistema, suas ameaças e vulnerabilidades;
- Verificar o impacto causado por possíveis falhas no sistema SCADA;
- Identificar possíveis soluções ao problema.

1.2 Justificativa

O Sistema SCADA é um sistema centralizado de supervisionamento, controle e aquisição de dados, que tem como requisito garantir a segurança e legitimidade na comunicação com diversos dispositivos e ao mesmo tempo prover escalabilidade. Diante disso, sistemas desse porte são considerados críticos e delicados, propensos a vulnerabilidades e ataques (FALCÃO, 2009; SILVA e SALVADOR, 2005).

Até pouco tempo o nicho dos sistemas SCADA era o setor industrial, onde normalmente não tinham acesso à internet e usavam protocolos proprietários. Por consequência os sistemas SCADA na maioria das vezes são isolados das redes públicas, com finalidade de proteger-se de possíveis ataques (NICHOLSON et al., 2012). Nesse contexto, o acompanhamento de um profissional de TI é essencial, para cuidar principalmente da segurança da informação.

Os sistemas SCADA estão evoluindo para sistemas abertos e com uma arquitetura fortemente centrada em conectividade. Neste modelo, os sistemas SCADA estão se conectando a intranets corporativas e consequentemente a própria rede Internet. Assim, os eventuais problemas de segurança, que antes eram restritos a cada ambiente de rede, agora passam a ser compartilhados. Desta forma, sistemas SCADA utilizados em Redes Elétricas Inteligentes, estão sujeitos a sofrer ataques. Devido à natureza crítica da tecnologia e serviços que ela oferece, a rede de comunicação se torna um alvo preferencial para atos de terrorismo e ataques cibernéticos (GHANSAH, 2009).

Dado a relevância das redes de comunicações e dos sistemas SCADA para o funcionamento das Redes Elétricas Inteligentes, torna-se importante a verificação dos mecanismos de proteção e o impacto das vulnerabilidades de segurança explorados na comunicação num sistema SCADA, no contexto de Redes Elétricas Inteligentes.

1.3 Organização do Trabalho

A estrutura deste trabalho está organizada da seguinte forma: no capítulo 2 apresentação da fundamentação teórica; Capítulo 3 explica-se a proposta do trabalho e sua implementação; Capítulo 4 descreve-se os testes realizados e os resultados encontrados e, por fim o Capítulo 5 define-se as considerações finais deste estudo e sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta uma fundamentação teórica sobre Redes Elétricas Convencionais e Inteligentes, explanando conceitos, características e problemas em sua estrutura. Num segundo momento, serão apresentadas tecnologias utilizadas em Redes Elétricas Inteligentes, dando ênfase aos padrões e protocolos utilizados por sistemas de controle. E por fim, serão exibidos as principais vulnerabilidades, ataques e riscos que as Redes Elétricas Inteligentes e sistemas que a controlam estão expostos.

2.1 Sistema Elétrico de Potência

A maioria dos sistemas elétricos de potência existentes, principalmente no Brasil, seguem o modelo convencional com geração, transmissão e distribuição. A geração na maioria das vezes é centralizada em usinas conectadas a redes de transmissão, e as redes de distribuição alimentam consumidores finais como mostra a figura 1.

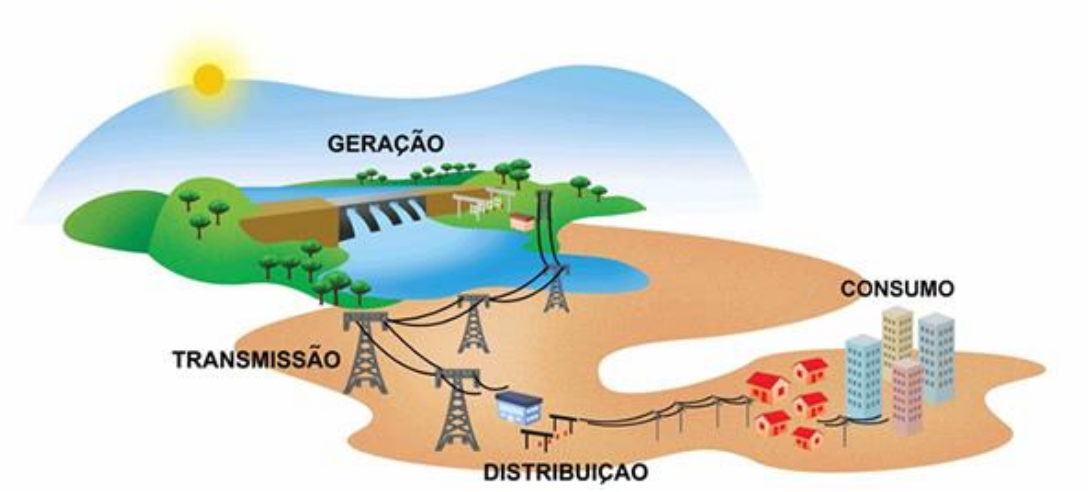

Figura 1: Subsistemas que compõem o SEP (Sistema Elétrico de Potência).
Fonte: ABRADEE.COM.BR

Os sistemas de energia elétrica cresceram e evoluíram tecnologicamente, tais que, centrais geradoras ficam cada vez maiores e os sistemas de transmissão elevaram a sua tensão nominal, para atender as distâncias e blocos de potência transmitidos (ONS, 2015). O Brasil possui o maior sistema interligado de energia, considerado único em âmbito mundial. O sistema de produção é dito hidrotérmico de grande porte, com múltiplos proprietários e com predominância de usinas hidrelétricas. Apenas 1,7% da energia demandada é produzida fora desse sistema interligado, produzida em sistemas isolados localizados principalmente na região do amazonas (ONS, 2015). A figura 2 mostra as diferentes linhas de transmissão de alta tensão no Brasil, projeções de linhas futuras e os centros hidrelétricos conectados pelo SIN (Sistema Interligado Nacional).

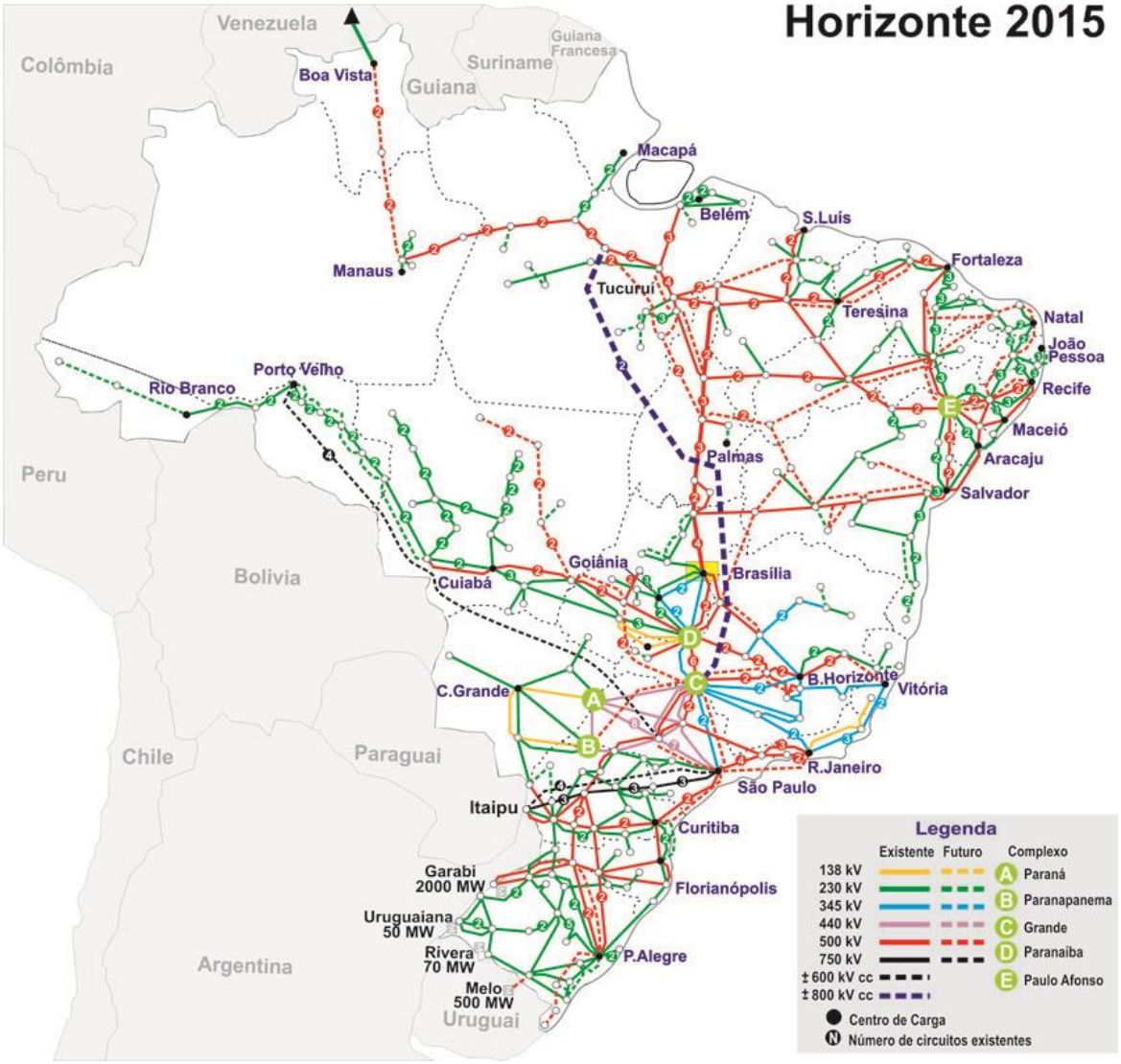

Figura 2: Sistema Interligado Nacional.

Fonte: ONS, 2015.

Arquiteturas de interligação de energia como a do Brasil estão propensas a falhas, em função da complexibilidade de controle e monitoramento dessa rede. Essas falhas podem resultar em indisponibilidade de energia, também chamados de apagão. O apagão (*blackout*), é o evento que demonstra a falta de qualidade no sistema elétrico, pois implica perdas financeiras e manifesta vulnerabilidades no sistema elétrico (BRUCH et al., 2011). Para exemplificar, cita-se:

- O apagão do dia 19-01-2015 que atingiu 11 estados e o DF, devido ao recorde de consumo de energia segundo notícia do Jornal da Globo (2015). Isso evidência que o Brasil possui problemas de controle de energia.
- Outro apagão ocorrido no Brasil em 10 de novembro de 2009, em que, chuva e ventos fortes causaram um curto-circuito em três linhas de transmissão provenientes da Usina Hidrelétrica de Itaipu (BRUCH et al., 2011). A queda brusca na demanda de energia causou o desligamento das 20 turbinas da usina deixando 90 milhões de pessoas sem energia durante 30 minutos. Pessoas ficaram presas em elevadores, metrôs e trens suburbanos pararam, o tráfego rodoviário também ficou caótico, e policiais foram colocados em estado de alerta, pois surtos de crime poderiam acontecer (BRUCH et al., 2011).
- Em 2003 os Estados Unidos e Canadá sofreram de um apagão que deixou mais de 50 milhões de pessoas sem energia durante 4 dias. O motivo do apagão se deu pela combinação da falta de manutenção, erros humanos e falhas de equipamentos (BRUCH et al., 2011).

Problemas de geração e abastecimento de energia acontecem em todo mundo, fato é que os países mais desenvolvidos investem mais para ter uma eficiência energética. Segundo CGEE (2012) as estimativas de investimentos federais e privados até 2030 da União Europeia é de US$ 1,88 trilhões, o Japão investirá US$ 1,7 trilhões, os EUA US$ 1,5 trilhões e o Brasil ocupa a sexta posição nesse ranking de investimentos não sendo informado o valor. Nesse cenário, sistemas complexos devem monitorar e controlar os sistemas de energia. Surgindo assim o conceito de Redes Elétricas Inteligentes denominada globalmente como *Smart Grid*.

2.2 Redes Elétricas Inteligentes (*Smart Grid*)

Redes Elétricas Inteligentes empregam um extenso conjunto de tecnologias e serviços inovadores como monitoramento, controle e comunicação inteligente, com a finalidade de reduzir custos e aumentar a confiabilidade e transparência. As Redes Elétricas Inteligentes são a modernização do Sistema Elétrico de Potência, trazendo consigo novos paradigmas, funcionalidades e características (GHANSAH, 2009; FERREIRA, 2010; VIJAYAPRIYA e KOTHARI, 2011):

- Facilitar o monitoramento e operação de geradores;
- Realizar o controle e o monitoramento em tempo real;
- Melhorar a eficiência energética;
- Permitir a participação ativa dos consumidores em resposta a demanda;
- Fornecer informações mais detalhadas sobre o abastecimento de energia;
- Integrar as fontes de energia distribuída e da microgeração;
- Reduzir emissões de gases e o impacto ambiental;
- Fornecer um abastecimento de energia resiliente e seguro;
- Realizar controle eficiente de tensão;
- Melhorar capacidade de armazenamento de energia;
- Implantar tarifas inteligentes;
- Promover detecção e isolamento automático de falhas, restauração e reconfiguração do serviço (*Self-healing*);

A automação da Rede Elétrica Inteligente compreende: geração, transmissão e distribuição. Comparado com o Sistema Elétrico de Potência, o setor da geração sofrerá poucas mudanças, pois este já utiliza tecnologias embarcadas na sua operação.

Na automação da transmissão de energia elétrica é possível verificar um impacto maior, pois faz-se necessário sistemas eficientes como SCADA e WAMPAC (*Wide Area Monitoring, Protection and Control*) para monitorar e controlar a dinâmica

do sistema de energia em tempo real (FALCÃO, 2009). Esse monitoramento facilita a identificação de instabilidades no sistema. A tecnologia proposta é baseada em PMU (*Phasor Measurement Units* - Unidades de Medição Fasorial), que consiste basicamente de sensores espalhados ao longo das linhas de transmissão (FALCÃO, 2009). A figura 3 exemplifica um cenário típico do conceito de Redes Elétricas Inteligentes. Essa apresenta possíveis mudanças do Sistema Elétrico de Potência começando pela automação da Geração, Automação da Transmissão e Automação da Distribuição. Entre as várias mudanças destaca-se a implantação de Dispositivos Eletrônicos Inteligentes em todos os setores, que visam facilitar o monitoramento e gerenciamento através de sistemas SCADA em tempo real.

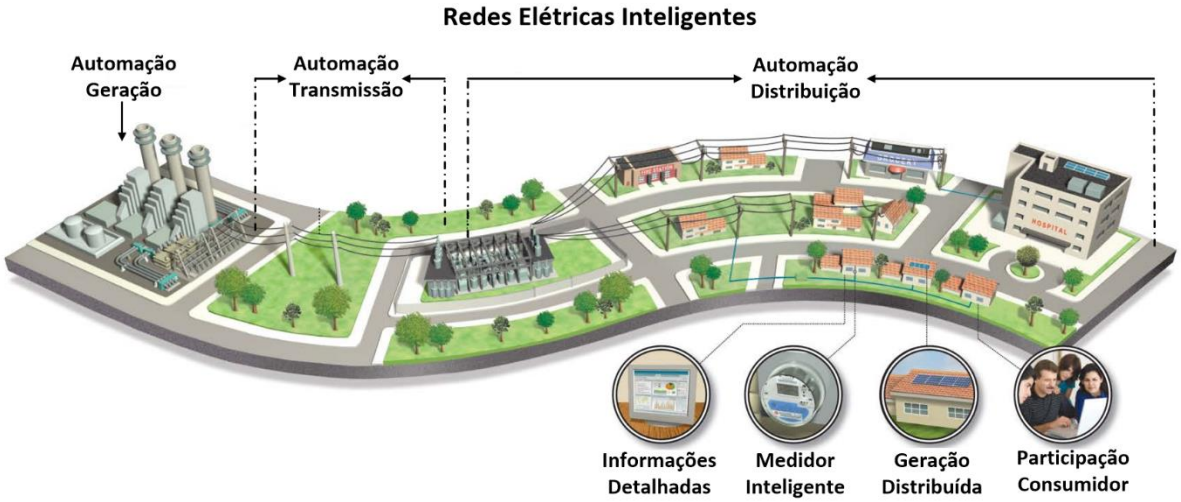

Figura 3: Rede Elétrica Inteligente.
Fonte: Adaptado de 2014 Smart Grid System Report.

A automação da distribuição receberá alterações a partir da convergência da distribuição de energia, infraestrutura de comunicação digital e processamento de dados, sendo a mais beneficiada no contexto de Redes Elétricas Inteligentes. Aplicações promissoras como AMR (*Automatic Meter Reading* - Leitura Automática do Medidor) e AMI (*Advanced Metering Infrastructure* - Infraestrutura de Medição Avançada), acrescentam funcionalidades importantes na automação da distribuição:

- AMR: sistema de leitura automática dos dados de medidores de energia que são transportados para um CCM (Centro de Controle de Medição), gerando a fatura, com a finalidade de melhorar a eficiência nas medições e diminuir custos (CGEE, 2012).
- AMI: representa um avanço em relação a AMR, pois propõe a incorporação da flutuação de preços em horários da energia por eletrodomésticos inteligentes. Realiza a coleta de dados e possui uma capacidade de processamento considerável, realizando assim uma gestão eficiente do uso da energia (CGEE, 2012).

As Redes Elétricas Inteligentes, também possibilitam a inserção do conceito de prossumidor, que define o cliente não somente como consumidor, mas também como produtor. A Microgeração e geração distribuída de energia elétrica em unidades locais do consumidor, torna-o um produtor de energia. A energia que não for consumida localmente poderá ser injetada no sistema da distribuidora. Essa energia injetada será convertida em créditos que poderão ser abatidos no consumo dos meses subsequentes (ANEEL, 2014).

A automação das subestações é importante, pois funciona como um ponto de controle e transferência de energia. A energia elétrica que chega da rede de transmissão é transformada em níveis de tensão mais baixa. Essa energia transformada é repassada para a rede de distribuição que abastece os consumidores finais (CGEE, 2012). Nesse contexto, as subestações se beneficiam dos IEDs (*Intelligent Electronic Devices* - Dispositivos Eletrônicos Inteligentes) e das RTUs (*Remote Terminal Units* - Unidades Terminais Remotas) para melhorar a capacidade de controle e monitoramento do funcionamento das subestações. Para isso, sistemas como SCADA são utilizados em subestações que realizam a coleta, controle e monitoramento dos IEDs proporcionando um funcionamento com maior eficiência (STREHL, 2012).

2.3 Sistema SCADA

Um sistema SCADA é um sistema de automação ou de controle industrial, que através de protocolos de comunicação pode monitorar, controlar e se comunicar com sensores, atuadores, IEDs, efetuando leituras de informações, ou mesmo enviar comandos para estes (STREHL, 2012). Os protocolos utilizados na comunicação são variados, em função da multiplicidade de dispositivos presentes neste tipo de sistema. Da mesma forma, a rede de comunicação utilizada também é heterogênea, desde os protocolos legados, como MODBUS (RFC 2026, 2002; MAKHIJA, 2003), até os sistemas mais modernos, que convergem para a utilização de redes baseadas em IP (GHANSAH, 2009).

A segurança das Rede Elétricas Inteligentes é de suma importância, considerada uma parte crítica desta infraestrutura pública. Algumas capacidades de segurança em tempo real são necessárias ao sistema SCADA, sendo elas: legitimidade, autenticidade e integridade dos pacotes (GHANSAH, 2009; GIEHL, 2013). Além disso, no caso de uma emergência, é desejado, que o técnico responsável seja capaz de obter acesso imediato ao sistema.

2.4 Protocolos utilizados no Sistema Elétrico

Existem vários protocolos historicamente utilizados pelos sistemas supervisores e controladores, como FieldBUS, Modbus, DNP3, entre outros. Esses possuíam pouca ou nenhuma segurança associada a comunicação (NICHOLSON et al., 2012). Diante da necessidade de padronização e de melhorar a segurança da comunicação, foram criados novos padrões, dentre eles IEC 61850 e IEC 62351.

2.4.1 Modbus

O protocolo Modbus ainda é bastante utilizado pelos sistemas SCADA, pela sua facilidade de implementação. Modbus estabelece uma estrutura de mensagem para comunicação entre dispositivos cliente-servidor. Porém, não é um protocolo que foi projetado para ambientes críticos, que necessitam de alguma segurança mínima. A falta de autenticação das mensagens, e de verificação de integridade, são vulnerabilidades que podem ser atacados neste protocolo (RFC 2026, 2002; ALOUL et al., 2012).

2.4.2 Padrão IEC 61850

O IEC 61850 é um padrão, que normatiza as comunicações dentro do ambiente de subestações. O padrão IEC 61850 ganhou aceitação global, tanto por fornecedores quanto pelos clientes, representados pelas empresas concessionárias de energia. O padrão estabelece regras estritas de interoperabilidade entre dispositivos independentes do fabricante, proporcionando, proteção, monitoramento, controle e automação (IEC 61850-8-1, 2005).

O padrão compõe-se de 10 partes, cada uma trata de um tópico específico, que aborda de forma ampla o tópico proposto no que se refere aos sistemas de automação de subestações. A série IEC 61850 prevê, além da transferência de dados, uma estrutura completa, que separa a aplicação da estrutura de comunicação através do uso de uma interface abstrata (IEC 61850-8-1, 2005).

A figura 4 mostra os principais serviços de comunicação definidos pelo padrão IEC 61850 e também o protocolo Modbus (RFC 2026, 2002; IEC 61850-8-1, 2005). O padrão IEC 61850 também especifica classes de desempenho de cada tipo de mensagem, documentadas como tempo de duração de transmissão de cada mensagem. Esses serviços são providos na camada de aplicação, onde diferentes modos de comunicação são utilizados, como: Comunicação cliente-servidor para

serviços MMS (*Manufacturing Message Specification*) através da pilha de protocolos TCP/IP e Ethernet; Comunicação de alta velocidade de tempo real, mensagens GOOSE (*Generic Object Oriented Substation Event*) e SV (*Sampled Value*) (HOU e DOLEZILEK, 2008).

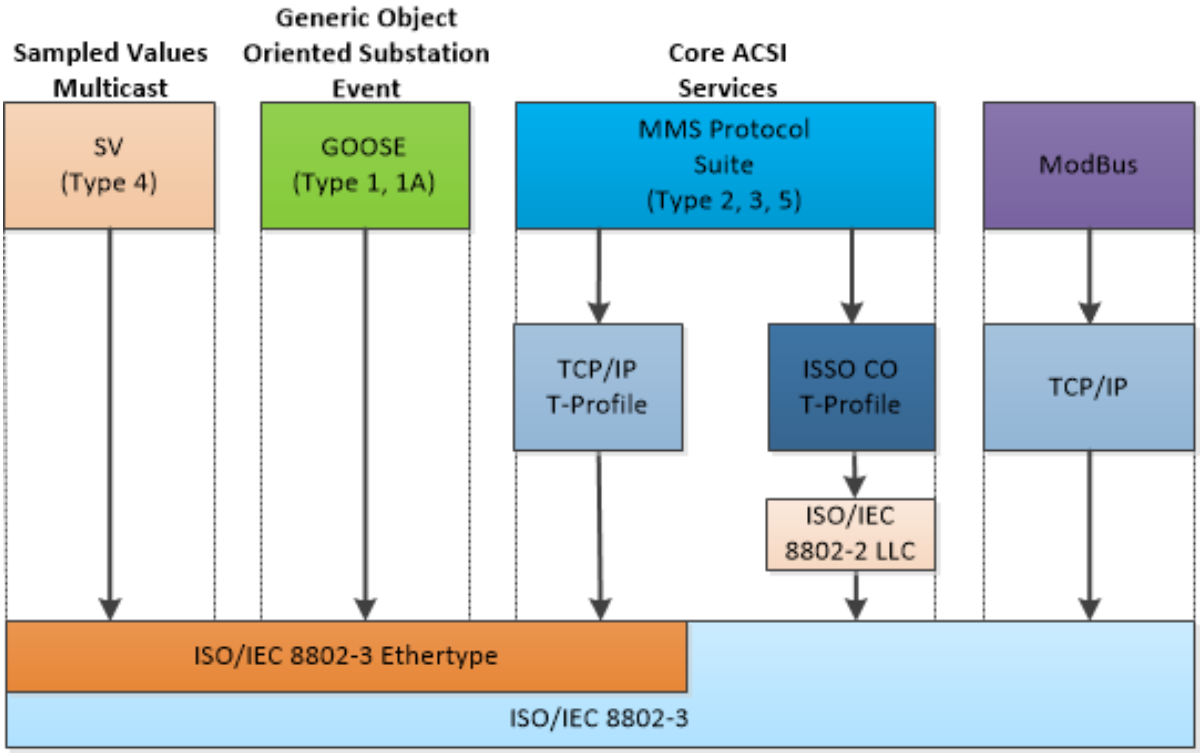

Figura 4: Serviços de Comunicação do padrão IEC 61850.
Fonte: Adaptada de IEC 61850-8-1, 2005.

As mensagens SV transmitidas são dados brutos de transdutores e transformadores, enviadas para relés. Os relés, por sua vez, possuem um conversor incorporado, que trata esse dado e o utiliza em suas proteções. Essa comunicação acontece sobre a camada de enlace do modelo OSI. Desta forma atinge os requisitos necessários de tempo de transmissão estabelecidos pelo padrão IEC 61850 (HOU e DOLEZILEK, 2008).

Mensagens GOOSE pertencem ao grupo de mensagens rápidas, que devem ser transmitidos no prazo de 10 ms, e alguns eventos específicos possuem prazo de 3 ms. GOOSE utiliza um mecanismo de comunicação conhecido por "*publish-*

subscribe” entre IEDs. Desta forma as mensagens são enviadas em *multicast* para IEDs da subestação (HOU e DOLEZILEK, 2008).

Mensagens MMS são basicamente utilizadas para o controle de IEDs fornecendo um conjunto de serviços como leitura, escrita, definição e criação de objetos de dados. Os tempos máximos de transmissão estabelecidos são: Mensagem do Tipo2 100 ms, Mensagem do Tipo3 500 ms e Mensagem do Tipo5 ≥1000 ms (HOU e DOLEZILEK, 2008).

Portanto, estes mecanismos de comunicação permitem melhorar esquemas de proteção e controle tradicionais, reduzindo os custos de projeto de sistema, instalação, operação, manutenção e, ao mesmo tempo, aumentar a confiabilidade do sistema de energia. IEC 61850 é um padrão de mensagens que irá garantir a interoperabilidade quando implementadas de acordo com o padrão (IEC 61850-8-1, 2005).

2.4.3 Padrão IEC 62351

O padrão IEC 62351 estabelece normas de segurança da informação para operações de controle do sistema de potência. A norma IEC 62351 está atualmente dividida em 11 partes, cada parte trata de um tópico específico (IEC TS 62351-3, 2007). IEC 62351 fornece métodos diferentes para garantir os tipos de comunicações do padrão IEC 61850 (IEC 61850-8-1, 2005).

A proteção do tráfego de mensagens MMS é realizado na camada de aplicação e na camada de transporte. Na camada de transporte é usado um conjunto de tecnologias chamado TLS (*Transport Layer Security*). Neste é especificada a porta de comunicação, o preenchimento obrigatório, e recomenda que os dispositivos tenham capacidade de suportar no mínimo cifras de AES_128 e AES_256. A autenticação compreende um certificado X.509 (IEC TS 62351-3, 2007; HOHLBAUM, et al. 2010).

No entanto, a utilização do conjunto de tecnologias TLS é prejudicada pois os dispositivos RTUs (*Remote Terminal Units*) e IEDs utilizados em sistemas de energia possuem limitações de processamento e memória, o que dificulta a implementação de criptografia ou assinatura digital utilizando chaves assimétricas. Desta forma, os

prazos de entrega de mensagens GOOSE e SV definidos pelo padrão IEC 61850 ficariam comprometidos. Além disso, alterações de hardware e software para suportar tais recomendações demandam tempo e geram custos (HOU e DOLEZILEK, 2008; HOHLBAUM, et al. 2010).

Segundo Hohlbaum, et al. (2010), as aplicações de assinaturas digitais através de software não atenderiam aos requisitos de tempo real com os IEDs atuais. A solução de hardware que atenderia seria a implementação de assinatura de chave publica e privada RSA de 1024 bits utilizando cripto-chips, que realizam a operação em menos de 23,8 microssegundos podendo até suportar taxas de amostragem de 12 kHz (HOHLBAUM, et al. 2010). Porém, em curto prazo essa solução não é viável, pois exigiria uma grande reformulação de hardware, incluindo memória externa, sistemas de refrigeração, entre outros.

Além da dificuldade de aplicar segurança em sistemas de energia, existe a preocupação da diversidade de equipamentos utilizados. A interoperabilidade atinge não somente a implementação de protocolos e interfaces de comunicação, mas também depende da utilização de padrões criptográficos, capacidade de implementação de SSL/TLS, sendo compatíveis entre si (IEC TS 62351-3, 2007; HOHLBAUM, et al. 2010).

2.5 Ataques em Sistemas SCADA

Os sistemas SCADA fazem parte da infraestrutura de controle e monitoramento da rede elétrica. A mudança na adoção de padrões e protocolos abertos, cada vez mais baseados no protocolo IP, permite uma análise mais ampla da segurança. As implicações de um ataque deliberado em qualquer um dos sistemas SCADA seria grave, porque colocam em risco a confidencialidade, integridade e disponibilidade dos sistemas envolvidos (ALOUL et al., 2012; NICHOLSON et al., 2012).

Em função das diversas vulnerabilidades que podem ser exploradas num sistema SCADA, alguns dos principais tipos de vulnerabilidades existentes serão

considerados a seguir, (GHANSAH, 2009; ALOUL et al., 2012; NICHOLSON et al., 2012; SUKEYOSI et al., 2013):

- Mascaramento do IP do computador, substituindo-o por endereços falsos. Isso possibilita ataques a dispositivos sem medo de ser rastreado, pois o endereço que é enviado para os destinatários é falso;
- Espionagem e sabotagem de pacotes de rede, a fim de encontrar informações críticas ou adulterar os pacotes levando o sistema a um estado inconsistente;
- Ataque de Negação de Serviço (DoS) e Ataque de Negação de Serviço Distribuído (DDoS). O DoS é utilizado para inundar um recurso específico com vários pedidos, a fim de sobrecarregá-lo, tornando-se indisponível. Desta forma, os pedidos legítimos não podem ser tratados devido à sobrecarga causada pelos pedidos desnecessários. A versão distribuída (DDoS), onde os ataques são realizados por vários dispositivos ao mesmo tempo, torna-se ainda mais intenso, e difícil de evitar. No contexto de Redes Elétricas Inteligentes, ataques realizados num sistema SCADA podem tornar seus dados obsoletos ou mesmo inacessíveis para os aplicativos que fazem uso destes. Assim aplicativos disponíveis, sem a devida proteção, podem deixar de funcionar, causando sérias consequências para o sistema de energia.

3 COMUNICAÇÃO DE SISTEMAS SCADA

O sistema SCADA, como um cenário comum, obtém dados através de uma rede IP de dispositivos, monitorados por ele. Neste cenário podem ser facilmente verificadas as vulnerabilidades na comunicação do sistema, utilizando-se ferramentas para análise da segurança de redes de comunicação. Na literatura sugere-se a utilização de técnicas de mascaramento, como IP *Spoofing*, onde um ataque altera seu endereço parecendo um dispositivo legítimo (GHANSAH, 2009).

Sniffers de rede, como wireshark (WIRESHARK.ORG) ou TCPDump (TCPDUMP.ORG) podem ser utilizados para analisar o tráfego de rede, pois informações críticas poderão ser interceptadas e, adulteradas, se a mensagem não utilizar uma forma de criptografia. Além destes, um ataque do tipo Homem-do-Meio facilmente poderá interceptar os pacotes e adulterá-los, levando o sistema a um estado inconsistente como por exemplo, adulterando informações de leitura de um sensor. Da mesma forma, um ataque DoS ou DDoS pode ser simulado, fazendo com que diversas requisições, aparentemente legítimas, sejam enviadas, sobrecarregando o sistema SCADA e tornando-o indisponível. Para efetuar este ataque, ferramentas de inserção de pacotes, como por exemplo o HPING (HPING.ORG), podem ser utilizadas. A figura 5 mostra o cenário típico do funcionamento do sistema SCADA, e também, ataques sendo efetuados.

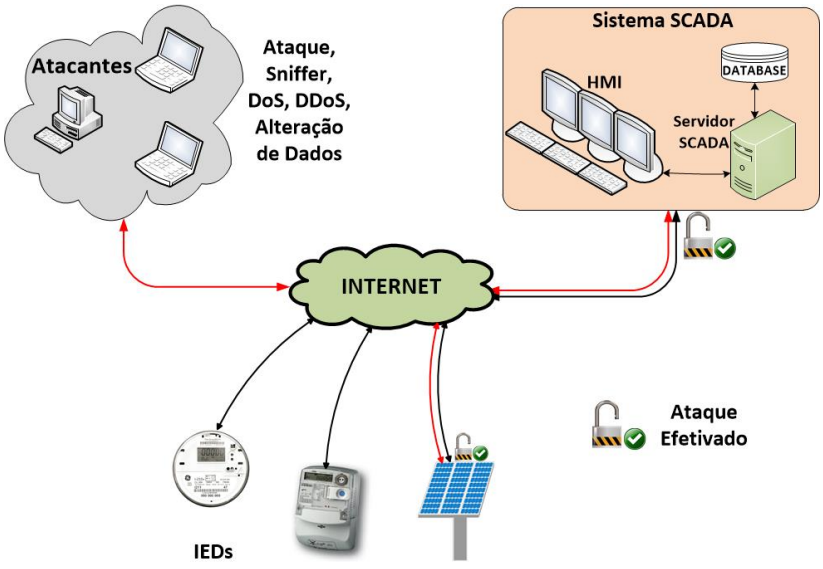

Figura 5: Cenário Típico

Com base nas vulnerabilidades e desafios de segurança apresentados, possíveis soluções foram traçadas para amenizar as vulnerabilidades. Procurou-se inclusive ter uma atenção especial para com os prazos de tempo de mensagem, estabelecidos no padrão IEC61850 (IEC 61850-8-1, 2005; HOU e DOLEZILEK, 2008), pois a utilização de assinatura digital e ou criptografia que exigem muito poder de processamento e memória ainda são considerados problema.

3.1 Proposta de uma arquitetura segura para comunicação de sistemas SCADA

Padrões como IEC 61850 e IEC 62351 apresentam arquiteturas de mensagens e segurança respectivamente, visando universalização da implementação de Redes Elétricas Inteligentes (IEC 61850-8-1, 2005; IEC TS 62351-3, 2007). Contudo, não é especificada a implementação de segurança, pois existem incompatibilidades de hardwares antigos e novos, que possuem capacidade de processamento restritos, mensagens com prazos de tempos diferentes, muitos IEDs ainda implementam protocolos legados como Modbus.

Nesse contexto, a utilização de componentes adicionais que possam prover as funcionalidades relativas à segurança caracteriza-se uma alternativa promissora. O middleware de segurança SECOM (*Security Communication Middleware*) desenvolvido por (SILVA, 2015) visa implementar requisitos que atendem as normas IEC 62351 (IEC TS 62351-3, 2007; HOHLBAUM, et al. 2010).

3.1.1 Middleware de comunicação segura SECOM

O middleware de segurança SECOM foi desenvolvido para ser utilizado em diferentes aplicações onde há necessidade de garantir os parâmetros de autenticidade, integridade e confidencialidade. Desta forma, implementa uma

infraestrutura de chaves assimétricas, controladas por uma entidade central, onde para qualquer comunicação a aplicação poderá utilizar funções do sistema que proveem os serviços de segurança necessários (SILVA, 2015).

3.1.2 Estrutura do middleware SECOM

O middleware SECOM tem como base um servidor de chaves responsável por conhecer e armazenar informações sobre todos os dispositivos autorizados da rede. Este servidor será responsável por autenticar os dispositivos da rede, bem como armazenar e distribuir chaves criptográficas, conforme necessário. Os dispositivos da rede apenas irão se comunicar com outros dispositivos que já estiverem devidamente autenticados pelo servidor. O servidor de chaves possuirá um par de chaves assimétricas para utilizá-las na comunicação com os dispositivos. Cada dispositivo cliente deve ter posse de um par de chaves provisórias, uma pública e outra privada, além de já possuir a chave pública do servidor. Para essa implementação se utilizou o algoritmo assimétrico mais popular atualmente, conhecido como RSA (MOLLIN, 2002; KUROSE e ROSS, 2012). Além das chaves, os dispositivos devem possuir também um identificador único de tamanho fixo, criado aleatoriamente, que servirá para identificar o dispositivo, no momento da autenticação com o servidor. Esse ID (identificador) gerado deve ser de conhecimento exclusivo do dispositivo e do servidor de chaves (SILVA, 2015).

A figura 6 representa a arquitetura do sistema, onde se tem (SILVA, 2015):

- *Server:* serviço responsável por gerar, manter e distribuir as chaves assimétricas de cada dispositivo autorizado da rede. Cada novo dispositivo ao ingressar na rede deverá ter um cadastro previamente realizado neste servidor utilizando um identificador único gerado para cada dispositivo pelo *daemon* do sistema instalado nos nós.
- *Daemon*: Software que deverá executar junto a todos os dispositivos da rede. Ele será responsável por manter, localmente, as chaves públicas dos demais dispositivos que irão se comunicar com o dispositivo onde ele está

executando. O serviço *daemon* mantém uma estrutura de cache para minimizar as consultadas ao servidor de chaves. Desta forma, a busca da chave pública do dispositivo com que deseja se comunicar é realizada somente na primeira vez, após é utilizada a cópia já existente na cache.

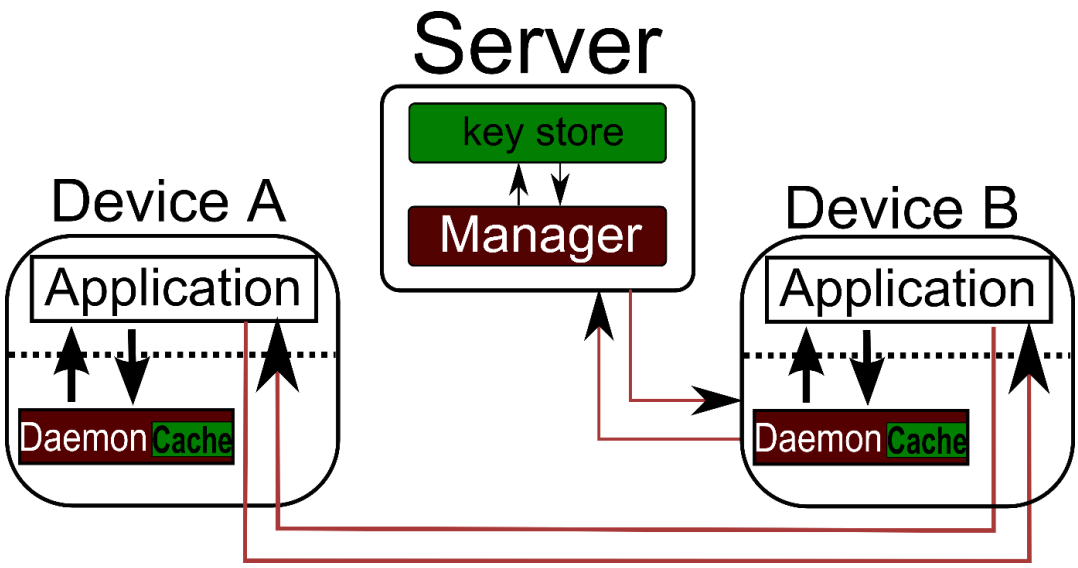

Figura 6: Estrutura do Middleware SECOM.
Fonte: (SILVA, 2015).

3.1.3 Autenticação

A autenticação do dispositivo será feita utilizando criptografia assimétrica e assinatura digital. A primeira etapa inicia com o cliente enviando uma requisição de autenticação para o servidor de chaves. Essa requisição deve possuir o ID único do dispositivo e a chave pública do dispositivo, criptografados com a chave pública do servidor para garantir que apenas ele tomará posse desse ID (SILVA, 2015).

Na segunda etapa, com o servidor já de posse do ID e de sua chave pública provisória do dispositivo, é realizada uma busca no banco de chaves do servidor, por alguma referência ao dispositivo solicitante. Caso o ID não se encontre entre os cadastrados, a conexão é encerrada e o dispositivo não é autenticado. Porém no caso

de o servidor encontrar o ID, o mesmo gerará um novo par de chaves para o dispositivo solicitante que será criptografado com a chave pública provisória deste, para que então possa ser enviado a ele. Após a confirmação de recebimento, por parte do cliente, o processo de autenticação e a conexão são encerrados (SILVA, 2015).

3.1.4 Comunicação entre dispositivos

Sempre que um dispositivo desejar se comunicar com outro dispositivo da rede, o mesmo deverá ter efetuado previamente o processo de autenticação com o servidor. Devidamente autenticado, o dispositivo que desejar se comunicar com outro dispositivo da rede, do qual ainda não possui a chave, deverá enviar uma requisição de chaves para o servidor. Esta requisição deve possuir o endereço IP do dispositivo desejado, com uma assinatura, provando ser um dispositivo válido da rede (SILVA, 2015).

O Servidor deverá enviar a chave pública do dispositivo de interesse para o dispositivo requisitante, devidamente assinada. Dessa forma o dispositivo emissor criptografará sua mensagem com a chave pública do dispositivo de destino para então enviá-la. O dispositivo de destino deverá efetuar o mesmo processo de pedido de chaves, caso ainda não possua a chave pública do emissor, para responder as mensagens originadas do mesmo. Essa troca de mensagens entre servidor e nós está ilustrado na figura 6. Para que esse processo não tenha que ser repetido com tanta frequência, será mantida uma tabela em cada dispositivo, com os dispositivos já contatados e suas respectivas chaves, durante um período de tempo (SILVA, 2015).

3.2 Modelo Proposto

Neste trabalho, optou-se pelo uso do MEPA (Mediador de Pacotes), e do middleware de segurança SECOM (*Security Communication Middleware*) (SILVA,

2015) que visam implementar requisitos que atendem ou superam as normas de segurança do padrão IEC 62351 (IEC TS 62351-3, 2007; HOHLBAUM, et al. 2010). Através do uso do Mediador de Pacotes e do middleware, todas as comunicações entre sistema SCADA e IEDs são realizadas de forma segura, resolvendo as questões referentes a autenticidade, integridade e confidencialidade dos dados, além de prevenir ataques de DoS/DDoS ao sistema SCADA.

3.2.1 MEPA (Mediador de Pacotes)

O Mediador de Pacotes foi reconstruído a partir de um código base, disponível na internet (JAVA2S.COM). Essas modificações foram necessárias, para que esse possa realizar as operações de captura e envio de pacotes, como também através da utilização dos serviços providos pelo Middleware SECOM, verificar a integridade, legitimidade e autenticidade de cada pacote capturado. No caso quando o pacote estiver indo para a rede, o MEPA intercepta esse pacote e aplica as devidas medidas de segurança, que posteriormente serão verificadas antes desse pacote ser entregue ao destino final.

O MEPA é um software de importância significativa para a implementação de segurança na comunicação entre os sistemas SCADA e IEDs, sendo que sua função é aplicar as polícias de segurança aos pacotes como também decidir se esse pacote será entregue ao destino final ou não. Dessa forma MEPA e SECOM executam em paralelo, sendo fundamental a sincronia entre os dois softwares para o perfeito funcionamento.

O MEPA implementa métodos que utilizam um protocolo de comunicação para se comunicar com o middleware, baseados em pedidos de serviço como: criptografar, descriptografar, assinar_digitalmente, verificar_assinatura_digital. Além disso, também implementa os métodos de captura e reenvio de pacotes, conversões de bytes para base64 e vice-versa. Implementa ainda um método que verifica o tempo que o middleware levou para realizar as verificações de segurança. O código MEPA

é flexível quanto as novas classes e métodos, que visam garantir a integridade e autenticidade dos pacotes entregues aos sistemas finais como SCADA e IEDs.

Nesse contexto, todas as funções relativas à segurança são abstraídas pelo MEPA e pelo middleware. Essa característica torna a proposta flexível para poder utilizá-la em qualquer cenário onde se utilize o sistema SCADA e IEDs que possuem limitações de hardware.

Em dispositivos e softwares que podem ser modificados, o MEPA e o middleware podem ser inseridos de forma embarcada. No entanto, para a arquitetura legada, pode-se adicionar um dispositivo na rede, cuja única finalidade é implantar as funcionalidades providas pelo MEPA e pelo middleware. Na figura 7 pode-se observar a estrutura proposta, onde os serviços MEPA e SECOM executam em paralelo.

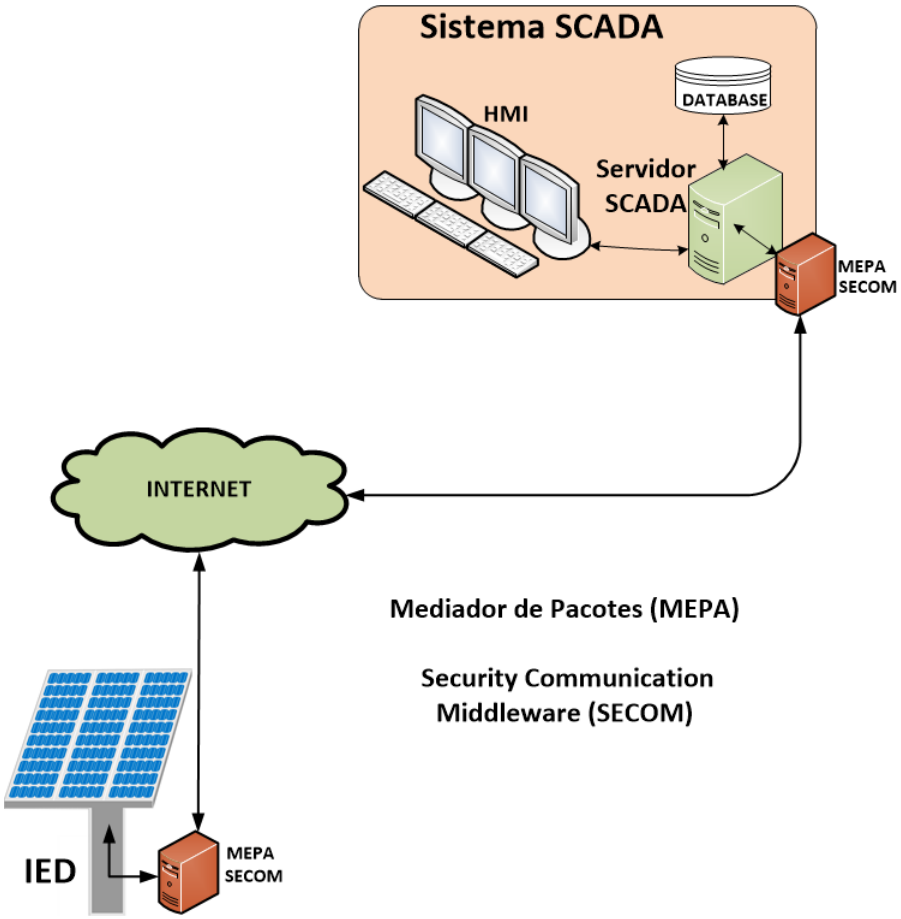

Figura 7: Cenário de funcionamento, com MEPA e SECOM

3.2.2 Modo de operação

O MEPA e o middleware podem estar localizados tanto dentro do dispositivo quanto próximo a ele, rodando como um serviço. Todo pacote enviado é interceptado pelo MEPA e enviado para o middleware SECOM através de uma comunicação local. Esse pacote será criptografado ou assinado pelo middleware e reenviado pelo MEPA ao destino. Ao chegar no destino, o MEPA interceptará o pacote repassando-o ao middleware que fará as verificações de segurança necessárias. Caso a resposta do middleware da verificação for negativa, esse pacote não será entregue ao sistema destino e será excluído automaticamente. Neste processo ocorre a verificação da autenticidade, integridade e legitimidade do pacote. A figura 8 ilustra um fluxograma detalhado sobre o envio de um pacote do sistema SCADA para um IED. O caminho inverso do pacote é semelhante, invertendo-se, porém, a ordem de verificação e da realização da criptografia e descriptografia.

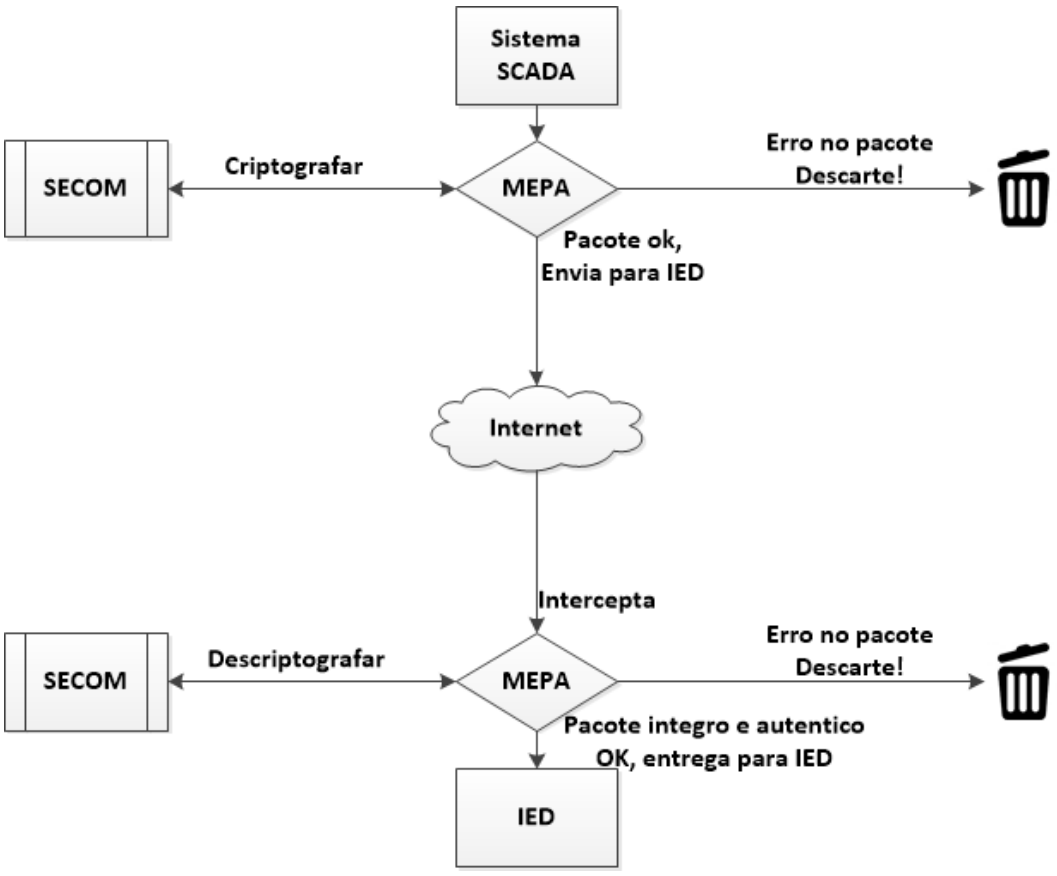

Figura 8: Fluxograma do envio de pacotes

4 TESTES E RESULTADOS

Para verificar os problemas de segurança existentes nas comunicações via internet de um sistema SCADA utilizou-se um cenário real, composto por um sistema SCADA e um painel fotovoltaico. O painel converte a luz solar em corrente contínua, que em seguida é convertida em corrente alternada por um inversor, pronta para ser consumida. A energia é ligada em paralelo à rede elétrica. O painel fotovoltaico possui suporte a monitoramento e gerenciamento remoto, obtidos através da utilização de um sistema SCADA.

Para o monitoramento da placa foi utilizado um sistema SCADA chamado Elipse Power® (ELIPSE POWER®), pois oferece funcionalidades específicas para o gerenciamento de IEDs voltados à Redes Elétricas Inteligentes. O Elipse Power® monitora em tempo real o funcionamento da placa fotovoltaica, por exemplo fazendo a leitura do sensor que especifica a quantidade de energia gerada em tempo real. A troca de mensagens é realizada utilizando-se o protocolo ModBus sobre TCP (RFC 2026, 2002). O sistema Elipse Power® (ELIPSE POWER®) estabelece uma comunicação TCP na porta 502 da placa fotovoltaica. Estabelecida a comunicação inicial, o sistema SCADA realiza a sondagem de informações a cada segundo, sendo possível a alteração deste tempo, conforme a necessidade. Os dados dessa leitura são apresentados em uma interface HMI (*Human Machine Interface* – Interface Homem-Máquina), na qual o técnico pode intervir no funcionamento caso esses dados estejam fora do padrão (BJÖRKMAN et al., 2010). Também há possibilidade de que o sistema SCADA possa intervir automaticamente, quando programado para tal função, diante de políticas de funcionamento.

4.1 Testes usando a arquitetura proposta

Após a implantação da arquitetura proposta integrando o Mediador de Pacotes e o middleware de segurança, realizaram-se testes no sistema e a verificação do

impacto que estas modificações causam nos resultados. Foram utilizados dois computadores com configurações diferentes, executando o MEPA e o Middleware SECOM em paralelo para prover a segurança necessária na comunicação. Dos computadores utilizados o primeiro identificado como PC_i5 é constituído de um processador i5 da Intel® de 3320M de cache com clock de 2.6GHz, 8 GiB de memória DDR3 de 1600 MHz. O segundo computador identificado como PC_AMD, é constituído de um processador AMD Phenom II X2 B55 de 7256M de cache com clock de 1,5GHz, 4 GiB de memória DDR3 de 1333MHz. A figura 9 ilustra o *setup* do sistema, utilizado nos testes.

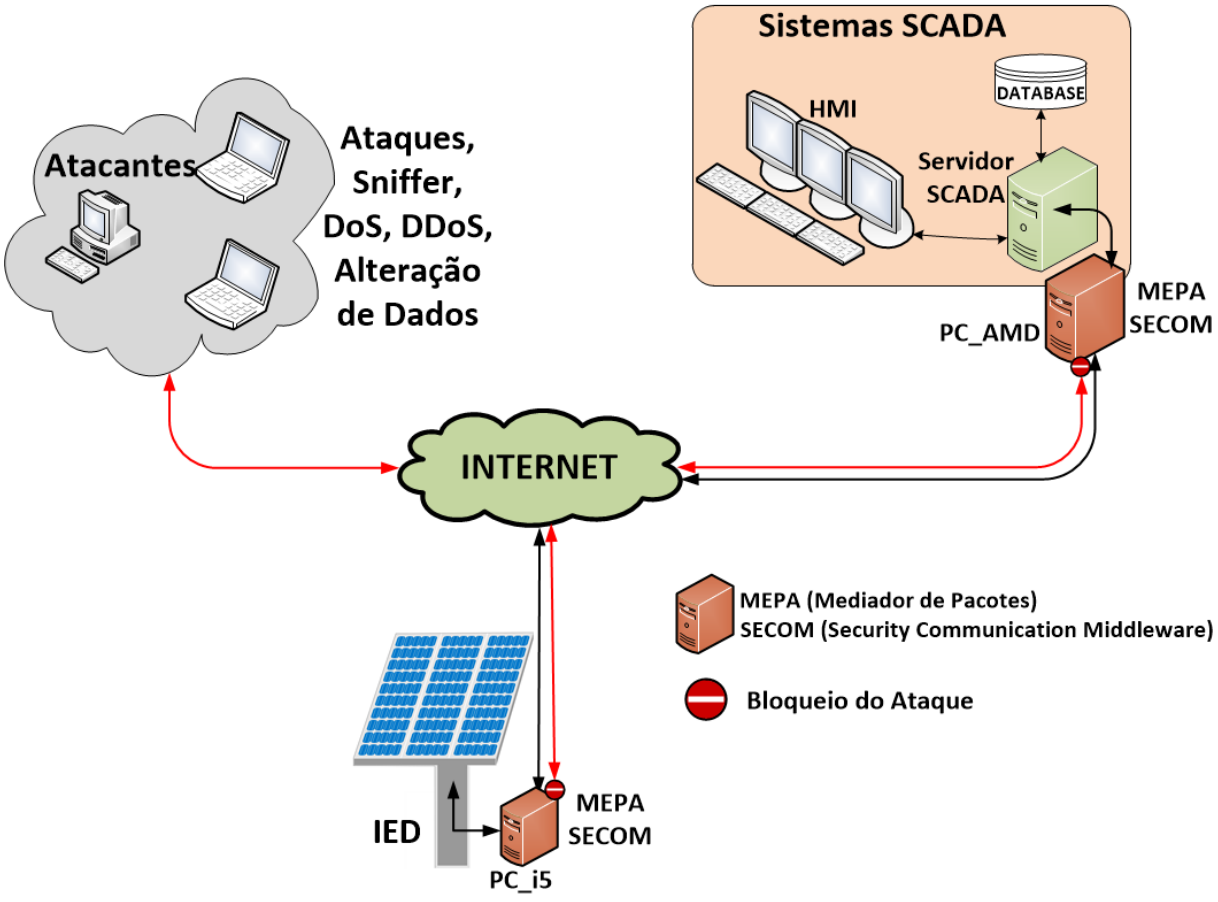

Figura 9: *Setup* de testes

4.1.1 Inserção de Pacotes

Foi realizado o ataque de Homem do Meio (GHANSAH, 2009), inserindo pacotes modificados, pacotes falsos e aplicando retardos na comunicação. Este ataque consiste na inserção de um novo elemento na comunicação de preferência entre os dispositivos que estão com a comunicação estabelecida e de modo transparente. Para realizar esta tarefa adaptou-se o código inicial (JAVA2S.com).

Como resultado os pacotes modificados e pacotes falsos foram descartados pelo MEPA, já que suas características estavam alteradas, o middleware não conseguiu descriptografar, nem validar sua assinatura digital. Porém os retardos e sequestros de pacotes foram efetivados, deixando os dados do sistema SCADA obsoletos. Como trata-se de sistemas críticos, relacionados a Redes Elétricas Inteligentes, isto é um problema grave. Para amenizar este problema sugere-se um dispositivo *backup* local que assuma o sistema enquanto outro estiver fora de alcance.

4.1.2 Ataques DoS

A ferramenta HPING3 (HPING.ORG) é utilizada para auditoria de segurança de rede e também permite o envio de pacotes TCP/IP personalizados. Neste estudo HPING3 foi utilizado para testar ataques DoS no sistema SCADA e painel fotovoltaico, efetivando uma inundação de requisição SYN na porta especifica do sistema SCADA.

Como em toda e qualquer comunicação antes mesmo de chegar ao sistema SCADA foi interceptada pelo MEPA, redirecionando essa requisição para a verificação de segurança. No teste a partir da resposta negativa do middleware, o MEPA descartou todas requisições indevidas. Além disso, todas as mensagens com criptografia incorretas, quebra de integridade do pacote e/ou confidencialidade foram descartadas. No entanto, o sistema ficou mais lento ao ser atacado, mas não chegou a paralisar, pois possui um controle de conexões simultâneas. Nesse aspecto uma alternativa para melhorar a proteção, seria a aplicação de QoS (*Quality of Service*)

(KUROSE e ROSS, 2012) nos pacotes com alta prioridade para garantir que os dados dos IEDs cheguem ao sistema SCADA.

4.1.3 Atrasos nos pacotes provocados pela aplicação de criptografia

Testes de tempo necessário para aplicar criptografia por cada hardware foram realizados. Divididos em sessões de 100 sondagens do sistema SCADA à placa fotovoltaica, efetuadas 10 vezes em diferentes horários do dia, totalizando 1000 sondagens. A média de tempo que o computador PC_i5 levou em cada sondagem, foi de 4,09 milissegundos para criptografar e descriptografar os dados. A média de tempo que o computador PC_AMD levou foi de 10,97 milissegundos. Assim sendo, com a utilização do Middleware SECOM nas duas extremidades realizando a verificação de segurança, os pacotes demoraram em média 15,06 milissegundos a mais numa sondagem.

A figura 10 apresenta o gráfico que mostra a notável diferença de desempenho de um computador para outro. O computador PC_i5 levou menos tempo para aplicar a segurança à informação do que o computador PC_AMD. Isso acontece porque os computadores utilizados possuem características diferentes, impactando no tempo em que cada um necessita para realizar as tarefas. Pode-se afirmar que no contexto de Redes Elétricas Inteligentes, isso é um problema comum, pois há heterogeneidade de dispositivos com limitações de processamento e memória.

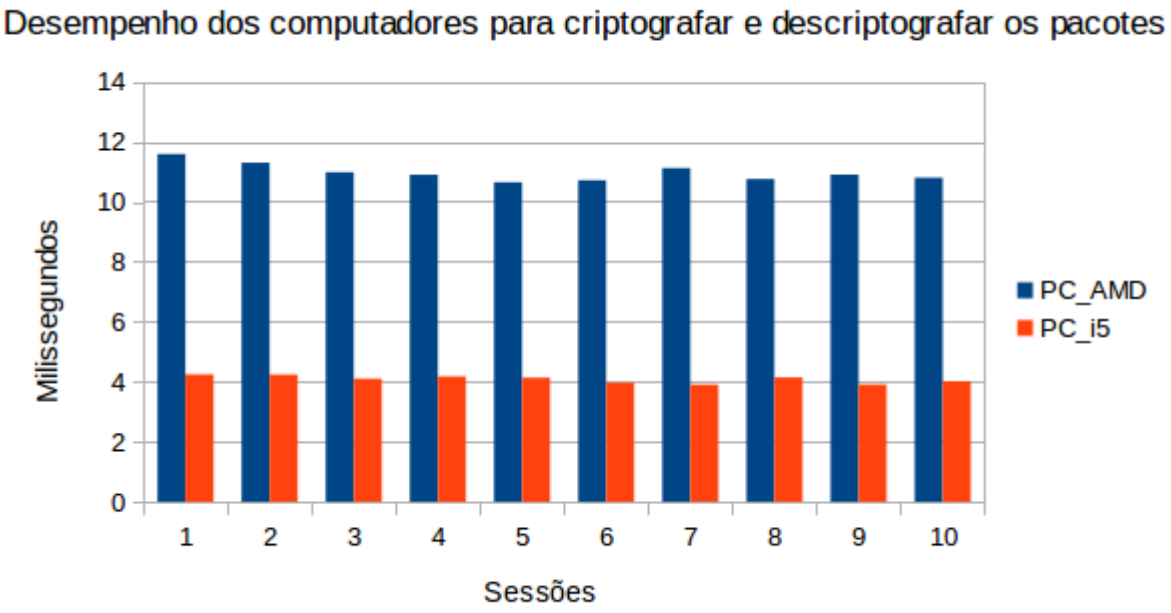

Figura 10: Gráfico de desempenho dos computadores utilizados nos testes.

5 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

A implementação do conceito de Redes Elétricas Inteligentes em sistemas de energia tem sido uma tendência, assim como, as preocupações com a segurança da comunicação desses sistemas. Neste trabalho, as principais tecnologias utilizadas pelo sistema, suas ameaças e vulnerabilidades foram levantadas.

Diante disso, para amenizar parte desses problemas, propôs-se a utilização de um Mediador de Pacotes e de um middleware de segurança, que proveem segurança às comunicações de sistemas SCADA com IEDs. As arquiteturas, Mediador de Pacotes e middleware SECOM (SILVA, 2015) possibilitam ser implantadas em qualquer cenário que utilize o sistema SCADA. Com isso, todos os equipamentos dessa rede podem utilizar este serviço. Desta forma, a comunicação entre o sistema SCADA e IEDs passa a ser assinada digitalmente ou criptografada, provendo assim integridade, legitimidade e autenticidade das mensagens. Além disso o Mediador de Pacotes controla todas as comunicações de entrada e saída do sistema SCADA e dos IEDs. O middleware SECOM realiza o gerenciamento e armazenamento das chaves e identificadores dos IEDs e também do sistema SCADA, que fazem parte dessa rede. Nesse contexto, a utilização do Mediador de Pacotes e do middleware SECOM proporcionam bons resultados, garantindo que os dados que chegam são de um IED da rede, e que os dados são autênticos e íntegros.

Durante os testes no cenário real, observou-se os tempos necessários para aplicar criptografia ou assinatura digital na comunicação. No entanto, pode-se afirmar que diante da diversidade de dispositivos utilizados em Redes Elétricas Inteligentes, é possível implementar segurança em mensagens cuja a comunicação acontece através de uma comunicação TCP/IP cliente/servidor e também atender os prazos de tempo, especificados no padrão IEC 61850 em mensagens MMS (IEC 61850-8-1, 2005; HOU e DOLEZILEK, 2008).

Para trabalhos futuros sugere-se o a otimização do código do Mediador de Pacotes, para melhorar a performance e modificá-lo para que execute suas tarefas de forma transparente na rede. Outra proposta, é a otimização do middleware SECOM para a aplicação de assinatura digital e ou criptografia em mensagens com prazos de

tempo reduzido como GOOSE e SV especificados pelo padrão IEC 61850 (IEC 61850-8-1, 2005; HOU e DOLEZILEK, 2008).

5.1 Publicações

As publicações abaixo relacionadas, bem como o desenvolvimento desta monografia, são frutos do trabalho do grupo de pesquisa do Curso Superior de Tecnologia em Redes de Computadores coordenado pelo Prof. Me. Tiago Antonio Rizzetti.

RIZZETTI, TIAGO ANTONIO; WESSEL, PEDRO; RODRIGUES, ALEXANDRE SILVA; SILVA, BOLÍVAR MENEZES; MILBRADT, RAFAEL; CANHA, LUCIANE NEVES. Cyber security and communications network on SCADA systems in the context of Smart Grids. In: 2015 50th International Universities Power Engineering Conference (UPEC), 2015, Staffordshire University. 2015 50th International Universities Power Engineering Conference (UPEC), 2015.

RIZZETTI, TIAGO ANTONIO; RODRIGUES, ALEXANDRE SILVA; SILVA, BOLÍVAR MENEZES; RIZZETTI, BRUNO AUGUSTO; WESSEL, PEDRO; CANHA, LUCIANE NEVES. Security of communications on a high availability mesh network applied in Smart Grids. In: 2015 50th International Universities Power Engineering Conference (UPEC), 2015, Staffordshire University. 2015 50th International Universities Power Engineering Conference (UPEC), 2015.

6 REFERÊNCIAS

ABRADEE.COM.BR. **A distribuição de energia.** Disponível em: <http://www.abradee.com.br/setor-de-distribuicao/a-distribuicao-de-energia>. Acesso em: 9 jun. 2015.

ALOUL, F. et al. **Smart Grid Security: Threats, Vulnerabilities and Solutions**. Smart Grid and Clean Energy Smart, p. 1–6, 2012. Disponível em: <http://www.aloul.net/Papers/faloul_ijsgce12.pdf>. Acesso em: 13 abr. 2015.

ANEEL. **Micro e Minigeração Distribuída: Sistema de Compensação de Energia Elétrica.** 2014. Disponível em: <http://www.aneel.gov.br/biblioteca/downloads/livros/caderno-tematico-microeminigeracao.pdf>. Acesso em: 22 jun. 2015.

ARAUJO, A. R. de. **Aplicação da norma IEC61850-8-1 nas redes de proteção do sistema elétrico.** p. 1–55, 2011. Disponível em: <http://tcc.ecomp.poli.br/20111/TCC_Oficial_Alana_FINAL.pdf>. Acesso em: 14 abr. 2015.

BJÖRKMAN, G. et al. **SCADA system architectures:** Vital Infrastructure, Networks, Information and Control Systems Management. 7th Framework Programme, 2010. Disponível em: <http://www.diva-portal.se/smash/get/diva2:495729/FULLTEXT01.pdf>. Acesso em: 13 abr. 2015.

BRUCH, M. et al. **Power Blackout Risks:** Risk Management Options. CRO, 2011. Disponível em: <https://www.allianz.com/v_1339677769000/media/responsibility/documents/position_paper_power_blackout_risks.pdf>. Acesso em: 13 abr. 2015.

CGEE. **Redes Elétricas Inteligentes: contexto nacional.** Brasília, DF: Centro de Gestão e Estudos Estratégicos, 2012. Disponível em: <www.cgee.org.br>. Acesso em: 13 abr. 2015.

ELIPSE POWER®. **Elipse Power®** Disponível em: <http://www.elipse.com.br/port/power.aspx>. Acesso em: 13 abr. 2015

FALCÃO, D. M. **Smart Grids e Microredes: o futuro já é presente**. Rio de Janeiro, RJ: VIII Simpase, p.1–11, 2009. Disponível em: <http://www.researchgate.net/publication/228473062_Smart_Grids_e_Microredes_o_futuro_j__presente>. Acesso em: 13 abr. 2015.

FERREIRA, M. C. A. F. **Perspectivas e Desafios para a Implantação das Smarts Grids: um estudo de caso dos EUA, Portugal e Brasil.** Rio de Janeiro, 2010. Disponível em: <http://www.ie.ufrj.br/gee4/index.php/get-monografia/132-perspectivas-e-desafios-para-a-implantacao-das-smart-grids-um-estudo-de-caso-dos-eua-portugal-e-brasil>. Acesso em: 13 abr. 2015.

GHANSAH, I. **Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks.** PIER, 2009. Disponível em: <http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf>. Acesso em: 13 abr. 2015.

GIEHL, A. **Development of a Co-Simulation framework to analyse attacks and their impact on Smart Grid.** Munich: Technische Universität München, 2013. Disponível em: <https://www.sec.in.tum.de/assets/Uploads/ThesisGiehl20130712-final.pdf>. Acesso em: 13 abr. 2015.

HOHLBAUM, F. et al. **Cyber Security Practical considerations for implementing IEC 62351.** 2010. Disponível em: <https://library.e.abb.com/public/b3427a5374a35468c1257a93002d8df5/1MRG006973_en_Cyber_Security_-_Practical_considerations_for_implementing_IEC_62351.pdf>. Acesso em: 13 abr. 2015.

HOU, D.; DOLEZILEK, D. **IEC 61850 – What It Can and Cannot Offer to Traditional Protection Schemes.** 2008. Disponível em: <http://www.ucaiug.org/Meetings/CIGRE_2014/USB%20Promo%20Content/SEL/Technical%20Papers/IEC%2061850%20What%20it%20Can%20and%20Cannot%20Offer%20to%20Traditional%20Protection%20Schemes.pdf>. Acesso em: 13 abr. 2015.

HPING3.ORG. **Hping3**. Disponível em: <http://www.hping.org/download.html>. Acesso em: 13 abr. 2015.

IEC 61850-8-1. International Standard IEC 61850-8-1**. Communication networks and systems in substations** – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. p. 1–140, 2005.

IEC TS 62351. Technical Specification IEC 62351-3. **Power systems management and associated information exchange** – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP. p. 1-14, 2007.

JAVA2S.COM. **Asimple proxy server: Proxy Server << Network Protocol << Java.** Disponível em: <http://www.java2s.com/Code/Java/Network-Protocol/Asimpleproxyserver.htm>. Acesso em: 9 abr. 2015.

JORNAL DA GLOBO. **Apagão de energia elétrica atinge 11 estados e o Distrito Federal.** Disponível em: <http://g1.globo.com/jornal-da-globo/noticia/2015/01/apagao-de-energia-eletrica-atinge-11-estados-e-o-distrito-federal.html>. Acesso em: 13 abr. 2015.

MAKHIJA, J. **Comparison of protocols used in remote monitoring: DNP 3.0, IEC 870-5-101 & Modbus.** 2003. Disponível em: <https://www.ee.iitb.ac.in/~esgroup/es_mtech03_sem/sem03_paper_03307905.pdf>. Acesso em: 13 abr. 2015.

MINISTÉRIO DE MINAS E ENERGIA. Disponível em: <http://www.mme.gov.br>. Acesso em: 13 abr. 2015.

MOLLIN, R. A. Public-key Cryptography: Theory and Practice. 1ª. ed. [S.l.]: Chapman & Hall/CRC, v. I, 2002.

NICHOLSON, A. et al. **SCADA security in the light of cyber-warfare.** Elsevier Ltd. SciVerse ScienceDirect, v. 31, p. 418–436, 2012. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404812000429>. Acesso em: 13 abr. 2015.

OPERADOR NACIONAL DO SISTEMA ELÉTRICO. ONS, 2015 Disponível em: <http://www.ons.org.br/home/>. Acesso em: 13 abr. 2015.

PIRES, P. S. M. et al. **Aspectos de Segurança em Sistemas SCADA uma Visão Geral.** v. 1, p. 1–11, 2004. Disponível em: <http://www.dca.ufrn.br/~affonso/FTP/artigos/2004/isa_scada_2004.pdf>. Acesso em: 13 abr. 2015.

ROSS, K.; KUROSE, J. **Computer Networking: A Top Down Approach.** 6 ed. Pearson, 2012.

_____. **RFC 2026**. Fremont, 2002. Disponível em: <https://tools.ietf.org/html/draft-dube-modbus-applproto-00>. Acesso em: 13 abr. 2015.

SILVA, A. P. G. da; SALVADOR, M. **O que são sistemas supervisórios?** p. 1–5, 2005. Disponível em: <http://www.wectrus.com.br/artigos/sist_superv.pdf>. Acesso em: 13 abr. 2015.

SILVA, B. M da. **Um Middleware para prover Comunicação Segura entre os Dispositivos.** Santa Maria, RS: 2015.

STREHL, L. C. **Prospecção de tecnologias para aumentar a segurança em sistemas scada.** Curitiba, 2012. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1905/1/CT_CEAUT_III_2012_15.pdf>. Acesso em: 13 abr. 2015.

_____. **2014 Smart Grid System Report**. U.S. Departamento of Energy, 2014. Disponível em: <https://www.smartgrid.gov/files/2014-Smart-Grid-System-Report.pdf>. Acesso em: 13 abr. 2015.

SUKEYOSI, W. A. P. et al. **Ambientes Controlados de Geração de Anomalias: Uma Reprodução de Ataques de Negação de Serviço.** Computer on the Beach, 2013. Disponível em: <http://www6.univali.br/seer/index.php/acotb/article/viewFile/6204/3466>. Acesso em: 13 abr. 2015.

TCPDUMP.ORG **TCPDump.** Disponível em:<http://www.tcpdump.org>. Acesso em: 13 abr. 2015.

VIJAYAPRIYA, T; KOTHARI, D. P. **Smart Grid: an overview.** Scientific Research, 2011, p. 305-311. Disponível em: <http://www.scirp.org/journal/PaperInformation.aspx?paperID=8269#.VPcQa8vsuBs>. Acesso em: 13 abr. 2015.

WIRESHARK.ORG. **WIRESHARK.** Disponível em: <https://www.wireshark.org/docs> Acesso em: 13 abr. 2015.